A Framework for Acceptance and Implementation of Global Data Privacy and Security Policies by States (A Case Study of Sri Lanka and United Kingdom)

A thesis submitted in partial fulfilment of the requirement for the degree of Doctoral of Philosophy.

Vibhushinie Bentotahewa

School of Technologies, Cardiff Metropolitan University

CERTIFICATE

“A framework for acceptance and implementation of global data privacy and security policies by states (A case study of Sri Lanka and United Kingdom)”

by

Vibhushinie Bentotahewa

Registration 20149904

Submitted in the partial fulfilment of the requirements for the degree of the

DOCTOR OF PHILOSOPHY

Cardiff School of Technologies

Cardiff Metropolitan University

Wales United Kingdom

Director of Studies
Dr Chaminda Hewage
Associate Professor
School of Technologies
Cardiff Metropolitan University
Wales United Kingdom

Dated: 29/10/2021

Cardiff Metropolitan University | Prifysgol Metropolitan Caerdydd

DECLARATION

This Work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed..(candidate)

Date 14. 02. 2022 ....

STATEMENT 1

This thesis is the result of my own investigations, except where otherwise stated.Where correction services have been used, the extent and nature of the correction is clearly marked in a footnote(s).

Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed..(candidate)

Date 14. 02. 2022 ....

STATEMENT 2

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations and that I do hereby give Cardiff Metropolitan University the right to make available the Work.

Signed..(candidate)

Date 14. 02. 2022 ....

Candidates on whose behalf a bar on access has been approved by Cardiff Metropolitan, should use the following version of ***STATEMENT 2****:*

I hereby give consent for my thesis, if accepted, to be available for photocopyingand for inter-library loans **after expiry of a bar on access of period approved by Cardiff Metropolitan. After such period I do hereby give Cardiff Metropolitan University the right to make available the Work.**

Signed..(candidate)

Date 14. 02. 2022 ....

TABLE OF CONTENTS

ABBREVIATIONS

AI	Artificial Intelligence
DPA	Data Protection Act
EU	European Union
GDPR	General Data Protection Regulation
IoTs	Internet of Things
ICT	Information Communication Technology
IP	Internet Protocol
IT	Information Technology
ICC	International Criminal Court
NRI	Network Readiness Index
OPCW	Organisation for the Prohibition of Chemical Weapons
OSAM	Online Shopping Acceptance Model
PAM	Policy Acceptance Model
RFID	Radio Frequency Identification
SAARC	South Asian Association for Regional Cooperation
TAM	Technology Acceptance Model
UN	United Nations
UK	United Kingdom
US	United States
UTAUT	Unified Theory of Acceptance and Use of Technology

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENT

I, the researcher, wish to offer my profound gratitude to the supervisors, Dr Chaminda Hewage and Dr Jason Williams, for their guidance, sustained support, contribution to the research study, and valuable inputs to the preparation of the thesis and completion of the PhD. I also take this opportunity to express my gratitude to Professor Edmond Prakash and Professor Neil Richard and my appreciation of the support received from the entire academic and the administration staff at Cardiff Metropolitan University, School of Technologies.

On a personal note, I wish to thank my uncle, Mr Jay Sellahewa, for his unwavering support and standing by me throughout my academic journey to completion of the PhD. It was his caring guidance, persistent encouragement, and generosity that helped me achieve my targets and eventually reach my goal. He has been the pillar of my strength; I could not have made this journey without him. Finally, I dedicate this thesis to my parents, Mr Vipul Bentotahewa, Mrs Champa De Silva, my two sisters, Nadeeja Bentotahewa and Hasika Bentotahewa, my partner, Damith Walpita, for their continued support and encouragement, and to my grandmother, late Mrs N A E De Silva who I remember with eternal love for her affection and support during my childhood to adulthood.

Vibhushinie Bentotahewa

The Researcher

ABSTRACT

The existing data protection laws are undergoing a step-by-step process of reviewing, considering, and scrutinising by the law makers and state governments across the regions where existing legislation is believed inadequate. Therefore, the aim should be to reach a consensus amongst like-minded nations to find fundamental discrepancies and variables, resolve contentious/inhibiting factors, with a view to producing proposals to fill the lapses in the law, and conform to a consolidated conceptually meaningful policy framework for sharing with other nations.

The main contribution of this research is to develop a Policy Acceptance Model that is meant to be an influencing tool and a guide to develop a data privacy, and security policy. From the purpose angle, it will be an influencing tool for decision making and developing data protection mechanisms and, could be adapted by the states for developing national and regional data protection mechanisms of their own. Cyberspace is not country-specific, not limited to a region or a continent; it belongs to the global community. Therefore, this model is also meant to help develop global level data protection mechanism. Also, the researcher has added new knowledge to the current literature through her publications. These publications addressed contemporary issues such as Huawei row, WhatsApp privacy issue and privacy and security issues associated with COVID-19.

CHAPTER ONE

INTRODUCTION

1.1 Background

The advancement in digital technology has taken remarkable conspicuous steps forward into the IoTs (Internet of Things) driven world, and the resulting step changes in lifestyles have introduced new dimensions to the way in which people, organisations, and the state interact. The growing trends in the use of IoT and the new lifestyles that we have become accustomed to, whether working in a conventional office environment or in a home environment, underwent testing during the COVID-19 pandemic, and the positive outcomes gave reasons to be optimistic about the post-COVID future. However, the benefits from the advancement of technologies could also be superseded by the challenges arising from widespread collection, processing, and sharing of personal information, and the detrimental impact of data breaches on individual privacy. Also, the providers of technology may place more emphasis on the benefits from IoTs than inherent risks involved in their use, and the users themselves may do likewise. Such a scenario has the potential to create a conflict between the use of technology driven lifestyles and data breaches unless robust data protection measures introduced to prevent them.

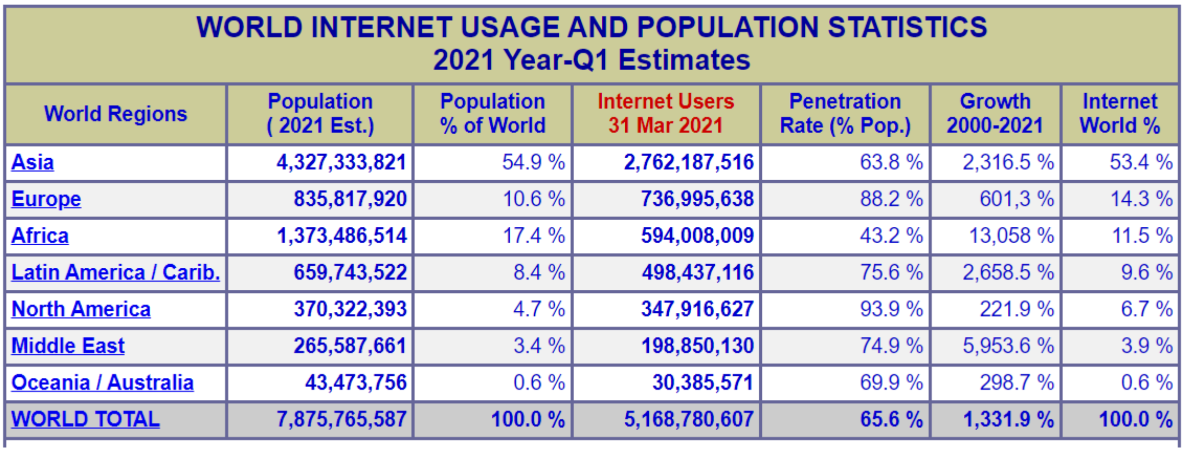
The 'working from home' concept has introduced flexibility to manage family life whilst remaining fully engaged with occupational commitments, thereby allowing the entire family to take full advantage of technology for mutual benefits. The use of the cyberspace has become an integral part of people's behaviour, whether it is online shopping, communication, entertainment, watching Television, online gaming, booking holidays, banking, or even exploring and researching, using the array of digital devices available. However, the use of cyberspace also carries substantial risks because of the ability of the service providers, media platforms, network providers, governments, commercial enterprises, state security services, health authorities, and a host of other organisations to collect, process, and share personal information of the user (OECDiLibrary, N.D).

The evolution of the Zoom learning concept, combined with website searches to access and download learning material, and engage in leisure activities during the lockdown, potentially expose the students to the risks associated with cyberspace (UNICEF, 2020).

On accessing a website, the IP (Internet Protocol) address and location information recorded at the source (Weissman, 2015); hence personal information of anyone accessing a website could become widely exposed, leaving them at the mercy of the cybercriminals who constantly prey on vulnerable individuals or groups, especially the younger groups for malicious purposes. The use of cyberspace in this way will impact individual privacy with serious repercussions to the organisation, unless legislated to prevent unauthorised intrusions.

There has been an increase in the number of people using the internet from 2009 to 2020 (See table 1.2). The reports indicate that out of the total world population (7.8 billion) more than half of the people around the world used the internet in March 2021 (See table 1.1). That represents a 7.3 percent (316 million) increase since January 2020 (Kemp, 2021). This increase would have been due to the widespread use of the internet during the COVID-19 pandemic. The concerning issue is the increase in the number of recorded data breaches (36 billion) in the first half of 2020, of which 95% accounted for cyber security breaches caused by human error, 58% of personal data breaches in 2020, all at the cost of $3.86 million during the same period (Sobers, 2021).

Table 1.1: Internet usage worldwide and population statistics 2021 year (International Telecommunications Union at el., 2021)



WORLD INTERNET USAGE AND POPULATION STATISTICS
2021 Year-Q1 Estimates

World Regions	Population (2021 Est.)	Population % of World	Internet Users 31 Mar 2021	Penetration Rate (% Pop.)	Growth 2000-2021	Internet World %
Asia	4,327,333,821	54.9 %	2,762,187,516	63.8 %	2,316.5 %	53.4 %
Europe	835,817,920	10.6 %	736,995,638	88.2 %	601,3 %	14.3 %
Africa	1,373,486,514	17.4 %	594,008,009	43.2 %	13,058 %	11.5 %
Latin America / Carib.	659,743,522	8.4 %	498,437,116	75.6 %	2,658.5 %	9.6 %
North America	370,322,393	4.7 %	347,916,627	93.9 %	221.9 %	6.7 %
Middle East	265,587,661	3.4 %	198,850,130	74.9 %	5,953.6 %	3.9 %
Oceania / Australia	43,473,756	0.6 %	30,385,571	69.9 %	298.7 %	0.6 %
WORLD TOTAL	7,875,765,587	100.0 %	5,168,780,607	65.6 %	1,331.9 %	100.0 %

To address the issues on cyberspace, in 2004, the global community developed an international treaty, named the Council of Europe Convention on Cybercrime which is also known as the Budapest Convention (Clough, 2014, P.698-736). For example, Russia refused to ratify the convention for two reasons. One was that they had not participated in the drafting process, and the other was that the convention was an infringement on their sovereignty (Peters, 2019).

The primary focus of data security and privacy regulations and law is on protecting the privacy rights of individuals without compromising their personal data, collected, processed, and stored by the state institutions and other organisations including commercial and utility companies. The developed and developing countries of the world community are proactively continuing to update their statute (See figure 1.1) to strengthen the law to protect cyberspace and prevent its unethical use, and the respective countries have found it necessary to strike a balance between national security and privacy rights.

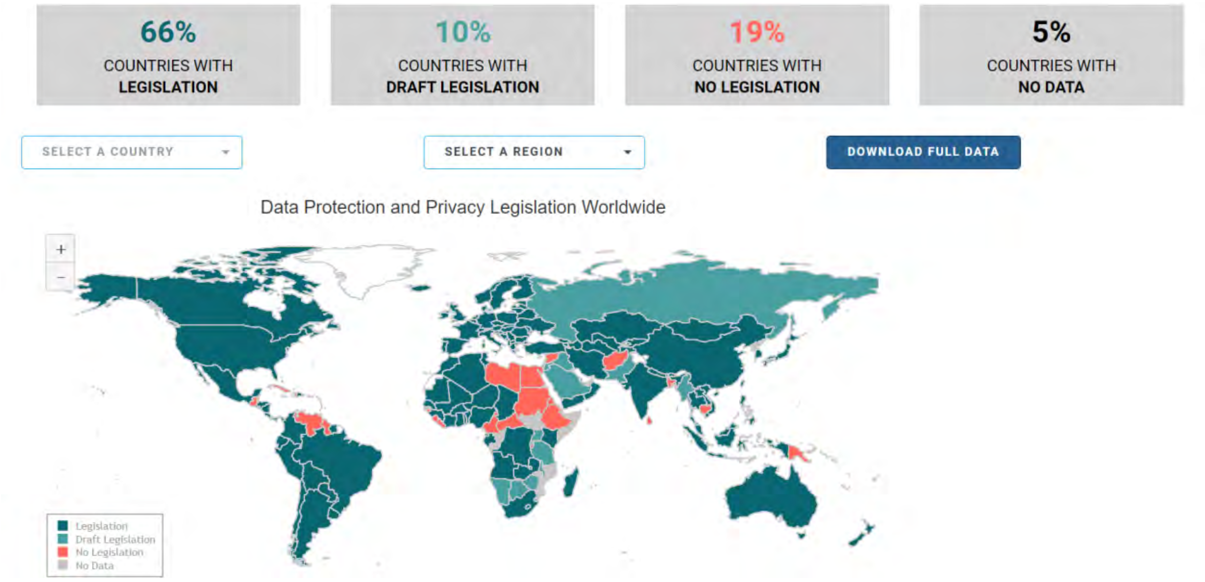
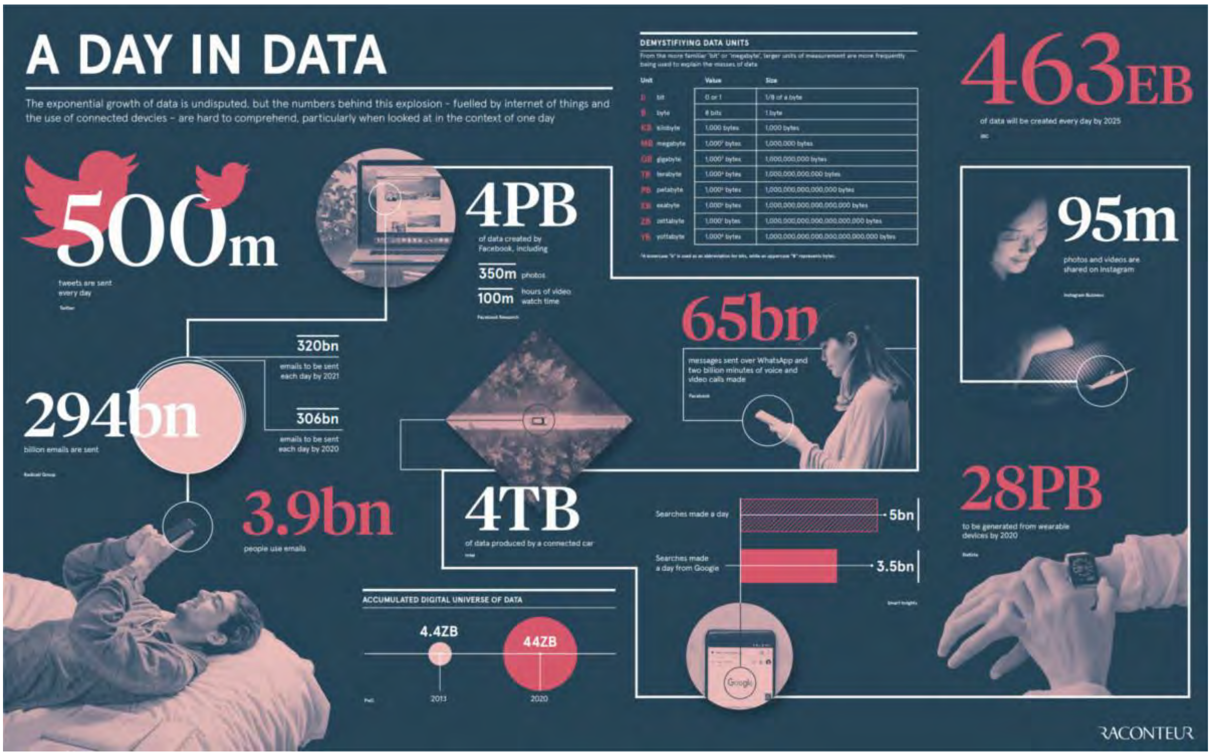

66% COUNTRIES WITH LEGISLATION
10% COUNTRIES WITH DRAFT LEGISLATION
19% COUNTRIES WITH NO LEGISLATION
5% COUNTRIES WITH NO DATA
SELECT A COUNTRY
SELECT A REGION
DOWNLOAD FULL DATA
Data Protection and Privacy Legislation Worldwide
+
−
Legislation
Draft Legislation
No Legislation
No Data

Figure 1.1: Data protection and legislations worldwide (UNCTAD, 2020)

The cyber threats characteristically migrate across the world undetected; therefore, a comprehensive global response needed to meet these challenges. It is incumbent on all nations to review existing legislation, identify loopholes and gaps, adapt new laws, be equipped to combat cybercrimes, and enforce the law to protect the state and the citizens from cybercriminals. To that end, the researcher believes that those nations having technological know-how and resource capacity should engage in participatory coordinated action with other nations to develop a viable and robust mechanism that all member states should sign up to preferably lead by the United Nation (UN) which has an influential voice. In doing so, it should be possible to avoid individual states taking arbitrary action, except in exceptional cases, in accordance with the UN Charter that stipulates all members of the UN agree to accept and abide by the decisions of the Security Council (UN, N.D).

The use of technology is a strategic necessity in the industrial sector to achieve success, and it generates large volumes of data (see figure 1.2). The by-products of technology are the rapidly developed information technologies, such as cloud computing, IoT, and Artificial Intelligence (AI), and their use brings wide benefits to the enterprise in terms of productivity and increased revenue regardless of the size of the organisation (Kark, Briggs, and Terzioglu, 2019). Also, the technology-driven commercial sector attracts customer attention, potential investors, entrepreneurs and contributes to the sustainability of the industrial sector.



A DAY IN DATA

The exponential growth of data is undisputed, but the numbers behind this explosion - fuelled by internet of things and the use of connected devcies - are hard to comprehend, particularly when looked at in the context of one day

DEMYSTIFIYING DATA UNITS

From the more familiar 'bit' or 'megabyte', larger units of measurement are more frequently being used to explain the masses of data

Unit		Value	Size
b	bit	0 or 1	1/8 of a byte
B	byte	8 bits	1 byte
KB	kilobyte	1,000 bytes	1,000 bytes
MB	megabyte	$1,000^2$ bytes	1,000,000 bytes
GB	gigabyte	$1,000^3$ bytes	1,000,000,000 bytes
TB	terabyte	$1,000^4$ bytes	1,000,000,000,000 bytes
PB	petabyte	$1,000^5$ bytes	1,000,000,000,000,000 bytes
EB	exabyte	$1,000^6$ bytes	1,000,000,000,000,000,000 bytes
ZB	zettabyte	$1,000^7$ bytes	1,000,000,000,000,000,000,000 bytes
YB	yottabyte	$1,000^8$ bytes	1,000,000,000,000,000,000,000,000 bytes

*A lowercase "b" is used as an abbreviation for bits, while an uppercase "B" represents bytes.

500m
tweets are sent every day
Twitter
4PB
of data created by Facebook, including
350m photos
100m hours of video watch time
Facebook Research
463EB
of data will be created every day by 2025
IDC
95m
photos and videos are shared on Instagram
Instagram Business
320bn
emails to be sent each day by 2021
306bn
emails to be sent each day by 2020
294bn
billion emails are sent
Radicati Group
65bn
messages sent over WhatsApp and two billion minutes of voice and video calls made
Facebook
3.9bn
people use emails
4TB
of data produced by a connected car
Intel
Searches made a day
5bn
Searches made a day from Google
3.5bn
Smart Insights
28PB
to be generated from wearable devices by 2020
Statista
ACCUMULATED DIGITAL UNIVERSE OF DATA
4.4ZB
44ZB
2013
2020
RACONTEUR

Figure 1.2: The amount of Big Data generated in a day (Desjardins, 2019)

The health sector is one of the beneficiaries of the technological revolution. The use of advanced technologies has helped make substantial improvements to the delivery of health care services, diagnosis of diseases, treat patients speedily to save lives, with added benefits of extended life spans (Thimbleby, 2013, P.160-167.). In the education sector, the concept of virtual learning and teaching during the lockdown periods provided a new experience to the students as well as to the teachers to conduct lessons online instead of face-to-face teaching. The group learning experience became the turning point in the delivery of education and the pupils/student became the biggest beneficiaries as they were able to make use of technology to acquire new knowledge over and above the outside the school curriculum and share their experiences with the group. Learning in this way would have been impossible without the aid of technology (Li and Lalani, 2020). However, the use of technology in this way also generates a large volume of Big Data by the network service providers as well as data management organisations using remote means, and the humans by means of virtual interaction through the internet facilities (See figure 1.3). The e-documents, e-mails, presentations, spreadsheets, audio, and video file formats created at an unprecedented level, (Sobers, 2020) and the use of communication systems such as the most popular ones, Microsoft Teams, Zoom, Skype, also create Big Data shared widely by the people. The extent of collected data sets can give an insight into the lifestyle behaviour pattern of the consumers and their usage preferences when purchasing products and services using the online option, but unwittingly they also give away their personal information and risk long-lasting privacy implications.

All that said, there is also a need to justify the reasons for collecting an excessive amount of personal data. Millions of people around the globe are constantly making use of evolving advanced communication technology, and personal information becomes prone to hacking by cybercriminals whose locations are impossible to trace. In such an environment, safeguarding personal identities has become virtually impossible against the increasing threats from unauthorised access by hackers and the clandestine activities of various groups such as commercial enterprises. New challenges are also emerging in the form of modern technologies, tracking and profiling (Privacy International Organisation, N.D).

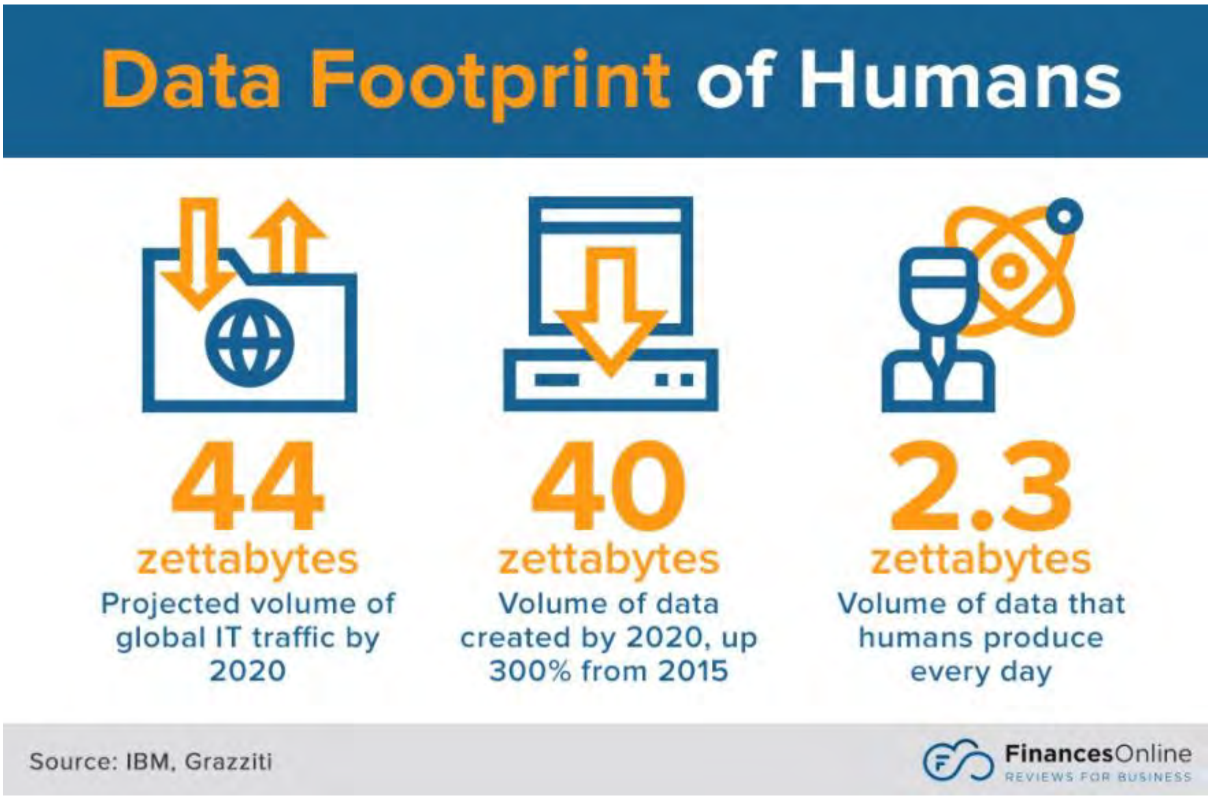
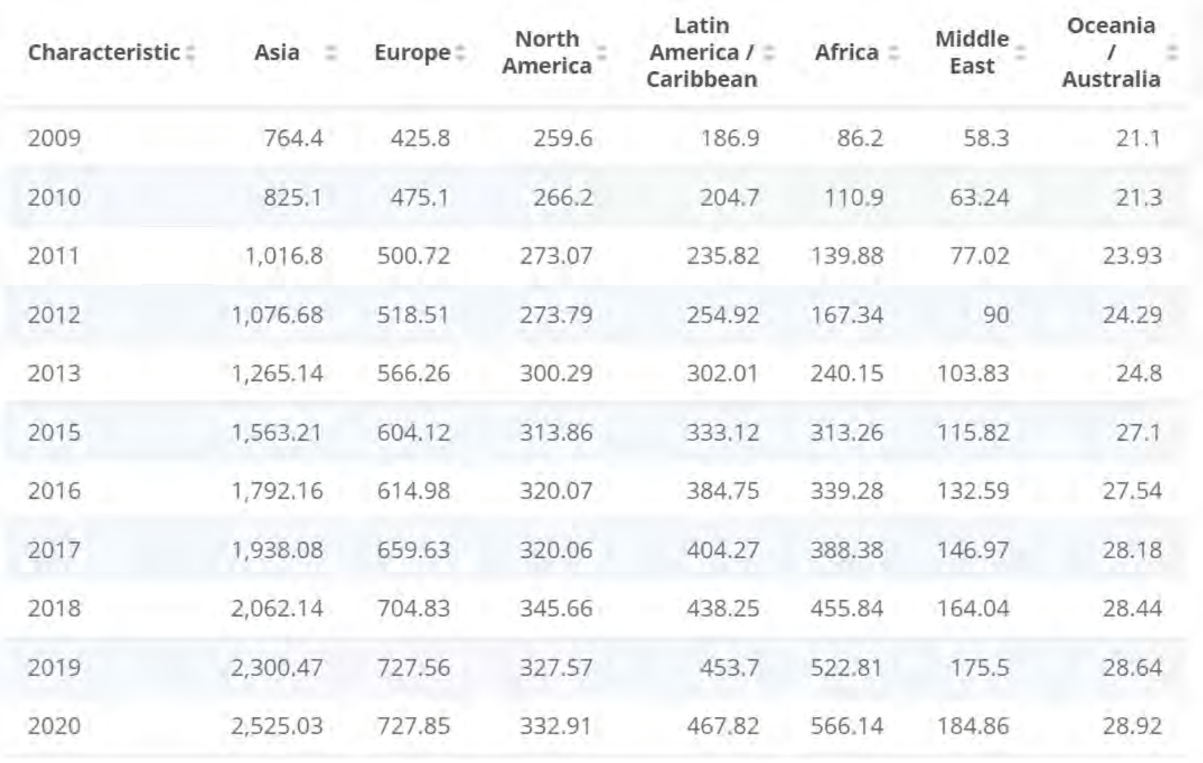


Figure 1.3: Data footprint of human (Finances Online Research Centre, N.D)

The collection of Big Data from variety of sources is for variety of reasons (Bentotahewa and Hewage, 2020, Challenges and Obstacles to Application of GDPR to Big Data) and the collection shall be permissible only within the parameters set out in the data protection law. It is however worth considering whether gathering Big Data serves its purpose in its entirety or the purpose is to gather information about the personal lifestyles led by the people in a liberal environment. The leading question then arises whether it is all necessary or justifiable. In that context, the researcher believes that, given the sensitivity of the concerning issues in the use of evolving technologies and privacy and security implications to the individuals, it is important to strike a balance and the adaptation of data protection law is the most effective way to do that. Against that background, a number of countries found the lapse in the existing data protection law/s and are actively reviewing their legislation to update their own laws and bring them to align with General Data Protection Regulation (GDPR) (Woodward, 2021). That positive action will keep them in touch with progress in developing privacy protection measures at the global level and keep the risks under constant check when sharing data with other countries. This cautious approach is regarded as reassurance in strengthening user trustworthiness and confidence in sharing personal data.

Table 1.2: Number of internet users worldwide from 2009 to 2020, by region (in millions) (Johnson,2021)



Characteristic	Asia	Europe	North America	Latin America / Caribbean	Africa	Middle East	Oceania / Australia
2009	764.4	425.8	259.6	186.9	86.2	58.3	21.1
2010	825.1	475.1	266.2	204.7	110.9	63.24	21.3
2011	1,016.8	500.72	273.07	235.82	139.88	77.02	23.93
2012	1,076.68	518.51	273.79	254.92	167.34	90	24.29
2013	1,265.14	566.26	300.29	302.01	240.15	103.83	24.8
2015	1,563.21	604.12	313.86	333.12	313.26	115.82	27.1
2016	1,792.16	614.98	320.07	384.75	339.28	132.59	27.54
2017	1,938.08	659.63	320.06	404.27	388.38	146.97	28.18
2018	2,062.14	704.83	345.66	438.25	455.84	164.04	28.44
2019	2,300.47	727.56	327.57	453.7	522.81	175.5	28.64
2020	2,525.03	727.85	332.91	467.82	566.14	184.86	28.92

In the scope of this research, the researcher chose two specific regions: South Asian Association for Regional Cooperation (SAARC) and European Union (EU) because Asian and the Europe region represent a considerable proportion of the internet users worldwide (see table 1.2). The member nations of the EU do have satisfactory data protection mechanisms at the national and regional level. However, member countries of the SAARC region do not have a unified data protection mechanism in place at the regional level, but number of countries have at least draft data protection mechanisms at the national level.

The EU is in constant engagement with SAARC and encouraging them to take initiatives towards institution-building, promoting democracy and good governance, and human rights through regional integration and support, whilst it recognises the border security concerns of the region (Soutullo, and Masur 2021). Furthermore, the European Parliament whilst continuing to monitor the situation in the South Asia, provides support to their effort to address the COVID-19 crisis (Soutullo, and Masur, 2021). The researcher believes that, given their close working relationships, the EU and the SAARC should work together to develop a data protection mechanism. However, there are social, economic, and political differences between the two regions. Nevertheless, the SAARC region can benefit from the EU experiences in the development and, acceptance and implementation of GDPR. In consistence with the objectives of the study, for the purpose of data collection, the focus narrowed down to the United Kingdom (UK), a high-income country (World Bank, 2020), and Sri Lanka, a developing country (World Bank, 2020), to get a comparison between the statehoods in the development of a mechanism for global level data protection.

1.2 Research aim

The main aim of this research is to identify the barriers faced by the states in accepting and implementing global data policies and, to develop a Policy Acceptance Model meant to be an influencing tool and a guide to developing a global data privacy and security policy. The model development process involves a comprehensive literature review and collection of information by way of a survey questionnaire and analysis of the responses collected to get an understanding of the challenges faced by the states in accepting and implementing the policies.

The primary aim of the proposed Policy Acceptance Model is to identify common factors that are obtrusive but considered important to developing a global data protection mechanism. It consists of two stages; the pre-adaptation stage and the adaptation stage. In the pre-adaptation stage, the focus will be on the external factors that are likely to affect the decision-making process. The adaptation stage will seek to develop a data privacy and security policy on need dependent basis. From the purpose angle, it will be an influencing tool for decision making and developing data protection mechanisms and, could be adapted by the states for developing national and regional data protection mechanisms of their own. It is also meant to help develop trust between the nations at the global level.

The application of the law must be effective, appropriate, and must ensure uniformity in data protection and privacy law devoid of ambiguities implications. It is also incumbent on all nations to review existing legislation, identify any loopholes, ambiguities, gaps, adapt (new if necessary) robust laws to combat cybercrimes, and ensure stringent law enforcement to protect the state and the citizens from cybercriminals. For those reasons, the researcher believes that UN is the appropriate organisation to facilitate and coordinate a participatory way forward, leading to developing a mechanism for endorsement by the member states and underwritten by the UN. This will avoid individual states taking arbitrary action, except in exceptional cases.

1.3 Research Objectives

1. Undertake a comprehensive literature review to frame the literature for socio-political, economic, cultural background and national cyber legislations of countries in each region, and to identify their commitments regarding protection of personal privacy.

2. Based on the identified parameters during the literature review, conduct a primary research data collection to evaluate responses from individuals of diverse background.

3. Critically analyse the gathered survey data and develop a Policy Acceptance Model.

1.4 Research Questions

Q1: Have the countries at individual level committed to protect personal privacy?

The researcher conducted a thorough literature review to understand and analyse the commitment of countries to protect personal privacy at the national. The findings indicated a good understanding of the importance of protecting personal privacy within the countries, and most of them were in the process of revisiting their current data protection mechanisms. It is also the case that many of them used GDPR as a model to upgrade and bring their data protection mechanisms to current standard.

Q2: Are the national data privacy and security policies in South Asian and European regions robust enough to protect the personal privacy of the citizen?

The researcher narrowed down the scope to South Asia and the European region and then conducted a comparative analysis to understand the commitments in those two regions to protect personal privacy. The researcher identified that the European region countries have a standardised robust data protection mechanism at national level, as well as adequate data protection mechanisms at regional level. However, the South Asian region countries seem to have made little progress in developing data protection mechanisms at the national level. Some countries have drafted GDPR inspired data protection mechanisms, and some have none in any meaningful way.

Q3: To what extent does the South Asian data privacy and security policies meet the adequacy of the GDPR?

The researcher observed that the current data protection mechanisms in the South Asian region fulfil the adequacy of the GDPR. In parallel to the requirements set out in the GDPR, the data protection mechanisms in the South Asian region do flag up broadly individual rights, data subject consent compulsory for processing information, data sharing limited to the countries having adequate level of data protection mechanisms and mandatory data breach notifications. However, although the countries are bound by the requirement to send a notification following a data breach, time duration varies from one country another. In an incident of failure to protect personal data, the value of the fine and the punishment also varies from one country to another. In addition, although the GDPR stipulates the requirement for appointing a Data Protection Officer, not all countries have considered it as a requirement. However, despite minor regulatory differences between GDPR and GDPR inspired legal mechanisms in the South Asian region, the existing data protection mechanisms seem sufficient to protect the data subject's personal privacy.

Q4: What are the data privacy and security policies in Sri Lanka and the UK, and the challenges faced by states towards accepting and implementing policies?

The researcher narrowed down the area further to ascertain what the data privacy and security policies in Sri Lanka and the UK were. The United Kingdom is a developed country, and it developed its own version of the Data Protection Act 2018, but following the BREXIT transition process, the modified version of the EU GDPR became integrated into the UK legal system named 'UK GDPR' with effect from January 2021. Despite being a developing country, Sri Lanka has a Draft Personal Data Protection mechanism pending approval from the parliament.

Having gone through a thorough literature, the researcher sought to identify the challenges faced by the countries in developing data protection mechanisms. The identified factors are listed in chapter 2. The researcher then used the identified factors to develop the research questionnaire (See annexe A) which aimed to ascertain the accuracy and timeliness of the barriers referred to in the literature. The public opinion of the importance of developing a global level data protection mechanism and the factors for consideration in developing one helped the researcher develop a Policy Acceptance model.

Q5: Is there a need to revisit the current data protection mechanisms to address the privacy risks associated with evolving technologies and Big Data?

The researcher observed the extent of deployment of devices and collection of Big Data to mitigate the pandemic. That led the researcher to conduct a thorough literature review to ascertain whether the current data protection mechanisms were robust enough to address the privacy risks associated with evolving technologies and Big Data. Based on the literature reading the researcher strongly believes that there should be flexibility in the data protection mechanism to allow adjustments deemed as necessary in respect of emerging technologies, also a requirement to review current policies at least once a year to keep up with the challenging demands of advanced technology. It is also important to frequently update and maintain legal mechanisms to avoid policy implementation failures.

Q6: To what extent the privacy and security challenges associated with COVID-19 surveillance measures addressed through the available data security policies?

Through the literature review, the researcher gathered information on the devices and technologies deployed by the countries, and privacy and security risks associated with them, and evaluated the legal/policy mechanisms in place to address potential threats and whether they were adequate to address them. Where there were no robust mechanisms in place, the researcher proposes recommendations for risks mitigation. The researcher used these findings for sharing knowledge and, to contribute to current literature, by way of publications.

1.5 Significance of the study

The case for developing an (having an) international strategy for data security and privacy is important, despite the efforts made by the individual and regional countries (Government of UK, 2016, P.63-64). The ongoing debate focuses on the application of international law to cyberspace, but the contentious issue is the feasibility of doing so. (Adonis, 2020) (Moynihan, 2019) (UN, 2018) (Koh, 2012). As an example, international law does not contain tailored-made rules for regulating cyberspace, and it (usually) does not intervene in the affairs of the ICT companies or that of the individuals. The applicability of international law in relation to cyberspace is dependent strictly on the identification of the culprit, whether it is the state, state-sponsored actor, non-governmental organisation, criminal group/s or an individual. However, identifying the origins of malicious cyber behaviour is often difficult (Skopik and Pahi, 2020,P.1) and time-consuming, and the attribution of accountability faces challenges.

The absence of a stern voice would be a weak response to malicious behaviour in the eyes of the law and, naming and shaming may not have the desired effect on the offenders (Hollis, 2021, P.3-4); besides, bringing them to account in such situations will be a challenging task. Historically, there have been instances where states made accusations against each other for incidents of cyber-attacks, but the states rarely acted to invoke international law to prosecute the perpetrators, although sanctions imposed in exceptional cases against those found guilty of launching cyber-attacks (Hollis, 2021, P.4). One such occasion, the European Council had imposed restrictive measures on six individuals and three entities responsible for their involvements in various cyber-attacks (Council of EU, 2020, EU imposes the first ever sanctions against cyber-attacks). As cited, this included attempted cyber-attacks on the OPCW (Organisation for the Prohibition of Chemical Weapons), and WannaCry, NotPetya, and 'Operation Cloud Hopper' attacks (Council of EU, 2020, EU imposes the first ever sanctions against cyber-attacks).

Against that background, most countries revisited and updated their data protection mechanisms for the purpose of protecting personal privacy of the individuals aftermath of the GDPR in 2018 (DLA Piper, 2021). However, a number of countries remain without sufficient data protection mechanisms, even without any means to protect their citizen’s personal privacy (UNCTAD, 2020), and the reason is the lack of resources and the shortage of professionals with sufficient understanding of the issues (Tovi, and Muthama, 2013, P.5). That makes cooperation between states even more important, whether it is at the regional level or global level. For an example, member states of the EU enacted the GDPR which provides a legal framework inclusive of a set of guidelines for the collection and processing of personal information of individuals (European Union, 2016, P.88). This initiative has encouraged countries outside the EU to revisit their own data protection mechanisms, modelling on the GDPR. For an example, countries in the South Asian region have developed GDPR inspired bills, and a number of them have at least a draft data protection mechanism in place (Greenleaf, 2019, P. 1-7.).

There has been a lack of, or no attention paid to the factors outside the region when developing the GDPR and, it was a missed opportunity on the part of the policy makers. The process of developing GDPR inspired regulations faces country-based challenges that are not common in nature and attributable to various country-specific internal factors. For instance, the appointment of a data protection officer was an obligatory requirement in the developed countries of the EU, but it was not a challenge they faced. However, the developing countries would have found it difficult to match the same level of obligatory requirements for resource shortages. Also, at the national level, each country faced with internal difficulties compelled to grapple with different challenges, which makes it even more important to understand such inhibiting factors and make allowances and flexibility to the adaptation of the framework in emerging scenarios.

The Data Protection mechanisms provide guidance to the organisations and the government and outline the rules and best practices to follow when collecting, storing, and processing personal data. That makes the organisations accountable for the protection of personal information, and in the event of a data breach, the originations will become liable for negligence and incur heavy fines for the failures to protect personal information (Wolford, N.D). Furthermore, the data subjects also have self-responsibility to protect their own privacy. Therefore, the need to have a robust and meaningful data protection mechanism should not be underestimated, and it is the most effective or even the only way forward to safeguard personal privacy and national security.

The implementation of new policies across layers of governments and institutions will face challenges, and taking prior action to identify them would help develop a model matching the widely used models known as Technology Acceptance Models (TAM) (See section 5.6). TAM used by different researchers to integrate different technologies, but there is little evidence to suggest that there has been a number of known Policy Acceptance Models except for one developed by Pierce at el., (USA in 2014) by expanding TAM to integrate the acceptance of the policies (Pierce at el., 2014). In this case the researcher had considered only age and ethnicity when analysing and evaluating people's attitudes toward the emerging health care reform. However, considering latest trends in the digital world, the challenges and threats faced by the global community are complex and different to what there was years ago.

1.6 Limitations

A number of participants failed to complete the questionnaire distributed through e-mail thinking it was spam, and that led to delayed responses to the questionnaire and resulted in laps in the analysis. Added to that, the questionnaire could not be translated into the local language of Sri Lanka; hence it failed to draw the attention of the wider audience.

The contradicting information on data privacy and security policies was also a challenging factor that affected the progress of literature review. Unknown number of countries are in the process of reviewing and modernising their legal mechanisms to protect personal privacy in the climate of evolving technologies. That, in a way, has inundated literature published in the previous years.

1.7 Publications

The researcher published the following articles/papers based on the content presented in this thesis.

Bentotahewa, V., Hewage, C., and Williams, J. (2021) Security and Privacy Issues Associated with Coronavirus Diagnosis and Prognosis. In: Paiva S., Lopes S.I., Zitouni R., Gupta N., Lopes S.F., Yonezawa T. (eds) Science and Technologies for Smart Cities. SmartCity360° 2020. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol 372. Springer, Cham. Available at:https://doi.org/10.1007/978-3-030-76063-2_8

This paper investigates the security and privacy challenges associated with SARS-CoV-2 diagnosis and prognosis using case studies from different countries. The urgency of the need to manage and find a cure for the COVID-19 has made it necessary to share information. This makes it important to strike a balance between protecting individual privacy and collecting information to combat the virus; however, responsibility for doing so rests with the state. To that end, the researcher concluded that, whether permissible under extenuation circumstances or not, the need to protect privacy cannot be overlooked when sharing and handling of information for medical diagnosis and prognosis. The contributions of this chapter cover a comprehensive review of the strategies implemented by the countries for tackling the pandemic, the privacy and risks assessment of the devices deployed, the roles and responsibilities of healthcare professionals and media personnel to protect personal privacy, and proposed solutions to minimise the threats to the personal privacy.

Bentotahewa, V. Yousef, M. Hewage C. Nawaf, L and Williams. J. (2021) Privacy and security challenges and opportunities for IoT Technologies during and beyond COVID-19

The prevailing COVID-19 pandemic has put IoT based technologies to the test. It has given rise to diverse predictions for the future, and the expectations are that IoT inspired technologies will play a significant role in the new normal. However, a key challenge to the success of IOTs is the privacy and security issue associated them. This publication presents a comprehensive review of privacy and security challenges and opportunities for IoT inspired solutions. Also, it provides an in-depth analysis of IoT inspired Big Data issues, data protection, and security concerns around IoT. The contributions of this chapter cover a comprehensive review of the IoT privacy issues and data protection policies, regulations, and laws, IoT security challenges and opportunities that need to be addressed in the next normal.

Bentotahewa, V. Hewage, C. and Williams, J. (2021) 'Solutions to Big Data privacy and security challenges associated with COVID-19 surveillance systems', Frontier. Available at: doi: 10.3389/fdata.2021.645204

Most of the countries use digital surveillance technologies for tracking and monitoring individuals and populations to prevent the transmission of the new coronavirus. The technology has the capacity to make an effective contribution to success, but it comes at the expense of privacy rights. This paper focuses on Big Data challenges associated with surveillance methods used within the COVID-19 parameters. The aim of this research is to propose practical solutions to Big Data challenges associated with COVID-19 pandemic surveillance approaches. To that end, the researcher identified the surveillance measures used by countries in different regions, the sensitivity of generated data and the issues associated with the collection of data in large volumes, and finally, to propose feasible solutions to protect the privacy rights of the people, during the post-COVID-19 era.

Bentotahewa, V. Hewage, C. and Williams, J. (2019) Could Huawei jeopardise Five Eyes partnership?, *CardiffMet Symposium*, Cardiff Metropolitan University, Cardiff, 2019.

The Huawei company faced a barrage of accusations from the US and the international community, and action against Huawei was called for, claiming it posed significant security threats. However, the UK decided to go ahead with Huawei equipment in its 5G network despite the US stand and its misgivings. In this article the researcher has addressed the impact of this decision on the Five Eye Alliance, and it led the researcher to conclude UK's decision to allow Huawei involvement resulted in disagreements between Five Eye partners, and in turn, undermined the unity of the members and collaboration in intelligence sharing.

Bentotahewa, V. Hewage, C. and Williams, J. (2021) WhatsApp Chaos: Time for a Comprehensive Data Security and Privacy Law? (Available on https://www.infosecurity-magazine.com/next-gen-infosec/whatsapp-chaos-privacy-law/)

WhatsApp hit the headlines with the launch of its new terms and conditions, a policy agreement that the users are obliged to accept if they wish to continue using the app after 8 February 2021 deadline. Amongst the proposed changes specified by WhatsApp, the most concerning issue was under its own new policy, Facebook would have access rights to millions of user information (metadata) held in WhatsApp, and it led an outcry from the subscriber's. In this article the researcher has addressed the security and privacy concerns of WhatsApp's new terms and conditions, and it concludes that the proposed new changes to terms and conditions are not in the public interest and contravene privacy policies of many nations, especially those in the GDPR, the UK and EU member states. WhatsApp has also faced legal challenges as its updated privacy policy on the grounds that it interferes with India's user surveillance operations and threatens national security. The regulatory vacuum is a real concern in terms of data protection as most of the countries are in the process of developing their legal mechanisms. Therefore, the countries should produce a personal data protection law and policy, including guidance to technology companies on the ethical use of data for processing.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) BREXIT FOR EXIT; Is there an effect on cyber security?, *CardiffMet Symposium*, Cardiff Metropolitan University, Cardiff, 2019.

In this article the researcher aims to address the concerns of Brexit's impact on national security, particularly on cyber threats. To that end, the researcher provided an in-depth analysis of the areas covering skilled labour gaps, information sharing and regulatory compliance. The researcher, having considered all possibilities, concluded that UK would not compromise her security under any circumstances, regardless of Brexit outcome.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) BREXIT ON CYBER THREATS: Would it make UK less safe?, *CRESTCon-2019*, London, 2020.

The purpose of this article is to explore the vulnerability of the UK, and whether it would be prone to cyber-attacks after BREXIT. In this article the researcher addressed the concerning factors such as skilled labour shortages, likely difficulties faced in attracting talented EU nationals, potential reduced level of cooperation between the UK security agencies and Europol in intelligence sharing. After analysing the possibilities and the probability factors, in the conclusion the researcher predicted that the UK-EU cyber security partnerships would hold and remain high. The researcher remains optimistic that, despite the differences, the UK intelligence agencies would maintain its partnerships with Five Eyes and NATO to reap the benefits of collaboration.

Bentotahewa, V. Hewage, C. (2019) *Is SL becoming a potential target for cyber-attacks launch by terrorist groups* [Online]. Available at https://www.pressreader.com/sri-lanka/daily-mirror-sri-lanka/20190716/281857235114846

Sri Lanka has faced repeated cyberattacks in recent years, and the researcher took account of the attacks in the analysis and proposed feasible solutions to mitigate the risks from future incidents. The solutions suggested by the researcher include collaboration between

Sri Lanka Computer Emergency Readiness Team Coordination Centre, Computer Emergency Response Teams, and the Finance Sector Computer Security Incident Response Team by pooling their technical resources. The failure to engage in close cooperation would make the country vulnerable, and it would not be easy to prevent cyber-attacks as the source of the attacks would be hard to trace.

In addition, there is a necessity for reviewing cyber-security aspects and the new Cyber Security Bill to set up a National Cyber Security Agency with delegated responsibility for all cyber security activities. Also, Sri Lankan security forces should be competent in cyber security capabilities and seek to develop further to effectively engage in the prevention of cyber threats against the state, by sharing information with other relevant authorities. In addition, Sri Lanka would benefit by seeking support from the EU region and obtaining technical and financial support for implementing projects designed to increase awareness of decision-makers on cyber security issues and organizational capacity to prevent cybersecurity incidence.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) Gender Balance in ICT: Sri Lankan Perspective in Data Protection, *IEEE International Women in Engineering Symposium*, Sri Lanka, 2020

In this work, researcher seeks to evaluate the actions the government should initiate to support women to become sufficiently aware of cyber security and encourage them to take advantage of employment opportunities in the ICT sector. The results indicate a higher level of cyber security awareness amongst men than amongst women, despite the satisfactory level of cyber security awareness training the women have received from their organisations. The key indicator is that training alone would fall short of required level, and it is important to facilitate awareness programs, ideally from the school level, by making information security a part of the school curriculum. The organisations like the national CERT and the SLCERT (Sri Lanka Computer Emergency Readiness Team) work together alongside the academics and organisations to make the delivery of awareness programs effective. SLCERT also should seek to establish collaborations with commercial entities and academic institutions outside the country to bring in new knowledge and technical training to reap mutual benefits.

Bentotahewa, V. Hewage, C. and Williams, J. (2021) Infodemic: Have the countries done enough to tackle fake news to protect the people? UK government Global Security Event 2021.

Governments are obliged to provide adequate access to accurate information as prescribed by international human rights law. However, the COVID-19 pandemic has created an unprecedented environment for spreading misinformation online, manipulation, and abuse with unforeseen consequences. The aim of this research is to investigate the impact of an emerging infodemic in the pandemic environment. To that end, this article provides a comprehensive review of fake news that appeared in the public domain, the actions taken by the countries, and the recommendations proposed to stop the spread of fake news and minimise the damage.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) *Are cyber criminals exploiting Corona pandemic for malicious purposes?* [Online]. Available at: https://www.defence.lk/Article/view_article/1353

In the prevailing pandemic situation, each nation is engaged in implementing preventive measures, including a curfew and social isolation with restrictions on the normal lifestyles of the citizens. But the use of the internet is at the highest level, that makes everyone online exposed to cybercrime while the world is grappling with the effects of the Coronavirus (COVID-19). It makes us all vulnerable and the mercy of the hackers who would exploit every opportunity for malicious purposes. In this article the researcher has explored the potential threats posed by the perpetrators during the ongoing pandemic and proposed solutions for staying safe while online.

Bentotahewa, V. Hewage, C. and Williams, J. (2021) Do we need to revisit GDPR in the wake of Big Data during COVID-19?, *Breaking Boundaries Conference*, Cardiff, 2021, Available at: https://miro.com/app/board/o9J_lHO0lqA=/)

In the modern digital age, data is collected using multiple sensors and various applications designed to monitor and record user movements, communications, interactions, and transactions. The generation of Big Data in this way by countries and organisations to control the pandemic has become a common practice, especially during the current pandemic. Therefore, it is important to ensure that the information is securely collected, processed, transmitted, stored, accessed, and retrieved. This piece of work focuses on challenges associated with the generation of a large volume of data (Big data) during COVID -19 and, whether there is a necessity to revisit GDPR in the wake of emerging challenges. Following an in-depth analysis, the researcher appraised the importance of striking a balance between privacy of individuals and, security of the state and the organisations. In the researcher's view,

the case for understanding the importance of Big Data generated, and the need to develop a 'Big Data friendly' data protection measures that would serve the interests of organisations as well as the individuals. Not doing so in effect will have an impact on the privacy of individuals in the long term.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) *Do Privacy Rights Override #COVID19 Surveillance Measures?* (Available on https://www.infosecurity-magazine.com/next-gen-infosec/privacy-rights-covid19/)

The volume of transfer and handling of Big Data during COVID-19 has risen, and the need to protect privacy cannot be ignored, regardless of whether permissible under extenuation circumstances or not. Therefore, states cannot simply ignore individual privacy in the name of tackling a public health crisis. In this article the researcher has analysed technological solutions provided by the countries and their potential impact on personal privacy. The researcher concludes that technology has the capacity to make an effective contribution towards tackling the pandemic, but it comes at the expense of privacy rights. The biggest concern is the potential risks associated with the deployment of any sort of digital device/software and the long-term impact of the degree of surveillance. Therefore, a pre-deployment risk assessment should be done as a precautionary measure.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) *Big Data in the wake of Data Protection Laws – Asian Perspective*. (Available on http://southasiajournal.net/big-data-in-the-wake-of-data-protection-laws-asian-perspective/)

In generating Big Data, it is important to ensure that the information is securely collected, processed, transmitted, stored, and accessed. However, given the enormous amount of Big Data generated every day, there is an apparent conflict between gathering and protecting Big Data particularly in terms of privacy. Even well-established privacy regulations such as General Data Protection Regulation (GDPR) has recently come under scrutiny in the wake of Big Data. This paper investigates the challenges Big Data faces with the enactment of data security and privacy regulations and laws across the South Asian region.

1.8 Organisation of the thesis

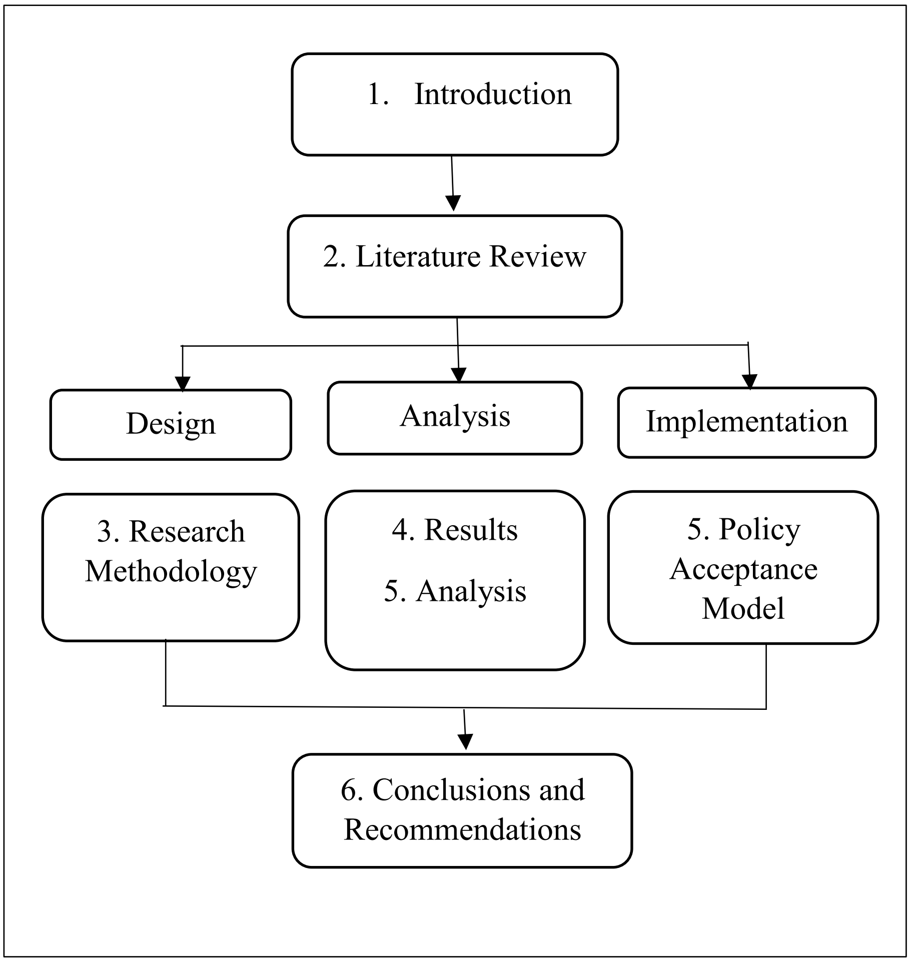


Figure 1.4: Organisation of the thesis

Chapter 1

This chapter consists of the background of the study, research aims, objectives, questions, the significance of the study, limitations, publications, and organisational layout of the thesis.

Chapter 2

Chapter two contains the literature review focussing on the national level legal mechanisms, regional level cooperation to protect personal data and outlines, the challenges associated with evolving technologies and the acceptance and implementation of the data protection mechanisms.

Chapter 3

The chapter three comprises the methodology used for the research, including research philosophy, research design, data collection and data analysis.

Chapter 4

This chapter consists of a descriptive analysis of the data gathered from the questionnaire. The responses were categorised based on the country, gender, age, working experience and their employment.

Chapter 5

In this chapter, the researcher undertook a comparative analysis, based on the country, gender, age, working experience and their employment, and identified the factors that the participants believed to be important in accepting and implementing a global level data protection mechanism. Based on the identified factors, the researcher developed the Policy Acceptance Model.

Chapter 6

The chapter six contains the conclusions of the study and the recommendations made by the researcher, also highlights the areas for future research.

In chapter one, the researcher has highlighted the importance of accepting and implementing data protection laws by emphasising the increased use of the internet and the amount of Big Data generated in a day. Also, the research questions, objectives, aims, significance of the study, the limitations, publications, and the organisation of the thesis (See figure 1.4) were set out in this chapter.

CHAPTER TWO

LITERATURE REVIEW

The researcher has dedicated this chapter to the discussion on the options available to govern the cyber space, the impact of the advancement of technology and generation of Big Data on personal data, the available data protection mechanisms at the national and regional level focusing on Sri Lanka and the United Kingdom, and finally the barriers to developing data protection mechanisms, faced by the countries.

The increased dependency on modern technology and cyber space has allowed nations to reach all corners of the world, whilst the same space is used by states, individuals and third parties for unethical purposes. Technology is advancing rapidly, but the laws fall far behind technological advances. Cyber space is not owned by anyone and can be exploited by attackers located anywhere without borders. In such instances, intelligence agencies find it difficult to trace their locations and take measures necessary to mitigate risks and prevent crime. According to an official in Joe Biden's administration, the cyber threat is here now and is here to stay (Sankaran, 2021), which emphasises the need for urgent action to ensure global security. Adding to that, the Chinese president has stated "Without cybersecurity, there is no national security" (Cuihong, 2015. P.472).

Cyber criminals exploit loopholes in cyber legislation currently in place in developed and developing countries, and cyber hacking consequently poses substantial threats to state infrastructure and the human. The use of cyber space and the threats originating from it are not new phenomena for developed countries when compared to developing countries. The developed countries are known to have mechanisms in place to tackle cybercrimes, and the developing countries are in the process of having their own mechanisms to tackle the challenges they face from cyber threats (UNCTAD, 2020). However, countries without legal mechanisms in place to safeguard personal data risk losing national credibility and confidence in their commercial activities. Also, they risk isolation from participation in international trade activities because cross-border data transfers are subjected to minimum legal requirements.

The global challenges currently facing the international community cannot be adequately addressed single-handed by any international actor regardless of their status or power. When considering contemporary global issues such as climate change, international terrorism, or cyber threats, the need to have a framework for international co-operation becomes a necessity to face up to those challenging phenomena. The perpetrators seek sanctuary outside their country of origin, by taking advantage of weak or inadequate cyber legislation, to avoid prosecution. There is also an apparent reluctance of some countries to strictly implement cyber legislation (UNCTAD, 2020), and that lack of cooperation makes these countries potentially susceptible and vulnerable to cyber intrusions. However, some researchers are engaged in exploring the possibilities of applying international law to the cyber space to address these issues.

2.1 Application of international law

The debatable issue is the application of international law, which states the response to an attack should be proportionate to the attack received (Kretzmer, 2013), and identifying the attacker is important to justify the response (Hollis, 2021, P.3). Another constraint is that the International Criminal Court (ICC) has jurisdiction to prosecute the identified individual only (International Criminal Court of Justice, N.D). Also, for international law to be an efficient governance tool, it must have the flexibility to adapt to new phenomena without the need to reinvent the entire regulatory framework. Therefore, given the information set out above, the researcher believes that the practicalities of applying international law to cyber space will not serve any useful purpose. It is also the case that, most importantly, the authorities have not focused on the cyber space when developing international law. However, there are alternatives that exist for filling the gaps until the nations develop a collaborative, coordinated global level data protection mechanism.

2.2 Alternative solutions

2.2.1 The United Nations (UN)

The UN, as an influential organisation, has the prerogative to make recommendations to the governments. Also, the Security Council has power manifested in it to take decisions at their own discretion to instruct the member states to act in accordance with the UN Charter (UN, N.D). It is vitally important for the UN to play a proactive role in bringing all the countries together and encourage them to harmonize their domestic laws to find an effective way forward. It will speed up momentum for negotiating a global level data protection mechanism instead of leaving it to the time-consuming diplomatic route, which will take longer and not deliver a successful outcome.

However, some of the states have been slow to accept the necessity to have a strategic international plan to tackle the issues concerning cyberspace (Anderson-Fortson, 2016), but recently has become a pressing need to have one to stabilise and sustain international peace. Even though the member states of the UN contribute to creation of the international law applicable to cyberspace, it is only applicable in practice at the state level, and not at the individual level (Anderson-Fortson, 2016). Therefore, the responsibility for enforcement of international law to the citizens rests with the individual states.

2.2.2 Cyber norms

Cyber norms can also be considered as an option, but they differ from international law because they are nonbinding on the states (Katagiri, 2021). That allows flexibility to some extent for the states to converge chosen principles or values without compromising the statutory legal status. The implementation of cyber norms provides the state with justification to respond, through diplomacy, trade sanctions or other means, in instances of violation of any standards by the state (Bannelier, et al, 2019, P.21-32).

2.2.3 Cyber diplomacy

In the process of negotiating strategic objectives, inclusive participation and constructive dialogue with partners are key to achieving consensus through diplomacy. That underscores the necessity for engaging with the stakeholders of the global community in a structured dialogue to address the issues concerns of member states and resolve any conflicts before developing and implementing a global mechanism. Any attempt to do so in an arbitrary manner by developing and imposing a legal framework is bound to end up in failure, also state-level diplomacy alone will not be sufficient to achieve the set objectives. Therefore, it is important to reach out to the secondary stakeholders in the wider community and bring together non-state actors such as civil society organizations, researchers, academics, social media activists, public and private sector representatives, including internet providers.

Cybersecurity is not an institutionalized component of the main agenda of the UN Security Council (Plantera, 2019). However, it is increasingly becoming a recognised integral component that contributes to ensuring the privacy of individuals and keeping the cyber space free from threats and attacks. To respond to these challenges, the influential countries should lead the process to introduce proposals for a legal mechanism and use the diplomatic channels available to them to firm up on a consolidated way forward to protect the cyber space from threats whilst at the same time enhancing the privacy of the individual.

The nations of the world have become an integrated community; just so, the people are having to adapt to rapidly evolving changes in lifestyles, the dependency on progressive advancement of technology is one of them. There are challenges associated with these new changes, and one of them is protecting the privacy of the individuals. The failure to securely protect data would have far-reaching consequences and potentially a catastrophic impact on personal privacy; therefore, it is crucially important to have national, regional, and global data protection policies and regulations to prosecute the perpetrators.

In the next section, the researcher evaluates the impact of the latest advanced technology introduced by Huawei. Over a long time, Huawei mobile phones have become a popular attraction to consumers worldwide and gained a competitive edge over other brands. This caught the competitors by surprise and pointed the finger at Huawei, claiming its involvement in the 5G technology had other intentions going beyond a network provider. Presumably so, but these accusations lack substance and are likely meant to be one-off, but they cannot be discounted without further exploration. For those reasons, the researcher proposes to examine the Huawei as a case study to analyse pros and cons of the impact on privacy and national security, and what effect it would have on cooperation between the countries. Any adversity to arise from the Huawei dispute is likely to sour cordiality between the countries and will hamper the efforts intended to reach consensus and unanimity towards fulfilling the common objective for establishing a lasting policy to protect the personal data of the individual.

The introduction of Huawei 5G technology is claimed to be the next generation of wireless technology of the world, with a built-in capacity to provide faster access to mobile broadband and online connections to multiple devices (Government of UK, 2020, P.10). However, according to the former Head of the Secret Intelligence Service, 5G would have far-reaching implications for the UK's national security and, to a large extent, on all aspects of civic life (Government of UK, 2020, P.13). In a different context, the European Commission refused to impose a ban on the use of Huawei devices and referred it to the Member States to conduct a risk assessment not only on the grounds of confidentiality and the impact of privacy requirements but also on the integrity of available networks, all of which became major national security concerns and a major security challenge (NIS Cooperation Group, 2019, P.32).

2.3 Case study: Huawei 5G technology

Huawei is a Chinese based major high-tech company. It produces consumer devices such as smartphones and trading in more than 70 countries, providing telecommunications services (Leskin, 2018). Its share in the smartphone circuit has surpassed Apple to become the world's second-largest smartphone seller, with Samsung topping its market share (Leskin, 2018).

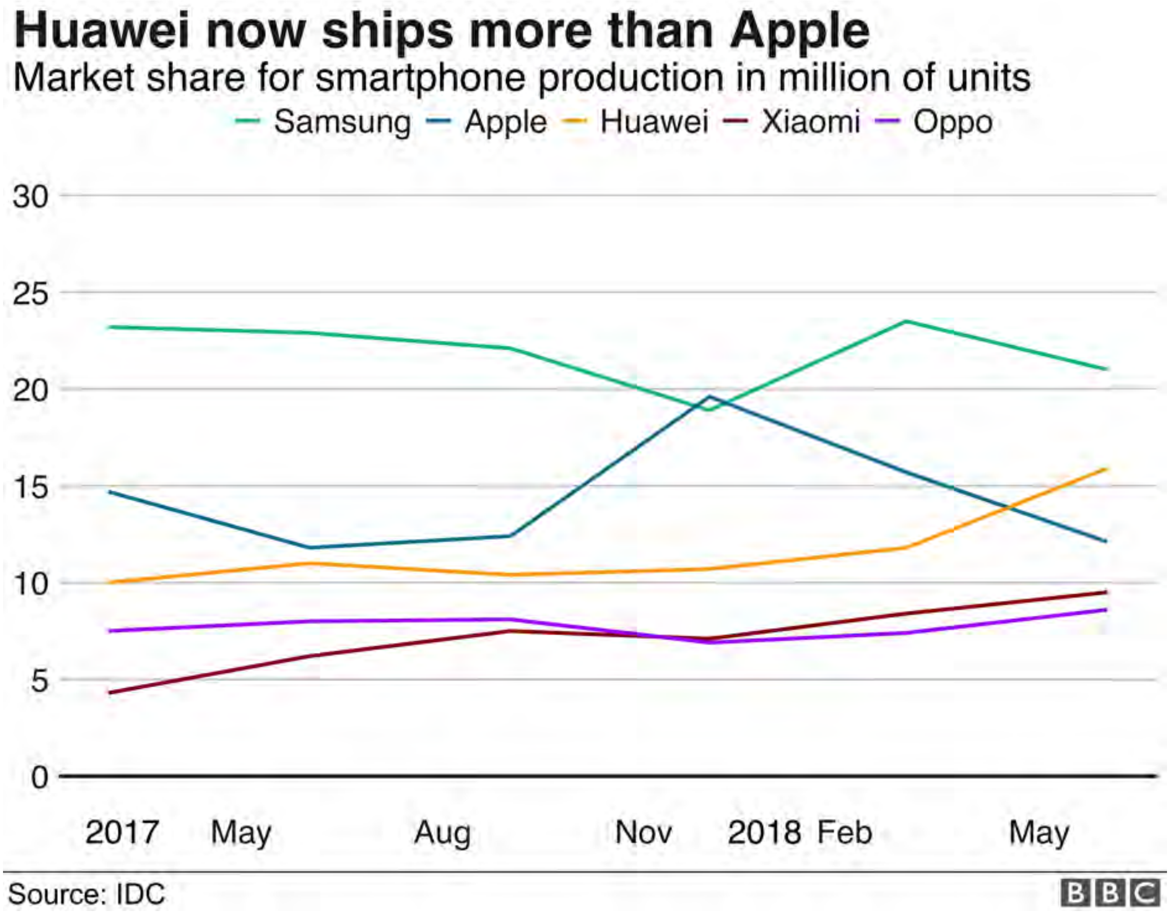


Figure 2.1: Huawei now ships more than apple (Hooker and Palumbo, 2018)

In 2019, the company was subjected to a barrage of accusations against Huawei, the United States (US) claiming Huawei posed potential security threats. That prompted criticism and challenges from the international community, and the US led actions to ban

Huawei (Lecher and Brandom, 2019). The arrest of the Chief Financial Officer, Meng Wanzhou, in Canada had led to a souring of relations between Canada and China and in what appeared to be a ‘tit-for-tat’ response, China arrested two Canadian citizens (Ma, 2019).

The report says that the allegations made against Meng Wanzhou refer to misleading HSBC, and the failure of one of the subsidiaries of Huawei to comply with US sanctions against Iran, whilst Huawei itself was complying with sanctions (Sputnike International, 2018, China Slams Treatment of Huawei Executive Held in Canada as 'Inhumane'). It then raises question whether the imposition of unilateral sanctions by US should be followed by the international community. The report also questions whether financial transactions involving an international bank such as the HSBC and flowing through the United States on its way to or from Iran potentially violates American law (Goldstein, et al., 2018), and could the bank risks liability for violating US sanctions. It is questionable whether the US could apply their domestic law internationally in an arbitrary manner.

Huawei row has gone beyond boundaries. It started between China and the US, but reportedly, it has spread to key allies and partners in the world under US influence, resulting in those countries breaking ties with Huawei. In response to a US-initiated campaign against Huawei, Australia, New Zealand, Britain, Canada, India, Japan, France, Germany, and even the Czech Republic have also joined in expressing their concerns about security issues (International the news, 2018).

2.3.1 Who is in this row and why?

The US had imposed a ban on selling Huawei phones to military bases (The Guardian, 2019). British Telecom (BT), the largest mobile network provider in the UK with whom Huawei has been in a long-standing (17years) collaboration partnership, providing Huawei equipment to BT Mobile network. However, BT has announced that it was removing Huawei equipment from its 3G, 4G and 5G network (Griffin, 2018). This decision follows the security concerns raised by the head of the MI6 (UK Foreign Intelligence Service), despite Huawei equipment has been constantly monitored by a special company laboratory overseen by government and intelligence operators (Griffin, 2018). Therefore it is surprising that BT has taken the decision it has, unless BT had come under pressure to do so.

This is not all. The Japanese government also has banned the purchase/use of Huawei and ZTE telecommunication equipment by public institutions (Sputnik International, 2018, Analyst on Huawei Case: Incident May Have 'Extremely Unpleasant Consequences). Furthermore, India, New Zealand and Australia have banned Huawei's involvement in the installation of 5G mobile network (The Guardian, 2019). Germany has also stated that Huawei's role in its future telecom infrastructure was under review, and a decision would follow to restrict the use of Huawei equipment (Moskwa, et al., 2019). This has the hallmark of a concerted effort, presumably instigated by the US, to punish Huawei for something it may not be guilty of. The worrying aspect of this sustained pattern of accusations is the hardening of attitudes and retaliatory action China is likely to take against political/psychological posturing by western countries to undermine competition from Huawei in the wake of a major trade war and a climate of heightened security risks to western countries. Whatever the case may be, it is bound to affect stability and sustainability of world order, sour international cooperation, and jeopardise any chance of achieving unanimity accepting and implementing meaningful privacy protection policy framework at the global level.

EU is faced with a similar dilemma in the Huawei affair having to decide whether to join the US in imposing a ban on Huawei equipment within the EU. This is a challenge the EU faces as it maintains close economic relations with US and China, and its dependency on both countries for trade makes it difficult for the EU to take such action. However, the UK, France, Germany, Norway have publicly raised concerns about using Huawei equipment for next-generation mobile networks, but Spain, Portugal and Hungary have been more welcoming to Chinese involvement (Moskwa, et al., 2019). This is a clear indication of a split of opinion amongst EU member states.

2.3.2 Divisions in the EU

Poland relies on the EU for financial support (Polish Investment and Trade Agency, N.D) and depends on the US for its security with the presence of US troops on its soil (US department of states, 2021). The arrest and detention of employees of Huawei by Polish authorities for spying on behalf of China is another incident of this saga involving China and the West. Huawei's local sales director in Poland was arrested along with a Polish citizen who worked for the main local business partner of Huawei, who was once a senior manager in a Polish intelligence agency (Birnbaum, 2019). Is this another case where the

US is seeking to involve soft targets in the EU to extend its campaign, or is Poland acting alone in its self-interest based on security concerns?

In contrast, Portugal taking a different line, has joined hands with Huawei. One best example is Altice Portugal has signed a contract with Huawei for the supply of Chinese hardware and software (Sputnik International, 2018. Analyst on Huawei Case: Incident May Have 'Extremely Unpleasant Consequences). According to the agreement, China would help to modernise number one telephone network of Portugal to 5G standards by 2019, to become 15th 5G client of Huawei in Europe (Sputnik International, 2018. Analyst on Huawei Case: Incident May Have 'Extremely Unpleasant Consequences). This divergence of policy on Huawei factor within the EU states provides a clear indication of mixed behaviour of individual states within the EU. That brings into question whether some countries support the Huawei factor campaign led by the US, whilst others ignore and move on building technical links with Huawei.

If Huawei is supposedly posing a national security threat, it will not be limited to one or two countries and would have to be considered within a global dimension. It is apparent that the US and allies are banning whilst others are welcoming Huawei. This raises the question of whether the accusations made against Huawei are relatively political pressure exerted based on security threats. Analysing the case study further, it is important to pinpoint to what extent this threat would impact the society and privacy of individuals.

2.3.3 Why Huawei appears to be a threat?

The US consider Huawei poses a threat to global security for several reasons:

- The tendency to use Huawei phones and electronics to spy on US government officials (Vincent, 2018)
- National Intelligence Law of China passed in 2017 states that organisations must support, co-operate with and collaborate in national intelligence work ((BBC, 2018, Should we worry about Huawei?)

The vision to achieve tech dominance made the US one of the most advanced industrial nations, but that status has changed with the emergence of the high-tech revolution in China becoming a dominant player in the world. Is the US concerned about China’s rise in the technology field and considers it a threat to its tech dominance?

The world is no longer a unipolar system. China is an upcoming actor in the international arena. Comparatively, both are economically and technologically powerful actors, and they always face a challenge amongst themselves (Council on foreign relations, N.D). For example, Huawei incident is another challenge to the US and they are trying to find their way forward with newly developing Chinese technology.

If America succeeds in an exclusion of Chinese tech firms and uses its extra territorial sanctions to force countries to stop obtaining Chinese technology, it will have serious repercussions on small states that are trapped between two powerful nations.

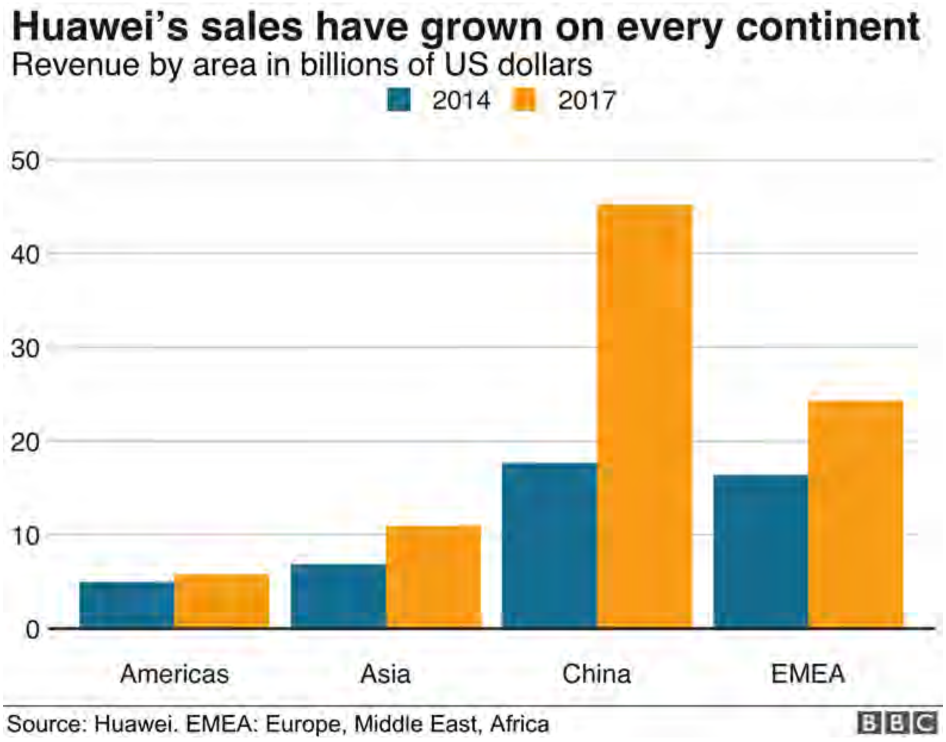


Figure 2.2: Huawei's sales have grown on every continent (BBC, 2018, Huawei: The rapid growth of a Chinese champion in five charts)

Collective accusations on Huawei puts it under immense pressure and Huawei needs to respond to the allegations made against it by the international community to restore the credibility of the company, the corporate image, and confidence of the customers whose loyalty to the company is crucial.

2.3.4 What is the response from Huawei?

The arrest of the CEO of Huawei by Canadian authorities, apparently on a request from the US (Young, 2018), induced a diplomatic rift between China and Canada. The reaction from China was swift and demanded unconditional release of the accused, warning that failure to do so would have a heavy price to pay (Lendman, 2018). It is evidently clear that Canada has been caught up in a bilateral dispute between the rival powers, China and US.

The world telecommunication companies handle a variety of data, including personal details. The US believes, The National Intelligence Law of China, passed in 2017 (BBC, 2018, Should we worry about Huawei?), could hire these organisations to spy for them (Vincent, 2018). The experts found that not only the Chinese government sought support from their organisations to ensure national security, but others are also known to have done the same as in the case of Apple seeking support to find criminals (Fox and Lee, 2016). It is not the case when western countries access protected data on threat security grounds; it is acceptable and, when others do the same, it is termed as espionage.

However, Huawei has denied all the allegations and emphatically stated that neither Beijing had any influence over Huawei nor that they had received any request from the Chinese government for access to information (International the news, 2018). Huawei insisted on its status as an independent company and reaffirmed that it was under no obligation to provide information to the government except paying due taxes (Karl, N.D). The rotating Chairman of Huawei is quoted as saying that banning a particular company would not remove cyber security concerns and solve the problem (International the news, 2018). The researcher sees the validity of the statement and agrees that banning one organisation would not lead to a lasting solution. Therefore, consensus-based swift action is the sensible and credible approach to follow instead of pointing the finger at each other.

The biggest challenge Huawei is faced with is to satisfy the partners by providing evidence to prove that the quality of its cyber security services are sound and is second to none, and are protected from backdoor intrusion. The researcher believes that setting up of an impartial regulatory body and a mechanism to monitor potential threats will be the effective way to avoid friction between the nations, and to achieve that a coordinated response sponsored by the international community is essential. Their remit should be to build a secure environment free of potential cyber threats by implementing amenable policies collectively endorsed by the parties.

The Huawei dispute has gone beyond boundaries and has become the most contentious issue affecting major countries. The claims made by the US accusing Huawei and the number of incidents that followed has soured relations between a number of countries, but there is no indication of a speedy resolution to the dispute. Against that background, it is important to assess what the consequences would be and what impact they would have on the relationship between US and China and, Huawei as a company.

2.3.5 Consequences of the Huawei dispute?

The US president has made Huawei the biggest story by imposing a ban on the use of Huawei equipment in the US, and as a result, US companies associated with Huawei have been forced to fall in line (Lecher, 2019). The basis for the controversy was the long-held belief of the US intelligence community that Huawei acting on behalf of the Chinese government, has the capacity to undermine US national security whilst at the same time jeopardising customer privacy (The Verge, N.D).

In 2012 espionage allegations against China first came to light (Reiff, 2019). US congressional panel in a report stated that both Huawei and ZTE Corporations could pose a potential security threat. In another report in early 2018, Senate Intelligence Committee has issued warnings about potential threats to national security from Huawei and ZTE (Reiff, 2019). The allegations made by US intelligence agencies pointed to Huawei equipment possessing backdoors which would allow the Chinese government to spy on users (Reiff, 2019), but Huawei has denied all the allegations emphatically stating neither Beijing had any influence over Huawei nor that they had received any request from the Chinese government for access to information (International the news, 2018)

Huawei is faced with a potential threat to its business following the actions initiated by the US. The US Commerce Department has imposed an embargo on Huawei from trading with US companies without government approval (Lecher, 2019). The ban has already affected companies like Google, Corning, Intel, Qualcomm, Broadcom and ARM (Lecher, 2019). Microsoft is one of Huawei's biggest software partners; however, it has not yet joined the bandwagon (The Verge. N.D).

The Huawei ban has led to the Chinese hardware company losing its membership in the SD Association (Gartenberg, 2019). As a result, Huawei is only allowed to use SD and micro-SD cards on existing Huawei hardware and is barred from using future products (Gartenberg, 2019). In addition to that Huawei's membership has been temporarily restricted by the Wi-Fi Alliance (Gartenberg, 2019).

The law firms have stated that any company granted a technology licence from the US has to adhere to the same restrictions (The Verge, N.D), which means effectively severing partnership with Huawei. It is likely why ARM, based in the UK and owned by the Japanese SoftBank Group (Warren, 2019), using US-origin technology (The Verge, N.D) has taken necessary precautions to sever its partnership with Huawei.

However, according to reports, Huawei is arguing against the US government ban, claiming it is a bill of attainder (Lecher, 2019). The Constitution of the United States forbids legislative bills of attainder targeting specific people or groups of people in accordance with federal law under Article I, Section 9, and in state law under Article I, Section 10 (Encyclopedia, N.D). This decision put the government into conflict with the constitution. But the US government has defended its decision stating that it is well within its national security powers (Lecher, 2019).

Huawei phones use the Android system and depend on google updates and other technical services which are essential to maintaining product reliability and sustainability. The losing android licence will prevent access to the google play store, consequences of which will be the loss of access to key apps like Facebook, Instagram, and Google Maps (Vincent, 2019). This will be a significant blow to Huawei's commercial interests and will without a doubt affect the sustainability of existing Huawei devices and those in the pipeline.

It is unlikely that US actions would prevent Huawei products despite any short-term impact on the company. However, Huawei maintains that the impact on their company is not a detrimental one, as has been reported. Huawei says that they are in the process of developing an alternative operating system (Yu, 2019) called HongMeng (Reichert and Keane, 2019) that they expect to release after losing access to Google's Android OS and popular apps. Huawei's own brand of Nano Memory Cards will replace microSD cards (Gartenberg, 2019), and AppGallery in its new OS will replace Google Play Store (Lang, 2019), and Huawei remains upbeat and confident about their future. Huawei may not actually benefit from having a standalone operating system incorporating apps unique to their products unless other Chinese phone manufactures use Huawei's own operating system.

Given that Huawei is not a big player in the US market (Stat counter, N.D), if Huawei is considered a threat to US national security, why not just ban Huawei's role in network infrastructure instead of Google ban on Huawei. One can assume that US actions are designed to back up their trade war with China using Huawei as a means of achieving their strategic objectives influenced by their superpower mentality. Accusations have been made against China for violating intellectual property rights and stealing trade secrets; if that was the case, similar accusations should apply to other Chinese mobile phone companies and DJI technology company who manufactures unmanned aerial vehicles. If China wishes to extract sensitive data and information, despite the ban imposed on Huawei, China will use other means to do so. In such circumstances, would the US has effective means to prevent it?

In the next section, the researcher seeks to assess whether the Huawei dispute will lead to souring of relations between China and the international community, and how it would affect China.

2.3.6 Break down of relations

The Huawei row is likely to sour relations between China and the countries that are entangled in it and jeopardise diplomatic channels between them. According to recent reports, China has already cancelled off talks with forest industry businessmen from the province of British Columbia (Sputnik International, 2018, Analyst on Huawei Case: Incident May Have 'Extremely Unpleasant Consequences). The scholars also believe that this incident will badly affect Chinese-Canadian free trade zone negotiations. Also, the experts predict that China may take action to influence crucial Canadian industries, such as the export of mineral resources and ready-made industrial products, including cars and equipment for energy and mining industries (Sputnik International, 2018, Analyst on Huawei Case: Incident May Have 'Extremely Unpleasant Consequences). The Global Times has added its voice in a report that China may retaliate by boycotting Canadian tourism and products like Canada goose jackets (Goldstein et al., 2018).

The researcher strongly believes that neither party would wish to cross the red line because repercussions of such action would not serve the interest of anyone. The experts anticipate a trade war between US and China (Reiff, 2019) that will have a negative impact on global economic growth that will in turn have serious limitations on the development of national economies. As far as trade between US and China is concerned, the reports say that both countries have been going through a shaky patch prior to the arrest of Ms Meng Wanzho (CFO of Huawei) (Leskin, 2018). The two governments have been locked in a trade war, and both have imposed tariffs on key imports worth billions of dollars (Leskin, 2018). Given the strength of distrust and animosity in the current climate, it is very likely the trade relations may get worst. The report noted that as a consequence of the controversial incident and the impact it has on trade, a closed-door meeting between representatives of large American companies have been called for by US (Sputnik International, 2018, Analyst on Huawei Case: Incident May Have 'Extremely Unpleasant Consequences). But the participants have already expressed their concerns about possible countermeasures by China against American firms and their leadership.

The review seeks to understand the context/motives of this incident and what hidden factors lead to it. The accusations against Huawei and the sequence of actions that followed appeared to have raised more questions than answers. It has opened a gap between China and the powerful states of the Western alliance, and indications are that some countries remained calm and taken a ‘wait and see’ approach.

The Huawei case cannot be taken on isolation to point the finger at one nation and should be looked upon as a global phenomenon. In a nutshell, powerful nations engage in cyber espionage, that is unethical behaviour for various purposes and accuse each other of being ‘bad boys’. Therefore, to avoid further deterioration of the world order concept, it is imperative to find unanimity and form a basis for resolving differences and move forward. The failure to do so will undoubtedly lead to conflict amongst powerful nations, breakdown of world order, and even regional alliances grouping into West and East.

In annexe C.1 the researcher focused on the introduction of Huawei 5G technology, disagreements between five eye partnership, and potential impact on national security (See annexe C.1). The new privacy policy introduced by WhatsApp was discussed as another case study and, the privacy concerns associated with it was also discussed (See annexe C.2).

The narrative above refers to the Huawei dispute and its impact on cordiality between the countries, trust amongst the nations, and privacy of individuals. The researcher then focuses on evaluating the challenges the states faced with the advancement of technology.

2.4 Challenges faced by the states with the advancement of technology

The introduction of Information Technology (IT) systems and the deployment of advanced technology such as Artificial Intelligence and the Internet of Things is gaining momentum amongst a wide spectrum of users. These systems generate a vast amount of data which is the by-product of advanced technology, and it continues to grow at an unprecedented rate. The data is collected, processed, and stored unbeknown to the individual as well as to the public at large. The processing of data in this way by using technologies like Artificial Intelligence, the Internet of Things, and Big Data is continuously challenging the legal framework in every jurisdiction (See annexe C.9).

In the digitalised world, the right to privacy goes hand in hand with data protection, and that makes the right to privacy an essential element of democratic values. The increasing dependency on technology brings national security to the forefront of concerns of the 21st century. The developing and developed nations face many challenges in the fight against cyber threats and the associated risks. The military of the United States, for instance, Army, recognises cyberspace as the most important battle space after land, water, and sea (Dhungel, 2019). A former CIA director and senior ranked General has stated that the cyber threats across the world had a similarity, and the nations should recognise that as a critical part of national security (Dhungel, 2019).

Today the internet is a lawless society; hackers can break into computers with relative impunity. The countries without data protection and privacy laws have failed to successfully prosecute convicted offenders for cyber-crimes commonly known as stealing data and identity, spamming, scamming, and the culpable offenders escaped with impunity. Many developed countries have drafted and approved appropriate legislations and are going through implementation to some effect (UNCTAD, 2020). Also, an increasing number of nations are beginning to enact Personal Data Protection laws that resemble European style General Data Protection Regulation (GDPR) (See section 2.7). The Asian nations take a diverse approach than the straightforward process in the European nations, due to the politically, ethnically, linguistically, and culturally evolved diverse jurisdictions of the colonial background.

In May 2018, the European Union adopted the GDPR as a legal measure to provide a set of standardised data protection laws across its member states (Burgess, 2020). Following similar lines, countries of the Association for South-East Asian Nations (ASEAN) have enacted and implemented legislations that uphold the data protection mandate (Raghunath, 2019, P.56-68). However, in the SAARC region, most of the countries are in the process of developing data privacy laws (Greenleaf, 2019, P.1-7), but there are no relevant regional developments resulting from the SAARC agreements (Greenleaf, 2019, P.7).

The UN General Assembly, in its Resolution on the Right to Privacy in the Digital Age, noted that the rapid pace of technological development enables individuals all over the world to use new Information and Communication Technologies (ICT) (De Soysa, 2017). This concurrently enhances the capacities of governments and companies to undertake surveillance, interception, and data collection, the process that may particularly violate the right to privacy (De Soysa, 2017). On that score, the UN General Assembly together with the Office of High Commissioner for Human Rights, has affirmed that the rights held by people offline must also be protected online (De Soysa, 2017). Therefore, the case for undertaking an extensive review to develop a consistent legal framework is crucially important and stronger than ever before.

The researcher then focuses on the General Data Protection Regulation (GDPR) implemented to safeguard personal privacy, and evaluate the type of mechanisms it does suggests to address privacy issues associated with new technologies and devices.

2.5 General Data Protection Regulations (GDPR)

The European Union (EU) enacted the GDPR (Wolford, N.D., What is GDPR, the EU's new data protection law?) governing the protection of personal data to promote establishment of a regional strategy for information security, based on fundamental rights underpinned by democracy. Amongst other factors, personal data protection is one important element of the rights of the people, and it offers peace of mind to individuals and makes them feel protected from unauthorised intrusions to their personal data. Regulatory privacy protection will encourage governments to acknowledge different privacy interests in a respective country and ensure that appropriate provisions embedded in a legal framework protect the victims affected by privacy breaches.

The collection, the use of, and disclosure of personal information of individuals are concerning issues in a climate of rapidly developing information processing technology, and an increasing number of people are becoming concerned about their privacy being compromised in the process. Therefore, the overriding concern is how secure the collection, disclosure, processing and managing personal data are. That leads to emphasising the crucial importance of having adequate data privacy laws around the world.

GDPR prescribes eight Data protection principles, Lawfulness, Fairness and Transparency, Purpose Limitation, Data Minimization, Accuracy, Storage Limitation, Integrity and Confidentiality, Accountability (Eur-Lex, 2016). Some changes have been introduced in the field of data protection by harmonizing the data privacy laws across Europe (See section 2.7.6). The EU prohibits the transfer of data from an enterprise in the EU region to countries that do not match the same level of EU Regulations on data protection (Eur-Lex, 2016). The implication is that an organisation or an individual from any part of the world handling information of citizens, even based in an EU member state, comes under the purview of GDPR. The new rules also provide the EU citizens with a set of rights ranging from the right to access to the right to be forgotten of personal information (Eur-Lex, 2016).

The enterprises that undertake activities relevant to the processing of personal data are required to employ a data protection officer, and (Eur-Lex, 2016) reporting of data security breaches is mandatory as recommended by the commission. The enterprises are obliged to alert both their data protection authority and the people affected by the data breaches within 72 hours of detection and provide a detailed report of the incident, including a recovery plan proposal for mitigating its effects (Eur-Lex, 2016). Those organisations found to be in violation of the GDPR set rules would be liable for substantial fines. The maximum fine for a GDPR violation is 20 million euros or 4 percent of a company's annual global revenue from the year before, whichever is higher (Eur-Lex, 2016). European Union by endorsing the GDPR, has taken the lead in instituting data privacy regulations. It is incumbent on other countries to follow suit and come up with a strong, meaningful legislative framework for data protection worldwide. To this end, Asian countries are also now showing signs of catching up aligning with the rest of the world (Greenleaf, 2019, P.1-7) (See section 2.7.1).

Some also argue that the GDPR would not create more harmonisation but rather create even more national differences than today (Albrecht, 2016, P.287-289). The GDPR has set standards that no data controller will be able to ignore, and other governments will be under pressure to raise their data protection standards to allow their economies to access the single digital market of the European Union. The effects of this can be seen already today, where some countries like Japan intends to introduce similar provisions to the GDPR (Albrecht, 2016, P.287-289). The UK businesses are also doing their best to make sure the GDPR applies to its full extent in post-Brexit Britain, and the UK remains committed to the privacy principles enshrined in the EU Regulation (See annexes C.3 and C.4). The UK Government has also pledged to introduce a new 'digital charter' with the aim of ensuring the UK remains the safest place to use online facilities (Government of UK, 2017, The Queen's speech 2017, P. 59-60).

The data protection regulations ensure sharing of information without causing infringement on personal data. The emerging modern technologies generate a vast volume of data, and it is important to ensure the information is securely collected, processed, transmitted, stored, and accessed. However, given the enormous amount of data generated daily, there could be a tendency for conflicts to occur between gathering and protecting data, particularly in terms of privacy.

In the modern digital age, data is collected using multiple sensors as well as through various applications that are designed to monitor and record user movements, communications and transactions. It is common practice for organisations to use systems to process and store what is known as Big Data. In professional literature, the definition of big data refers to, volume of data collected, the variety of sources, the speed of analysis and interpretation, that could be achieved through the analytical process (Zarsky, 2017, P.999).

In the next section, the researcher investigates how Big Data is generated, what mechanisms countries have put in place to protect Big Data, and what the challenges be in protecting Big Data. Combining all these topics, the researcher has also produced an article which was published in the South Asian journal (Bentotahewa, Hewage and Williams, 2020, Big Data in the wake of Data Protection Laws – Asian Perspective)

2.6. Introduction and deployment of IoTs and generation of Big Data

(Bentotahewa, Hewage and Williams, 2020, Big Data in the wake of Data Protection Laws – Asian Perspective)

The growth in the emerging trends in the use of IoT and the deployment of other digital systems by the states, organisations, security services, government apparat has become the norm to gather information about people, businesses, lifestyles, purchasing behaviours, travel, consumption patterns, to a limitless extent. The onset of COVID-19 made the health authorities and the governments resort to IoTs to manage the coronavirus and to prevent its transmission. The deployment of an array of sophisticated digital tools made it possible to collect personal information in large volumes for processing and storing in the digital systems without the knowledge of the data subjects. That made humans become a part of innovative technologies and connected devices, bringing the inherent challenges to privacy protection.

As increasing dependency on digital technology is becoming a way of life, the use of video technology (CCTV) for surveillance operations to collect data of personal identities raises concerns. This method has become a common practice in gathering information about people, their movements at the workplace as well as in public places. The use of CCTV has grown globally for various purposes, for instance, in Australia uses this technology in public places for monitory purposes (Wilson and Sutton, 2004), and the same technology is used in Singapore for enforcement of traffic regulations and to prevent littering (Rengel, 2013). Philippines mandated the installation of CCTV cameras in hospitals under the Filipino Hospital CCTV Act of 2008 and established penalties for releasing any footage without a court order (No author, 2012., P.7). Thailand, in response to the bomb explosions in Bangkok during the 2007 New Year's Eve celebrations, also gave the go-ahead for the installation of more than 10,000 CCTV cameras for traffic monitoring and security purposes (No author, 2012, P.13). However, there are different legal constraints on video surveillance worldwide. Britain and the US have limited legal constraints, whilst Austria, Germany, Norway and Sweden, employers are obliged to seek consent from the workers for such purposes (Ascher, 2005, P.239).

Wide ranging methods are used to gather personal information and behaviour patterns of employees. The most commonly used techniques are phone tapping, accessing emails, and monitoring computer screens for surveillance operations. Added to that, there are other methods in use such as remotely bugging conversations, analysing computer and keyboard usage, tracking devices to monitor personal movements. The use of smart ID badges to track an employee's movement around a building is common practice, particularly in sensitive areas. Range of other methods in the form of psychological tests, general intelligence tests, aptitude tests, performance tests, personality tests and lie detector tests are all electronically assessed.

In the motor industry advanced technology is widely used for broadcasting their location, speed, steering-wheel position, brake status, and a variety of other data that determine performance and safety of the car and the driver (Safari, 2017, P. 844). On the other hand, the automobile insurance companies gather location data using satellite (GPS) systems, using mobile phones to track the customer's movements, and their driving habits are logged using telematics data from on-board IT systems (Kemp, 2014, P.5). Similarly, smart domestic sensors are being used to enhance responsiveness to domestic emergencies such as fire risks, flooding and theft. Health apps and wearable technologies (Fitbit) have inbuilt technical capacities to provide recorded data and information that are used for health purposes (Kemp, 2014, P.5).

Gathering and storing some specific data on individuals brings obvious benefits in many areas. The aviation industry, including airlines, generates and holds vast amounts of data on passengers' personal preferences and travel habits at all stages of their journey (Kemp, 2014, P.5-6). Although the airlines do take measures to protect such personal data, they are under obligation to share the passenger information with security organisations to combat terrorism and serious crimes, but there are inherent risks of compromising such data held by the airlines. The long-term retention, sharing and use of this data for those purposes without adequate safeguards has been controversial and has attracted criticism from privacy groups and security experts (Kemp, 2014, P.5-6).

Video and audio data generate a range of signals; for example, to detect Parkinson's disease voice recordings are used and smartwatches are used to measure heartrate (Altman, et al. 2018. P.29–51). Research has shown it may even be possible to extract conversations from video recorded images of vibrations on surrounding materials, or to determine the occupancy of a room based on Wi-Fi signal strength (Altman, et al. 2018, P.29–51).

Online sales outlets such as e-Bay use consumer shopping history to promote their own brands of products. In a different context, social media platforms such as Facebook collects information on subscriber habits and preferences in using its services, content types, the devices used, language and time zones (Bagley and Brown, 2015, P.514). According to the reports, by 31 January 2020, the Population in Asia using Facebook has reached 867,984,000, and it is a significant number when compared to the rest of the world (Internet World Stats, N.D). Retailers use the information on consumer shopping habits and social interactions for direct marketing and to promote alternative products to the consumer. For instance, Uber tracks its drivers to make their service effective and rapidly respond to public needs. However, this data could also be used to monitor driver behaviour, road traffic breaches and productivity estimation (Koch, N.D).

Section 5(1)(b) of the GDPR article sets out the fundamental notion that personal data must be collected for a specific, explicit and legitimate purpose (Eur-Lex, 2016) but with the Big Data purpose is not clearly defined. As you have observed from the above examples, Big Data is generated using different devices, and it is impossible to give a legitimate reason for collecting data. Also, the GDPR specified that the collected data should be limited to what is necessary (Eur-Lex, 2016), but in practice such limitations are very difficult to enforce.

In the next section, the researcher sought to ascertain the process of generating Big Data during COVID-19 as a case study. The researcher discussed the devices deployed to mitigate the pandemic and the generation of Big Data through these devices.

2.6.1 Deployment of new devices during COVID-19 and generations of Big Data

The urgency of the need to manage and find cures for the COVID-19 has also made it necessary to collect data in volumes, and necessary to share information between the research institutions. The sharing of information also means the transfer of Big Data, which inevitably will infringe on individual privacy. Therefore, the transfer of Big Data in this way, whether permissible under extenuation circumstances or not, the handling of Big Data requires responsibility and the need to protect privacy cannot be ignored.

A number of countries are developing contact tracing apps as a digital tool to diagnose the presence of the virus and to prevent it from spreading thereby mitigating the risk of worsening of the pandemic. For an example China is using COVID-19 tracking apps which generally work by assigning a colour code (green, yellow or red) using an algorithmic assessment of the user's travel history and health status (Utzerath, et al. N.D). The Hong Kong government operates a mobile app that uses geofencing technology to track and monitor a quarantined person's movement to ensure he remains in the location (Utzerath, et al. N.D). The Japanese government has also developed a Bluetooth technology integrated contact tracing app (Utzerath, et al. N.D). The contact tracing app developed by the Government of India processes users' travel history, symptoms, and location data to calculate the risk they are exposed to contracting the coronavirus, but that approach has come under widespread criticism from the public (Agrawal, 2020). The government has made the app mandatory for public and, according to the reports those caught without the app could face fines of $13 or a six months jail sentence (Agrawal, 2020). This mandatory requirement leaves people with no choice and unwilling or willingly obliged to participate in gathering data in large volumes. That makes a case for implication for violations of individual privacy rights.

The Google/apple apps provide a decentralised software architecture and save a log of the user contacts within the app without uploading to a government server (Kelion, 2020) (Bentotahewa, Hewage and Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?). In contrast, the initially proposed NHS contact tracing app in the UK logged information of users in a centralised database of government servers (Kelion, 2020) (Bentotahewa, Hewage and Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?). There is an issue of public concern about this method of holding personal data in a one for all centralised database, which the government departments and law enforcement agencies use for surveillance operations on a scale never seen before.

France is one of the few European countries to have opted for a centralized model for coronavirus contacts tracing. The French government has chosen to have user information fed into a central server. However, downloading and installation of the app is voluntary (Osborne, 2020) (Bentotahewa, Hewage and Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?). The UK also adopted a centralized approach to track and trace (Kelion, 2020, NHS rejects Apple-Google coronavirus app plan) (Bentotahewa, Hewage, and Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?), and to allay any public concerns about the contact-tracing app, those who developed the NHS app, gave assurances that collected data would not be shared with other government departments or private companies (Sabbagh, et al., 2020) (Bentotahewa, Hewage and Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?). However, the UK discontinued the contact tracing app in use at the time and shifted to a model provided by Apple and Google (Kelion, 2020, UK virus-tracing app switches to Apple-Google model).

These contact-tracing apps do generate a large amount of Big Data. The impact of contact tracing apps cannot be taken in isolation, and the focus should also be on the implications of facial recognition cameras, wearable bands and police surveillance drones. For instance, the Chinese authorities have been using Street cameras with facial recognition systems to apprehend, shame and fine citizens (Ng, 2020) venturing outside without face masks Kuo, L. (2020) and even used similar tools to identify and quarantine individuals who appeared to have carrying the virus (Kharpal, 2020). South Korea has also employed a broad surveillance mechanism, and according to a report, the Seoul government has heavily relied on information collected from CCTV footage, bank card records, and mobile phone data to deal with the outbreak (Fahim, Kim, and Hendrix 2020). The reports also claim that the UK has used drones to track people who were ignoring COVID-19 social distancing rules (Lancefield, 2020). Whatever and whoever uses such mechanisms will be infringing on public privacy in one way or another.

The world is in an unprecedented pandemic, but the application of human rights laws stands. Therefore, states cannot simply turn a blind eye to privacy in the name of tackling a public health crisis. That has prompted some human rights and civil society organisations around the world to speak with one voice calling all governments to adhere to human rights laws when employing digital surveillance technologies to track and monitor individuals and populations in combatting the spread of the novel coronavirus. In support, the Amnesty International UK director has pointed out that the Government should be looking at decentralised app models where contact-tracing data stays on a user's device (Amnesty International UK, 2020). It is a fact that the contact tracing app entails data gathering on an unprecedented level, and that makes it open to unauthorised disclosure.

The response of the government and the tech industry to the coronavirus outbreak has already raised concerns about the implication of using contact tracing apps on privacy, during and after COVID-19 pandemic. Hence, the general public should be vigilant and be aware of the technological developments which will affect user privacy. On the other hand, concerns raised by the public in the use of technical solutions to combat COVID-19 demonstrate the extent of their awareness of the risk.

Even though the technology has the capacity to contribute to tackle the pandemic effectively, it comes at the expense of privacy rights. The biggest problem we face is visualising the degree of surveillance and what surprises it will bring. Given a choice between privacy and health, people are likely to choose health, but it is desirable that they should choose both. The privacy and security challenges associated with the generation of Big Data during the pandemic are discussed and analysed in annexe C.10, C.11 and C.12.

In the aftermath of collecting Big Data, a significant conflict emerged between the principle of GDPR and the data generated. The researcher having evaluated this issue in detail, suggested recommendations in next section on how to overcome the conflicts.

2.6.2 Challenges and obstacles to the application of data security and privacy regulations and laws to Big Data (Bentotahewa, Hewage and Williams, 2020, Big Data in the wake of Data Protection Laws – Asian Perspective)

Even though there is a considerable development in data security and privacy regulations and laws, these regulations and laws face many challenges in the digital age, and the emergence of Big Data is perhaps considered to be the greatest. In the Big Data era, the public enjoys many benefits that internet technology offers to them. But at the same time, they also do face potential breeches on privacy laws affecting personal data. Failure to protect user accounts and personal data will directly threaten the privacy of users and the security of data.

At present, many organisations believe that once information is processed anonymously, the identifiers will be hidden, and then the information will be released, but the reality is that the protection of privacy cannot be effectively achieved through anonymous protection only (Brogan, 2019). Another concern is the ability of criminals to intentionally fabricate and forge data in Big Data (Zhang, 2018, P.276). The wrong data will inevitably lead to erroneous results. Some people may make up data to create data illusions that are beneficial to them, leading people to make wrong judgments (Zhang, 2018, P.276). For example, some websites contain false comments and ratings, and users can easily be lured into buying these goods and services based on the faked comments and ratings. The impact of false information is difficult to measure against the popularity of internet technology, and the use of information security technology to screen these data is also very difficult (See annexe C.7).

The technological advancement highlights the difficulties in sustaining data security and privacy policies inspired by GDPR in its entirety, and the right to be forgotten (Eur-Lex, 2016) is one such area of concern. This is particularly relevant in circumstances in which an individual from the Euro zone is having a rare disease faced with the option to removing personal files containing genetic variance, and if that person happened to be the only known person with that variance, and access to medical records was denied, that would be an obstacle to the medical investigation into the disease. Furthermore, with the increased use of blockchain-based technologies in public and private domains (Shahaab et al., 2020) (Khan, et al., 2019, P.1-15), implementation of certain clauses such as the right to be forgotten will be challenging due to the tamper-proof nature of the technology.

The biggest challenge for Big Data from a security point of view is the protection of individual privacy. Big Data often contains huge amounts of personal identifiable information, that makes privacy of users a huge concern. Given the large amount of data stored, breaches affecting Big Data would have devastating consequences that would be more serious than the data already exposed as a result of the security breach. The outcome of such a scenario would potentially affect a much larger number of people, with detrimental consequences and legal repercussions.

There is also an obviously visible conflict between the data minimization principle and the practices of Big Data analysis. Under the Big Data concept, firms do provide a clear incentive to collect and retain as much data as they can for as long as possible. In theory, more data will provide greater knowledge and greater benefit to organisations and society in general. Therefore, enforcing the data minimizations will limit the success of Big Data. According to the GDPR, data minimization could be achieved by pseudonymization (Zarsky, 2017, P.999). On the contrary, one can argue that removing identifiers to achieve pseudonymization could potentially undermine the quality of the results derived, as the data would be purposefully altered.

Given the number of difficulties in carrying out Big Data analysis, there could be a potential migration of local entrepreneurs to other countries where they would have the flexibility to pursue their objectives without obstacles in the use of Big Data. In circumstances where local residents look for foreign companies to obtain their services, protection of privacy could become vulnerable and is like to be compromised.

In the next section, the researcher sets aside GDPR and concentrates on data protection mechanisms in place in individual countries. For the study, the researcher created a separate table for each region.

2.7 Data Protection mechanisms around the world

2.7.1 Asian context

2.7.1.1 South Asia

Table 2.1: Current legal mechanisms in South Asia

Name of the country	**Legal mechanism/s**
India	The Draft Personal Data Protection Bill 2019 (Government of India, 2019)
Pakistan	The Draft Personal Data Protection Bill 2020 (Ministry of information technology & telecommunication, 2020)
Bangladesh	The Digital Security Act 2018 (Government of the People's Republic of Bangladesh, 2020)
Afghanistan	Comprehensive data protection legislation not yet enacted (Greenleaf, 2019, P.1)
Nepal	The Privacy Act 2018 (Nepal Law Commission, 2018)
Sri Lanka	The Draft Personal Data Protection Bill 2019 [Government of Sri Lanka, 2021)
Bhutan	Comprehensive data protection legislation not yet enacted
Maldives	Comprehensive data protection legislation not yet enacted (Greenleaf, 2019, P.1)

2.7.1.2 East Asia

Table 2.2: Current legal mechanisms in East Asia

Name of the country	**Legal mechanism/s**
China	The PRC Cybersecurity Law 2017 (Standing Committee of the National People's Congress, 2016).
Japan	The Act on the Protection of Personal Information of 2003 (Government of Japan, 2003)
Mongolia	The Draft law on Personal Data Protection 2021(er and Advocates, 2021)
Hong Kong	The Personal Data Privacy Ordinance 2012 (Government of Hong Kong, 2013)
Taiwan	The Personal Data Protection Act 2019 (Tseng, 2021)
South Korea	The Personal Information Protection Act 2011 (Wall, 2018)

2.7.1.3 Southeast Asia

Table 2.3: Current legal mechanisms in Southeast Asia

Name of the country	**Legal mechanism/s**
Indonesia	Draft of the Personal Data Protection Act (Yuriutomo, 2020)

Philippines	The Data Privacy Act of 2012 (Republic of the Philippines, 2012)
Vietnam	The Draft Decree on Personal Data Protection 2019 (McKenzie, 2021)
Thailand	The Personal Data Protection Act 2019 (Government of Thailand, 2019)
Myanmar	Comprehensive data protection legislation not yet enacted (Taylor, 2020)
Malaysia	The Personal Data Protection Act 2010 (Government of Malaysia, 2010)
Cambodia	Comprehensive data protection legislation not yet enacted (Cohen, 2020)
Laos	Comprehensive data protection legislation not yet enacted (ZICO law, 2019, P.9)
Brunei	Not enacted comprehensive data protection legislation (ZICO law, 2019, P.9)
Singapore	Personal Data Protection Bill 2012 (Republic of Singapore, 2012) Amended in 2020 (Republic of Singapore, 2020)

2.7.1.4 Central Asia

Table 2.4: Current legal mechanisms in Central Asia

Name of the country	**Legal mechanism/s**
Uzbekistan	**The Law on Personal Data 2019 (Republic of Uzbekistan, 2019)**
Kazakhstan	The Law of the Republic of Kazakhstan No. 94-V 2013 Republic of Kazakhstan, (2013) Ammended in 2020 (Kahiani, 2020)
Tajikistan	The Personal Data Protection Law 2018 (Republic of Tajikistan, 2018)
Kyrgyzstan	The Law on Personal Data 2008 (Republic of Kyrgyzstan, 2008)
Turkmenistan	The Data Protection Law 2017 (Yuldashev, 2020)

2.7.2 African Context

2.7.2.1 Northern Africa

Table 2.5: Current legal mechanisms in Northern Africa

Name of the country	**Legal mechanism/s**
Egypt	The Personal Data Protection Law 2020 (Matouk Bassiouny and Hennawy, 2020)
Algeria	A legal framework for the protection of personal data 2018 (Smart News, 2018)
Sudan	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)
Morocco	The Law No 09-08 (Data Guidance, N.D, Morocco)
Tunisia	The Draft law on the Protection of Personal Data 2018 (Enneifar, 2021)
Libya	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa
South Sudan	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)

2.7.2.2 Western Africa

Table 2.6: Current legal mechanisms in Western Africa

Name of the country	**Legal mechanism/s**
Nigeria	The Nigeria Data Protection Regulation 2019 (National Information Technology Development Agency, N.D)
Ghana	Data Protection Act 2012 (The Republic Of Ghana, N.D)
Burkina Faso	Framework for the Protection of Personal Data in 2004 (Fichet, 2020)
Guinea	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)
Sierra Leon	The National Cybersecurity and Data Protection Strategy 2017-2022 (In progress) (UNIDIR, 2021)
Gambia	The Draft Data Protection and Privacy Policy 2019 (Data Guidance, N.D)
Guinea-Bissau	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)

2.7.2.3 Eastern Africa

Table 2.7: Current legal mechanisms in Eastern Africa

Name of the country	**Legal mechanism/s**
Ethiopia	Draft Personal Data Protection Proclamation published in 2020 (Dube, 2021, P 9)
Tanzania	Comprehensive data protection legislation not yet enacted (Dube, H. 2021, P 9)
Kenya	The Data Protection Act 2019 (Republic Of Kenya, 2019)
Uganda	The Data Protection and Privacy Act 2019 (The Republic of Uganda, 2019)
Mozambique	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)
Madagascar	The Data Protection Law 2014 (Data Guidance, N.D)
Zambia	The Electronic Communications and Transactions Act (Chisenga, 2021)
Somalia	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)
Rwanda	The Data Protection Law 2020 (Mudavanhu, 2021, Rwanda - Data Protection Overview)

Burundi	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)
Mauritius	The Data Protection Act 2017 (Republic of Mauritius, 2017)
Djibouti	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)
Seychelles	The Data Protection Act 2003 (Moller, 2021)

2.7.2.4 Central Africa

Table 2.8: Current legal mechanisms in Central Africa

Name of the country	**Legal mechanism/s**
DR Congo	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)
Cameroon	Comprehensive data protection legislation not yet enacted (Deloitte, 2017, Privacy is Paramount- Personal Data Protection in Africa)

Congo	The Personal Data Protection Law 2019 Data Guidance, 2020, Republic of Congo: Personal Data Protection Law published in Official Journal)

2.7.2.5 Southern Africa

Table 2.9: Current legal mechanisms in Southern Africa

Name of the country	**Legal mechanism/s**
South Africa	The Protection of Personal Information Act 2020 (Republic of South Africa, N.D)
Namibia	Comprehensive data protection legislation not yet enacted (Gervasius, N.D, P. 5)
Botswana	The Data Protection Act 2018 (Government of Bostwana, 2018)
Lesotho	The Data Protection Act 2013 (Mudavanhu, 2021, Lesotho - Data Protection Overview)
Zimbabwe	Cyber security and data protection bill, 2019 (Republic of Zimbabwe, N.D)

2.7.3 Middle Eastern context

Table 2.10: Current legal mechanisms in Middle East

Name of the country	**Legal mechanism/s**
Turkey	The Law on the Protection of Personal Data 2016 (Government of Turkey, N.D)
Iraq	Comprehensive data protection legislation not yet enacted (Dabbagh, 2021)
Saudi Arabia	Comprehensive data protection legislation not yet enacted (Wilkinson, 2020)
Yemen	Comprehensive data protection legislation not yet enacted (Data Guidance, N.D, Yemen)
Jordan	Comprehensive data protection legislation not yet enacted (Data Guidance, N.D, Jordan)
United Arab Emirates	Comprehensive data protection legislation not yet enacted (Rizvi, 2020)
Israel	Protection of Privacy Law, 5741-1981 (Shiv, 2020)
Lebanon	The Electronic Transactions and Personal Data law 2018 (Data Guidance, N.D, Lebanon)

Oman	Comprehensive data protection legislation not yet enacted (Data Guidance, 2020, Oman: Latest developments in data protection and cybersecurity
Kuwait	Comprehensive data protection legislation not yet enacted (Data Guidance, N.D, Kuwait)
Qatar	The Data Protection Law 2016 (DLA Piper, 2021)
Bahrain	The Personal Data Protection Law 2018 (Alkoofi, 2021)
Iran	The Draft Personal Data Protection Act (Data Guidance, N.D, Iran)

2.7.4 American context

2.7.4.1 North and Central America

Table 2.11: Current legal mechanisms in North and Central America

Name of the country	**Legal mechanism/s**
Belize	The Draft Data protection bill 2021 (Government of Belize, 2021)
Elsalverdo	The Personal Data protection Law 2021 (One Trust Data Guidance, N.D)
Guatemala	Comprehensive data protection legislation not yet enacted (Data Guidance, 2019, Guatemala: Data protection thus far)
Mexico	The Federal Law on the Protection of Personal Data (Arceo, and Alcocer, N.D)
Nicaragua	The Personal Data Protection 2012 (Rizo, 2021)
Panama	The Data Protection Law 2019 (Lorenzo, 2021)

2.7.4.2 South America

Table 2.12: Current legal mechanisms in South America

Name of the country	**Legal mechanism/s**
Argentina	The Personal Data Protection ACT 2000 (Government of Argentina, 2000)
Bolivia	The Bill of Personal Data Protection (Sykes, 2020)
Brazil	The Brazilian General Data Protection Law 2018 (Deloitte, N.D)
Chile	The Constitution of the Republic of Chile, Art. 19 -4 (DLA Piper, 2021)
Ecuador	The Organic Law on the Protection of Personal Data 2021 (Data Guidance, N.D)
Guyana	The Draft Data Privacy Law 2020 (Morgan, 2021)
Suriname	The Data Protection Law 2018 (Balboni, 2018)
Uruguay	The Data Protection Act Law No.18.331, 2008 (Nougrères, 2021)
Venezuela	Comprehensive data protection legislation not yet enacted (Salazar, 2021)

2.7.5 Caribbean context

Table 2.13: Current legal mechanisms in Caribbean

Name of the country	**Legal mechanism/s**
Bahamas	Data Protection Act 2003 (Morgan, 2021)
Cayman Islands	The Data Protection Law 2017 (Morgan, 2021)
Dominican Republic	Comprehensive data protection legislation not yet enacted (Morgan, 2021)
Haiti	Comprehensive data protection legislation not yet enacted (Data Guidance, N.D, Haiti)
Jamaica	The Data Protection Act 2020 (Morgan, 2021)

2.7.6 European context

Table 2.14: Current legal mechanisms in Europe

Name of the country		**Legal mechanism/s**
Austria		The Data Protection Act 2018 (Marko, N.D)
Belgium		The Data Protection Act 2018 (Schrijver, and Fraeyenhoven, 2020)

Bulgaria		The Protection of Personal Data Act 2019 (Data Guidance, N.D, Bulgaria)
Croatia		Act on the implementation of the General Data Protection Regulation (Croatian Data Protection Agency, N.D)
Cyprus		The Provisions of the GDPR into local law 2018 (Ktenas, 2021)
Denmark		The Danish Act on Data Protection 2018 (Government of Denmark, 2018)
Estonia		The Personal Data Protection Act 2018 (Kukk, 2021)
Finland		The Data Protection Act of Finland 2019 (Ministry of Justice, N.D)
France		The General Data Protection Regulation 2018 (Saarinen, at el., 2019)
Germany		The German Federal Data Protection Act 2018 (Deloitte, N.D, The new German Privacy Act)
Greece		The Greek Law 4624/2019 (Karageorgiou, 2020)
Hungary		The Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Amended in 2019) (Orban, 2020)

Italy		The Italian data protection 2018 (Puddu, 2020)
Ireland		The Irish Data Protection Act 2018 (The electronic Irish Statute Book (eISB), N.D)
Latvia		The Personal Data Processing Law 2018 (Burkevics, N.D)
Lithuania		The Law on Legal Protection of Personal Data 2018 (Gumbis, 2020)
Luxembourg		The Law on the organization of the National Data Protection Commission (CNPD) and the general data protection framework 2018 (Government of Luxemburg, 2018)
Malta		The Data Protection Act 2018 (Zammit, 2021)
Netherlands		The Dutch GDPR Implementation Act (Gerlach, 2020)
Poland		The Personal Data Protection Act 2018 (Mencel, 2020)
Portugal		The Portuguese Data Protection Law 2019 (Santos, 2020)
Romania		The Law no. 190/2018 (Lazar, N.D)

Slovakia		The Slovak Data Protection Act 2018 (Mysicka, 2021)
Slovenia		The Draft Data Protection Act is still in the legislative process (Data Guidance, N.D, Slovenia)
Spain		The Spanish Data Protection and Digital Rights Act 2018 (Burgos and Pehlivan, 2020)
Sweden		The Data Protection Act 2018 (Government of Sweden, 2018)
Switzerland		The Swiss Federal Data Protection Act, 2020 (Rosenthal, 2020)

In the section above, the researcher outlined a summary of data protection mechanisms in each country. An interesting observation is the data protection mechanisms developed by most countries show a close alignment with GDPR, but they are not identical, yet they meet the criteria for providing an adequate level of data protection (See table 2.1-2.14). It appears that before doing the amendments, the countries had revisited their data protection mechanisms that were already in place before GDPR was established. The researcher noted the enthusiasm of the developing countries and believed their commitment to working together is the right way to go about developing a global level data protection mechanism. In the next section, the researcher evaluates the 'Organisational preparedness' for addressing the issues associated with protecting personal data.

2.8 Organisational cooperation

State-level measures are taken by individual countries to address protection of personal data, within their own capabilities but every developing country cannot match successes of developed countries. Therefore, it is necessary for developing countries to have close co-operation with developed countries in addressing the privacy of individuals.

2.8.1 Nigeria’s Economic and Financial Crimes Commission (EFCC)

Cyber threats have gone beyond boundaries, and even the responsibility to protect citizens and their territory has become a priority for most international organisations. For instance, government agencies such as Nigeria’s Economic and Financial Crimes Commission (EFCC), supranational institutions such as the African Union Commission (AUC), organisations are also strengthening technological and behavioural defence mechanisms such as employee compliance, effective decision-making (Pfleeger and Caputo, 2012) to resist cybercrimes.

2.8.2 The Council of Europe’s Convention on Cybercrime (the Budapest Convention)

The Budapest Convention stands as the only binding international instrument offering guidelines for developing comprehensive national legislation against cybercrime, also as a framework for international cooperation between the parties to this treaty (Council of Europe, N.D). The treaty was established in 2004 (Clough, 2014, P.700), and remains open to non-members such as Australia, Japan, Dominican Republic, Mauritius, Panama and the US, and they have ratified the convention (Clough, 2014, P.724). Also, countries such as Argentina, Pakistan, the Philippines, Egypt, Botswana, and Nigeria have made use of the Convention as a model in drafting parts of their legislation on Cybercrime (Clough, 2014, P.732).

Incidentally, most cyber-attacks are known to have been launched by foreign countries, such as China, Iran, North Korea, and Russia and China (Ward, 2019), and its allies have not joined expressing disapproval of the Convention. However, China and Russia have supported an alternative new cybercrime treaty, but the US and its European allies have rejected it (Peters, 2019). This is a prime example of a negative approach to building a global mechanism, and it is therefore necessary to identify common ground to reach a consensus-based approach.

2.8.3 The North Atlantic Treaty Organization (NATO)

NATO is also a leading organisation, and tackling cyber menace remains a key priority for them. In 2002, NATO adopted a cyber defence programme and created a NATO Computer Incident Response Capability (NCIRC) to prevent, detect and respond to cyber incidents (Healey and Jordan, 2014). NATO with the approval of the 'NATO Cyber Defence Policy' in 2008, it integrated cyber defence into NATO's defence planning process for the purpose of securing its own networks and also assisting allies reduce vulnerabilities in their critical infrastructure (Healey and Jordan, 2014,). In particular, NATO leaders have endorsed the possibility of invoking Article-5 following a cyber-attack, thus equating it with an armed attack in certain situations. Nevertheless, ambiguity persists about the exact conditions in which such a response would be required and the nature of that response, whether military or cyber (Pernik, 2014).

2.8.4 The UN

The UN is also actively focusing on cyber threats. This is a significant development in a meaningful international collaboration that is essential to encourage countries to join together for capacity sharing. In support of this approach, China, Russia, Tajikistan, and Uzbekistan had submitted a draft international code of conduct for information security to the U.N. Secretary-General, emphasising the necessity of maintaining international stability and security (UN, 2017). In another move, to emphasise the need for collective action, at the twelfth UN Congress on Crime Prevention and Criminal Justice, Latin America and Caribbean, Western Asia, Asia and the Pacific, and Africa called for the development of an international convention on cybercrime (International Telecommunication Union, 2014). The Personal Data Protection and Privacy Principles was adopted by the High-Level Committee on Management at the 36th Meeting in 2018 (UN High-Level Committee on Management, 2018). These principles set out a basic framework for processing personal data by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities (UN High-Level Committee on Management, 2018). These Principles apply to personal data, processed in any manner, and can also be used as a benchmark for processing non-personal data in a sensitive context (UN High-Level Committee on Management, 2018).

2.8.4.1 The United Nations Privacy Policy Group (UN PPG)

The UN Privacy Policy Group (UN PPG) is an inter-agency group convened in 2016, and it is co-chaired by UN Global Pulse and the UN Office of Information and

Communications Technology (OICT) (UN System Chief Executives Board for Coordination, N.D). The UN PPG's primary objectives are to develop dialogue on key issues related to data privacy and protection within the UN system, unite existing efforts on data privacy and protection, and develop a practical UN System-wide framework on data privacy and data protection (UN System Chief Executives Board for Coordination, N.D). During the COVID-19 pandemic, the group has played an active role in supporting privacy protection, and the use of data and technology. To this end, the group has highlighted the importance of protecting the rights of all the people involved in data collection, processing, and their use in tackling public health emergencies during pandemics (The UN privacy policy group, 2020).

2.8.4.2 The International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) of the UN is a specialised agency with responsibility for information and communication technologies related issue (ITU, N.D, About International Telecommunication Union). It launched the global security agenda and formed a group of eminent experts to appraise the issues and develop proposals for long term strategies to promote cyber security and data protection (ITU, 2021, Countries ramp up cybersecurity strategies).

2.8.5 The Organisation for Economic Co-operation and Development (OECD)

In the wake of the terrorist attacks of 11 September 2001, not only UN but also Organisation for Economic Co-operation and Development (OECD) developed a series of guidelines designed to counter cyber-terrorism, computer viruses, 'hacking' and related threats. The OECD has been active in the area of cyber-crime and online security, especially with regard to encryption technology, evaluating the balance between law enforcement and privacy concerns, and the means by which member states could coordinate encryption policy (Broadhurst and Grabosky, 2005).

2.8.6 The Asia-Pacific Economic Cooperation (APEC)

The Asia-Pacific Economic Cooperation (APEC) also has identified cybercrime as an important field of activity, and APEC leaders have called for closer cooperation among officials involved in the fight against cybercrime. In 2002, APEC leaders released a statement on fighting terrorism and promoting growth to enact comprehensive laws relating to cybercrime, data protection and develop national cyber-crime investigating capabilities (International Telecommunication Union. 2014). Nevertheless, in the absence of any provision for a legal framework on cyber-crime, APEC has referred to international standards such as the Budapest Convention on Cybercrime (International Telecommunication Union. 2014).

2.8.7 The African Union

The African Union Commission has also decided to join with the UN Economic Commission for Africa with the intention of developing a legal framework for African countries that addresses issues like electronic transactions, cyber-security, and data protection (International Telecommunication Union. 2014). In 2011 the African Union presented the draft on the establishment of a credible legal framework for cyber security in Africa with the intention to strengthen existing legislation in member states regarding information and communication technologies. One positive step was the mandate that was not limited to cybercrime but also included other information society issues such as data protection and electronic transactions (International Telecommunication Union. 2014).

2.8.7.1 The African Union Commission (AUC)

The African Union Commission (AUC) also adopted the Malabo Convention on cyber security and personal data protection to provide fundamental principles and guidelines to ensure the effective protection of personal data (Aston, 2018). Several other African intergovernmental organizations also have taken steps to enhance their capabilities and legislature by developing legal frameworks for cyber security. Most significantly, at the sub-regional level, the Economic Community of West African States (ECOWAS) has adopted a Directive on Cybercrime, and model laws have been adopted by the Common Market for Eastern and Southern Africa (COMESA) and the Southern African Development Community (SADC) (Orji, 2018).

The formation of a multilateral treaty is found to be not feasible without an acceptable governance regime, and in such situations, the development of norms to govern behaviour in the cyber domain may be the best and the only option. The proposed rule-of-norms advocacy by the US prohibiting intellectual property theft and other criminal actions in the cyber domain, including by supporting broad adherence to the Budapest Convention, can be seen as a good example (Sabbah, 2018). Such norms could sufficiently fulfil same purposes as the treaty, including coordinating state behaviour, promoting stability and order in the international system, and decreasing the risk of unintended conflict.

After discussing the national level data protection mechanisms in each country, and the organisational preparedness to protect personal data, the researcher narrowed the topic down to the South Asian Region. In the next section, the researcher focuses the discussion on the data protection mechanisms in the South Asian region.

2.9 Actions taken by countries in the South Asian region to protect personal data

The eight states of the South Asian region, India, Sri Lanka, Bangladesh, Pakistan, Bhutan, Nepal, Maldives, and Afghanistan, make up the SAARC (South Asian Area of Regional Cooperation) (Greenleaf, 2017, P.1). There is a strong possibility that South Asia will emerge with a law that matches existing international standards, but the indicators are some countries are well advanced whilst some are falling behind. However, having all that said, the development of important privacy protection ethics in South Asia is falling behind, and, at this moment in time, there is no sign of a SAARC regional initiative emerging to achieve a successful outcome (Greenleaf, 2019, P.1-7).

2.9.1 The Islamic Republic of Pakistan

In 2005, the Pakistan Ministry of Information Technology circulated a draft law on data protection, but it was not presented to the parliament (OneTrust Technology, 2019) (Privacy International and the Digital Rights Foundation, 2019). It appeared the legislation had been drafted primarily to meet the needs of the country's software industry for the purpose of conducting international business rather than to address actual privacy issues (Privacy International and the Digital Rights Foundation, 2019). Therefore, this draft legislation seemed to have been a half-baked red herring and fallen short of its applicability to processing of personal or corporate data by federal, provincial, or local government institutions (Privacy International and the Digital Rights Foundation, 2019).

The Personal Data Protection Bill 2020 was introduced by the Ministry of Information Technology and Telecommunications (MOITT) later it has been tabled before the National Assembly or presented to the Senate for its approval (Rehman, 2020). The Bill encompasses many provisions that are in line with the international data protection regulatory framework. The legal obligations for data controllers and processors are broadly in par with other international laws, including GDPR, and they encapsulate the requirements to provide notice of consent, retention, disclosure, breach notification, and cross-border transfers (OneTrust Company News, 2018). Similarly, the rights of individuals are broadly aligned with those in other jurisdictions and include the right to access and to amend data, to withdraw consent, request for erasure of data, and to request a data controller to cease processing their data (OneTrust Company News, 2018). However, there are certain aspects of the Bill that remain out of alignment with widely accepted privacy norms, including a potential data localization requirement (IFEX, 2020). One notable element in the Bill is the omission of the requirement to appoint a Data Protection Officer; however, the power of personal data protection authority of Pakistan bestow power to the Data Protection Officer (DLA Piper, 2020) (The global legal group, 2020).

The Bill states that a data controller shall not process personal data, including sensitive personal data of a data subject, unless the data subject has given consent to the processing of the personal data (Rehman, 2020). The bill contains provisions allowing a data subject to give notice in writing to withdraw his/her consent to the processing of personal data, and the data controller, upon receiving such notice, will have to stop the processing of personal data (Rehman, 2020). There are exceptions to the rule in cases of public interest, freedom of expression, and the security of the state as and when it becomes paramount. The bill also specifies that critical personal data shall only be processed in a server or data centre located in Pakistan, which indicates that Pakistan is to some extent shadowing the data localisation policies (Panakal, 2020).

The transfer of personal data collated by banks, insurance companies, hospitals, defence establishments and other ‘sensitive’ institutions to any individual or body is conditional on obtaining consent from the data subject (DLA Piper, 2020). Also, the bill categorically stipulates that the country receiving transferred data must have in place personal data protection provisions that are at least equivalent to those provided in the Bill, and the data so transferred should be processed in accordance with the Bill where applicable (DLA Piper, 2020).

The Bill provides guidance and follows up action in the event of a personal data breach. The data controller shall, without undue delay where reasonably possible, and within 72 hours of a reported personal data breach, notify the relevant authority except where the personal data breach is unlikely to result in a risk to the freedom and rights of the data subject (Government of Pakistan, 2018). The notification should be in writing, and the incident report should include the nature of the personal data breach, name and contact details of the Data Protection Officer or other contact points where more information can be obtained, likely consequences of the personal data breach, and the measures in placed or proposed to be adopted by the data controller to address the personal data breach (Government of Pakistan, 2018). The Bill states that anyone found to be in violation of any of the provisions of the Bill, such as processing, disseminating, or disclosing personal data shall be prosecuted and incur a fine of up to PKR 15 million (Rehman, 2020). For any subsequent offences, unlawful processing of personal data and sensitive data, the threshold of fines would rise to as high as PKR 25 million (Rehman, 2020). Furthermore, the Bill states that anyone failing to adopt the security measures that are necessary to ensure data security and failing to comply with the orders of the personal data protection authority of Pakistan, shall punish and incur a fine up to PKR 5 million (Rehman, 2020).

Table 2.15: Draft Data Protection Law of Pakistan compared with GDPR

General Data Protection Regulation (GDPR)	**The Draft Personal Data Protection Bill of Pakistan (2020)**
The rights of the individuals are broadly aligned (Eur-Lex, 2016).	Individuals' rights are broadly aligned (OneTrust Company News, 2018).
There is a requirement to appoint a Data Protection Officer (Eur-Lex, 2016).	The appointment of a Data Protection Officer is not a requirement (DLA Piper, 2020) (The global legal group, 2020).
The data controller shall not process personal data without obtaining consent from the data subject (Eur-Lex, 2016).	Processing personal data by the data controller is prohibited without obtaining consent from the data subject (Rehman, 2020).
Data transfer to a third country with 'adequate' restrictions will be comparable	The Bill categorically stipulates that transferred data recipient country has to have personal data protection

with data transmission within the EU (Eur-Lex, 2016).	provisions that are at least in par with provisions in the Bill (DLA Piper, 2020)
All organisations are duty-bound to report specific personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible (Eur-Lex, 2016).	The data controller should notify the data breaches to the relevant authority within 72 hours of the known incident, except when breaches are unlikely to affect the freedom and rights of the data subject (Government of Pakistan, 2018).
A data breach report should include a description of the nature of the personal data breach, name, and contact details of the data protection officer (if there is one in the organisation) or other contact points where more information can be obtained; description of the measures taken or proposed to take as consequences of a breach (Eur-Lex, 2016).	The notification should be in writing; the incident report should include the nature of the personal data breach, name and contact details of the Data Protection Officer or other contact points where more information can be obtained, likely consequences of the personal data breach, and the measures in place, or proposed measured to be adopted by the data controller to address the (personal data) breach (Government of Pakistan, 2018).
A penalty of up to 20 million euros or 4 percent of global annual turnover, whichever is higher, will be levied for failure to adhere to core principles of data processing, infringement of personal rights, transfer of personal data (Eur-Lex, 2016). A penalty of up to 10 million euros or 2 percent of the global annual turnover,	Anyone found to be in violation of any of the provisions of the Bill, such as processing, disseminating, or disclosing personal data, are liable for prosecution and will incur a fine of up to PKR 15 million (Rehman, 2020). For any subsequent offences, unlawful processing of personal data and sensitive data, the threshold of fines

whichever is higher, will be levied for failure to comply with technical and organisational requirements (Eur-Lex, 2016).	would rise to as high as PKR 25 million (Rehman, 2020). Failure to adopt stipulated data security measures essential for ensuring data security and non-compliance with instructions issued by the personal data protection authority of Pakistan will become liable, and a fine of up to PKR 5 million will be levied (Rehman, 2020).

The summary outlined in the table (See table 2.15) suggest that Pakistan provides an adequate level of data protection, in line with GDPR. However, the Bill has discrepancies in terms of the need to appoint a Data Protection Officer and liability in the form of fines.

2.9.2 The Republic of India

The Supreme Court of India has recognised informational privacy, also the right to privacy as a fundamental element under the Constitution and, has underscored the right to life and personal liberty (Panday, 2017). India is also a signatory to international declarations and conventions such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which recognises the right to privacy (Talwar Thakore & Associates, 2020).

The Information Technology Act 2000 governs the protection of personal information, specifically electronic data and transactions (Deloitte, 2019, The Asia Pacific Privacy Guide). Since 2011, various replicates of the Privacy Bill have been released, and the Data Privacy Bill 2017 is the latest. The draft of the Personal Data Protection Bill 2018 was intended to replace the Data Privacy Bill 2017 and still awaiting approval (Subramaniam and Das, 2020). As cited, the Indian Parliament is expected to vote on the Personal Data Protection Bill of 2019 during the 2020 budget session, and on parliamentary approval, India wanted to join the European Union, becoming the third-largest entity to implement formal legal frameworks governing the use and share of personal data (Cloen, 2020). The same criteria and standards would apply to all enterprises, including technology companies, e-commerce platforms, real-estate firms and brokers, banking business correspondents, auto dealers, hotels, and restaurants (Burman, 2020).

The Data Protection Bill serve to regulate the use of personal data collected, disclosed, shared, or processed in India, or associated businesses within India, conditional cross-border transfers requiring data fiduciaries to store data in India. The bill also sets out the obligations that would bind all entities processing data to adhere to a host of requirements such as data minimization, notice-and-consent, transparency, security safeguards and localization (Burman, 2020). Also, mandatory data breach notification, obtaining prior consent to collect data, and individual privacy rights remain stringent requirements of the Bill (Deloitte, 2019, The Asia Pacific Privacy Guide). These are clearly stipulated as obtaining consent in advance and in writing from the data subject specifying the purpose for which the data would be used before the collection of the data (Subramaniam and Das, 2020). There is also a provision for collecting sensitive information for lawful purposes connected with a function or purpose of the corporate entity on a necessity basis whilst ensuring that the information so collected was used for the intended purposes only (Subramaniam and Das, 2020). There is no specific time frame set for the retention of sensitive personal information (Subramaniam and Das, 2020), but the retention period should not be longer than necessary.

There are also conditional exceptions included in the PDPB, specifically on the processing of personal data for the purposes of national security, law enforcement, in legal proceedings, delivering medical or health services in emergencies situations and epidemics, providing services during disasters and breakdown of public order, research and archiving purposes or where processing is by small entities (Burman, 2020). PDPB is also applicable to entities outside the territories of India to the extent that the central government may regulate any cross-border data transfers outwards from India. The government has powers to permit such transfers subjected to the provision of an adequate level of protection of personal data, adherence to laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction (Deloitte. 2019, India Draft Personal Data Protection Bill, 2018 and EU General Data Protection Regulation A comparative view).

In the current legal framework, there is no specific level of penalties set for data security breaches, and the appointment or the role of a Data Protection Officer is not mentioned in the Bill. However, should the PDPB comes into force, the data fiduciary would be required to appoint a Data Protection Officer and set out his functional roles as specified in the PDPB, also the specific functions for the officer as deemed necessary (Walia, and Chakraborty, 2020). The failure to take appropriate action promptly in response to a data security breach, the data fiduciary shall be liable to a penalty which may extend up to either two percent of its total worldwide turnover in the preceding financial year or Fifty Million Indian Rupees (INR 50 million) whichever is the higher necessary (Walia, and Chakraborty, 2020). The same will apply in the case of a Data Protection Officer failing to fulfil his/her responsibilities necessary (Walia, and Chakraborty, 2020).

Table 2.16: Draft Personal Data Protection Bill of India compared with GDPR

General Data Protection Regulation (GDPR)	**Indian Draft Personal Data Protection Bill of India (2019)**
The lawfulness of processing depends on the necessity for processing, and the sensitive personal information retention period should not be longer than necessary (Eur-Lex, 2016).	There is also a provision for collecting sensitive information for lawful purposes, ensuring the information so collected was used for the intended purposes only (Subramaniam and Das, 2020). There is no pre-set timeline for retention of sensitive personal information (Subramaniam and Das, 2020), but the retention period should not be longer than necessary.
The data controller shall not process personal data without obtaining prior consent from the data subject (Eur-Lex, 2016).	Data controllers should comply with the requirement to obtain consent form the data subject prior to processing personal data (Deloitte, 2019, The Asia Pacific Privacy Guide).

The transfers to an ‘adequate’ third country will be comparable to a transmission of data within the EU (Eur-Lex, 2016).	Any cross-border data transfers from India outwards may be regulated by the central government, and the government has powers to permit such transfers subjected to the provisions of an adequate level of protection of personal data (Deloitte. 2019, India Draft Personal Data Protection Bill, 2018 and EU General Data Protection Regulation A comparative view).
There is a requirement to appoint a Data Protection Officer (Eur-Lex, 2016).	Appointing a Data Protection Officer is a requirement (Walia, and Chakraborty, 2020).
GDPR makes it the duty of all organisations to report certain types of personal data breaches to the appropriate supervisory authority within 72 hours of becoming aware of the breach, where feasible (Eur-Lex, 2016).	Data breach notification is mandatory (Walia, and Chakraborty, 2020).
Failure to adhere to core principles of data processing, infringement of personal rights, transfer of personal data: Penalties of up to 20 million euro or 4 percent of global annual turnover, whichever is higher (Eur-Lex, 2016). Failure to comply with technical and organisational requirements: Penalties of up to 10 million euro or 2 percent of the	Failures of the organisation to protect personal data will make it liable and incur a penalty of up to two percent (or more) of its total worldwide turnover in the preceding financial year, or Fifty Million Indian Rupees (INR 50 million) whichever is higher (Walia, and Chakraborty, 2020). The same will be applicable if the data protection officer

global annual turnover, whichever is higher (Eur-Lex, 2016).	fails to fulfil his/her responsibilities (Walia, and Chakraborty, 2020).

The table above (See table 2.16) infers that the Draft Personal Data Protection bill contains guidelines very similar to GDPR except for the level fines specified in the bill.

2.9.3 People's Republic of Bangladesh

It is only recently legal protection for infringement on personal data has become available in Bangladesh (Moniruzzaman, 2019), and prior to that, privacy or data protection specific statute was non-existent in the country. Also, data privacy and underlying protection rights and requirements appear to be new concepts. In many instances, the country appears to have been on the verge of facing major threats to privacy and personal data leakage (Hossain et al, 2018). Therefore, in the absence of a legal framework to curb future challenges of protecting citizens' privacy, the need to develop data protection laws became an imperative priority for the country.

The Information and Communication Technology Act of 2006 (The technology Act) and Digital Security Act addresses issues relating to wrongful disclosure, misuse of personal data, and violation of contractual terms in respect of personal data (Doulah, 2020). The Information and Communication Technology (ICT) Act of 2006 has provisions to bring prosecutions against the perpetrators for unauthorised intrusions and access to personal data, but the inherent loopholes allow the offenders to evade prosecution against crimes committed anonymously (Hossain et al, 2018). Under this act, those responsible for committing an offence of disclosing confidential and private information could be liable for punitive imprisonments up to two years, with or without a fine extendable up to BDT 200,000 (Doulah, 2020).

According to the Constitution of the People’s Republic of Bangladesh, every citizen shall have the right to privacy in correspondence and other means of communication (Molla and Nahar, N.D). In that respect, the basic framework for data protection and privacy sets out the rights of privacy granted under the Constitution of Bangladesh, alongside the

Information Communication Technology Act 2006 and the newly enacted Digital Security Act 2018 (Doulah, 2020).

The enactment of the Digital Security Act of 2018 has enabled Bangladesh to take a step forward in the right direction into the data or information protection regime. Its purpose is primarily to promote confidentiality, integrity, and availability of public and private information systems and networks and also to protect the rights of individuals and privacy, economic interests, and security in cyberspace (Mishbah, 2019). This act explicitly makes it a requirement to obtain consent or authorisation from data subjects before collecting, storing, and processing personal information (Mishbah, 2019). However, Bangladesh recognises that implementation of GDPR mandated requirements for Data Protection Officers, data protection impact assessments and audits, breach notifications and record keeping would prove to be difficult and costly for many small companies in Bangladesh (Goswami, 2021). The rules specify that anyone attempting to illegally access a computer or digital system and to interfere by making changes, transferring any data or information owned by any organisation, will be legally liable for committing a punishable offence, in the form of imprisonment not exceeding five years and/or a fine not exceeding BDT 1 million (Doulah, 2020).

Table 2.17: Digital Security Act of Bangladesh compared with GDPR

General Data Protection Regulation (GDPR)	**Digital Security Act of Bangladesh (2018)**
GDPR regulation to obtain prior consent from the data subject applies in the processing of personal data (Eur-Lex, 2016).	The data controller shall not process personal data without obtaining consent from the data subject (Mishbah, 2019).
There is a regulatory requirement to appoint a Data Protection Officer (Eur-Lex, 2016).	The requirement to appoint a Data protection officer is not indicated (Goswami, 2021).

All organisations are duty-bound to report specific personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible (Eur-Lex, 2016).	No reference was made to this requirement for data breach notification (Goswami, 2021).

In Bangladesh, the proposed Digital Security Act sets out provisions very similar to GDPR (See table 2.17). However, despite the close alignment, visible differences exist in terms of the requirement to appoint a data protection officer and a data breach notification.

2.9.4 Bhutan

The privacy issues in Bhutan have not been sufficiently articulated in the literature, policies or in guidelines. However, the reports suggest that seven of the ten second-generation principles in the 1995 EU Data Protection Directive have been included in the Information, Communications and Media Act of Bhutan, which came into force in 2018, but with limited coverage on privacy and privacy law (Greenleaf, 2019, P.5). Also, the Social Media Strategy and Guideline Policy of Bhutan (2011), the Information and Communications Technology Policy and Strategies (2004), and the Bhutan e-Government Master Plan (2014) have limited emphasis on privacy issues (Author unknown, 2015). Thus, these acts are considered only moderately strong for the Asian region. As such, non-EU businesses are losing European Partnership contracts because adequate protection of data in compliance with GDPR could not be guaranteed. Yet not all businesses or government organisations in Bhutan had been affected by GDPR simply because either the businesses in Bhutan do not have commercial links with European companies, or they do not require access to the personal data of EU citizens.

2.9.5 The Federal Democratic Republic of Nepal

The right to privacy as a fundamental right featured for the first time in the 1990 constitution of the Kingdom of Nepal, and so did the right to information, and later, the right to privacy was retained in the 2007 interim constitution (Pradhan, 2014). However, there was no reference made to the authority of the state to receive violations of privacy rights complaints, but the public had the freedom to submit such reports to the National Human Rights Commission (NHRC), with the option to take legal action against violation of privacy rights, in the Nepalese courts (Pradhan, 2014).

Nepal became the Federal Republic in 2015 with the promulgation of the new constitution, and substantial changes were made to the legal system of the country (National Forum of Parliamentarians on Population and Development, 2020, P.5). Key element is the right to privacy and protection of information as a fundamental right stipulated in the Article 28 of the Constitution, along with that constituted the criminal code and the Individual Privacy Act 2018 (Pradhan, 2020). The Criminal Code has a separate chapter on laws covering violations of privacy, breaches of confidentiality, taking and editing photos of a person without consent, and breaches of private information in electronic media considered criminal acts (Neupane and Karki, 2019)

Nepal enacted the Privacy Act of 2018 (Neupane Law Associates, 2019), and public entities operating in Nepal were obliged to pay careful attention to many provisions in the Act. For an example, personal data collected by corporate entities might only be used for the purpose for which such data was collected, and collection and disclosure were prohibited without consent (Neupane Law Associates, 2019). That is an endorsement of the need to obtain consent before the collection of private information and the restrictions on collecting data and using it only for the purposes for which it was collected.

These obligatory requirements generate more responsibility on businesses as commercial activities conducted online needs to collect the personal data of the users and restrict data sharing with third parties. However, in terms of collecting or using personal information belonging to a Nepalese resident from outside the territory of Nepal or involving an offshore entity within Nepal, the enforcement of the Act appears vague (Upreti, 2018). Therefore, the purpose for collecting data and information, and the intended use should be revealed with clarity. If the intention behind information gathering is for a particular need, academic study, specific research objectives, public opinion, then the nature of collection, the purpose for the collection, methodology and mode of information processing, along with assurance not to breach privacy of individual information must be presented.

The act requires public authorities or corporate bodies to obtain consent from the individual/s before disclosing personal information collected, stored, or retained by them (Pradhan, 2020). The violation of the Act is a criminal offence, and legal action commensurate with the offence may be taken by either an individual or the State, and proven liable, the offender would incur imprisonment of up to 3 years or a fine of up to NPR 30,000 or both. Also, the offender could be liable to pay compensation to the affected party (victim) for the violation of the provisions of the Act (Pradhan, 2020).

Table 2.18: The Privacy Act of Nepal compared with GDPR

General Data Protection Regulation (GDPR)	**The Privacy Act of Nepal (2018)**
The legality of necessary processing depends on the justification for doing so (Eur-Lex, 2016).	Organisations collecting personal data must use it for intended purposes only; if on a necessary basis, it must be justified (Neupane Law Associates, 2019)
The data controller shall not process personal data without obtaining consent from the data subject (Eur-Lex, 2016).	The data controller should obtain consent from the data subject prior to processing personal data (Neupane Law Associates, 2019).
The failure to comply with (adhere to) core principles of data processing, infringement of privacy rights, the transfer of personal data will incur penalties of up to 20 million euro, or 4 percent of global annual turnover, whichever is higher (Eur-Lex, 2016).	The violation of the Act constitutes a criminal offence, which if proven in a court of law and liable, imprisonment of up to 3 years or a fine of up to NPR 30,000 or both will be levied on the offender (Pradhan, 2020).

Non-compliance with, or failure to adhere to technical and organisational requirements: penalties of up to 10 million euro or 2 percent of the global annual turnover, whichever is higher (Eur-Lex, 2016).	Also, the offender could be liable for compensation payments to the affected party (victim) and for violating the provisions of the Act (Pradhan, 2020).

The Privacy Act, however, has failed to address the shortcomings and important aspects of it. The existing definition does limit wider interpretation of 'personal data.' Another Important shortcoming is that the Privacy Act does not define or specify some of the vital concepts of data protection such as 'controller' and 'processor.' This will make data management difficult and, in practice, will hamper legal enforcement of punitive action against breaches in Nepal.

2.9.6 The Islamic Republic of Afghanistan

The use of information and communication technologies in Afghanistan has been growing rapidly (The World Bank, 2013), and the popularity of modern technology has made its way into all aspects of the citizens making a difference to their way of life. In the absence of specific laws or regulations to manage data protection in Afghanistan (Kraemer, 2020), it is important to put in place legal frameworks that will safeguard private and enterprise data flowing through the ICT based infrastructures.

The Constitution of Afghanistan guarantees the right of confidentiality and privacy to its citizens using a wide spectrum of communications systems (Kraemer, 2020). It provides freedom and confidentiality of correspondence between individuals by way of a letter, telephone, telegraph, as well as other means (Kraemer, 2020). However, there is also a need to develop regulations to implement the privacy Laws associated with cyberspace.

2.9.7 the Republic of Maldives

The criteria for data protection in the Maldives fall under the right to privacy, and it was embedded in the 2008 Constitution of the Republic of the Maldives and the Penal code of the state (Ameen, 2020). The penal code prohibits obtaining private information or highly secured information without having the license or authority to do so, and disclosure of any such information to a third party (Ameen, 2020) (Robinson, 2006, P.150).

In 2016, the Ministry of Economic Development of the Government of Maldives announced the drafting of a new data protection bill and was circulated to the public, but it has not yet become law (Ameen, 2020). The purpose of the act was to promote small and medium enterprises, encourage e-commerce, and establish procedures to store, manage, and protect the confidential information of customers (Sun Media Group, 2016). The apparent shortcoming of the act was the absence of one important element, which is the provision to punish non-compliance but has made allowance for everyone the use of discretion to comply with the act (Sun Media Group, 2016). The main beneficiary of the act is identified as the commercial sector as they need an efficient system to manage, use and store confidential information in accordance with international standards and thereby boost customer confidence in the enterprises (Sun Media Group, 2016).

This analysis about the South Asia region demonstrates that whilst some countries do not have any mechanisms in place yet, but those having at least a draft data protection mechanism consider developing legal mechanisms matching GDPR. Taking the optimistic view, these positive trends at the national level lead to expectations that SAARC regions would be in a strong position to develop a consensus-based regional level data protection mechanism, maintain a constructive dialogue between the nations, and sustain the momentum towards developing a global level data protection mechanism. In the next section, the researcher narrowed the scope of the analysis to Sri Lanka and the United Kingdom, using them as a case study.

2.10 Case studies

2.10.1 Democratic Socialist Republic of Sri Lanka

Sri Lanka has a growing population, and the use of information technology and associated services is growing even at a faster rate (Gunawardana, 2018), so is the use of cyberspace.

A vast majority of the population use mobile phones to manage their daily lives, and amongst them, a new generation of professionals, youth, and those still in education are resorting to modern technology and associated IT systems using online network facilities available right across the country (Gunawardana, 2018). This trend will continue in a progressively developing country that is becoming increasingly dependent on advanced technology and the benefits it offers to the citizens.

That is all well and good. The concerning factor on the consumer front is the inevitable intrusion into the privacy of the users of information and technology and modern digital systems. That exposes the users, and there is a pressing need to develop laws to safeguard against the challenges of cyberspace crime faced by the state and the users. The most important of them is to legally protect the personal information of individuals, which cannot be ignored or treated mildly. In the formation of legislation, the parameters of the importance of the law and the guideline should be considered to ensure they are sound, unambiguous, and enforceable.

On the economic front, Sri Lanka needs data protection and information security laws as they are crucial to attracting foreign direct investment (FDI), and as pointed out by the economists, due to the lack of adequate legal rights, the foreign investors will be reluctant to invest in the country (The morning, 2020). In a different context, however, Sri Lankan entities that process data of European residents are faced with stringent obligations. The Computer Crimes Act 2007 appeared to have addressed the issue of data privacy to some extent by specifying penalty clauses for unlawful acquisition, illegal interception of data and unauthorised disclosure of information (Madugalla, 2016). Also, the right to privacy has been recognised by the judiciary under the common law of Sri Lanka (Madugalla, 2016). This indicates that despite the absence of a specific legislative mechanism, the right to privacy has the recognition of the Sri Lankan judiciary in a variety of legal contexts under common law.

Chapter III of the Sri Lanka Constitution (1978) provided adequate guarantees for the fundamental rights of its citizens, but not specifically for the right to their privacy (Berry, 2017). The proposed versions of the drafts of the Constitution in 1997 and 2000 had stipulated the right to privacy and family life as a fundamental right (Berry, 2017). The proposed October 1997 Constitution specifically stated, Every person has the right to have his or her private and family life, home, correspondence, and communications respected, and shall not be subjected to unlawful attacks on his or her character, esteem positions, and reputation (Berry, 2017).

The 19th Amendment to the Constitution makes minimal, half-baked reference to privacy. It states that a fundamental right to information cannot be complied with if the privacy of an individual is to be tampered with (De Soysa, 2017). To remove any ambiguity in the reference made to the constitutional right of privacy, the Minister for Telecommunications had confirmed that a Personal Data Protection Bill would be introduced in Parliament in 2019 (Deloitte, 2019, Unity in Diversity; The Asia Pacific Privacy Guide). The Data Protection Drafting Committee of the Ministry of Digital Infrastructure and Information Technology (MDIIT), and the Legal Draftsman Department, have initiated drafting legislation on data protection (Sirimane, 2020). The aim of the drafted bill is to cover the fundamental principles of privacy and data protection, shadowing legislation models introduced by other countries.

The Bill prescribes measures to protect the personal data of individuals held by banks, telecom operators, hospitals, and other entities amalgamating in processing personal data (Sirimane, 2020). It aims to regulate the processing of personal data, designate a data protection authority, and safeguard the rights of citizens (Ikigai Law, 2019). Under the terms of the Bill, data could be processed for specified purposes only, with a proviso that the data could be processed for purposes in the public interest, to respond to an emergency, and for scientific, historical, research, or statistical purposes (Ikigai Law, 2019).

The rights of data subjects provided in the Bill include the right to withdraw the consent given to controllers, the right to access, rectify, and erase data without undue delay, and to object to the processing of data (Ikigai Law, 2019). Consent is now required before the collection of private information, and even if consent is obtained, the collected data should only be used for the purposes for which it was collected (Ikigai Law, 2019). The final draft stipulates that every controller unless exempted from this Act or any written law is obliged to appoint a Data Protection Officer to ensure compliance (Ikigai Law, 2019). The data protection authority shall be responsible for all matters relating to personal data protection in Sri Lanka and for the implementation of the provisions of the Bill. The penalties for failure to comply with the provisions of the Bill shall not exceed a sum of LKR 10,000,000 in any given case (Sirimane, 2020).

The Bill stipulates that only public authorities may process personal data within Sri Lanka, and the processing of classified data overseas is subject to permission being granted by the DPA and any relevant supervisory body (Greenleaf, 2019, P.1-5). The private sector is not subjected to conditional data localisation stipulations except for transferring personal data to a third country prescribed by the Ministers (Greenleaf, 2019, 1-5).

The Framework for the Proposed Personal Data Protection Bill was first released on 12 June 2019 for stakeholder comments, and the final draft was released on 24 September 2019 by the Ministry of Digital Infrastructure and Information Technology (The morning, 2020). The Bill comprehensively covered both the public and the private sector in full. The legislation was to be implemented in stages, and the Bill was scheduled to become operational within a period of three years after ratification by the Parliament, allowing the Government and private sector a time-lapse to prepare for the implementation of legislation (The morning, 2020).

Table 2.19: Draft Personal Data Protection Bill of Sri Lanka compared with GDPR

General Data Protection Regulation (GDPR)	**Draft Personal Data Protection Bill of Sri Lanka (2019)**
The legality of necessary processing depends on the justification for doing so (Eur-Lex, 2016).	Data could be processed only for specified purposes (Ikigai Law, 2019)
The rights of the individuals are broadly aligned (Eur-Lex, 2016).	The provisions provided in the Bill include the rights of the data subject to withdraw consent given to controllers, to access, to rectify, and erase data without undue delay, and to lodge objections to the processing of the data (Ikigai Law, 2019).

The data controller shall not process personal data without obtaining consent from the data subject (Eur-Lex, 2016).	Data controllers should comply with the requirement to obtain consent from the data subject prior to processing personal data (Ikigai Law, 2019).
There is a regulatory requirement to appoint a Data Protection Officer (Eur-Lex, 2016).	The final draft stipulates that every controller, unless exempted from this Act or any written law is obliged to appoint a Data Protection Officer to ensure compliance (Ikigai Law, 2019).
The failure to adhere to core principles of data processing, infringement of privacy rights, the transfer of personal data will incur penalties of up to 20 million euros, or 4 percent of global annual turnover, whichever is higher (Eur-Lex, 2016). Non-compliance with, or failure to adhere to technical and organisational requirements: penalties of up to 10 million euro or 2 percent of the global annual turnover, whichever is higher (Eur-Lex, 2016).	The penalties for failure to comply with the provisions of the Bill shall not exceed a sum of LKR 10,000,000 in any given case (Sirimane, 2020).

Sri Lanka is a developing country; despite that status, its commitment to developing a data protection mechanism needs admiration. The summarised information in the table (See table 2.19) shows draft legal mechanisms in comparison to GDPR. The majority of the participants in responding to the questionnaire has underscored the need for data protection mechanisms (See figure 4.22, 4,55 and 4.88).

2.10.2 The United Kingdom (UK)

The UK, shadowing the other European countries, passed legislation designed to supplement the data protection requirements of the GDPR, which came into force in 2018 (Government of United Kingdom, N.D, Data protection). On 31 January 2020, the UK left the EU under the withdrawal agreement agreed between the UK and the EU, but the GDPR remained applicable until the end of the transition period, and the incorporation of GDPR into the UK law took place at that point (ICO, N.D, Binding Corporate Rules at the end of the transition period). The UK GDPR is the UK law, modified version of the EU GDPR format to make it effective in the UK, and it was established as the applicable law in the UK with effect from 1 January 2021, before the end of the BREXIT transition period (ICO, N.D., About the DPA 2018). In effect, UK's data protection law closely matched that of the EU (ICO, N.D., About the DPA 2018). This alignment of data protection laws of both the UK and EU was seen as sufficient reassurance to the citizens that their date would be protected if shared with the UK.

The Data Protection Act (DPA) 2018 formed the foundation for data protection in the UK. This act governs the way in which personal information is used by organisations, commercial enterprises, and the government. Those responsible for collecting personal data are obliged to adhere to the rules, termed as the data protection principles, and in compliance, they must make sure the information is: (Government of United Kingdom, N.D., Data protection).

- used fairly, lawfully, and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant, and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage

However, there are some significant variations between the General Data Protection Regulation and the Data Protection Regulation 2018.

Table 2.20: The Data Protection Act of the UK compared with GDPR

General Data Protection Regulation (GDPR)	**The Data Protection Act (DPA) of the UK (2018)**
A child can give consent to data processing at age 16 (Eur-Lex, 2016)	A child can give consent at age 13 (DPO centre, 2018).
Personal data defines as any information relating to an identified or identifiable natural person (‘data subject’) (Eur-Lex, 2016).	Personal data defines as any information relating to an identified or identifiable living individual (Government of United Kingdom, 2018).
Those processing criminal data must have official authority to do so (Eur-Lex, 2016).	Those processing criminal data do not require official authority (Government of United Kingdom, 2018).
Data subjects have the right to refuse automated decision making (profiling) (Eur-Lex, 2016).	Automated profiling permitted subject to legitimate grounds for doing so (Government of United Kingdom, 2018).
The rights of the data subject can be waived by the organisations provided there is a legitimate need for processing for scientific, historical, statistical, and archiving purposes (Eur-Lex, 2016).	The rights of the data subject can be waived by the organisations provided there is a legitimate need for processing for scientific, historical, statistical, and archiving purposes (Government of United Kingdom, 2018).

The maximum fine for non-compliance is (euros) €20 million or 4% of annual global turnover (Eur-Lex, 2016).	The Commissioner may specify the value of the fines at his discretion depending on the nature of the failures; the maximum fine is limited to 150% of the highest fine payable by a controller, in a financial year, in accordance with the regulations (Government of United Kingdom, 2018).
GDPR is governed by the Court of Justice of the European Union (Court of Justice of the European Union, 2021)	DPA comes solely under the UK justice system (Mars, 2020)
Personal data may be stored for longer periods if the data was processed for retaining in the public interest, scientific or historical research purposes or statistical purposes (Eur-Lex, 2016).	Personal data may be stored for longer periods if the data was processed for retaining in the public interest, scientific or historical research purposes or statistical purposes (Government of United Kingdom, 2018).

There are similarities between DPA and GDPR, and the exceptional variations in specific elements of the law do not make UK law less effective; in fact, the DPA 2018 covers a wide area in the application of the law. The UK decided to extend the legal mechanism and apply it, for instance, to situations like immigration (Government of United Kingdom, 2018). The DPA allows an exemption to the application of legal mechanisms for processing data for justifiable purposes such as safeguarding national security (Government of United Kingdom, 2018). This means that the organisations would be exempt from complying with data processing regulations, for example, for the purpose of prevention and detection of crime.

After Brexit, the GDPR became integrated into UK law as the 'UK GDPR', and it was tailored by the Data Protection Act 2018 (ICO. N.D., Overview – Data Protection and the EU*)*. The ICO remains the independent supervisory body for the UK's data protection legislation and explains data protection principles, rights and obligations (ICO. N.D., Overview – Data Protection and the EU)

In the next section, the researcher highlighted the similarities and disparities between the countries in the South Asian region in relevance to the proposed revised GDPR inspired Bills. These observations become important when taking collective actions to develop a binding regional level mechanism.

2.11 Similarities and Disparities between GDPR inspired bills in South Asian countries

The states and state apparat, organisations and individuals face sophisticated, complex cyber-security threats designed to cause significant damage to the economy and infrastructure dependent essential services. This has become a frequent occurrence specially in the countries in the Asia region where, unlike those in the West, the use of the internet has expanded at a rate in correlation with the internet revolution (See table 1.2). That has invariably aroused growing concerns in the community about the cybercrimes ranging from data breaches to transferring personal data and, to allay any concerns and fears, most of the Asian countries have taken steps to introduce new data protection legislation or enhance existing cybercrime countermeasures.

The commercial sector in the South Asian region is growing in line with modern technology and increasingly becoming digitalised and moving into online platforms to conduct business activities (Deloitte, 2019, Unity in Diversity; The Asia Pacific Privacy Guide). In the light of these changing environments, the public, private, and non-profit entities are all in the process of introducing Information and Communication Technology (ICT) to improve their computing capabilities, in a continuous process to keep up with the Western world. The number of ICT users is growing at an unprecedented rate, and they are constantly becoming attracted to ICT capabilities but many in general lack technical knowledge of cyber security and their privacy rights (Subedi, N.D). That exposes commercial enterprises and individual users to greater risks from cyber-attacks originating from locations anywhere in the world. Therefore, it is imperative for both the private sector and the individual users of cyberspace to have sufficient awareness of their exposure to the risks from cyber threats and their privacy rights. The rise in data breaches and privacy-related incidents has facilitated discussion around how much control people should really have over their personal information. Since then, there has been improved recognition of the right to privacy in the digital age and increased awareness amongst the public, in terms of how individuals can access or control their data. On another positive note, there has been a push for comprehensive rights for the individuals, such as the right to request consent for processing and the right to be forgotten; governments have responded by strengthening their privacy law frameworks (See table 2.21). In addition, the organisations, when collecting personal information and when processing and transferring personal information to a third party, are required to seek consent from the individuals (See table 2.21). The organisations engaged in processing personal data are also required to employ a Data Protection Officer within the organisation in most of the countries (See table 2.21). At the national level, the rise in data breaches in terms of frequency and volume has put pressure on governments to introduce data breach notification requirements making reporting of data security breaches mandatory (See table 2.21). The notification should include full details of the breach, the name and contact details of the data protection officer, a description of the likely consequences of the breach and an incident recovery plan proposal for mitigating its effects (See table 2.21). Those organisations violating the rules will become liable and incur a heavy fine (See table 2.21).

Since the GDPR came into effect, many commercial enterprises became obliged to re-examine their stand on privacy rights. The European Commission enabled the free flow of data between the EU and countries considered to have ‘adequate’ regulations in place. Many are currently seeking to strengthen their laws to obtain an adequate decision in the South Asian region.

Table 2.21: Comparison of features of data protection mechanisms in the South Asian region

Common features of Data Protection mechanisms in the region	**Disparities in Data Protection mechanisms in the region**
Rights of the individuals broadly aligned (OneTrust Company News, 2018) (Ikigai Law, 2019)	The appointment of a Data Protection Officer is not required for all countries (DLA Piper, 2020) (The global legal group, 2020)
Without the consent of the data subject, processing of personal data by the data controller is prohibited (Rehman, 2020) (Deloitte, 2019, The Asia Pacific Privacy Guide) (Neupane Law Associates, 2019) (Ikigai Law, 2019)	The time duration for notifying data breaches to the relevant authorities by the data controller is not specified by all countries.
Most countries categorically stipulate that the recipient country of transferred data has personal data protection provisions to match provisions in the Bill (DLA Piper, 2020) (Deloitte, 2019, India Draft Personal Data Protection Bill, 2018 and EU General Data Protection Regulation A comparative view)	Only some countries have specified the requirement for having data breach notification served in writing and the contents of data breach notification.
Data breach notification is mandatory in most countries (Walia and Chakraborty, 2020) (Government of Pakistan, 2018)	In some countries, anyone found to be in violation of any part of the Bill would be liable for prosecution and will incur a fine (Rehman, 2020), whilst in some countries, a fine only.
All countries have provision for collecting sensitive information for lawful purposes	The limit of the fine varies from country to country and is dependent on their capacity

whilst ensuring the information so collected would be used for intended purposes only (Subramaniam and Das, 2020) (Neupane Law Associates, 2019) (Ikigai Law, 2019)	and capabilities (Rehman, 2020) (Pradhan, 2020) (Sirimane, 2020)
Retention of sensitive personal information is not time-limited (Subramaniam and Das, 2020).	In some countries, an offender in violation of the Act could be liable for compensation payments to the affected party (Pradhan, 2020)

The literature-based evidence shows that there is a general disparity in the privacy policy and data protection legislation amongst states, but when looked separately at the national and regional level, the degree of disparity varies. These disparities are attributable to a number of factors that are both internal and external and influenced by specific laws of the state. What is also important is to identify the gaps in cyber legislation that allows cybercriminals to get away without impunity for the weaknesses in law enforcement and inconsistency in the laws themselves. These identified gaps/limitations/disparities in the regulatory frameworks, when scrutinised in real situations, make a case for having a unified global level privacy policy and strategic data protection laws to prevent states and organisations from taking arbitrary actions and to avoid perpetrators walk away without any proper punishments for the actions. All that said, there is an exception to the rule, ‘national security’ of the state overrides any emphasis on privacy protection, but it has essentially to be on a need basis.

The need to have a collective unified data protection mechanism is clear. Therefore, in accepting and implementing privacy laws, it is also important to to minimise any disparities and enhance trust between countries. To this end, the researcher strongly do believe it is important to identify the challenges faced by countries.

2.12 Barriers to developing a global legislation

In 1996, France put forward the earliest proposal titled the ‘Charter for International Cooperation on the Internet’ (Mačák, 2016, P.130). This was later followed by a jointly put together Russo-Chinese initiative, a Code of Conduct for Information Security, two proposals submitted to the UN General Assembly in 2011 and 2015, respectively(Mačák, 2016, P.130). However, these proposals received a lukewarm reception by the other states without much enthusiasm (Mačák, 2016, P.130). There has been a hesitancy and deep reluctance on the part of the other states to participate in the development of cyber specific customary international rules. There are also other potential external/internal factors hindering collective decision making.

2.12.1 Social differences

The assessment of social impacts prior to implementation of a policy is to determine what difference a policy will make to people’s lives. It enables the researcher to analyse the social impacts and, to consider the widest range of impacts that policies would have on individuals, communities, and society. A summary of social differences within the countries is outlined in figure 1.2.

Many of the wealthiest countries record the highest current-level development scores and they enjoy political stability, freedom of expression, and low levels of corruption (Beal, Rueda-Sabater, and Santo, 2012), and that allows the countries in this category space to focus more on developing data protection mechanisms in comparison to less developed countries that are struggling to reconcile the differences exist in them.

A country’s overall economic strength influences internet diffusion, and the resources and capital required for the expansion of technology (Hargittai, 1991, P.7), and there is also a demand for capital investment for developing data protection mechanisms. Therefore, the economic stability of the developed countries has the capacity to allocate funding towards the protection of privacy of their citizens and to assist in reviewing existing policies of the developing/underdeveloped countries.

The knowledge of the individuals also may influence the spread of communication technology (Hargittai, 1991, P.8). The knowledge is of many forms ranging from knowledge of the use of communication technology to privacy and security threats associated with technologies. This knowledge gives users an insight into technology and understands the necessity of having established data protection mechanisms. In addition, the literature suggests that some languages have greater recognition than others and they dominate certain areas of life, as an example, the use of the English language in the computer industry (Hargittai, 1991, P.8); hence the language barrier could be an obstacle to developing policies. Therefore, literature material should be translated into multilingual formats and made easily available and accessible to all countries for developing data protection mechanisms.

Furthermore, the cultural background also can contribute to the development of data protection mechanisms. In Asia, the interpretation of the perception of obscenity and pornography/erotica varies from country to country (Liu, Hebenton, and Jou, 2013. P.57). For example, the reports suggest that Japanese people have a higher tolerance to erotic materials in comparison to those in China, Taiwan and Hong (Liu, Hebenton, and Jou, 2013. P.57). The reports suggest that the Islamic countries also have a lesser tolerant approach to obscene materials. Hence, the countries such as China, Singapore, Pakistan scrutinise social networking sites or even block web access to filter out such sensitive material (Liu, Hebenton, and Jou, 2013. P.57). These social differences and beliefs form the biggest barriers to developing a global level data protection mechanism.

These social differences and beliefs are the biggest barriers facing developing a global level data protection mechanism. However, a report suggests that an increasing number of Europeans living in the border regions of the EU claims social and economic differences are not the problem affecting cooperation between their home and neighbouring country (Makszimov, 2020).

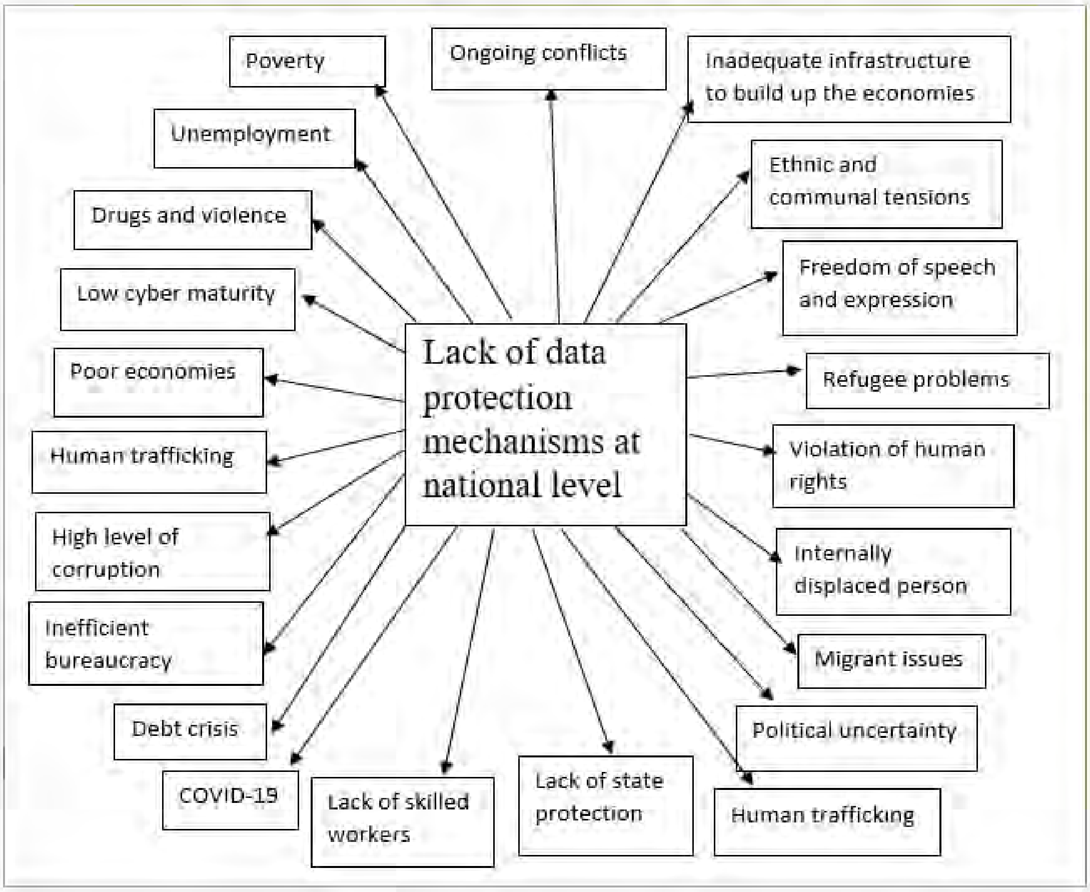


Figure 2.3: Social differences

2.12.2 Mistrust between countries

The emerged mistrust amongst the countries has come about for a variety of reasons, such as political differences, border disputes, and the persistence of ongoing conflicts. For an example, the relations between the USA and the USSR became adversarial and reached a peak when the Western nations interfered with the emergence of communism in the Soviet Union (Arena, 2009, P. 200). Russia, the former Soviet Union, was also prevented from joining the League of Nations in the 1917s (Trueman, 2015). In another scenario, the relation between China and USA also became sour with ups and downs for different reasons (Lee, 2021). These reasons have become a challenge in bringing everyone together to come up with a global level data protection mechanism.

2.12.3 Legal and ethical factors

The ways in the countries adhere to international or regional conventions differ between the countries, and these differences tend to influence the determination of specific initiatives for the development of their laws. Legal and technical disparities make it difficult to respond and investigate, enforce the law, and hinder international collaboration (Mendoza, 2017).

The level of understanding of ethics and legal background at the national level is of immense importance. The absence of commitments by the countries to develop national-level data protection mechanisms is one example of a hindrance to progress, and that prevents nations from coming together to fulfil their commitments to developing unified data protection mechanisms. It is also crucially important to ensure the legality of data protection mechanisms; they are justifiable and ethically consistent to avoid technical and ethical obstacles that may arise after implementation.

Also, several countries deployed apps during the pandemic to curtail the transmission of the coronavirus. Some countries made it an enforceable requirement to download the app and use it, whilst in others, it was voluntary, with the citizens granted discretion whether to use it or not (See Annexe C.12). According to GDPR, collecting and processing of personal data is conditional on obtaining prior consent, but when the citizens are forced upon to download the app and use it, they are obliged to do so. However, when in an unprecedented pandemic like COVID-19, the state also has a responsibility to protect personal privacy whilst bearing in mind the consequences of implementing long-term measures to manage the pandemic without contravening legal obligations.

The level of tolerance of social behaviour amongst the countries also affects progress towards developing unified mechanisms. One such example is the prohibition of pornography and obscene material by some countries, whilst in some countries, they are not (World population review, 2021). That means displaying, viewing, or creating pornographic material on a personal office computer will not always be considered a criminal act in some parts of the world (Tovi and Muthama, 2013) The use of technology in a manner that is not consistent with ethical principles creates ethical risks.

The meaning and practice of ethics may vary from one country to another depending on the level of understanding and the interpretation of ethical values. For an example, not every staff member would take the company-owned USB drive home at will (Tovi, and Muthama, 2013). Different interpretations of what is ethical and what is not, is a difficult one for a broader debate given the complex nature of ethical practices, developing a global level data protection mechanism becomes a challenge, unless all nations understand and respect international norms and standards of ethical behaviour in practice.

2.12.4 Identification difficulties

One of the most concerning and significant is the attribution hindrance (Yannakogeorgos, 2016). The perpetrators are becoming increasingly effective in concealing the authenticity of identities, and their operational locations and, also the identification of the origin of a cyberattack is extremely difficult, even impossible without international cooperation. Furthermore, the limitations in jurisdiction make investigation a complex process and a challenging task that makes prosecution of cyber perpetrators a futile effort.

2.12.5 Delays in the enactment of laws

The enactment law/s in different countries is driven by the decisions made at the national level, based on a variant of factors in different circumstances. They could be political, economic, and social issues. For example, the ratification of the Budapest Convention had taken too long by most of the countries for varying reasons; the delayed development of the law is one of them (Mendoza, 2017). In another scenario, UN negotiations of a new treaty on cybercrime will take an intense diplomatic effort lasting a considerable timescale without achieving a successful outcome (Hakmeh, 2017).

2.12.6 Laws and basic principles overlap

The internet has no physical borders and is freely available to the users, governed by national legislation, but constitutional or legal conflicts can arise on the grounds of privacy and freedom of expression. This could lead to debatable contentious issues of privacy and security, which may drag on unabated with no end to it.

2.12.7 Differences in national legislation

There are clear differences between national legislations of countries. For example, the defined expression of a data breach and the time limit for notifying the breach to the individuals and/or the authorities varies significantly (Bevitt, Retzer, and Lopatowska, N.D). In the EU, a data access breach alone, however minor, makes it a notifiable breach within 72 hours of being detected, in most cases (European Data Protection Supervisor, N.D). In China, the discovery of security flaws and vulnerabilities in network products and services necessitates informing the relevant government agencies and network users of such breaches (Luo, and Wang, 2020). In Japan, the only requirement is to ‘make the effort’ to notify the incident of a breach, (Hounslow, 2020), even that requirement is deemed a vague one.

2.12.8 Maturity in terms of technology

Taking Singapore as a model that has a high degree of cyber maturity (The Australian Strategic Policy Institute, 2017, P. 100-105), it will endeavour to adopt advanced norms, capacity-building measures, and other aspects of cyber policies, whereas a country like Myanmar is less likely (Taylor, 2020, Myanmar - Data Protection Overview) as their cyber maturity is law (The Australian Strategic Policy Institute, 2017, P. 100-105). The clear indication is that the commitment of South-East Asian states to cyber policy issues seems to be dependent on the level of their cyber maturity.

2.12.9 The degree of dependency on ICT

Singapore, Malaysia, and Thailand experience demonstrate that, given the high levels of ICT lead digital economy (Mia and Habaradas, 2020, P.37), the compelling need is to have strong security measures against potential threats. In contrast, Myanmar, Cambodia, and Laos have a low level of ICT dependency (Mia and Habaradas, 2020 P.37), and are unable to reap the economic benefits of cyberspace. However, a lack of dependency on ICT does not make these countries less vulnerable to cyber threats.

The Network Readiness Index (NRI) is one of the leading global indices that reflects the application and impact of information and communication technology (ICT) of the economies of countries around the world. According to the NRI 2021, Sri Lanka is ranked 78th in the listing, with India in 67th, Pakistan in 97th , Nepal 115th , and Bangladesh ranked 95 out of 130 economies (Portulans Institute, N.D). In contrast, in the European region, most countries are ranked top, with the United Kingdom in 10th place (Portulans Institute, N.D). An illustration published in a report shows an upward trend of ICT services exports for the period 2018–2025, for Bangladesh, India, Maldives, Nepal, Pakistan, and Sri Lanka, and growth rates forecast for 2025 will be around 50%, 30%, 46%, 56%, 58%, and 49% respectively (Saif, 2021).

Regarding reliance on technology, Bhutan and Afghanistan fall behind in comparison to other countries in the South Asian region. According to a report, Bhutan is a late entry to the ICT and is the last country to legalise television and internet (Baer, M 2018). Existing ICT capabilities of Bhutan, when analysed exposed key barriers affecting reliance of technology, weak domestic demand for ICT services and the absence of a proper e-commerce strategy, and e-commerce law (UNCTAD. N.D., Bhutan Rapid eTrade Readiness Assessment). Afghanistan, on the other hand, affected by the unstable governance systems, lost out on access to technologies until recently, and the nation depended on analogue devices during the Taliban administration between 1996 and 2001, according to the reports (Stokel-Walker, 2021). Access to the internet was effectively prohibited alongside music and women were banned from participating in any social activities, and most Afghans were deprived of emerging technological evolution (Stokel-Walker, 2021). That in effect isolated the Afghan community from the rest of the world without a stake in the IoTs dependent developing world.

The high level of dependency on technology as well as the degree of reliance on technology, enables organisations to collect, process, and store large amounts of information, and from the same token, they also have a responsibility to protect personal information. That said, the requirement for developing data protection mechanisms to protect collected data and the privacy of the data subjects also become an important factor in data handling. The failure to do so will have a detrimental impact on their finances as well as the trust and reputation of the organisation. Therefore, organisations and companies should urge their governments to accept and implement policies that would serve the interest of the citizens in the long term.

2.12.10 Public and private sector policy implications

The public and the private sector face challenges in accessing information for investigations. The dispute between the FBI and Apple Tech giant turned out to be a classic example, in which the US Judge requested the cooperation of the technology giant for its cooperation to unlock the iPhone owned by a terrorist involved in an attack (Fox and Lee, 2016). This request was turned down by the tech company claiming that breaking encryption for one phone could not be done without undermining privacy (Fox and Lee, 2016). The events of this kind clearly demonstrate the need to have local and cross-border agreements on collaboration to avoid conflicts of interests.

The researcher is using the PESTLE model (Political, Economic, Sociological, Technological, Legal and Environmental) to present key factors. It offers the people and the policy developers an understanding of and insight into external factors that would impact their organisation.

P	E	S	T	L	E
Political differences. (e.g. Democratic , Republic, Monarchy, Communist Dictatorship and other)	Economic differences. (e.g. Developed, Developing, Under developed and other)	Ranging from poverty to ongoing conflicts.	Maturity in terms of technology The degree of dependency on ICT.	Public and private sector policy implication Legal and ethical factors. Delays in enactment of laws Laws and basic principles overlaps Differences in national legislations	Mistrust between countries Identification difficulties

Figure 2.4: Summary of the barriers

The reliance on new technologies and IoT generates a large volume of information, and any data breach will have an impact on personal privacy; and to safeguard privacy, it is important to have data protection mechanisms. To meet that requirement, most of the countries revisited and developed data protection mechanisms at the national level lining with GDPR. However, some countries are yet to make up ground. Also, international organisations are actively supporting this approach recognising the risks and threats associated with cyberspace.

In this chapter, an intensive literature review was done to get an understanding of the extent of the commitment made to protect personal information by the countries at the national level and how the regional level organisations are engaged in protecting personal data. The next step was to undertake a country-specific case study on Sri Lanka and the United Kingdom to determine their progress and then discussed the challenges faced by countries in developing the existing mechanisms if any.

On analysing the available literature, the most important and encouraging discovery the researcher made was that many countries had either reviewed or were in the process of reviewing their national-level mechanisms in line with the GDPR. The researcher compared the GDPR inspired national level mechanisms in the South Asian region with the EU GDPR to get a deeper understanding of how robust the GDPR inspired bills in the South Asian region were. The conclusion was that, except for a few disparities in the applicable penalty limits and the requirement to appoint a Data Protection Officer, the South Asian countries had considered 8 principles of GDPR when developing their national-level mechanisms. The researcher also observed that at present, there was no consensus amongst the SAARC organisation members to achieve uniformity in a meaningful mechanism to protect personal information within the region, unlike the GDPR in the EU region. However, given the trends in developing data protection mechanisms in South Asian countries and the genuine desire to do so, the researcher firmly expects the SAARC organisation to find common ground to develop a regional data protection mechanism in the next 5-10 years.

There is a necessity to develop a global mechanism to bring perpetrators to account. Therefore, it is important to identify the challenges faced by countries when developing such mechanism. The researcher assimilated knowledge from literature readings and compiled a questionnaire for the purpose of gathering people's perspective and to identify the key factors that would contribute to developing a data protection mechanism. The researcher analysed these findings to develop the Policy Acceptance Model (using existing TAMs). The purpose of the proposed model is to give an indication of the key factors for consideration in developing a data protection mechanism, and the researcher suggests this model be used to develop a data protection framework collectively at the national, regional, and global level.

CHAPTER THREE

RESEARCH METHODOLOGY

Chapter three contains an overview of the methodology the researcher used, a description of research design and philosophy, and a discussion on the research tools used to collect and analyse the data.

3.1 Research philosophy

The research philosophy is a phenomenon about how data should be collected, analysed, and used (Saunders, Lewis, and Thornhill, 2009, P.135-143). The researcher collected data using secondary and primary data collection methods and conducted the analysis of the responses to answer the research question, and the outcome of the analysis will add new knowledge to the available literature.

There are four types of research philosophies pragmatism, positivism, realism or interpretivism (Melnikovas, 2018, P.34-37). The research philosophy will offer the researchers different types of methodologies purposed to avoid inappropriate and unrelated work. Understanding the basic meaning of research philosophy, its advantages, and benefits will help the researcher become creative and exploratory in the proposed research method used.

3.1.1 Positivism

Positivism adheres to the view that only the factual knowledge gained through observation is trustworthy (Akpi, 2019, P.2). Therefore, positivism depends on quantifiable observations that lead to statistical analyses (Akpi, 2019, P.2). Statistical and mathematical techniques are central to positivist research, which adheres to purposefully structured research techniques to uncover the reality. In positivism, the role of the researcher is limited to data collection and interpretation of that in an objective way (Dudovskiy, N.D, Bussiness Research Methodology). Positivism is governed by the realisation of the objectivity and quantifiable analyses of measurable data.

In this context, there are no provisions for human interests within the study. The positivist studies usually adopt a deductive approach (Dudovskiy, N.D, Bussiness Research Methodology) and prefer quantitative methods such as social surveys, structured questionnaires, and official statistics because of the high reliability (Revisesociology, 2015). This means that positivism is based on facts. However, there is a belief amongst the researchers that the downside to positivism is the lack of insight into in-depth issues (Dudovskiy, N.D, Bussiness Research Methodology). Therefore, this is not an ideal approach, especially that social scientists should take. However, the positivists argue that they see society as shaping the individual and believe that social facts shape individual action (Revisesociology, 2015).

Positivist researchers intend to remain detached from the object of the research by creating a distance and emphasise the importance of remaining emotionally neutral (Levy, N.D, P.374). They also maintain a clear distinction between science and personal experience, and fact and value judgement (Levy, N.D, P.374). In positivist research, it is also important to seek objectivity and use consistently rational and logical approaches to research (Edirisingha, 2012).

In this research, the researcher decided against the positivism approach as the research undertaken was not purely objective and, the researcher's expectation was to maintain a good interaction with the research participants.

3.1.2 Interpretivism

The development of interpretivism philosophy is based on the critique of positivism in social sciences (Dudovskiy, N.D, Interpretivism Research Philosophy). Interpretivism integrates human interest into a study (Dudovskiy, N.D, Interpretivism Research Philosophy). Therefore, in this philosophy the emphasis is on qualitative data collection (Žukauskas, Vveinhardt, and Andriukaitienė, 2018, P.125). Data collection uses methods such as interviews and case studies (Žukauskas, Vveinhardt, and Andriukaitienė, 2018, P.126). The data collected in this way cannot be generalized since data is heavily impacted by personal viewpoints and values. Therefore, the reliability and representativeness of data is undermined to a certain extent. Secondary data research is also popular with interpretivism philosophy (Dudovskiy, N.D, Interpretivism Research

Philosophy). Accordingly, interpretive researchers assume that access to reality is only through social constructions such as language, consciousness, shared meanings, and instruments (Antwi and Hamza, 2015, P.218).

However, on the plus side, qualitative research areas can be studied to an extensive level in interpretivism (Karamagi, 2021). The limitation of the positivist approach is the failure to address aspects such as personal beliefs, experiences, and motivations (Stainton, 2020). Interpretivism helps understand and analyse how and why something occurs in the way it does, and this cannot be achieved through numerical analysis. This approach requires in-depth assessment, and for that reason the inputs from the participants and the interpretations of their perceptions are considered important. Therefore, the supposition is the reality, and the perceptions of the individuals cannot be taken in isolation (The Editor, N.D, P.4); however, the likelihood of prejudices in the mind of a researcher can be considered a disadvantage in interpretivism (Karamagi, 2021).

Interpretivism argues that people interpret their environment and is dependent on their cultural environment in which they themselves live (The Open University, N.D). However, this is not just about the differences between societies; variations in cultural perceptions and behaviours exist in societies largely populated by diverse groups of people. Interpretivists question why people find it difficult to understand why the people do, what they do without understanding the distinctive nature of their beliefs and attitudes (The Open University, N.D). The researcher shelved this approach given its statistical insignificance in interpretivism. Also, for the purpose of this study, the researcher is satisfied that statistical significance is important, given the extent of the sample of the participants indicating the importance of identifying the factors widely considered necessary for developing a global level data protection framework.

3.1.3 Realism

The realism research philosophy is an assumption based scientific approach to develop knowledge, and the theory of realism means the reality of independence of the mind (Dudovskiy, N.D, Realism Research Philosophy); mainly qualitative methods such as case studies and convergent interviews (Smith and Elger, 2020, P.6). Realism can be divided into two groups: direct and critical (Dudovskiy, N.D, Realism Research Philosophy). Direct realism portrays the world through personal human senses (Saunders, Lewis, and Thornhill, 2009, P.138), whilst critical realism, on the other hand, argues that sensations and images of the real world can be deceptive, and they usually do not portray the real world (Dudovskiy, N.D, Realism Research Philosophy). Furthermore, the critical realists recognise that the researcher's senses and other factors may get in the way between the researcher and researched reality (Dudovskiy, N.D, Realism Research Philosophy).

A distinctive feature of all forms of realism is the denial that it is possible to have any objective or certain knowledge of the world and acceptance of the valid alternative accounts of any phenomenon. All theories about the world are not written in stone and fallible, and subject to change (Maxwell, 2012, p.5).

There are ongoing philosophical debates over realism that remain unresolved and there is disagreement on many of the issues amongst the realist philosophers themselves; most importantly, the realists reject theoretical concepts (No author, N.D, What Is Realism, and Why Should Qualitative Researchers Care? P.3). However, positivists do not ignore theoretical concepts and consider that theoretical terms and concepts as simply logical constructions based on observational data useful in making predictions (No author. N.D) What Is Realism, and Why Should Qualitative Researchers Care?, P.8). In contrast, critical realists underscore the concept of cause in both the natural and social sciences, but this concept has become the subject for criticism of both positivists and anti-positivists (No author, N.D, What Is Realism, and Why Should Qualitative Researchers Care?, P.8).

The Realism focuses on the actual perception of the physical world, but not on something imaginative, presumptuous, and sentimental. However, the sentimentality of public perceptions are as important as the actual perceptions of the physical world in (the process of) developing a framework for a common purpose, and that made the researcher disregard realism in this research.

3.1.4 Pragmatism

The philosophical movement of pragmatism began in the light of the fundamental agreement between the scholars over the rejection of traditional assumptions of the nature of reality (Kaushik and Walsh, 2019, P.2). They focus on the experience unlike other philosophies that emphasize reality (Kaushik and Walsh, 2019, P.3). The Pragmatists believe that people take actions based on the possible consequences of their actions, and they use the results of their actions to predict the consequences of similar actions in the future (Kaushik and Walsh, 2019, P.3). Therefore, Pragmatist philosophy holds that human actions can never be separated from the past experiences and the beliefs that have originated from those experiences (Kaushik and Walsh, 2019, P.3). Notably, pragmatists believe that the reality is not static, and it changes with turn of events (Stanford Encyclopedia of Philosophy, 2019).

Pragmatism is based on the argument that researchers should use the philosophical and/or methodological approach that works best for a particular research problem (Dudovskiy, N.D., Pragmatism Research Philosophy). Pragmatics recognise that there are different ways of interpreting the world. Pragmatism research philosophy has integrated more than one research approach (deductive/inductive) and research strategies (qualitative and/or quantitative) within the same study (SAGE publications, N.D. P.4) (See figure 3.1), To this end, according to the nature of the research question, Pragmatics combines both, positivist and interpretivism positions within the scope of a single research. In adopting this stance, the pragmatist researcher selects the research design and the methodology most appropriate for addressing the research question.

Pragmatists believe that no two people have identical experiences; therefore, their worldviews also cannot be identical; they believe that we are free to believe anything that we want, although some beliefs are more likely than others to meet our goals and needs (Kaushik and Walsh, 2019, P.3). However, there are always varying degrees of shared experiences between any two people; they lead to different degrees of shared beliefs. The likelihood of people behaving in a certain way in similar situations depends on the extent of shared beliefs on a certain set of circumstances. Therefore, there is no uniqueness in the world opinion and could change based on personal opinions and shared beliefs.

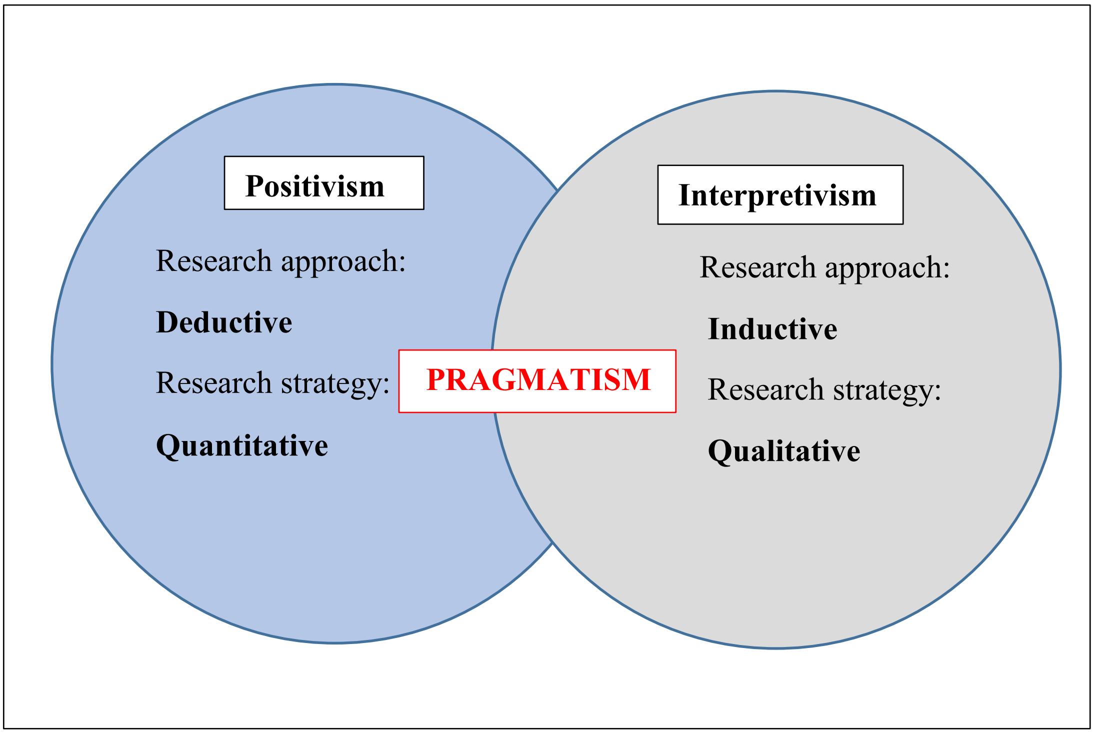


Figure 3.1: Research philosophy summary (Researcher, 2021)

The researcher selected the pragmatism approach because of the feasibility in the study to employ a diverse set of methodological combinations to address the research questions without the researchers having to commit to a specific method. In this research, the researcher addresses the lapses in the protection of personal data at the global level. In pursuit of that objective, to begin with, the researcher conducted a thorough literature review to familiarise with the available mechanisms and the challenges faced by the nations in developing data protection mechanisms. To do that, the researcher used the qualitative data collection method and conducted a qualitative data analysis to analyse the collected literature. The researcher relied on a quantitative data collection method to verify the identified challenges and developed the questionnaire which was then distributed to 186 individuals both in Sri Lanka and the United Kingdom. The quantitative analysis was used to analyse the response samples and to verify the accuracy and reliability of the challenges identified in the literature and, to identify the perception of the people. The importance of verification of accuracy and validity of the information collected through literature sources cannot be underestimated as the published articles although appear to be factual, can also be outdated. Also, doing qualitative research on a subject that would have a global impact would help the researcher gather deeper understanding of the research problem, and it would supplement the existing literature.

3.2 Data collection methods

Data collection is a process of collecting information from all relevant sources to test the hypothesis, evaluate the outcomes and to find answers to the research problem (Dudovskiy, N.D, Data Collection Methods). However, the selection of the data collection method depends on the nature, scope, and aims and objectives of the research. Data collection methods can be divided into two categories.

1. Primary data collection methods
2. Secondary data collection methods

3.2.1 Primary data collection methods

In this data collection method, the researcher gathered raw data directly from the source (Ajayi, 2017, P.5) to ensure the purity of data and the integrity of the collection process itself without exposure to tampering by humans or machines. The researcher believes that this prudent approach helped achieve a high degree of accuracy in the data samples. In this case, the researcher is the first person to interact with and draw conclusions from such data.

In this research, the primary data collection method was found useful because it contained both Qualitative and Quantitative data collection. Therefore, to get an impression of the commitments made by the countries at the national and regional level, and to identify the barriers to developing data protection mechanisms, the researcher used the qualitative data collection method. Also, the Quantitative method was used to verify the referenced literature and to identify the public opinion. The use of the above data collection methods within the primary data collection method would provide the researcher with a credible and realistic understanding of the factors relevant to developing a privacy protection Policy Acceptance Model.

3.2.1.1 Quantitative data collection

Quantitative methods are presented in numerical forms (University of Southern California, N.D). An example would be the use of a questionnaire with close-ended questions and transform them into numbers, charts, graphs, and tables. In this research, the researcher used an online close-ended questionnaire to collect data on public opinion and used qualtrics software to develop the questionnaire. At the predesign stage of the questionnaire, the researcher conducted a thorough literature review to identify the status of the countries and their perceptions on developing national and regional data protection mechanisms, followed by a further literature review to identify the barriers to developing data protection mechanisms. That provided the researcher the reference point for developing the questionnaire (See annexe A).

In preparing the questionnaire, the researcher gave particular attention to the collection of anonymous data by adhering to guiding principles set out in the GDPR and began by obtaining prior consent from the participants clearly stating the intended purpose for collection, how and what information would be collected, the processing, storage, and the retention period. Also included was an opt-out clause allowing the participants to withdraw their consent prior to commencement of the analysis.

Primarily, the questionnaire consisted of two parts; the first section was structured to gather anonymous personal information about employment status, workplace experience, age, and country of employment of the participants, and use gathered data to get an understanding of the participant's background. Section two contained a set of subject-specific questions.

The questionnaire (See annexe A) consisted of dichotomous questions ('yes/no'), multiple-choice questions, rating scaled questions and short answers. The dichotomous questions were limited to three, and the purpose was to obtain direct answers, maintain consistency and avoid any ambiguities. The space available to capture participants' views was limited and impacted on the analysis, and a brief answer option was included for the respondents to record justification for their answers. Also, the rating scaled question system is a universal method of collecting data, and thirteen of them were included in the questionnaire. It helped the researcher to make realistic judgements on the attitudes of the respondents and draw meaningful conclusions. The three multiple-choice questions gave the respondents the option to provide more than one answer.

The standard number of questions recommended in general ranges between 5 and 10 (Ainsworth, 2021), but for the purpose of this survey, that range exceeded to allow scope for wider scale data collection. It is important to collect data in sufficient numbers to carry out an in-depth analysis and to draw realistic conclusions that will support the research aim towards developing a global level data protection mechanism. This is an important approach that highlights the need to get a real-time understanding of the opinions, perceptions, and concerns of the participants, and meet the scope of the research objectives.

In this research, the literature review provided resources for the researcher to identify the challenges that the countries would face in developing data protection mechanisms, and the purpose of the questionnaire (See annexe B) was to ensure timeliness and accuracy of the identified factors. The researcher considered the importance of the protection of privacy equally to everyone and decided on selecting a randomised sample. The researcher distributed the survey questionnaire to public and private sector employees and undergraduate and postgraduate students. The total number of responses received was 233.

The literature stipulates that the pilot study population from which the sample is formed must be the same as the sample in the main study (Cadete, 2017). The implication is that the randomisation of the sample in the pilot study should follow the same process of randomisation in the full-scale project. On the other hand, the researcher felt that conducting a pilot test meant sending the questionnaire to the same participants again, and any delay in the response time would have resulted in a prolonged analysis process. Given the complex factors involved, the researcher intended not to conduct a pilot study; however, the researcher sought advice and guidance from the supervisors during the development phase of the questionnaire.

This method was selected because of factors such as easy to engage participants in sufficient numbers, cost-effective, easy to visualise and analyse, the practicality of covering different areas. However, it was a challenging task to ensure that the questionnaire was (in the right mode and) seen interesting by the participants and their attention to the questions remained throughout without losing interest. Only 4 questions sought justifications for their opinion, and the sample of the responses received was not sufficient to produce meaningful qualitative analysis. Added to that shortcoming was the incompleteness of the responses received.

3.2.1.2 Qualitative data collection

Qualitative research enables a deeper understanding of experiences, phenomena, and context (Cleland, 2017, P.61). Qualitative research allows asking questions that cannot be numerically expressed because it produces subjective knowledge. This includes observations, in-depth interviews, focus groups, existing documents, paper surveys with open-ended questions and online surveys (Dudovskiy, N.D, Data Collection Methods).

From the listed sources in this research, the researcher used journals, books, newspapers, websites, government reports, constitutions for collecting data. Books and journals provide good background information and offer an excellent source for widening the scope of the research. The contemporary data are sourced from the publications available in the newspapers and websites; despite the biased nature of such data, it is still a valid source for collecting data. The researcher decided not to conduct interviews due to the considerable amount of likely time consumption.

3.2.2 Secondary data collection methods

Secondary data consists of data already published in books, newspapers, magazines, journals, online portals by other researcher/s (Dudovskiy, N.D, Data Collection Methods), and they provide a large amount of data regardless of the nature of the research area.

It is difficult to find secondary data that matches 100 percent applicability to one's own situation, whereas in most cases, the primary data collection serves a specific purpose, and the challenge is the selection of appropriate data from secondary sources. However, (authenticity) credibility of the data collected from secondary sources has a direct impact on the research outputs.

3.3 Research approaches

The Research approach can be divided into three types: (Dudovskiy, N.D., Research Approach)

- Deductive research approach
- Inductive research approach
- Abductive research approach

3.3.1 Deductive approach

The deductive approach concerns developing an existing theory-based hypothesis/hypotheses and designing a research strategy to test the hypothesis (Dudovskiy, N.D., Research Approach) (See figure 3.2). The deductive research approach explores an existing theory and tests its validity, in each scenario (Dudovskiy, N.D., Research Approach). The deduction begins with an expected pattern tested against observations leading to either confirmation or rejection of the hypothesis (DeCarlo, N.D). This approach provides a baseline to measure concepts quantitatively and achieve generalisation of research findings (to a certain extent) (Hyde, 2000).

In this research, the researcher avoided the use of the deductive approach in the absence of any existing global level data protection mechanism. The testing of any available global level data protection framework not considered as it was not a requirement in the researcher's remit. The primary aim of this research is to develop a Policy Acceptance Model that would assist the process of developing a global level data protection mechanism. The growing usage of innovative technologies to tackle the pandemic continued, the reliance on technology increased, and that called for an increased level of personal privacy protection.

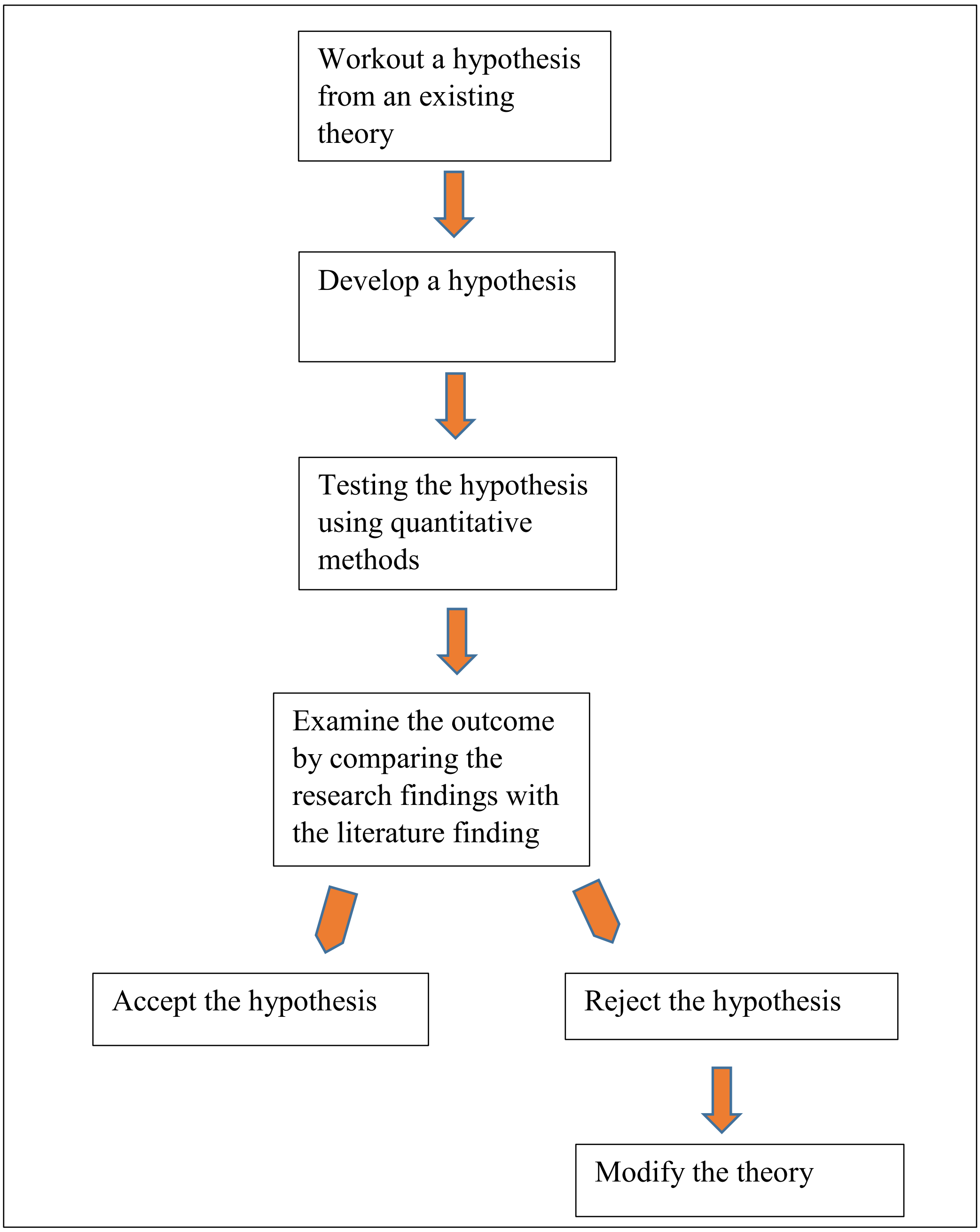

Workout a hypothesis from an existing theory
Develop a hypothesis
Testing the hypothesis using quantitative methods
Examine the outcome by comparing the research findings with the literature finding
Accept the hypothesis
Reject the hypothesis
Modify the theory

Figure 3.2: Deductive approach summary (Researcher, 2021)

3.3.2 Inductive approach

The inductive approach, also known as inductive reasoning, starts with the observations and theories proposed towards the end of the research process resulting from observations (Dudovskiy, N.D., Inductive Approach (Inductive Reasoning)). This approach aims to collect data sets to identify patterns and relationships to develop a theory (Streefkerk, 2019). The inductive approach begins with a topic. The application of the inductive approach relates to qualitative methods of data collection and data analysis (Soiferman, 2010, P.10) The researcher intends to develop empirical generalisations and identify preliminary relationships through the research process (Soiferman, 2010, P.18). The researcher could not find hypotheses at the initial stage of the research and was unable to establish the type and nature of the research findings until the completion of the research (Dudovskiy, N.D., Inductive Approach).

In this research, the researcher used a step-by-step approach, and to begin with decided on the topic, then conducted an intensive literature review to identify the patterns in the available literature, developed a tentative hypothesis leading to the development of the theory/model (See figure 3.3).

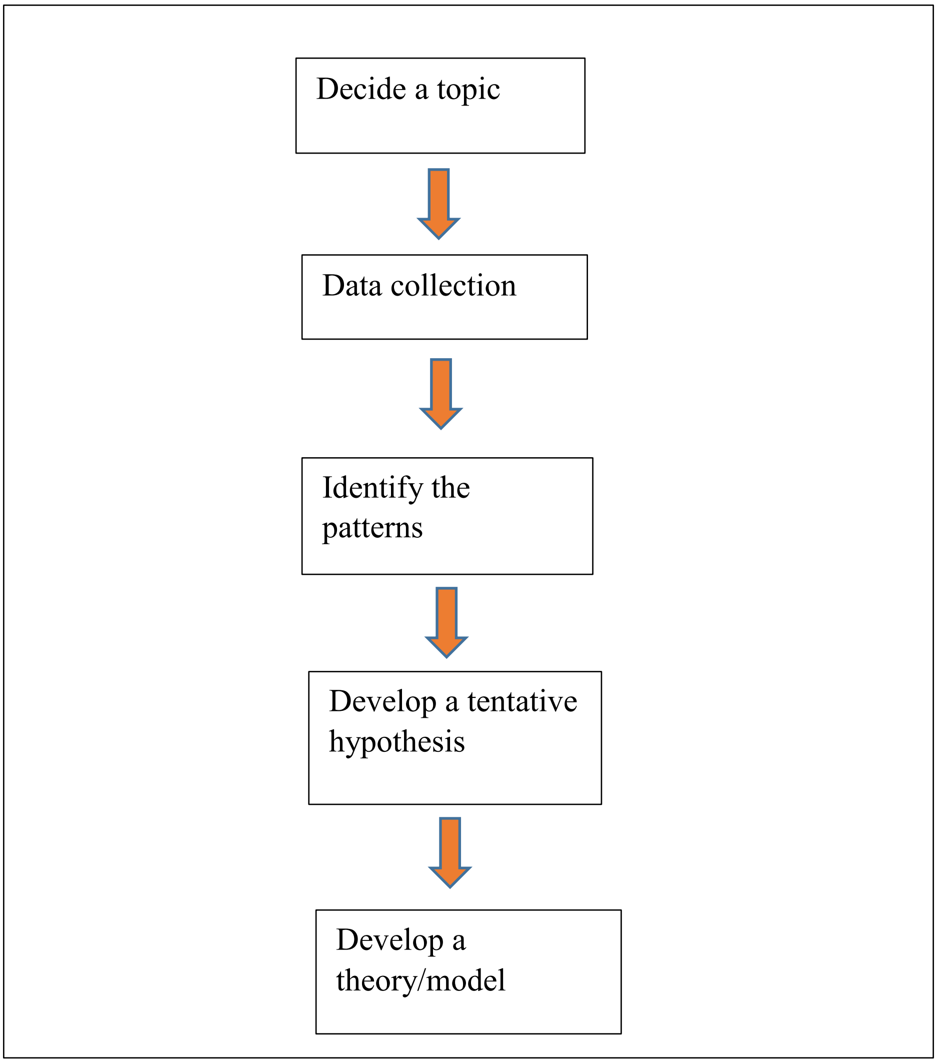


Figure 3.3: Inductive approach summary (Researcher, 2021)

3.3.3 Abductive research approach

This approach was developed as an alternative to inductive and deductive approaches. In the abductive approach, the research process starts with unexpected facts and the researchers look for explanations during the process (Dudovskiy, N.D., Abductive reasoning (abductive approach) (See figure 3.4). In the process of following an abductive approach, the researcher looks for the best possible explanation, both qualitative and quantitative methods can be used Mitchell, 2018, P. 106).

The researcher avoids this approach as it allows the researcher to relate one/few theories to the observation, but not to all. i.e. imagine the researcher observed different patterns in answering the question on the level of training received; it is difficult to believe that all the participants who claimed they did not receive regular training were because the organisation had no budget allocation. There is also the possibility that the organisations did not prioritise training on protecting personal information. Likewise, there could be many facts that contribute to the observation. Therefore, despite many possible explanations for any physical process, if the researcher tends to accept a single/ a few explanation/s for this process, the outcome will not have a high accuracy.

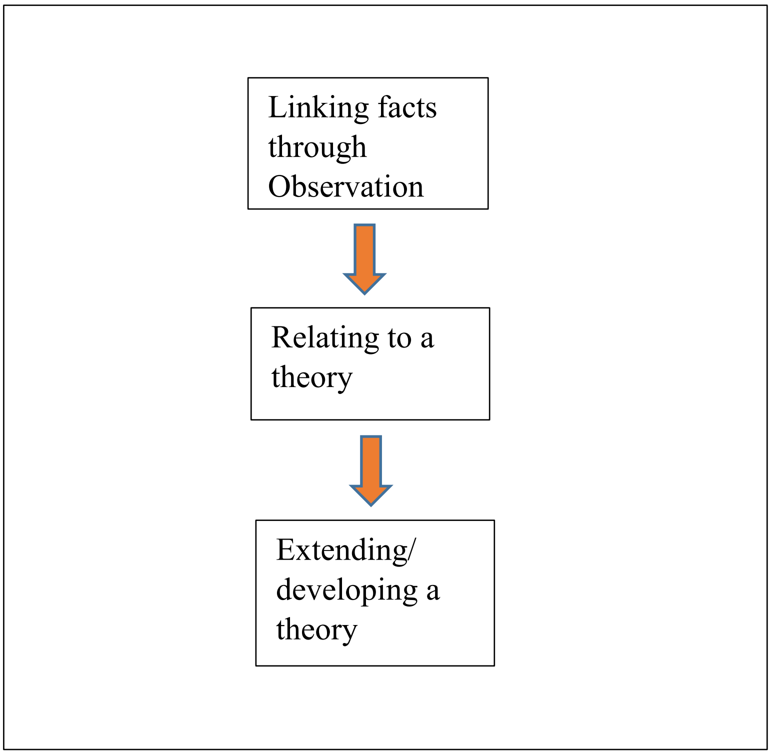

Linking facts through Observation
Relating to a theory
Extending/ developing a theory

Figure 3.4: Abductive approach summary (Researcher, 2021)

3.4 Data analysis method

Data analysis is the process of analysing collected data to extract insights that support decision-making (Calzon, 2021). There are several methods and techniques to perform analysis depending on the scope and the aim of the research. The two main methods of analysis are; (Calzon, 2021).

1. Quantitative data analysis
2. Qualitative data analysis

3.4.1 Quantitative data analysis

Quantitative data analysis is used to provide answers to questions such as who?, when?, where?, what? and how many?, and it explains a certain phenomenon, or it helps to make predictions (Formplus Blog, N.D). The quantitative data analysis techniques focus on the statistical or numerical analysis and deal with large datasets (Stevens, 2021). These findings are easy to present, summarize, compare, and generalize, and that is a good advantage of this method (Formplus Blog, N.D). For this research, the researcher completed a questionnaire using a sample of 233 participants; and for the analysis, the researcher categorised the responses based on gender, age, experience, and their employment in the industry. The findings were presented using descriptive analysis in columns and bar charts to identify the difference between the categories.

3.4.2 Qualitative data analysis

This approach mainly answers the questions such as ‘how’ and ‘Why.’ Qualitative studies aim to obtain a greater level of understanding and use smaller samples to build theories (Sobh and Perry, 2006, P. 1194). However, considering the sample size (of the research) the researcher decided not to conduct interviews but did collect data through existing documents. The intention was to get an in-depth understanding of the national and regional level data protection mechanisms and the challenges faced by the countries in developing data protection mechanisms. Based on the readings, the researcher developed a questionnaire to collect public opinion and an understanding of the factors the respondents would have considered most appropriate and important in developing a global level data protection mechanism to safeguard privacy of the individuals. Following a quantitative analysis, based on the findings derived from the responses, the researcher developed the discussion and produced the model (See chapter 5).

In developing the Policy Acceptance Model the researcher referred to existing Technology Acceptance Models (TAM) which includes TAM by Fred D. Davies (1989) (Surendran, 2012) (See figure 5.18), the final version of TAM (Venkatesh and Davis, 1996) (See figure 5.19), TAM 2 (Venkatesh and Davis (2000) (See figure 5.20), the Unified Theory of Acceptance and Use of Technology (UTAUT) (2003) (Alwahaishi and Snasel, 2013, P.25-39) (See figure 5.21), TAM (Mc Farland and Hamilton, 2006) (See figure 5.22) and TAM 3 (Venkatesh and Bala, 2008) (See figure 5.23).

TAM is an information systems theory that illustrates how users come to accept and use a particular technology (Surendran, 2012, P. 175). The model sets out several factors that influence the user make decisions to use the right technology for a chosen purpose. Technology Acceptance Models and theories have been applied in a wide variety of domains to understand and to predict user behaviour such as voting, dieting, family planning, blood donation, women's occupational orientations, breast cancer screening, mode of transport preferences, family planning, education, consumer choice and computer usage (Taherdoost, 2017, P.961).

The publications available show that TAM has been applied to different sectors. One such case is the investigation of the adoption by the banks and, acceptance by the bank customers of internet banking in the sultanate of Oman, authored by Bassam Khalil Hamdan Tabsh under the supervision of Dr Jason Williams (Tabsh, 2012). Also, there had been others, Alice M. Johnson had used the TAM as a basis for studying factors that might motivate organizations to invest (or not to invest) in information security (Johnson, 2005); Sek et al had used TAM to make predictions on User Acceptance and Adoption of Smart Phone for Learning (Sek et al., 2010); and Rauniar et al had used TAM in their paper titled social media usage: an empirical study on Facebook (Rauniar et al., 2013).

In this research, the researcher relied on both Qualitative and Quantitative data analysis. The researcher used Qualitative data analysis to get an understanding of the research background. This was considered necessary to identify the research gaps in the design stage of the questionnaire. Following the literature survey, the questionnaire was designed to validate the accuracy and timeliness of the factors, based on the identified key challenges to developing a data protection mechanism. Thereafter the Quantitative analysis was used to analyse the responses to identify the factors for consideration in the development of a global level data protection mechanism. Any research study intended to address contemporary issues could use both qualitative and quantitative data analysis to develop contemporary solutions.

This chapter consists of the introduction and the justification for the research approaches selected by the researcher. The research philosophy used by the researcher is Pragmatism, and it explains how data was collected, analysed, and used in this research. The researcher selected the inductive research approach to explain the step-by-step procedure to demonstrate how the research problems were addressed. Primary data collection method was used to collect data. The Qualitative data collection method was used to understand the commitments made by the countries at the national and regional level and to identify the barriers to developing data protection mechanisms, whilst the Quantitative method was used to verify the referenced literature and to gauge the public opinion. The researcher relied on both Qualitative and Quantitative methods to analyse the collected data. The Qualitative data analysis was used to get an understanding of the research background. Thereafter the Quantitative analysis was used to analyse the responses to determine the factors for consideration in the development of a global level data protection mechanism.

CHAPTER FOUR

RESULTS

4.1 Sri Lanka (Overview)

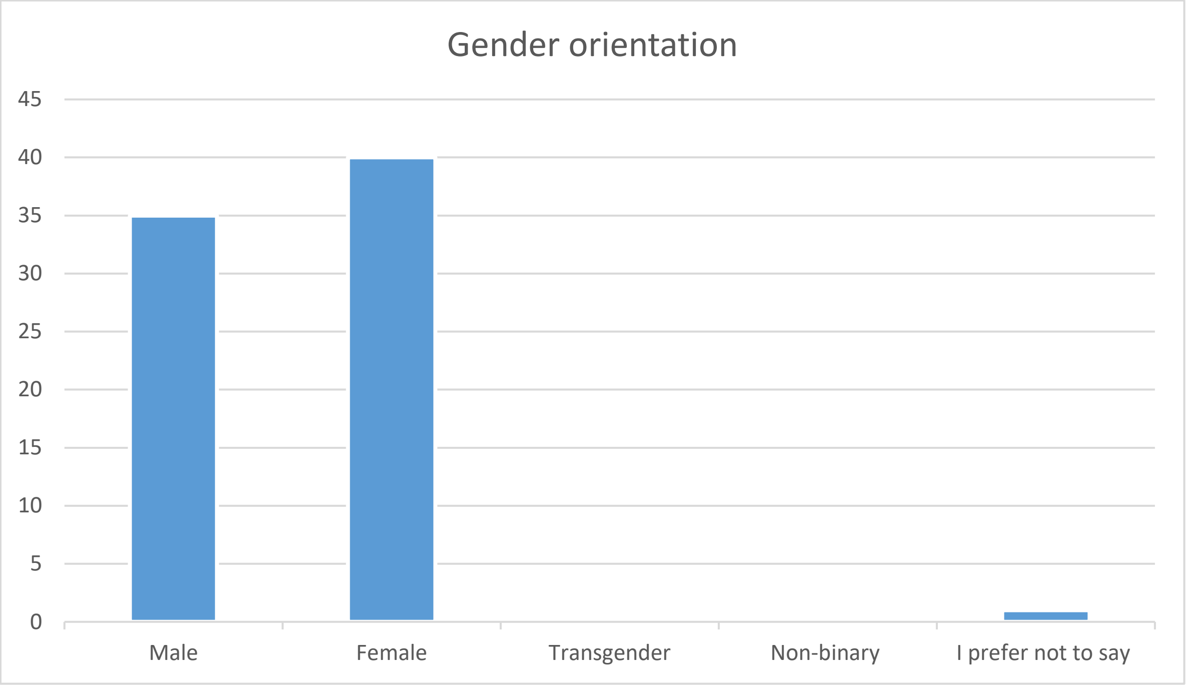


Figure 4.1: Gender orientation (Overview-SL)

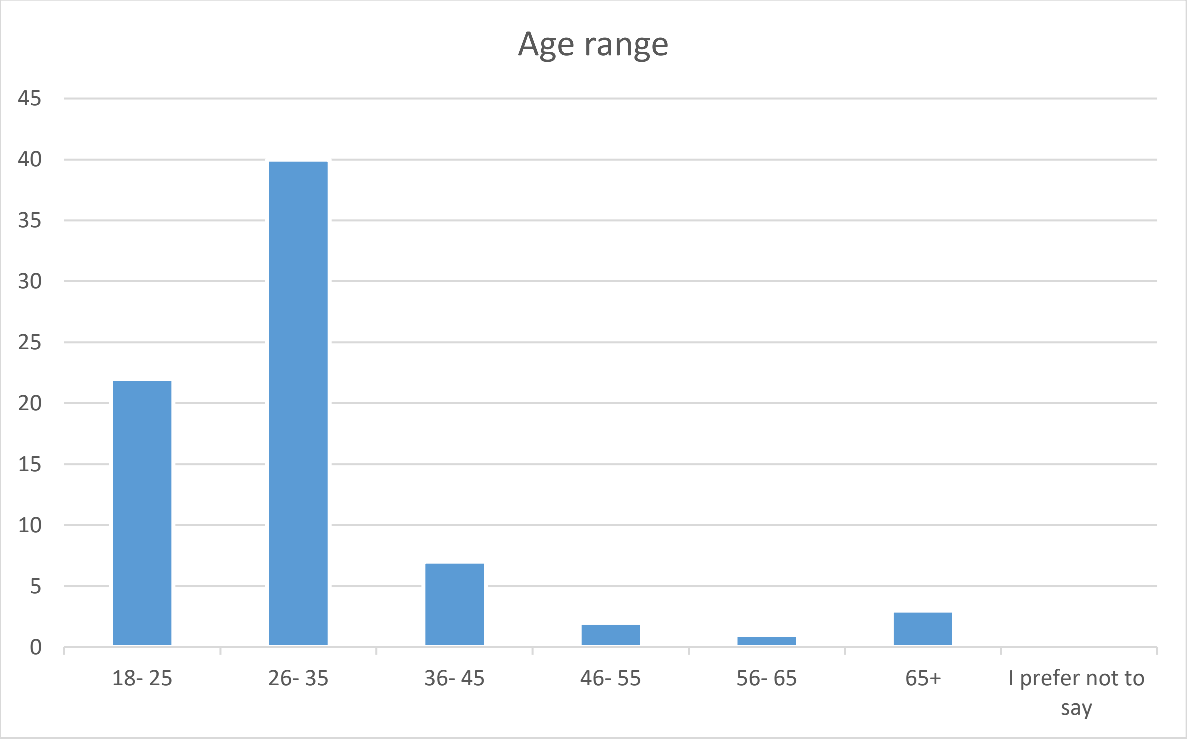


Figure 4.2: Age range (Overview-SL)

This analysis is based on the responses received from Sri Lankans. There were 76 participants, made up of 35 males, 40 females and 1 prefer not to say (See figure 4.1). Their age range spanned between 18-65, in groups of; 22 in the 18-25, 40 in the 26-35, 7 in the 36-45, 2 in the 46-55, 1 in the 56-65 and 3 in the 65+ range (See figure 4.2). There is a good gender balance, and most importantly, the participants are scattered into different age groups.

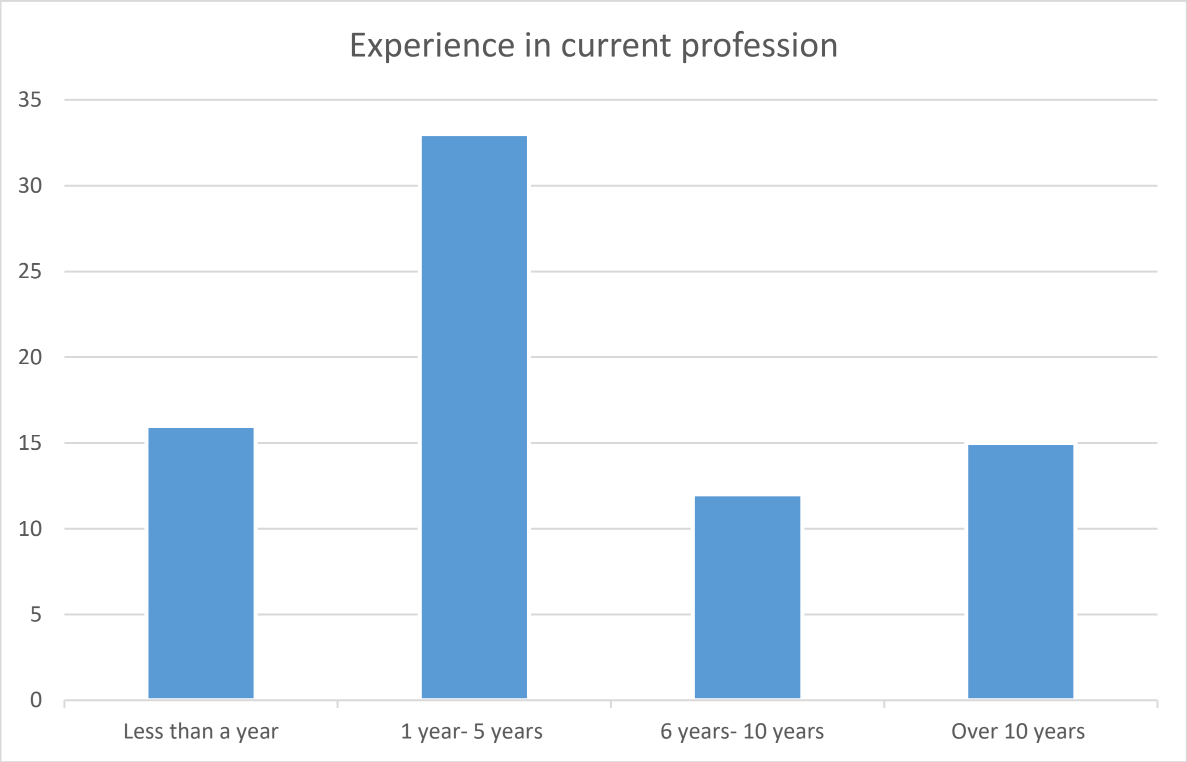


Figure 4.3: Experience in current profession (Overview-SL)

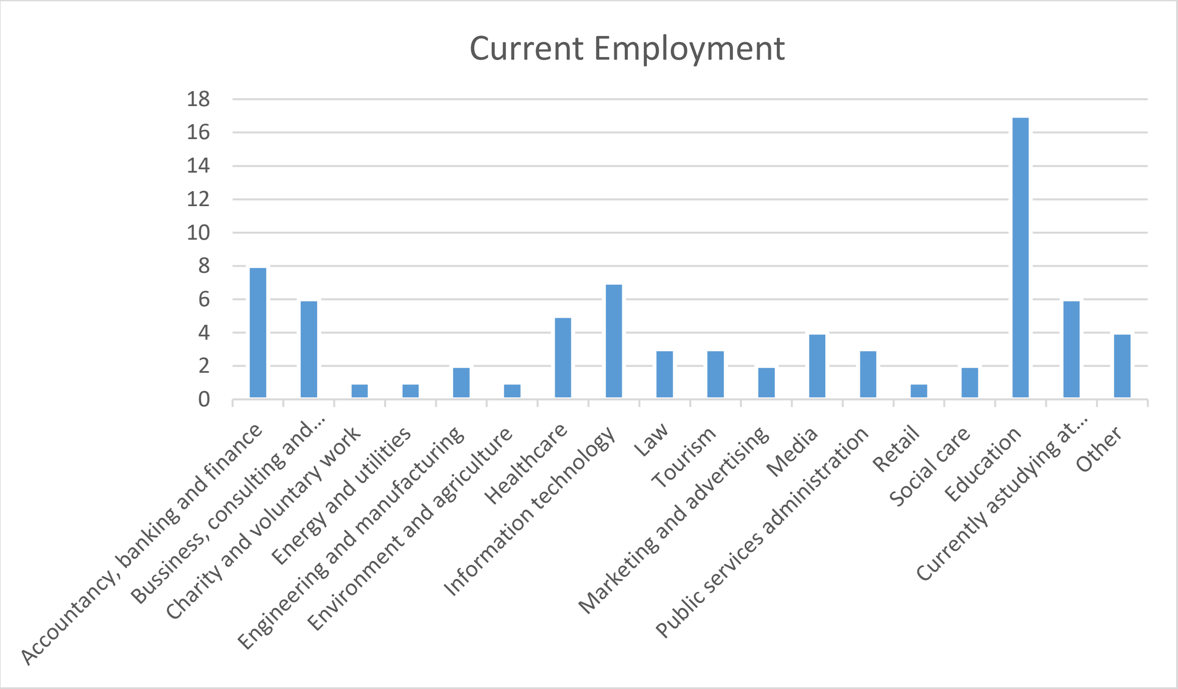


Figure 4.4: Current employment (Overview-SL)

The employment status of the participants and their experience in the industry has also been considered by the researcher. According to the responses, 16 have worked less than a year, 33 between 1-5 years, 12 6-10 years and 15 over 10 years in different industries (See figure 4.3). Notably, the majority of the participants in the 18–35 age range spent 1-5 years (See figure 4.3) in employment in different organisations (See figure 4.4). Noted with interest is the presence of undergraduate or postgraduate level employees amongst the participants. This will help the researcher to analyse and identify whether there are any disparities and similarities in their understanding of the importance of developing a global level data protection mechanism and the barriers they believed to have based on gender, age, experience or the profession.

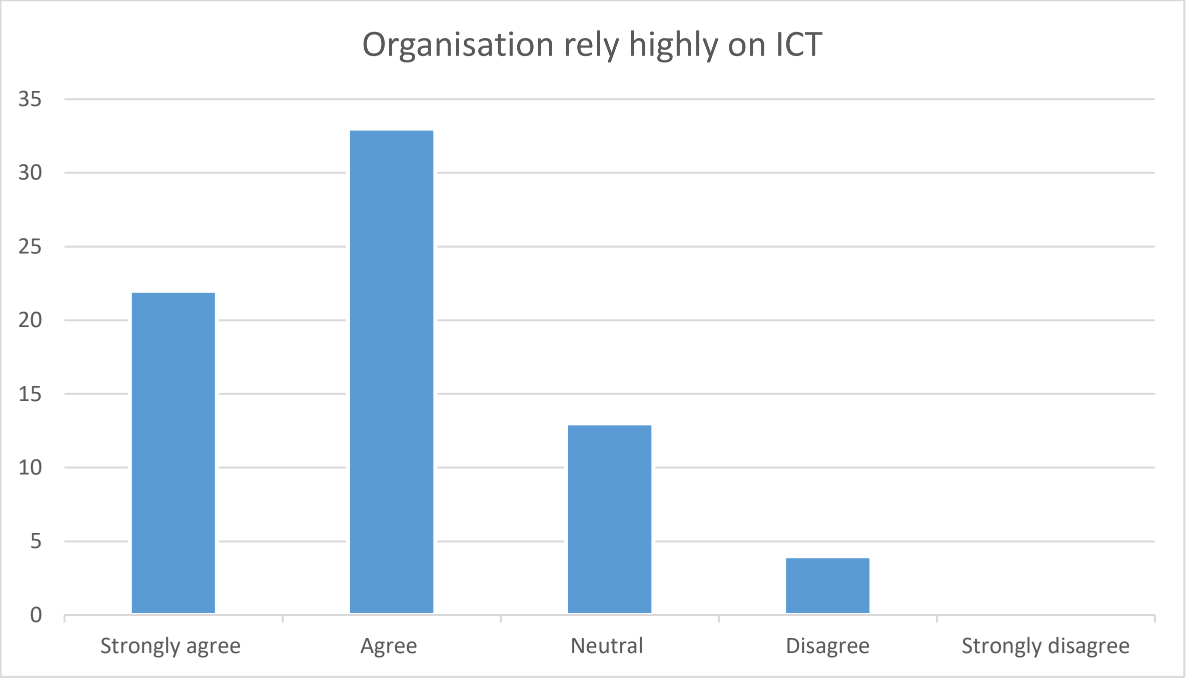


Figure 4.5: Organisation rely highly on ICT (Overview-SL)

The observed high reliance on ICT by the majority is of importance (See figure 4.5). The 4 disagreed make little impact. The inferences drawn from this set of samples show a gender balance between males and females (See annexe C.6). Sri Lanka has made impressive strides in the field of evolving technology, and its increasing reliance on modern computers and Information Technology feature prominently right across the government and the private sector alike. The increasing reliance on ICT and other technologies make organizations more vulnerable and prone to cyber-attacks. In recent years, Sri Lanka has had cyber attacks both on the government and private sector (See annex C.5).

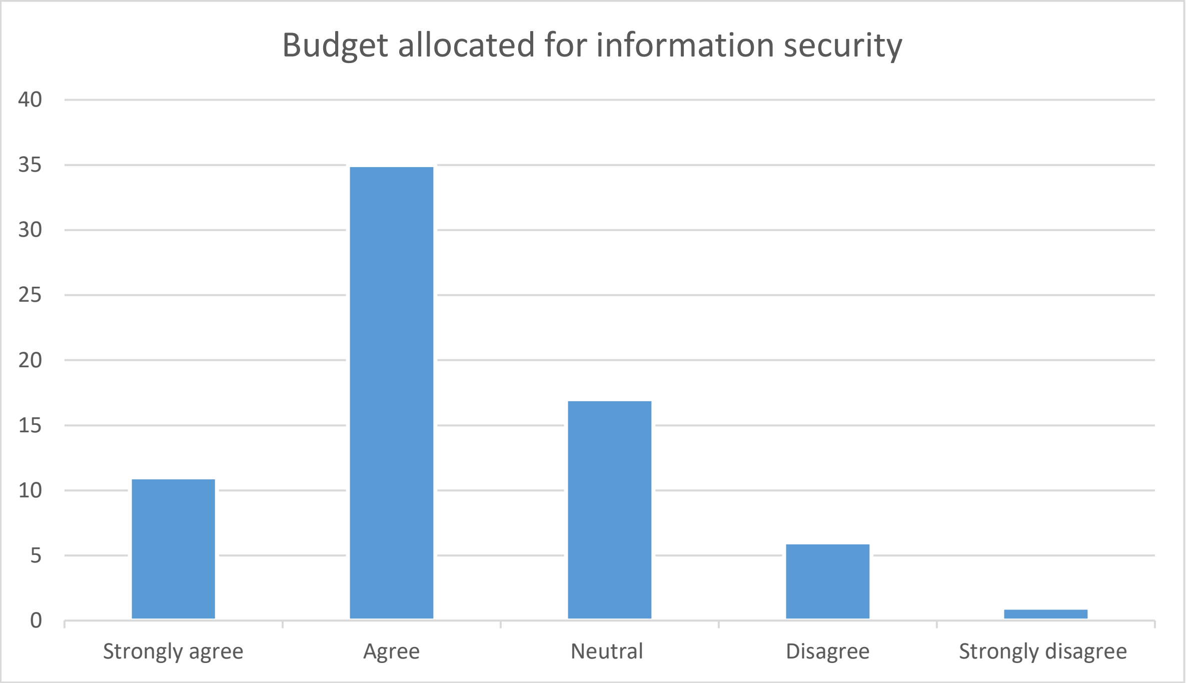


Figure 4.6: Budget allocated for information security (Overview-SL)

A mixture of responses for this category, 46 of the 76 participants indicating their organisations have an allocated budget for information security; 17 not expressing an opinion either way, 7 disagreeing (See figure 4.6). Having a budget for information security is important given the high reliance on technology and support needed by the staff. However, considering the economic status of countries, there may be some countries who do not have the capacity to have a separate budget for information security. Therefore, due to the nature of the cyber threats, it is important to have collaboration between developed and developing/less developed countries to support each other.

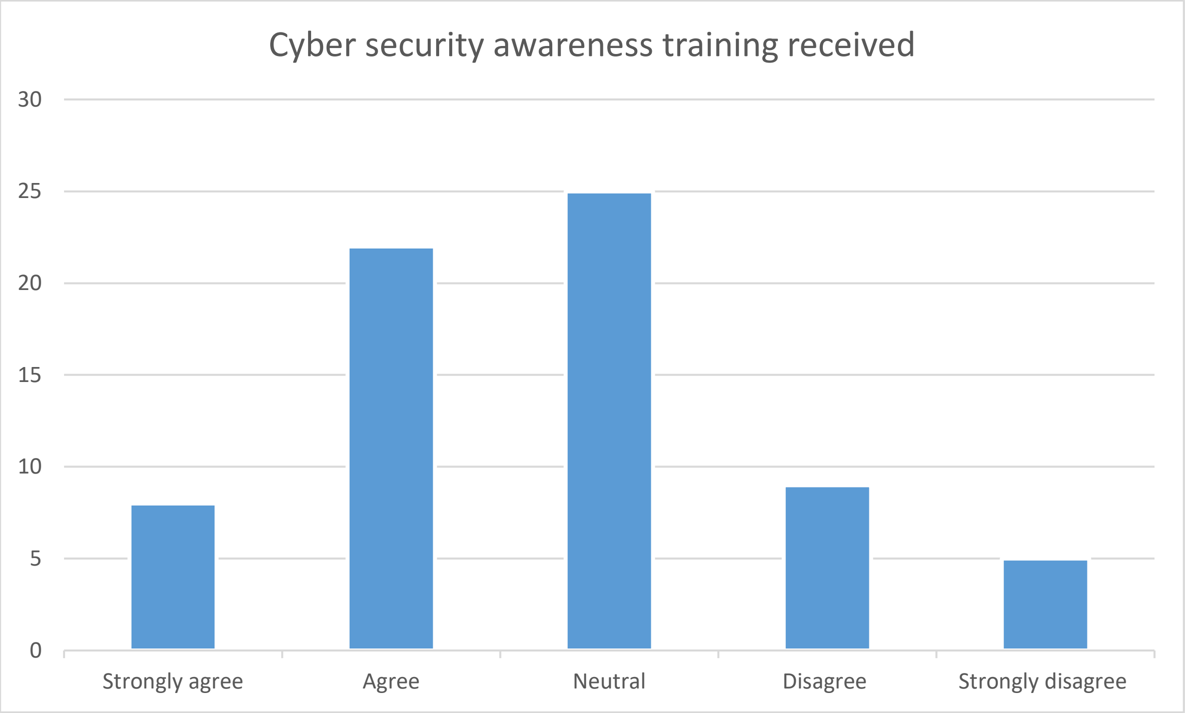


Figure 4.7: Cyber security awareness training received (Overview-SL)

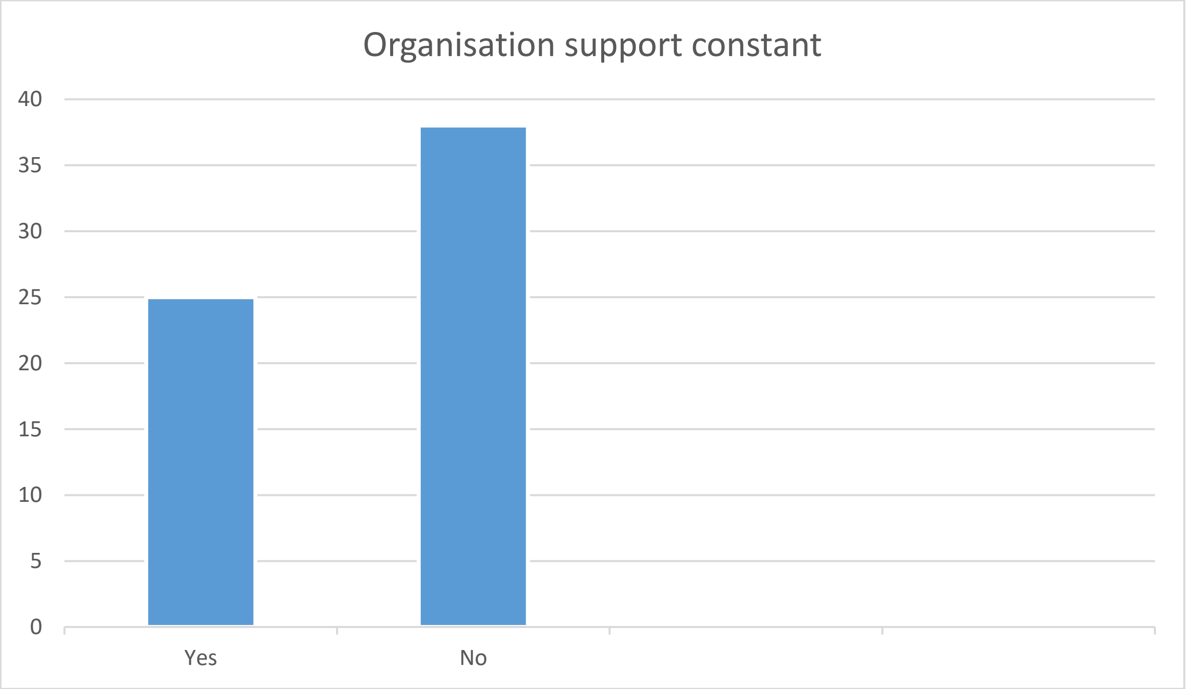


Figure 4.8: Organisation support constant (Overview-SL)

Some participants indicate the inadequacy of regular security awareness training they received balancing against the satisfactory level of resources allocated for information security. Only 30 participants received regular cybersecurity awareness training, 14 participants received none; 25 neither agreed nor disagreed (See figure 4.7). In response to the organisation support to protect personal information, 25 participants claim they did receive support, 38 received none (See figure 4.8). That is a clear indication of the imbalance in organisational support to protect personal information despite the budget allocation for this specific purpose.

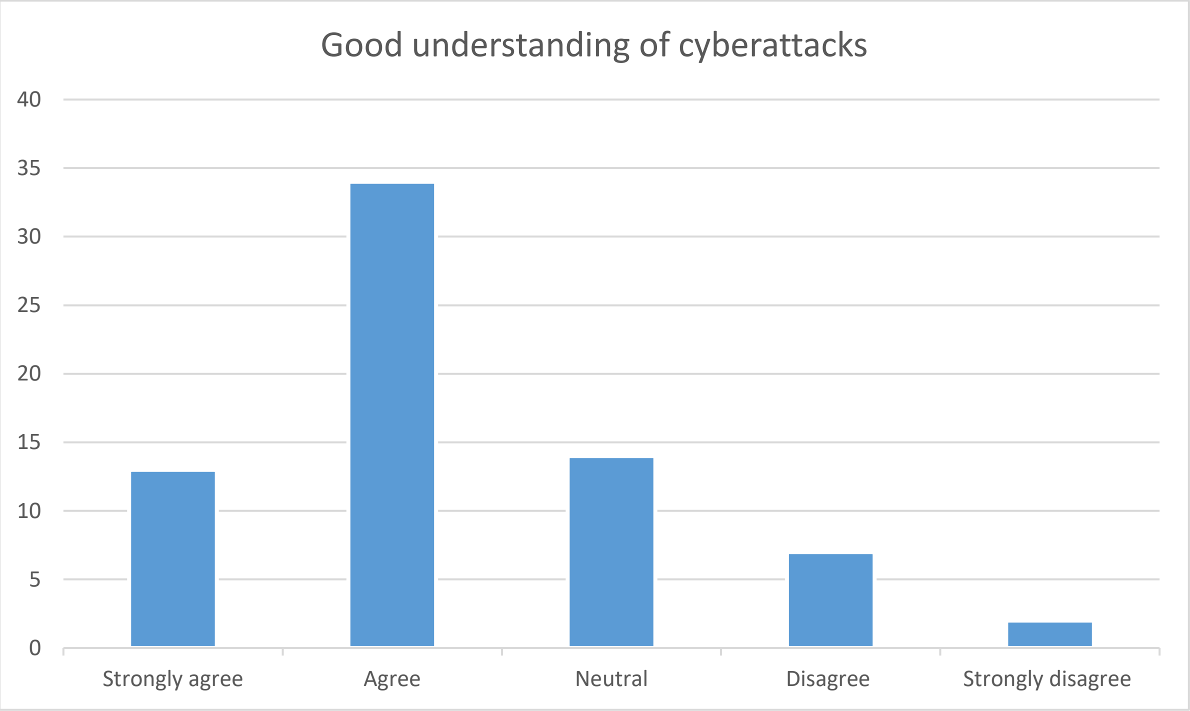


Figure 4.9: Good understanding of cyberattacks (Overview-SL)

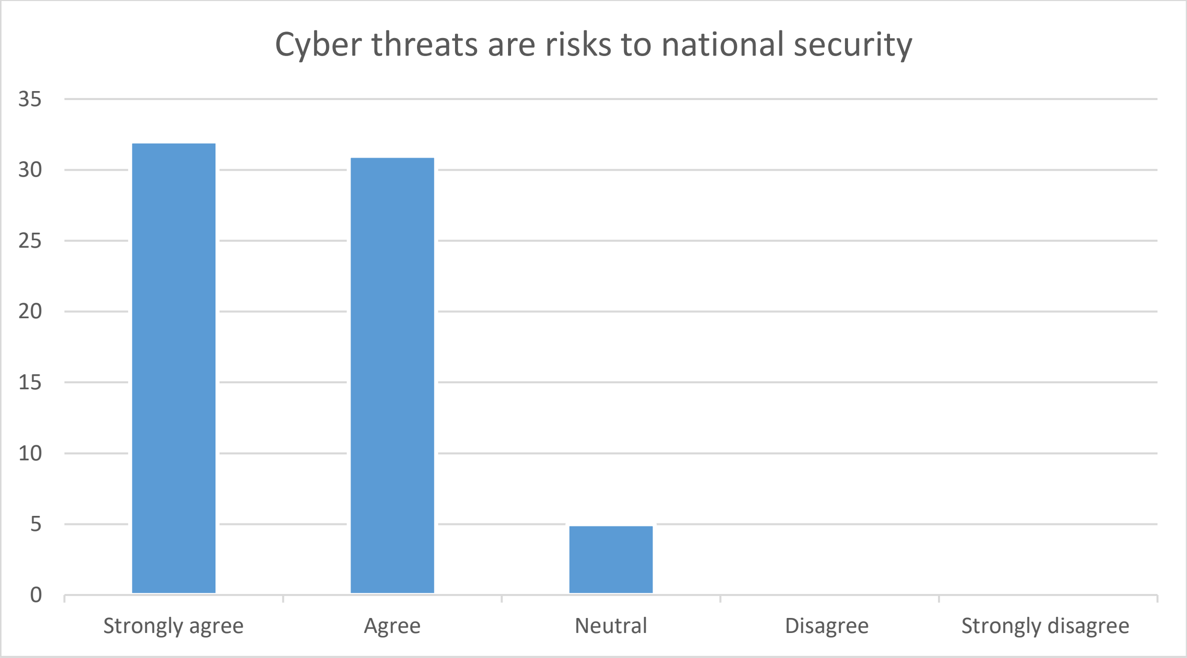


Figure 4.10: Cyber threats are risks to national security (Overview-SL)

Despite the lack of security awareness training, the participants appear to have a high level of understanding of the impact of cyber-attacks on the public and the organisation. 47 participants claim they have, 14 expressed no opinion either way, with only 9 not having any understanding (See figure 4.9). Also, 83 percent of the participants have an awareness of the potential threats to national security from cyber-attacks (See figure 4.10). In general, having an understanding of cyber threats and their impact on national security makes people act responsibly and minimise end-user errors, and their views would count as an influencing voice in accepting and implementing a national, regional and global level mechanism.

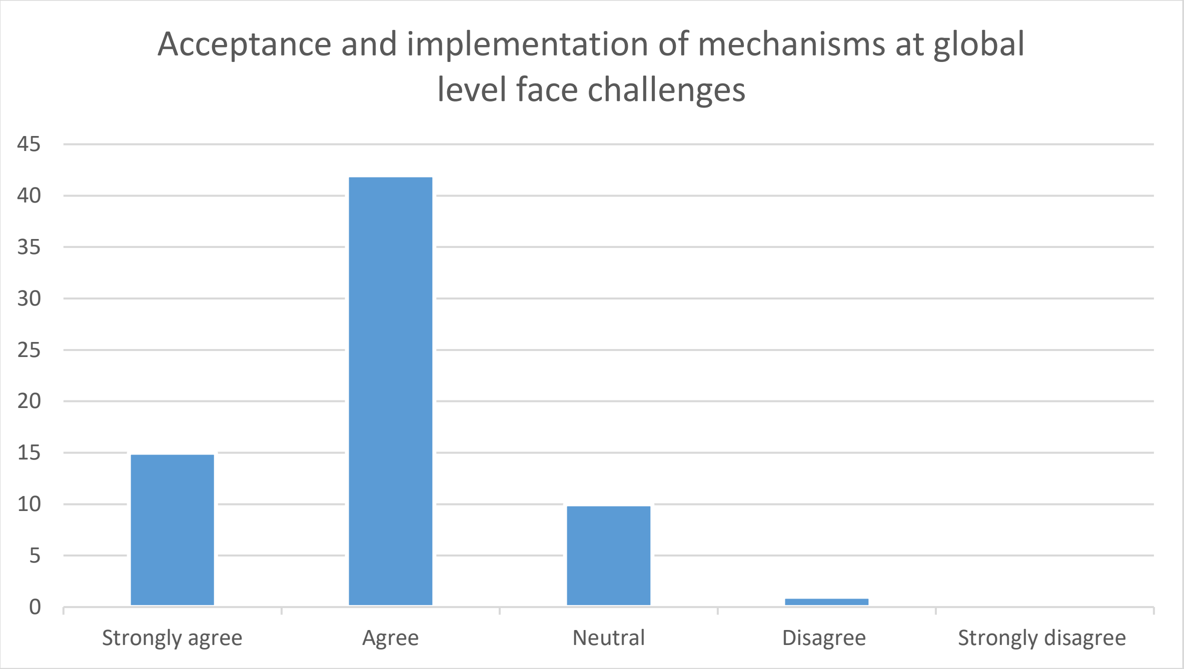


Figure 4.11: Acceptance and implementation of mechanisms at global level face challenges (Overview-SL)

The participants have clearly highlighted that acceptance and implementation of mechanisms at the global level face challenges. 15 strongly agreed, 42 agree, 10 neutral, 1 disagree and no one has strongly disagreed (See figure 4.11). Disagreement showed by one participant is not significant given the significance of the number of participants who have agreed or strongly agreed. The participants have highlighted the factors that affect the challenges to accept and implement a global level mechanism

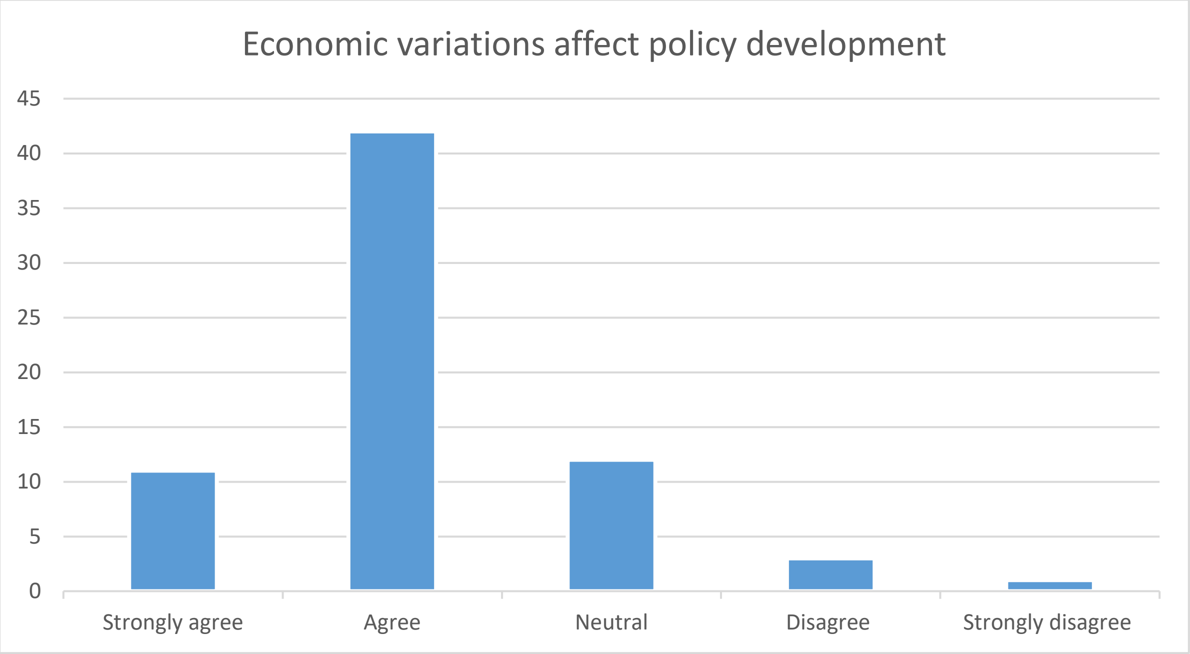


Figure 4.12: Economic variations affect policy development (Overview-SL)

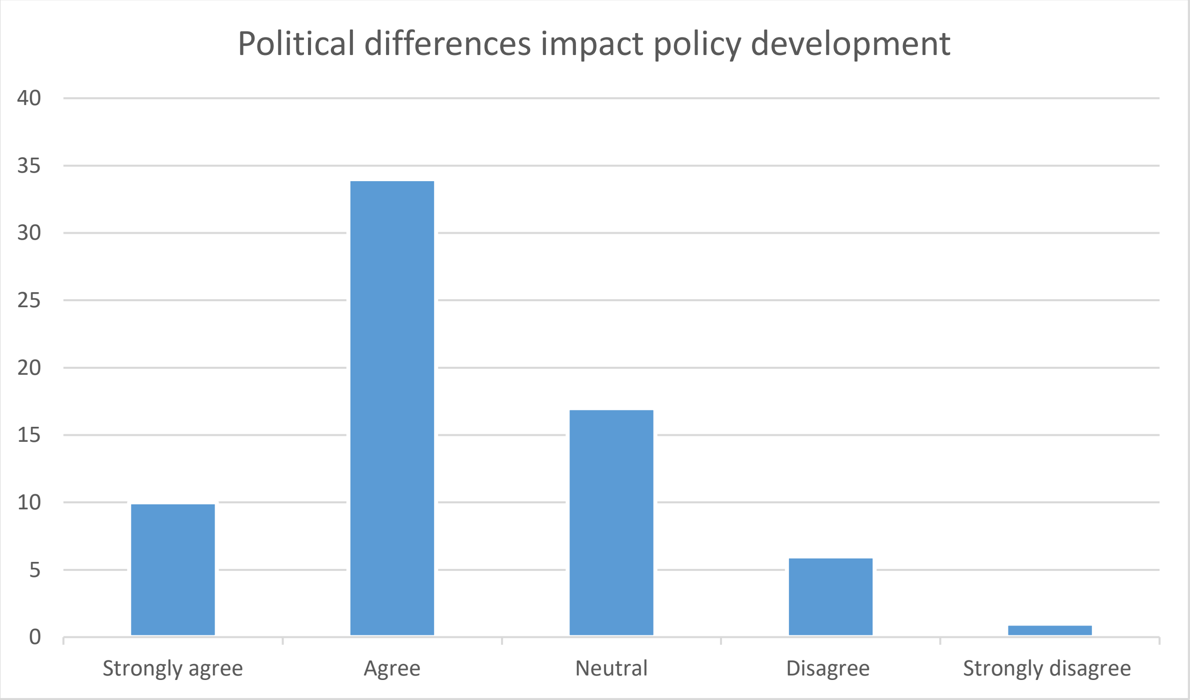


Figure 4.13: Political differences impact policy development (Overview-SL)

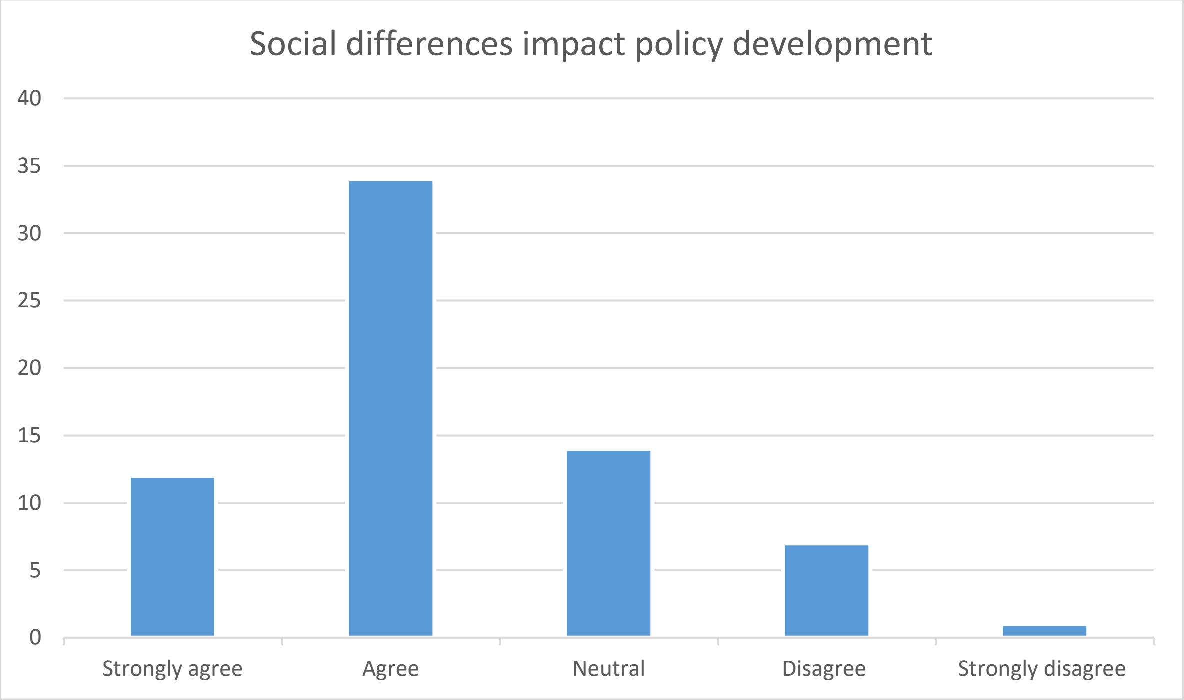


Figure 4.14: Social differences impact policy development (Overview-SL)

The participants agree that economic (See figure 4.12), political (See figure 4.13), and social differences (See figure 4.14) in/amongst the countries have an impact on policy development. This makes it hard for the policy developers to bring all the countries to agree to a unified mechanism. In responding to the questionnaire, the participants have highlighted the types of economic, political and social differences they believe to play a vital role in policy development (See figure 4.15-4.17).

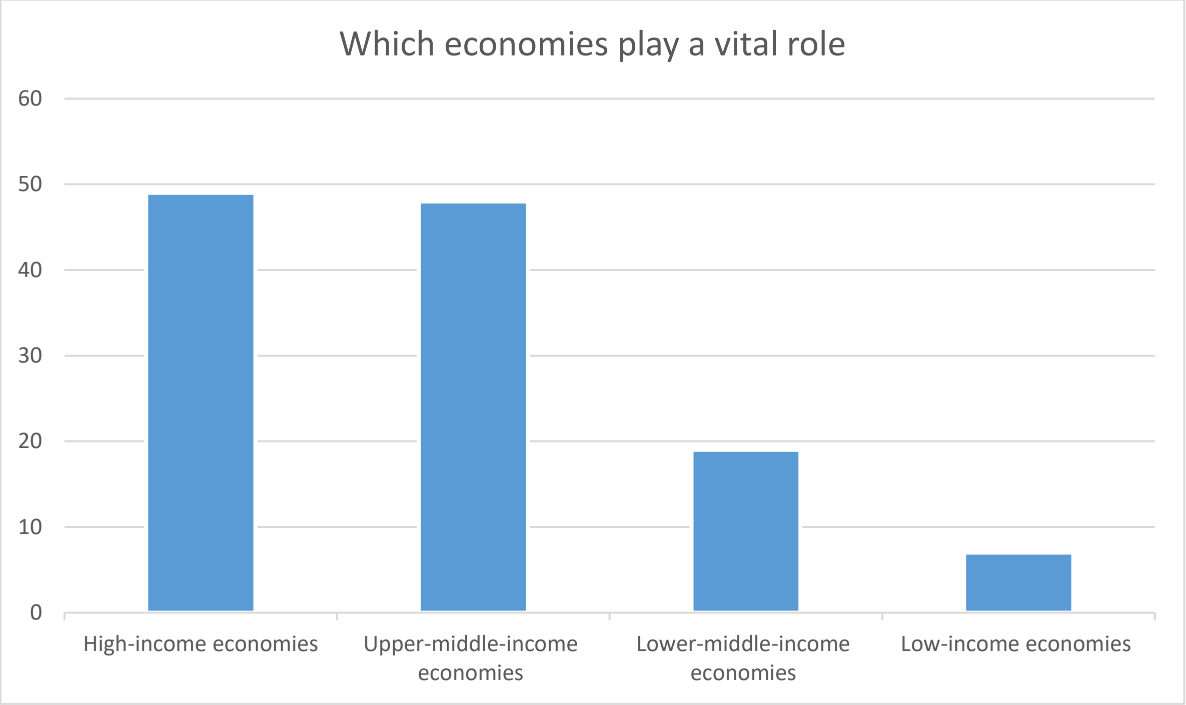


Figure 4.15: Which economies play a vital role (Overview-SL)

In response to the questionnaire, the majority is of the opinion that high income and upper-middle-income countries play a vital role in the policymaking process (See figure 4.15). The key stages involved in the process itself are to identify policymaker aims and the policies to achieve those aims, select a policy measure, identify the necessary resources, and then implementation and evaluation of the policy. These stages are time consuming, costly, and need resources. Therefore, the financial stability of a country counts essential to achieving a successful outcome in policymaking.

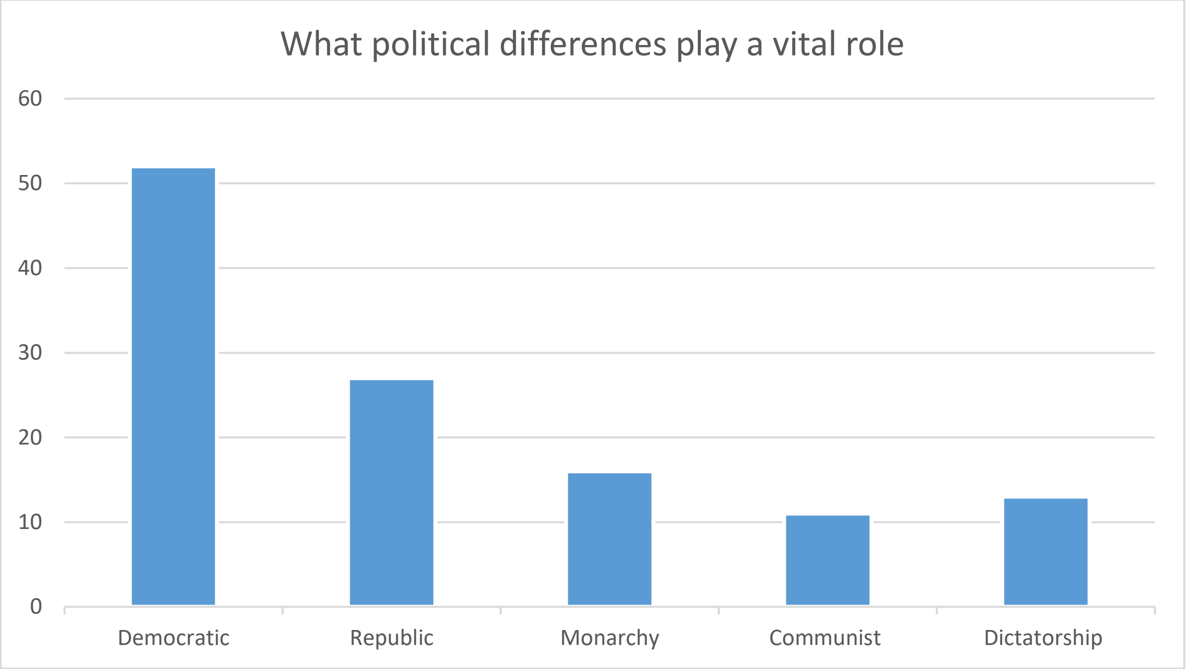


Figure 4.16: What political differences play a vital role (Overview-SL)

The majority favours a democratic political system in preference to other governance systems (See figure 4.16) due to the participatory approach allowing the public to contribute to the policy development process with the assurance of collective responsibility for their actions. This approach creates trust between the organisations and ensures transparency in the policy development process itself.

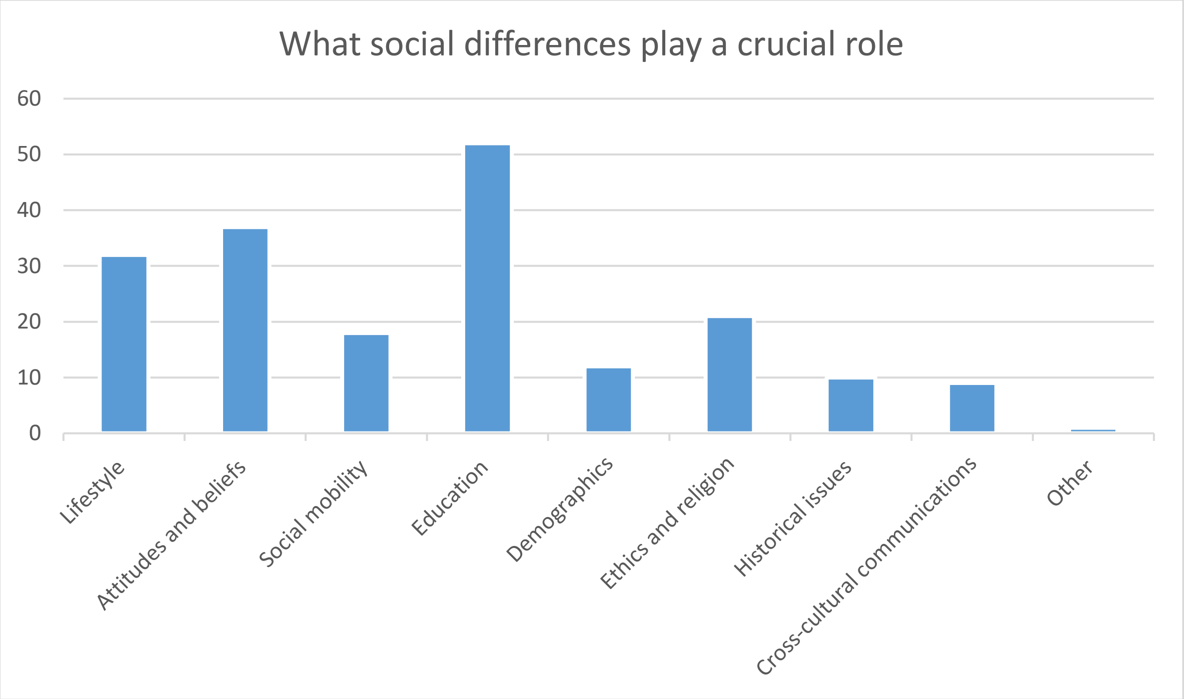


Figure 4.17: What social differences play a crucial role (Overview-SL)

The response to the questionnaire concerning social differences, according to the majority education plays a crucial role. (See figure 4.17). The awareness of potential cyber threats and the impact on people and national security make a strong case for accepting and implementing data privacy and security policies. The education and the provision of cybersecurity awareness training to the employees and the organisations are considered important to avoid end-user errors. It is imperative that awareness training is provided to employees to avoid mistakes from occurring when working from home with added pressures of multitasking workloads especially during the COVID-19 pandemic. In such scenarios, allocation of sufficient time for cyber threat awareness training is crucially important to ensure vigilance to the threats and to safeguard sensitive information of the organisation and their clients. However, in the eyes of the threat actors, there is no exception to the rule whether it is normal or extenuating circumstances, and their focus is on opportunistic vulnerabilities.

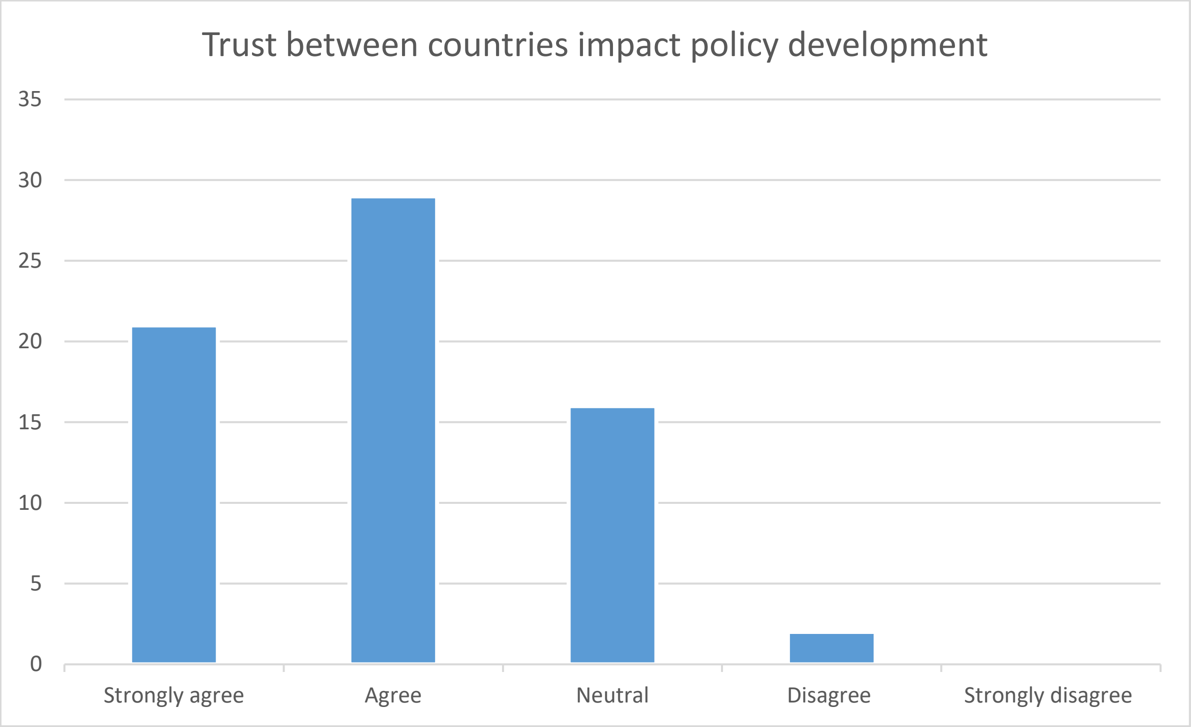


Figure 4.18 : Trust between countries impact policy development (Overview-SL)

The participants have highlighted the importance of trust between countries to a significant level. 21 strongly agree, 29 agree, 16 neutral, 2 disagree, and most importantly, no one has disagreed (See figure 4.18). Even though trust is a significant factor as highlighted by the participants, developing and maintaining trust is a challenging task given the differences amongst countries. However, as highlighted by participants having trust amongst participants would help countries to develop unified global level solutions to protect the personal privacy of the individual.

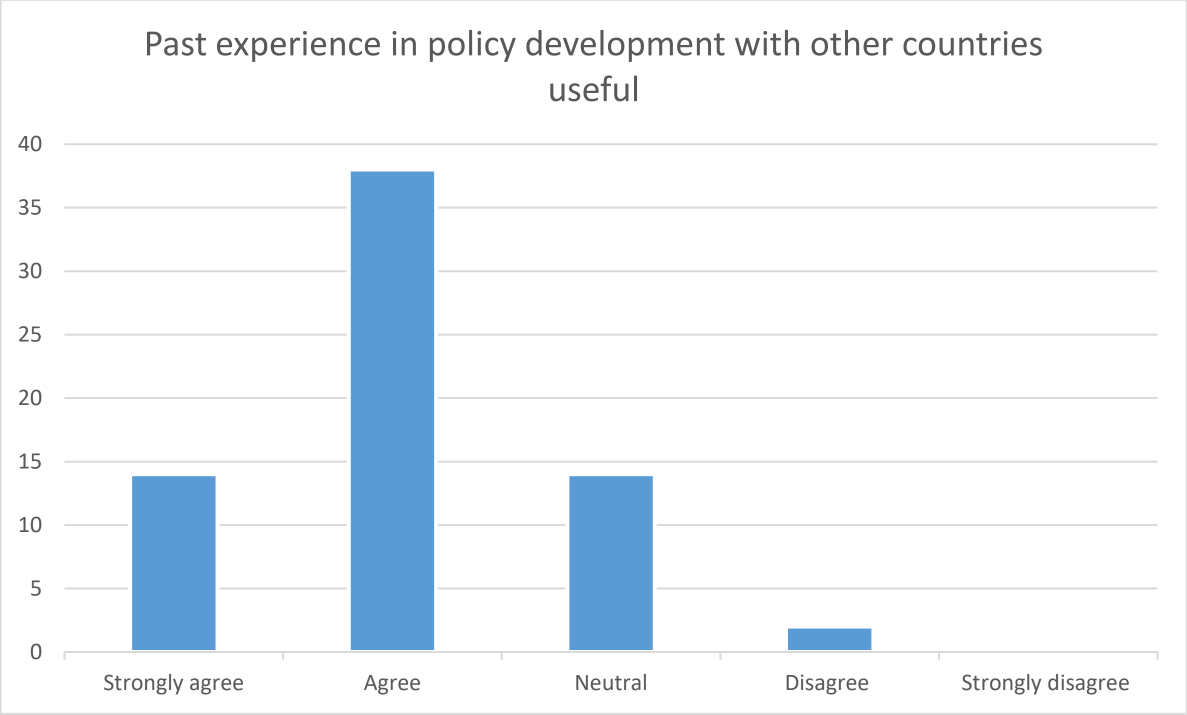


Figure 4.19: Past experience in policy development with other countries useful (Overview-SL)

The participants have highlighted the usefulness of past experience in policy development with other countries. 14 strongly agreed, 38 agreed, 14 neutral, 2 disagree, and no one has strongly disagreed (See figure 4.19). Considering the significant number of strongly agreed or agreed participants number of participants who have disagreed is considerably low.

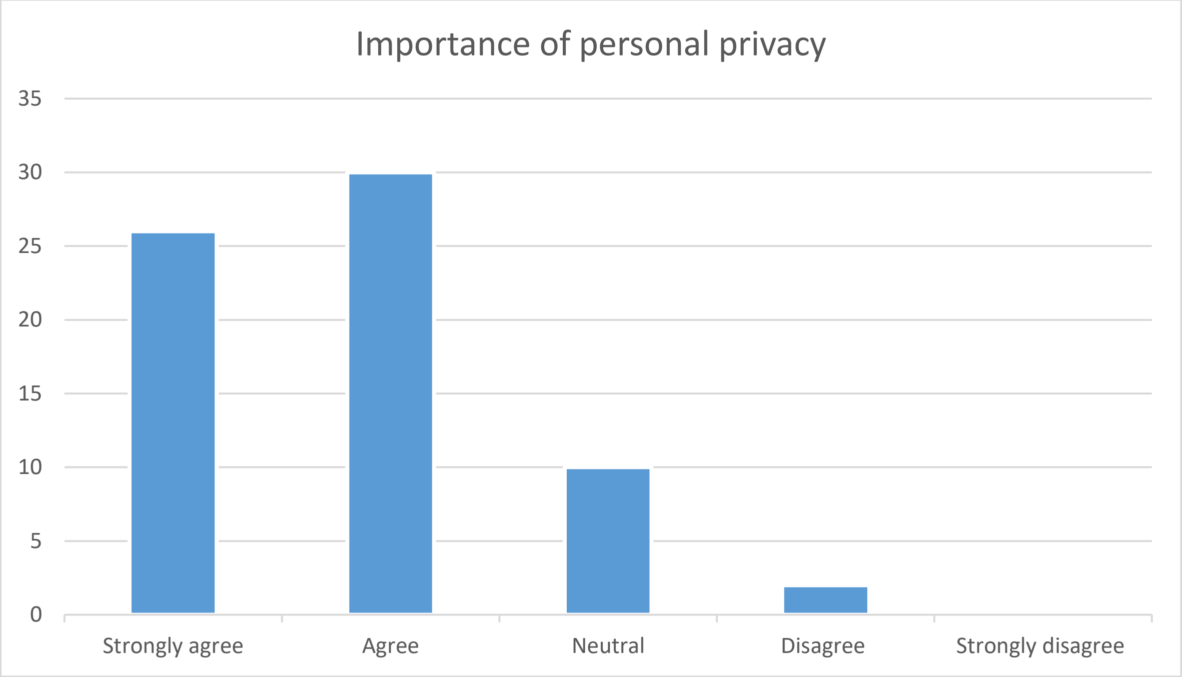


Figure 4.20: Importance of personal privacy (Overview-SL)

A significant amount of participants have indicated that personal privacy is important in accepting a global level data privacy and security policy (See figure 4.20)

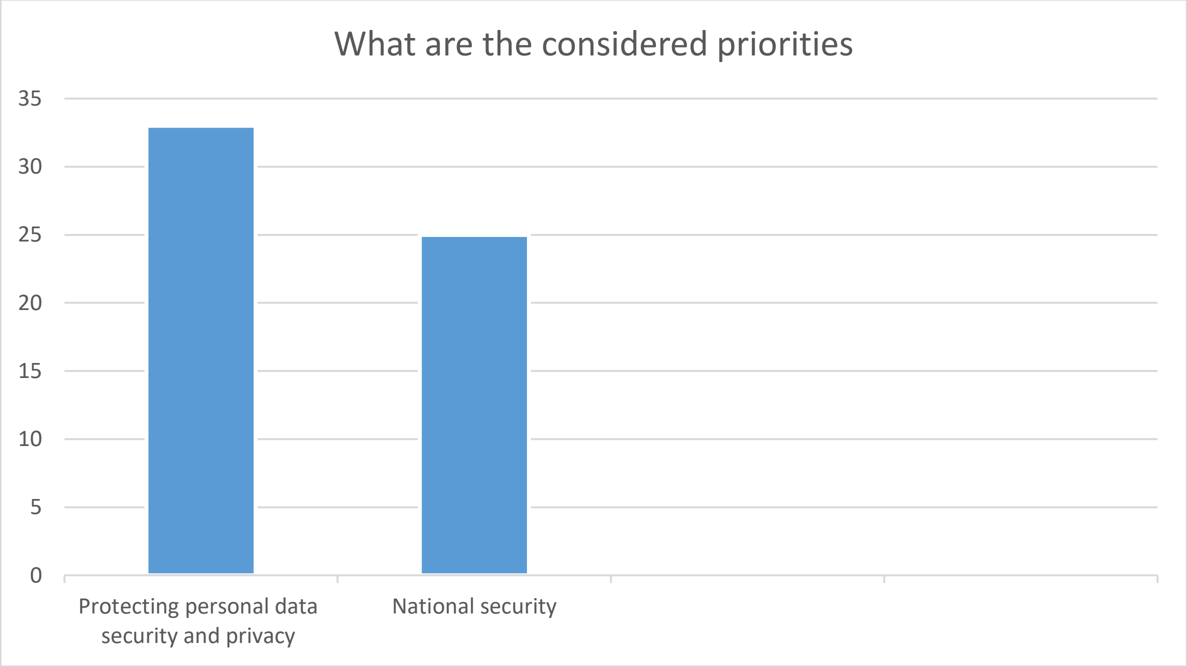


Figure 4.21: What are the considered priorities (Overview-SL)

The notable message coming out of the survey is the higher rating given to the importance of protection of personal data security and privacy over protection of national security when accepting and implementing data privacy and security policies at global level (See figure 4.21). However, in a personal data breach incidence, there is a potential knock-on effect on national security with repercussions felt right across the groups as well as the community alike.

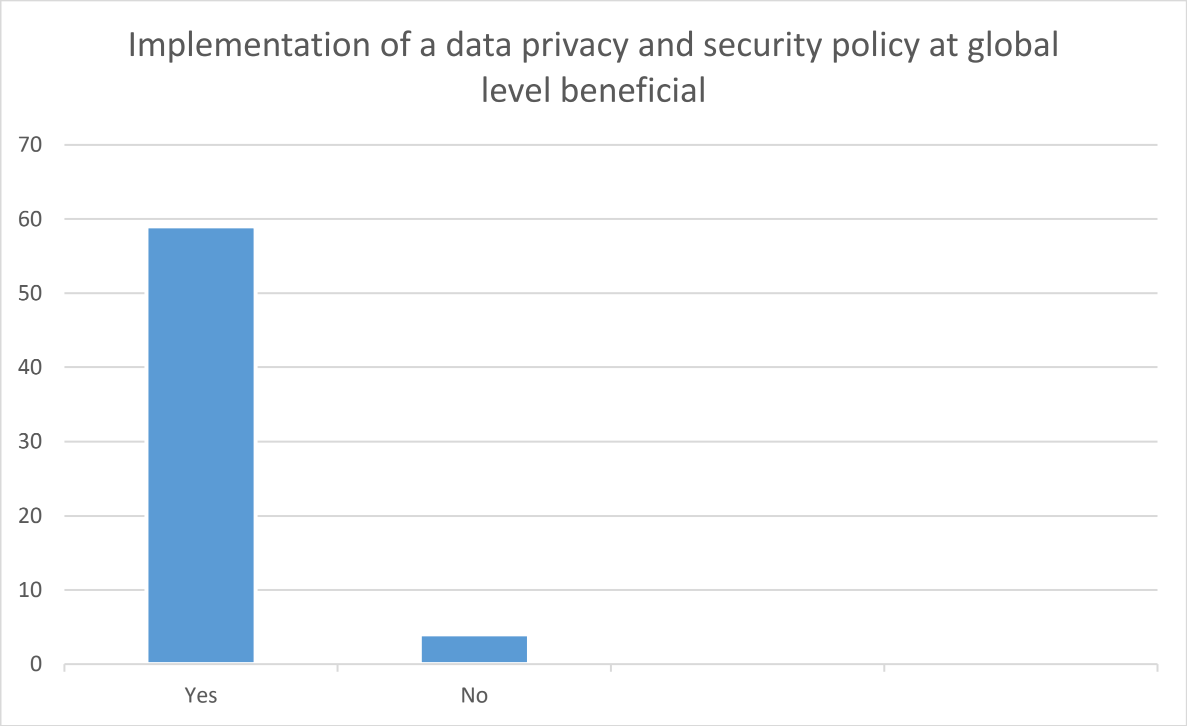


Figure 4.22: Implementation of a data privacy and security policy at global level beneficial (Overview-SL)

The clear message from 78 percent of the respondents is the imperative need to have a global level data protection mechanism (See figure 4.22). This shows that despite the prevailing challenges and differences amongst the countries, participants do strongly believe that it is important to have a global level data protection mechanisms to protect their personal privacy and national security of the country.

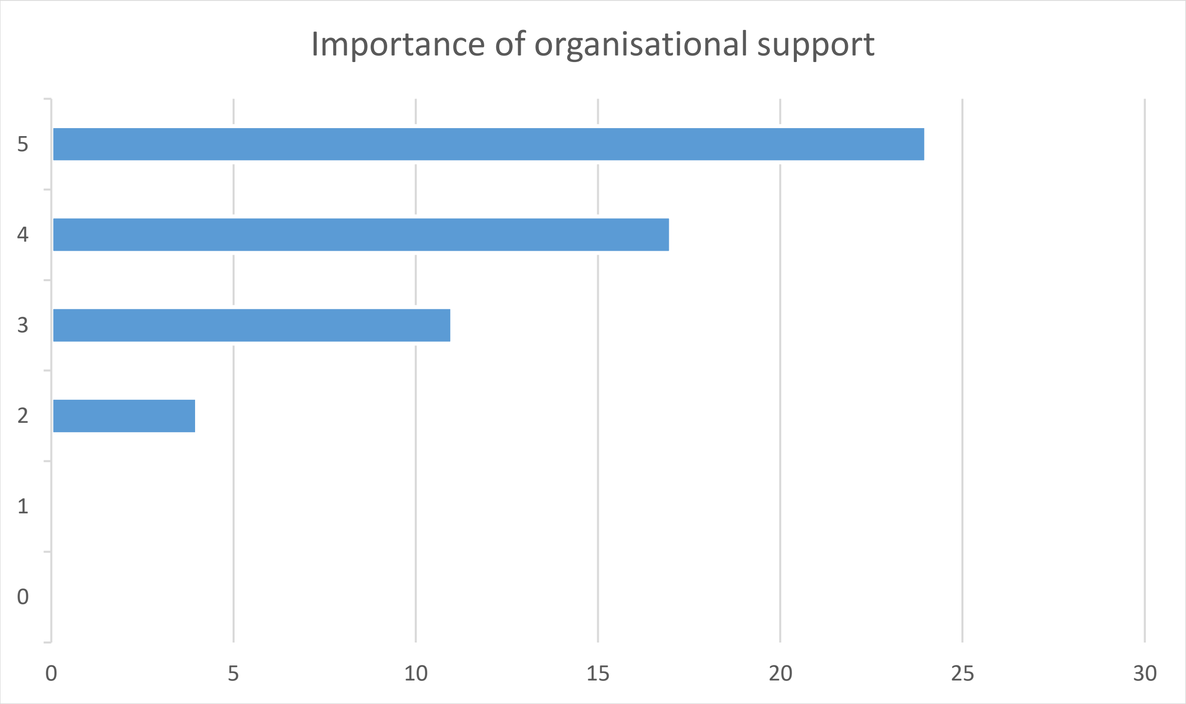


Figure 4.23: Importance of organisational support (Overview-SL)

A significant amount of participants have indicated that organisation support needs to be considered, and it is important in accepting a global level data privacy and security policy.

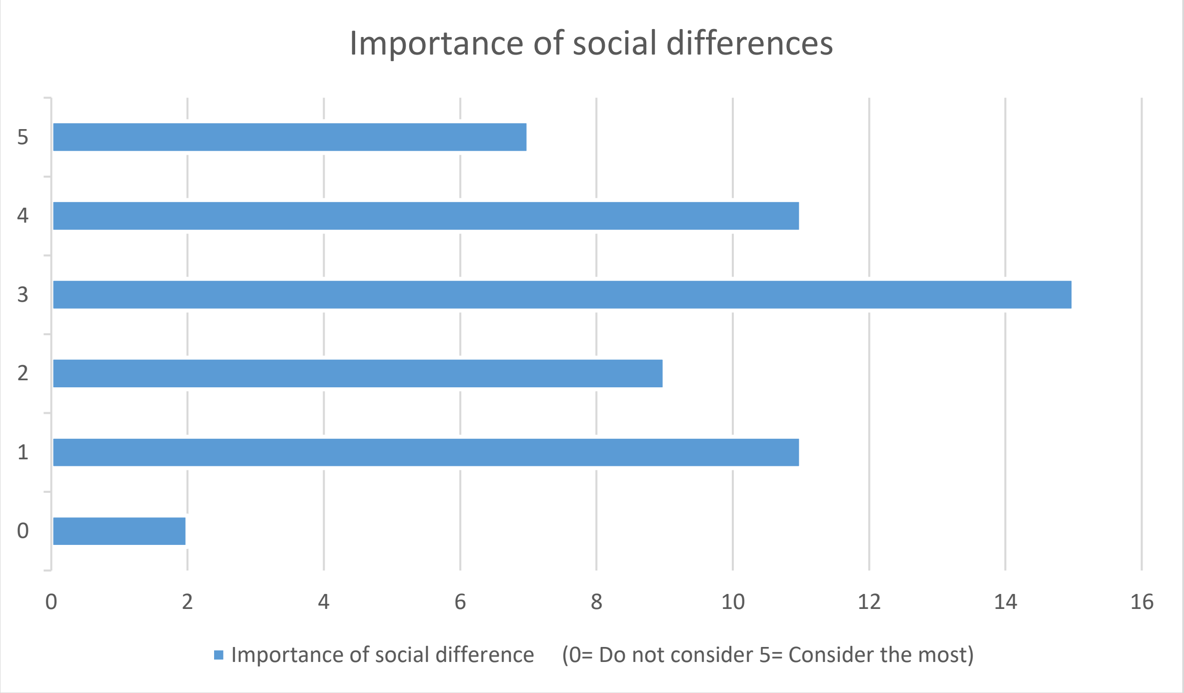


Figure 4.24: Importance of social differences (Overview-SL)

The majority of participants have not indicated that social differences need to be considered, and it is important in accepting a global level data privacy and security policy.

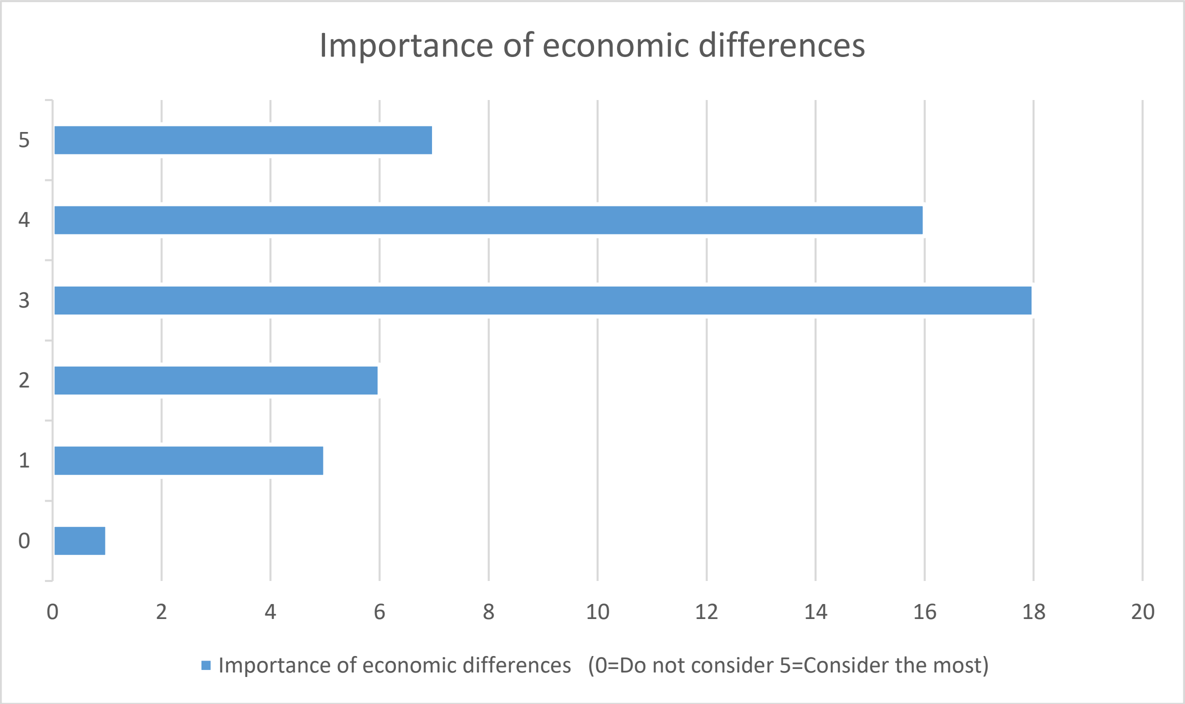


Figure 4.25: Importance of economic differences (Overview-SL)

The majority of participants have indicated that economic differences need to be considered, and it is important in accepting a global level data privacy and security policy.

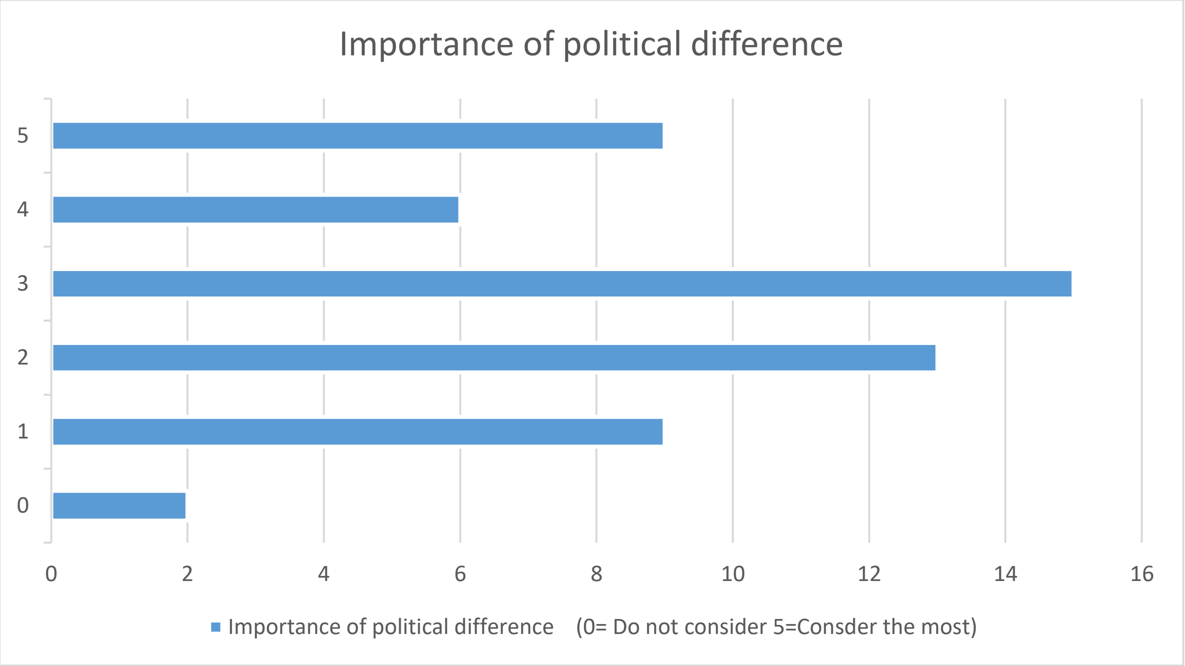


Figure 4.26: Importance of political difference (Overview-SL)

The majority of participants have not indicated that political differences need to be considered, and it is important in accepting a global level data privacy and security policy.

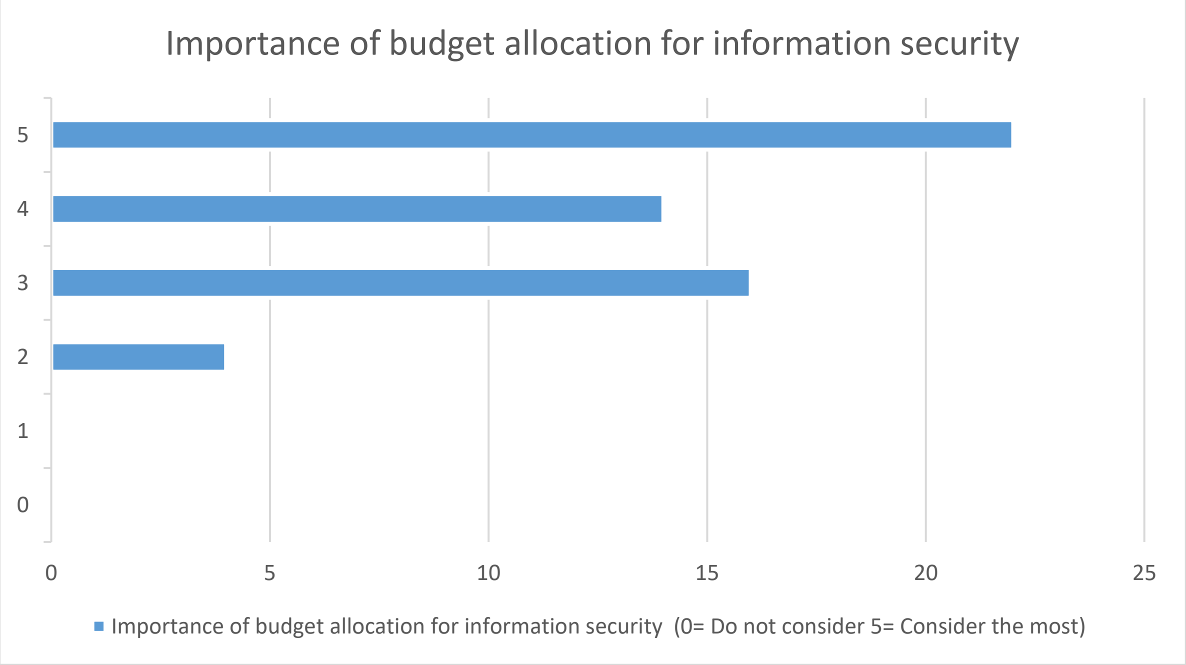


Figure 4.27: Importance of budget allocation for information security (Overview-SL)

A significant amount of participants have indicated the importance of budget allocation for information security needs to be considered, and it is important in accepting a global level data privacy and security policy.

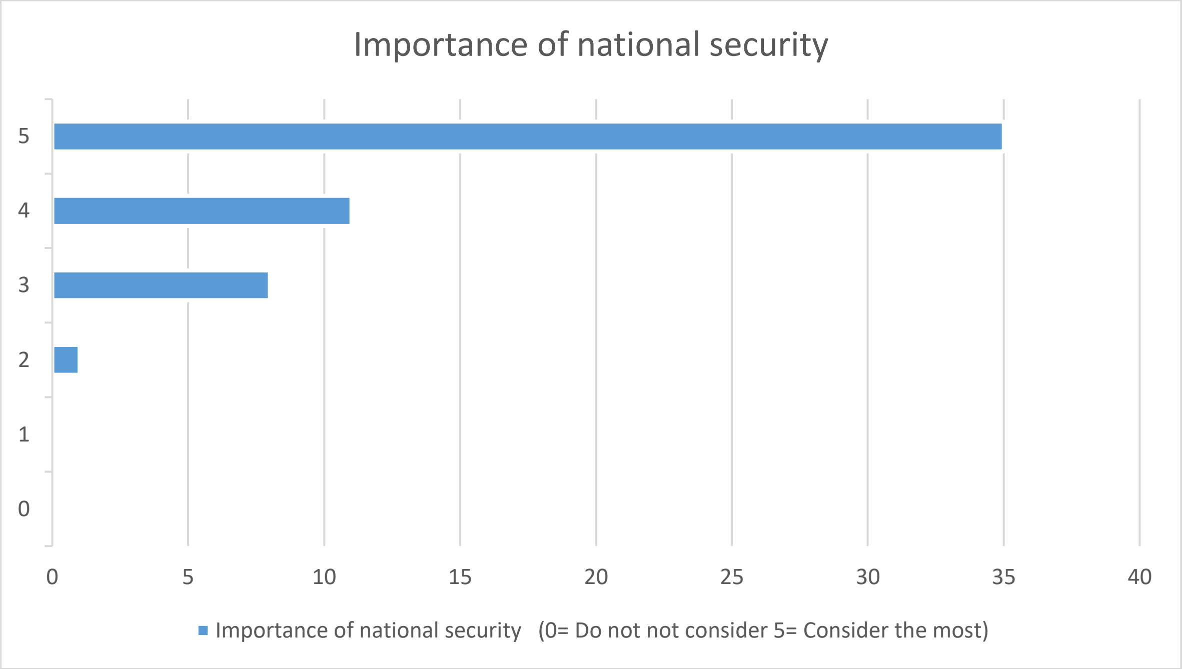


Figure 4.28: Importance of national security (Overview-SL)

A significant amount of participants have indicated that national security needs to be considered, and it is important in accepting a global level data privacy and security policy.

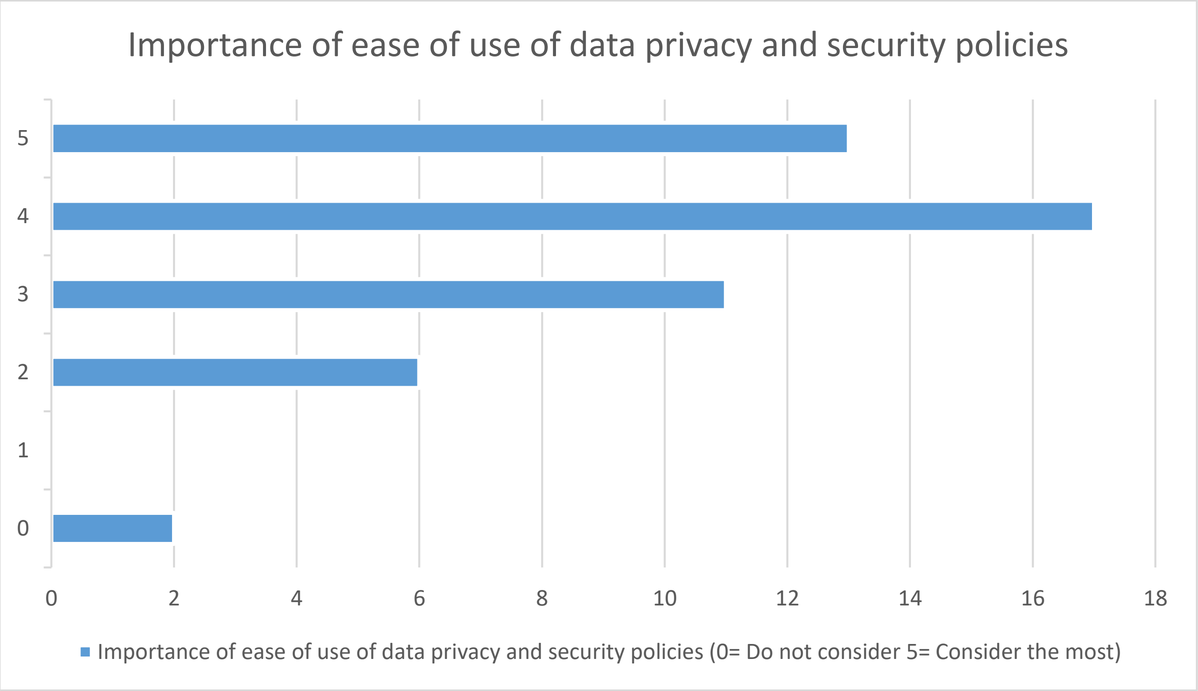


Figure 4.29: Importance of ease of use of data privacy and security policies (Overview-SL)

The majority of participants have indicated the ease of use of data privacy and security policies needs to be considered, and it is important in accepting a global level data privacy and security policy.

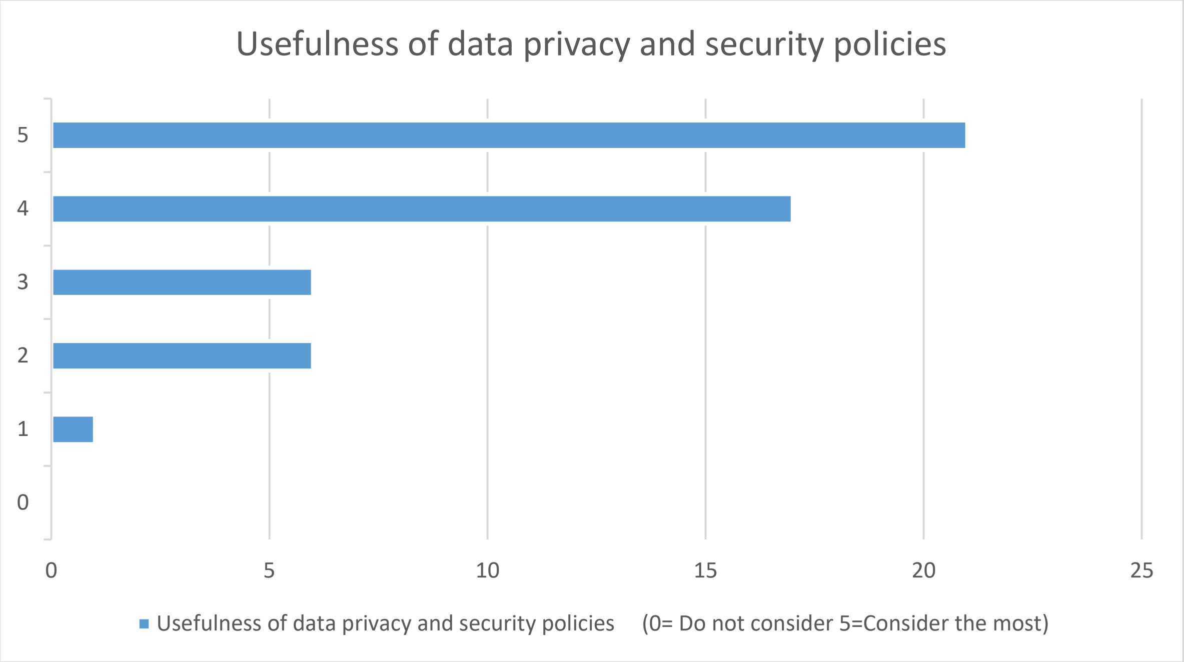


Figure 4.30: Usefulness of data privacy and security policies (Overview-SL)

The majority of participants have indicated the need to consider the usefulness of data privacy and security policies and its importance in accepting a global level data privacy and security policy.

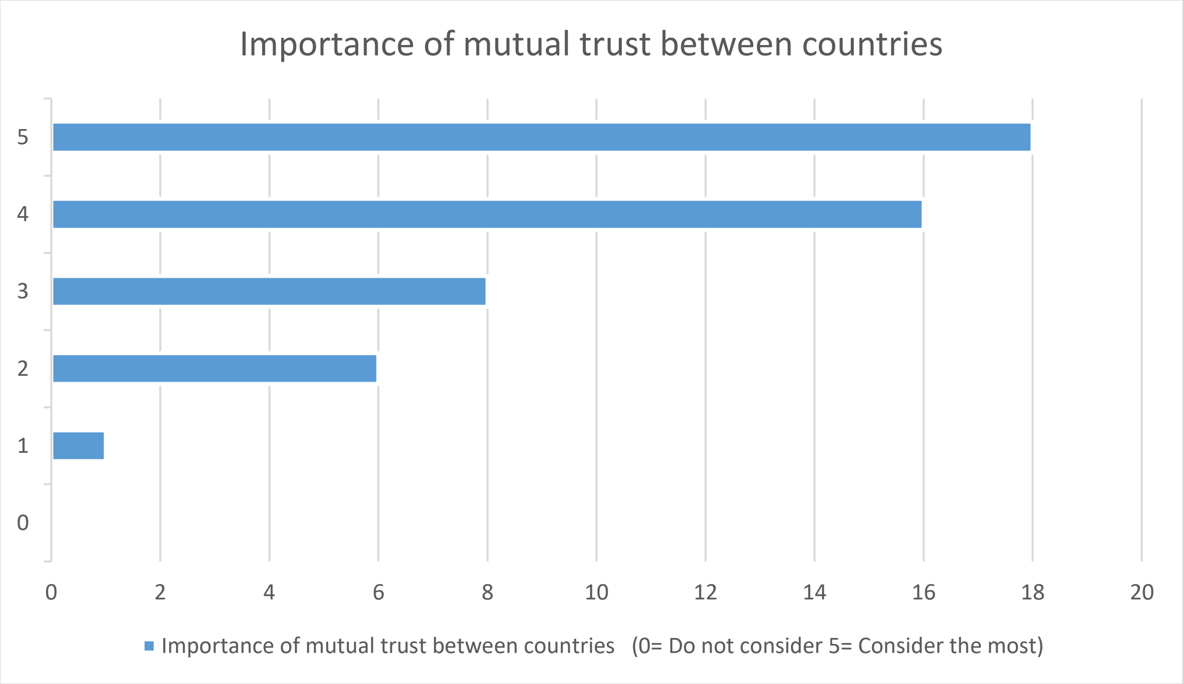


Figure 4.31: Importance of mutual trust between countries (Overview-SL)

The majority of participants have indicated the importance of mutual trust between countries and its importance in accepting a global level data privacy and security policy.

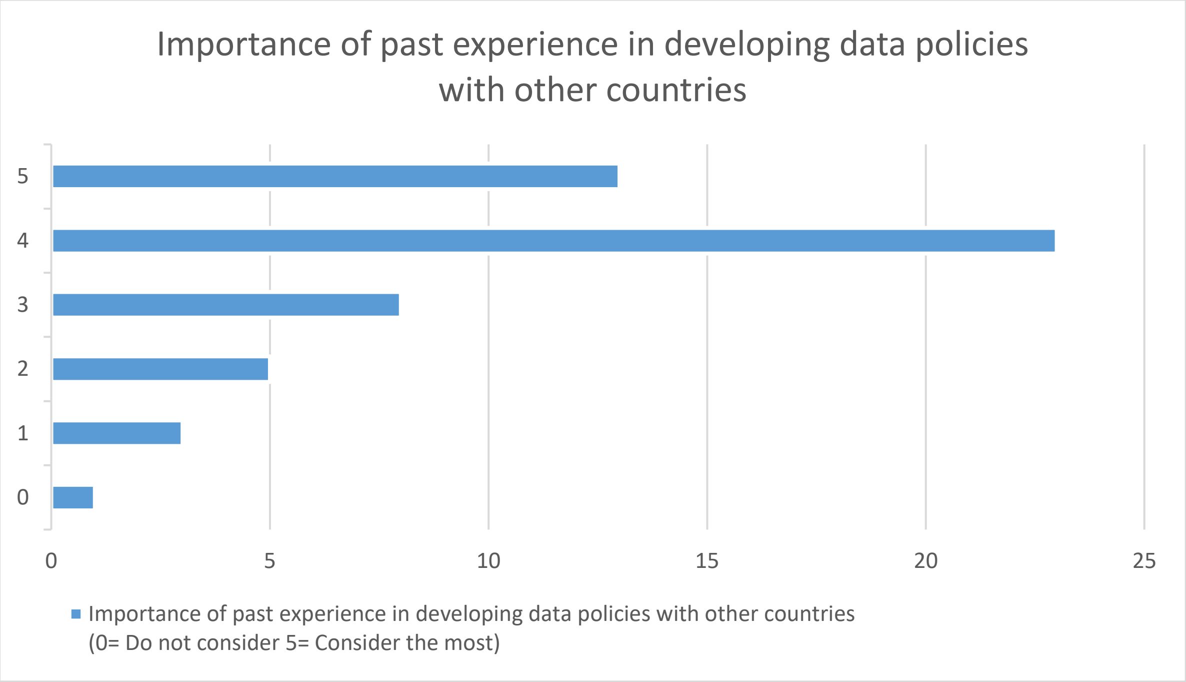


Figure 4.32: Importance of past experience in developing data policies with other counties (Overview-SL)

The majority of participants have indicated the importance of past experience in developing data policies with other counties and its importance in accepting a global level data privacy and security policy.

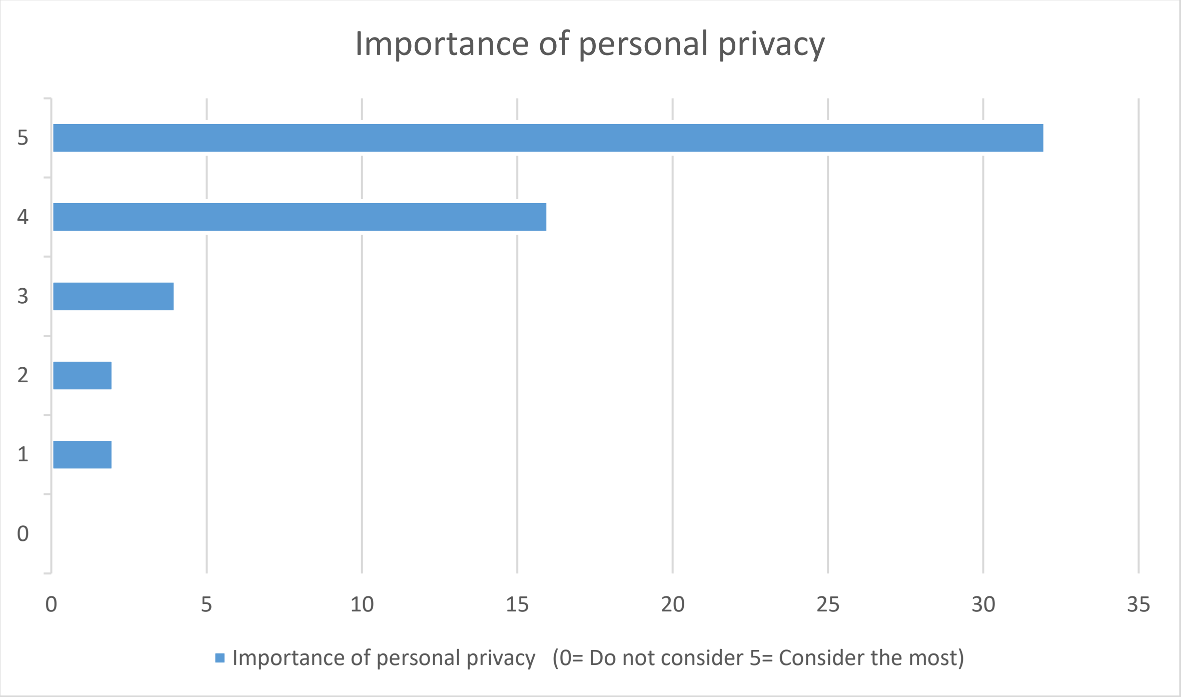


Figure 4.33: Importance of personal privacy (Overview-SL)

A significant amount of participants have indicated the importance of personal privacy and its importance in accepting a global level data privacy and security policy.

In summary, in accepting a global level data protection mechanism, the notable factors the participants would consider are organisational support, budget allocation, economic differences, personal privacy, national security, ease of data use, the usefulness of data privacy and security policies, mutual trust between the countries and previous experience with other countries in developing policies (See figure 4.23-4.33). However, the participants from Sri Lanka do not consider the premise that Social (See figure 4.24) and Political differences (See figure 4.26) play a significant role in accepting a global level data protection mechanism

4.2 United Kingdom- Overview

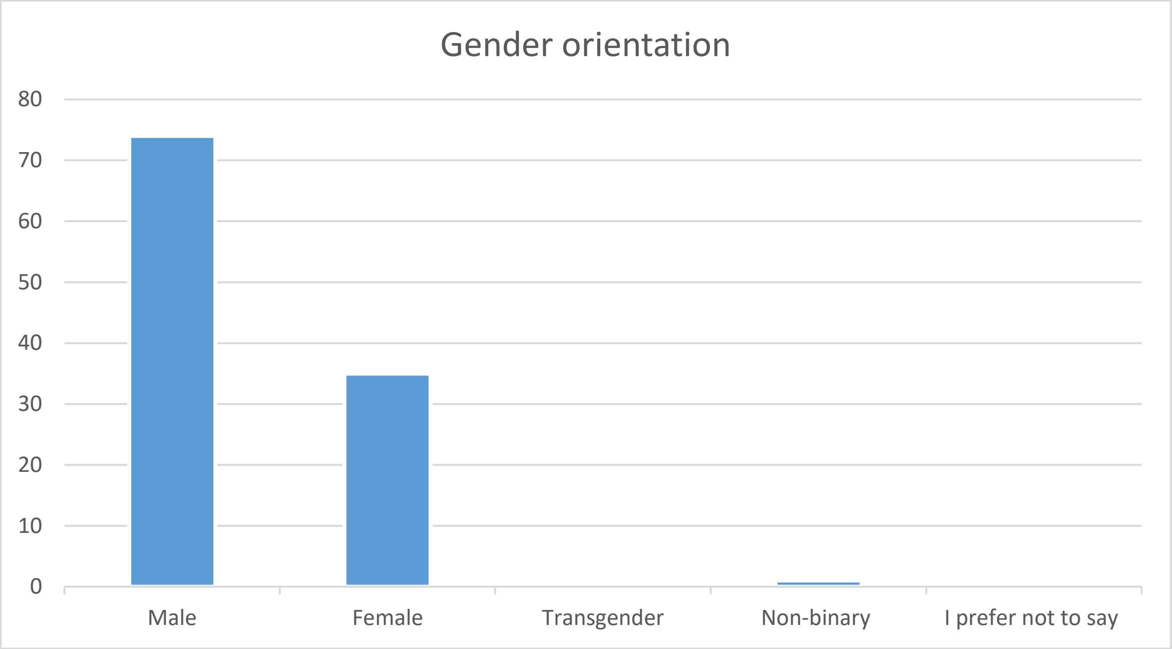


Figure 4.34: Gender orientation (Overview-UK)

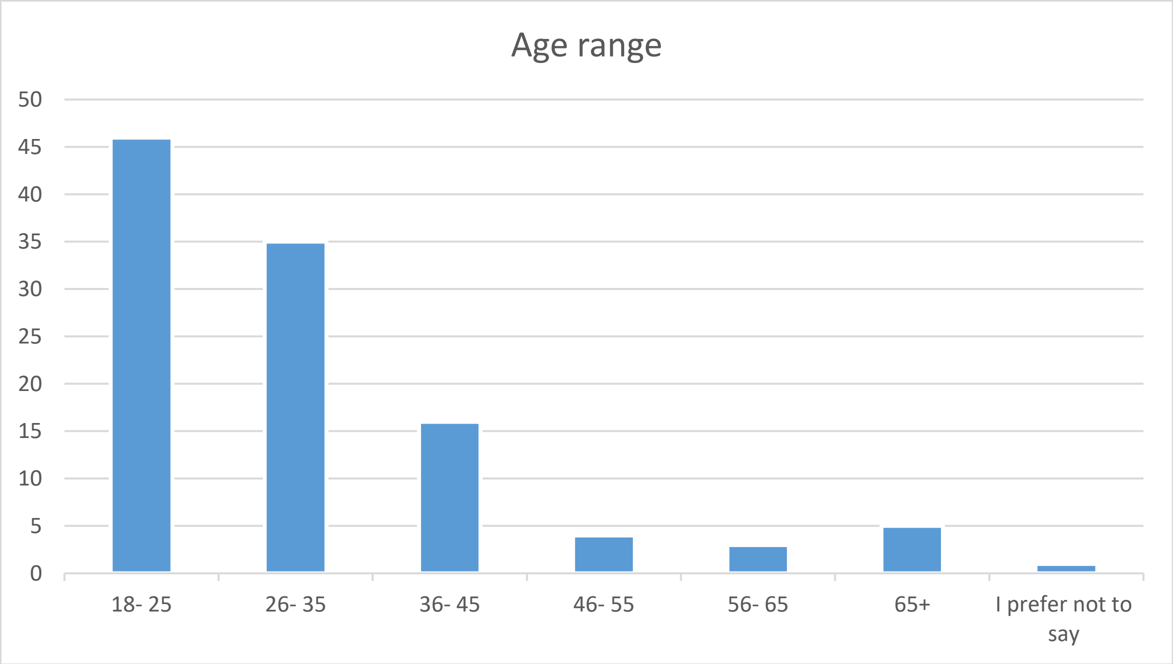


Figure 4.35: Age range (Overview-UK)

This analysis is based on the responses received from United Kingdom participants. There were 110 participants, 74 males, 35 females, and 1 non-binary (See figure 4.34). Their age range spanned between 18-65+ ; made up of groups of 46 in the 18-25, 35 in the 26-35, and 16 in the 36-45, 4 in the 46-55, 3 in the 56-65, 5 in the 65+ range with one exception not consented to reveal the age (See figure 4.35). Having participants from different gender groups and age groups is important in developing conclusions.

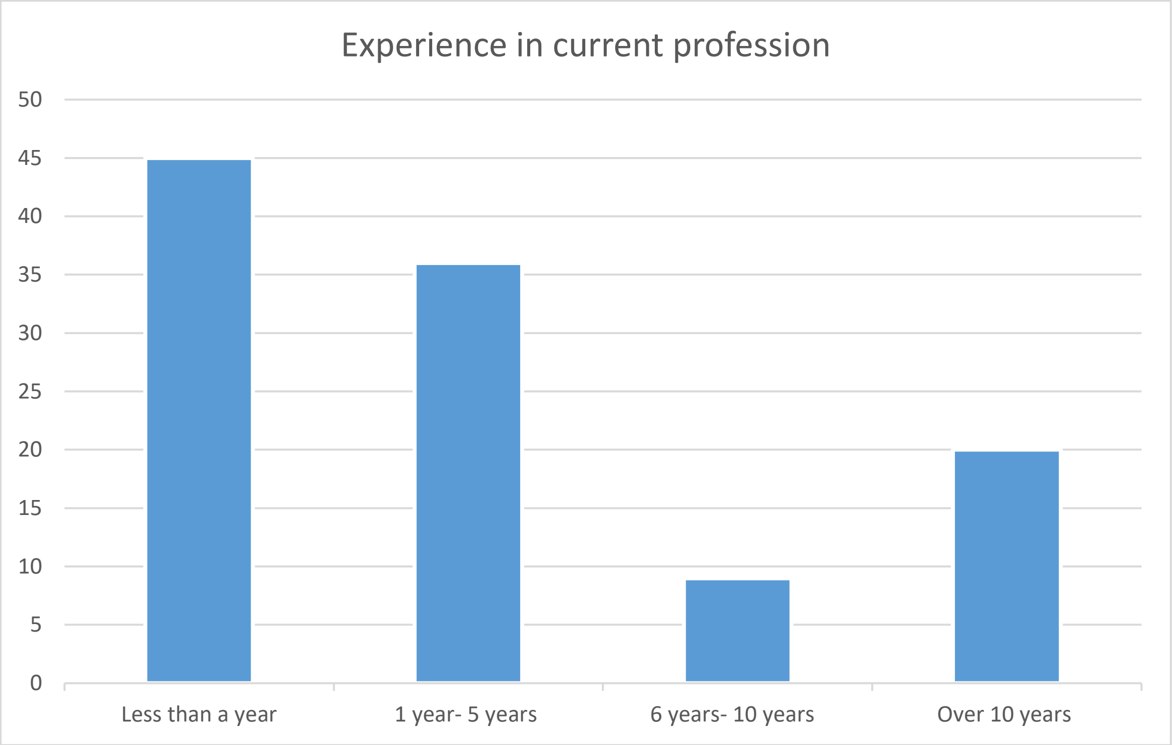


Figure 4.36: Experience in current profession (Overview-UK)

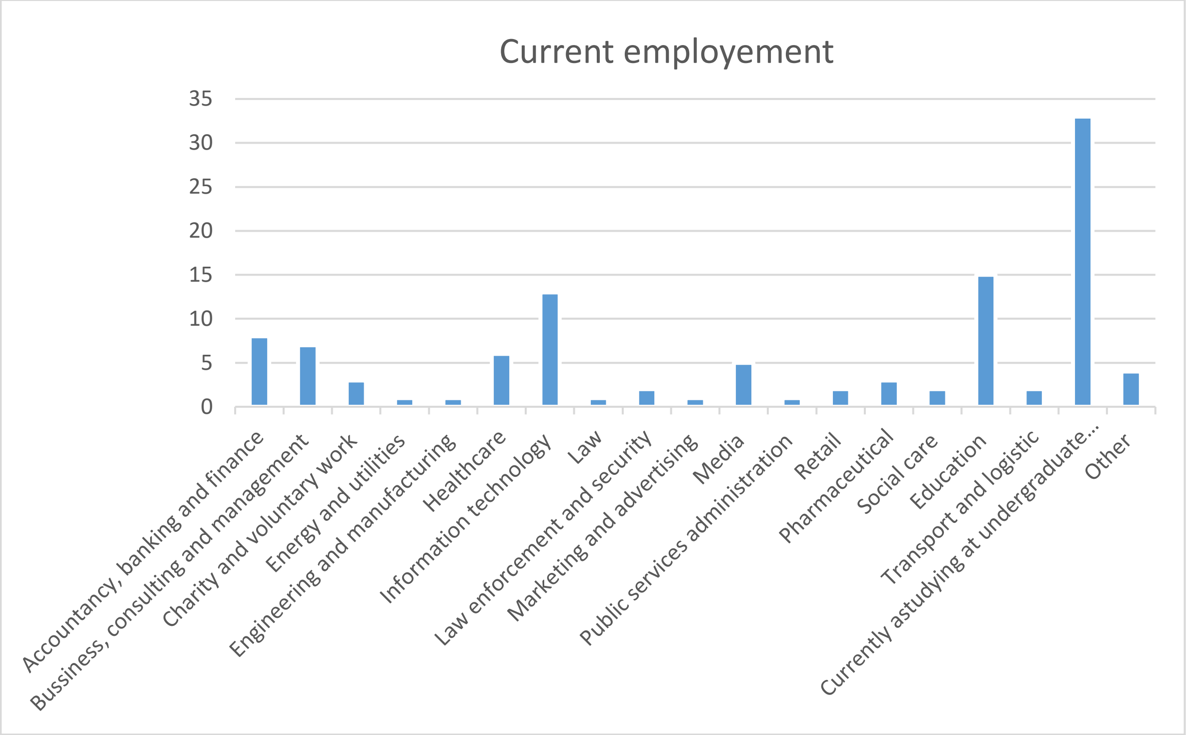


Figure 4.37: Current employment (Overview-UK)

The participants were employed in different industries (See figure 4.37) for less than a year to over 10 years (See figure 4.36). These participants have shattered across different industries. The diversity of the participants based on their gender, age, experience, and employment status is important for the researcher to critically analyse whether the participants think differently based on the above-mentioned factors.

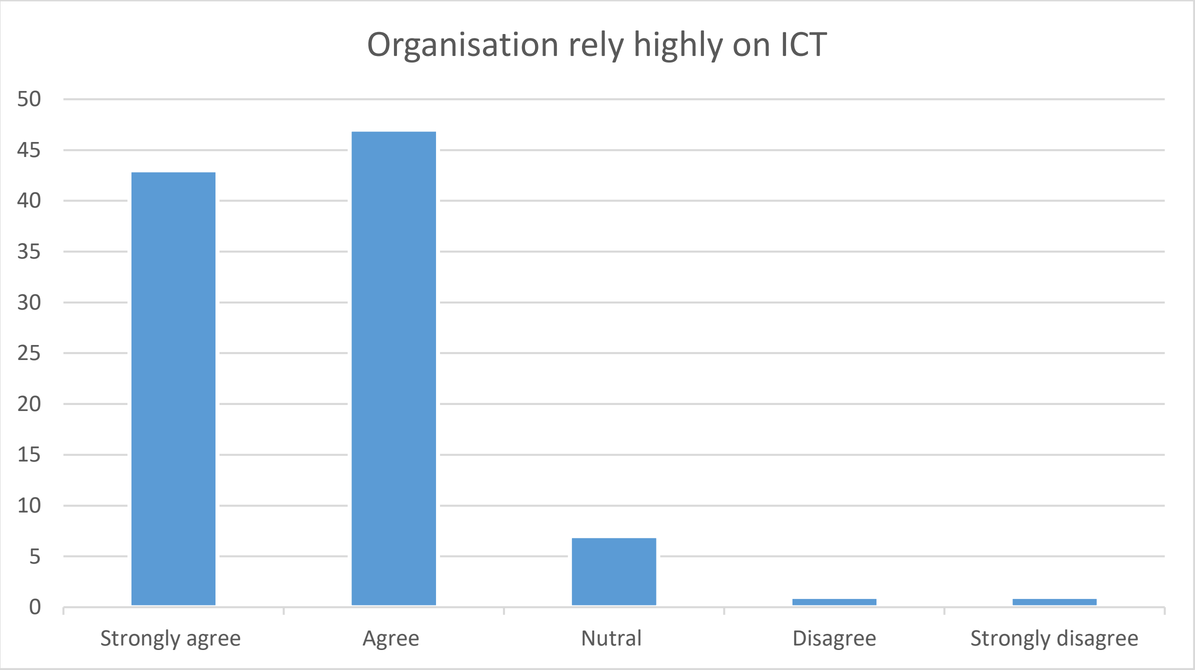


Figure 4.38: Organisation rely highly on ICT (Overview-UK)

Out of the 110 respondents, 90 were employed in a technology reliance working environment, 7 were unaware (of reliance on technology) because of the nature of the work assigned to them, 2 opted to 'disagree' (See figure 4.38). The supposition is that majority of the participants from the United Kingdom are employed in an ICT reliant working environment.

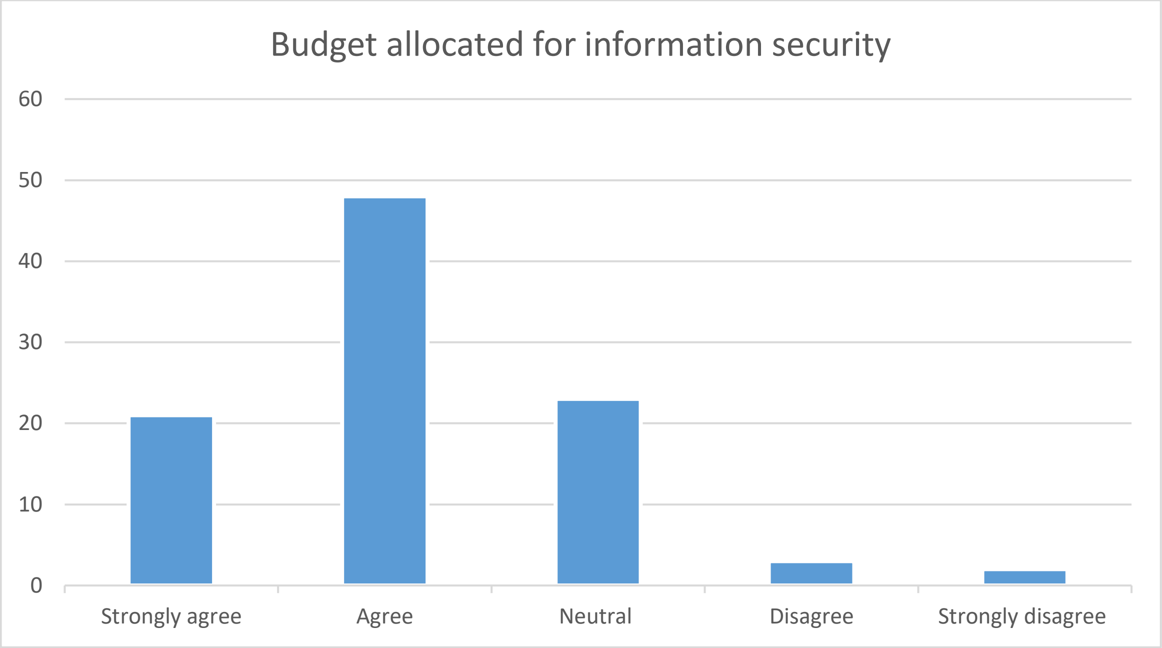


Figure 4.39: Budget allocated for information security (Overview-UK)

69 out of the 110 participants felt that their organisations made a budget allocation for information security, 23 not expressed an opinion either way, and according to the 5 disagreed, their organisations had no allocated budget for information security (See figure 4.39). The United Kingdom is a developed country, and there is no surprise in having a satisfactory level of budget allocation for information security given the significant level of reliance on technology amongst the individuals.

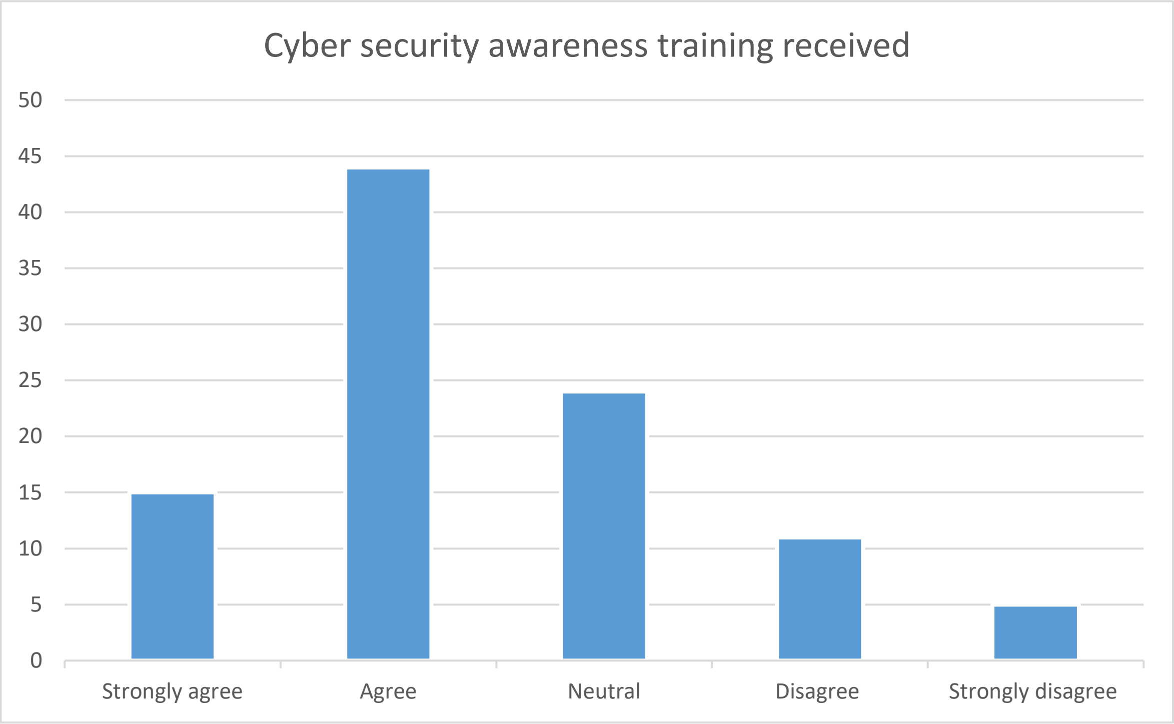


Figure 4.40: Cyber security awareness training received (Overview-UK)

Some participants claimed the regular security awareness training received was adequate despite the satisfactory level of resources allocated for information security. 59 participants received regular cybersecurity awareness training, whilst 24 neither agreed nor disagreed, and 16 participants did not receive regular security awareness training (See figure 4.40).

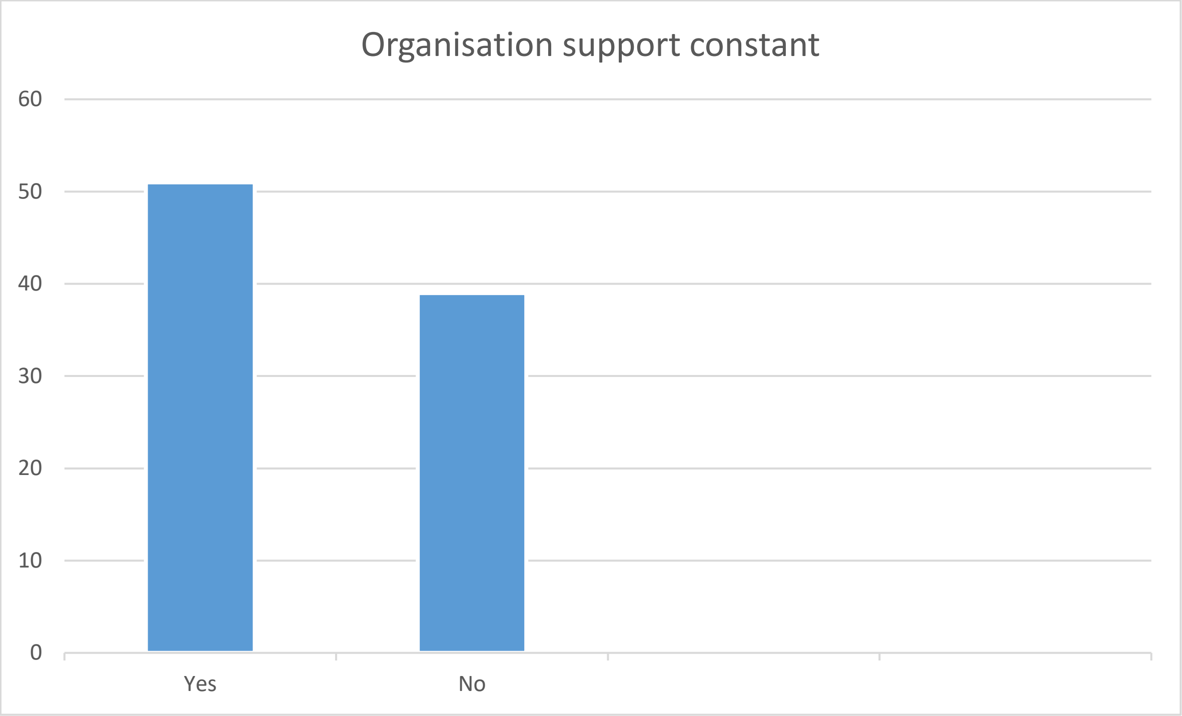


Figure 4.41: Organisation support constant (Overview-UK)

39 participants did not receive support from the organisation to protect personal information; only 51 did (See figure 4.41). This indicates the lack of organisational support to protect personal information despite the budget allocation for information security and high reliance on technology.

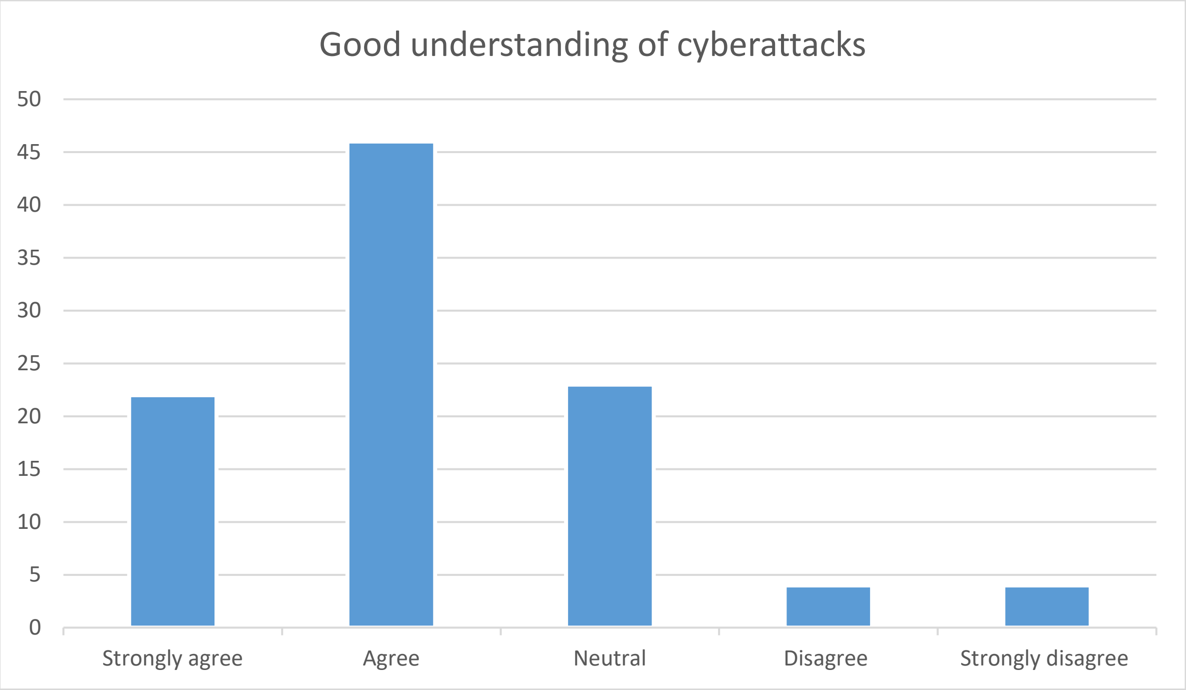


Figure 4.42: Good understanding of cyberattacks (Overview-UK)

68 participants agree they have a high level of understanding of the impact of cyber-attacks on the public and the organisation, 23 not expressed an opinion either way, and 8 without any understanding (See figure 4.42) despite receiving security awareness training.

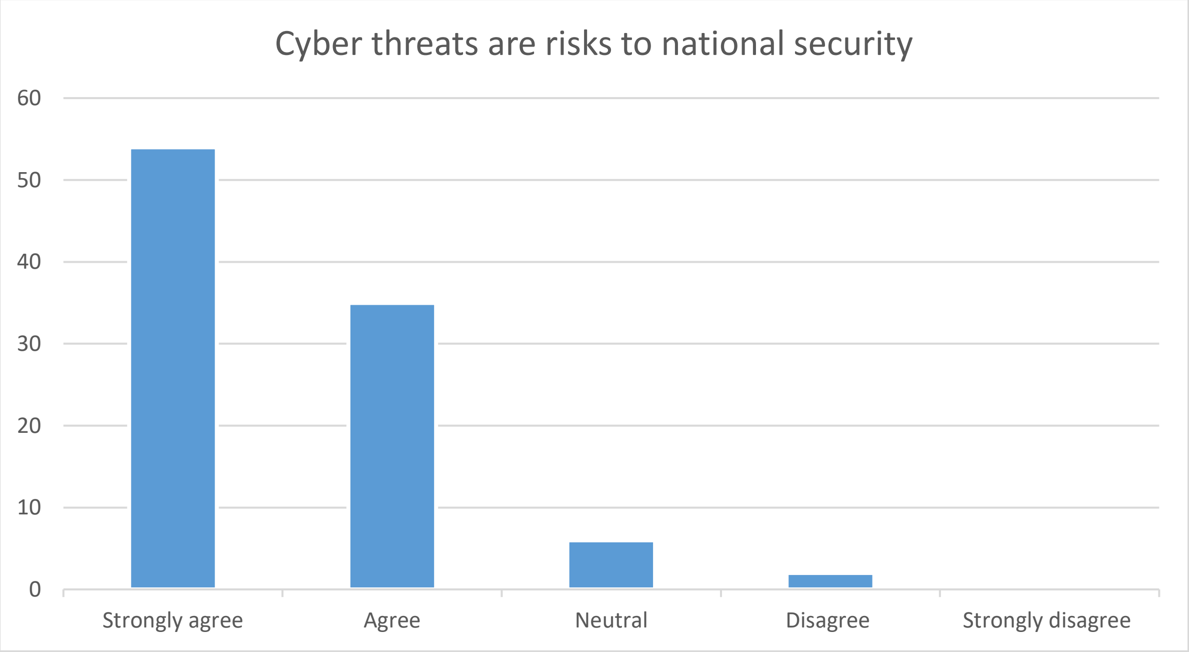


Figure 4.43: Cyber threats are risks to national security (Overview-UK)

Also, 81 percent of the participants aware of the potential threats to national security from cyber-attacks (See figure 4.43). In general, understanding cyber threats and their impact on national security make people act responsibly and minimise end-user errors; in time, their views will count and influence accepting and implementing a national, regional, and global level mechanism.

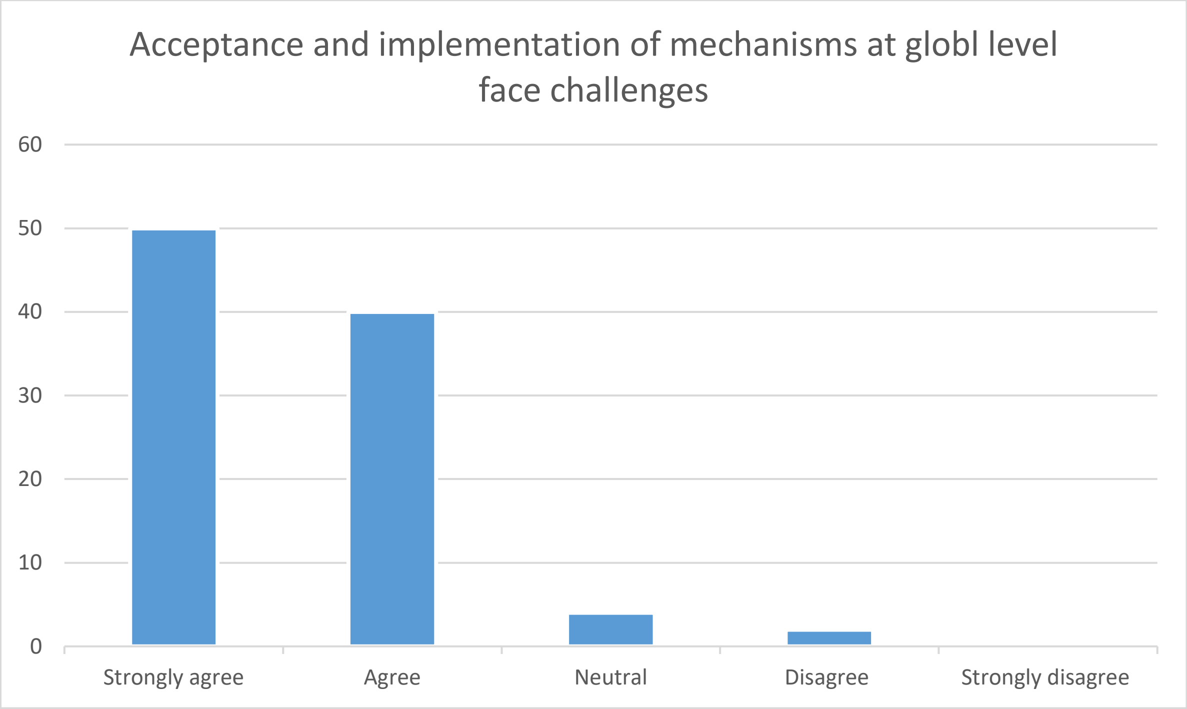


Figure 4.44: Acceptance and implementation of mechanisms at global level face challenges (Overview-UK)

The Majority of the participants appear to believe that acceptance and implementation of mechanism at global level face challenges. 50 strongly agree, 40 agree, 4 neutral, 2 disagree and no one has strongly disagreed (See figure 4.44). The number of participants who have believed that acceptance and implementation of mechanism at the global level do not face challenges is significantly low.

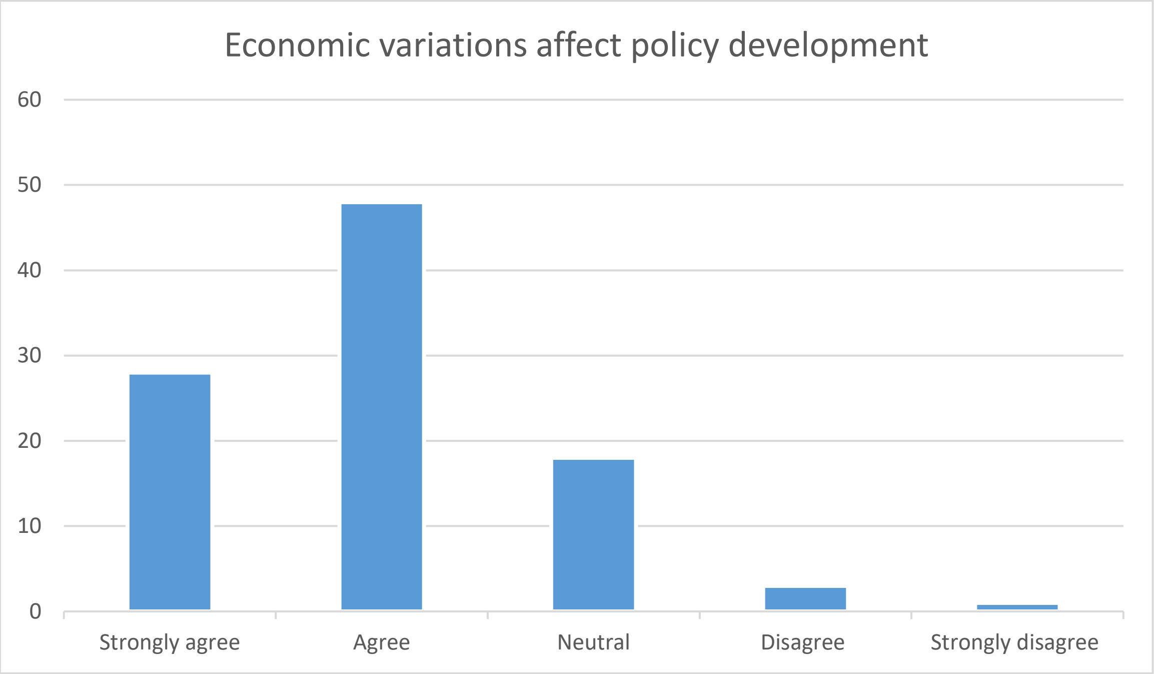


Figure 4.45: Economic variations affect policy development (Overview-UK)

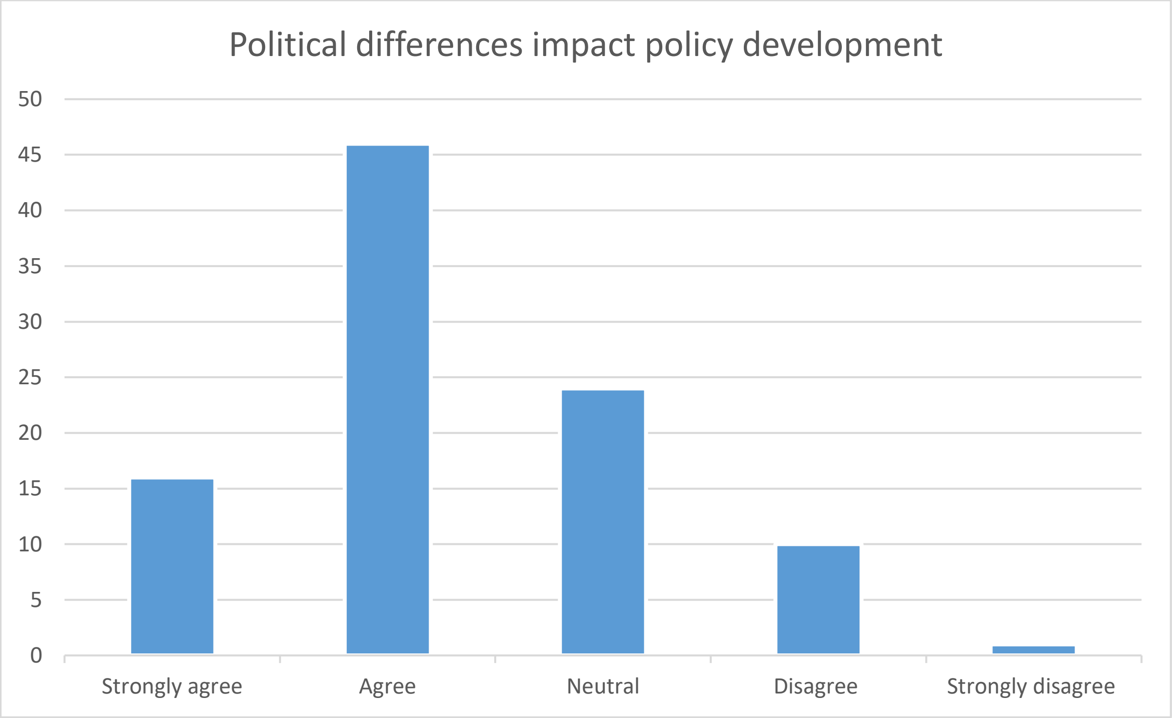


Figure 4.46: Political differences impact policy development (Overview-UK)

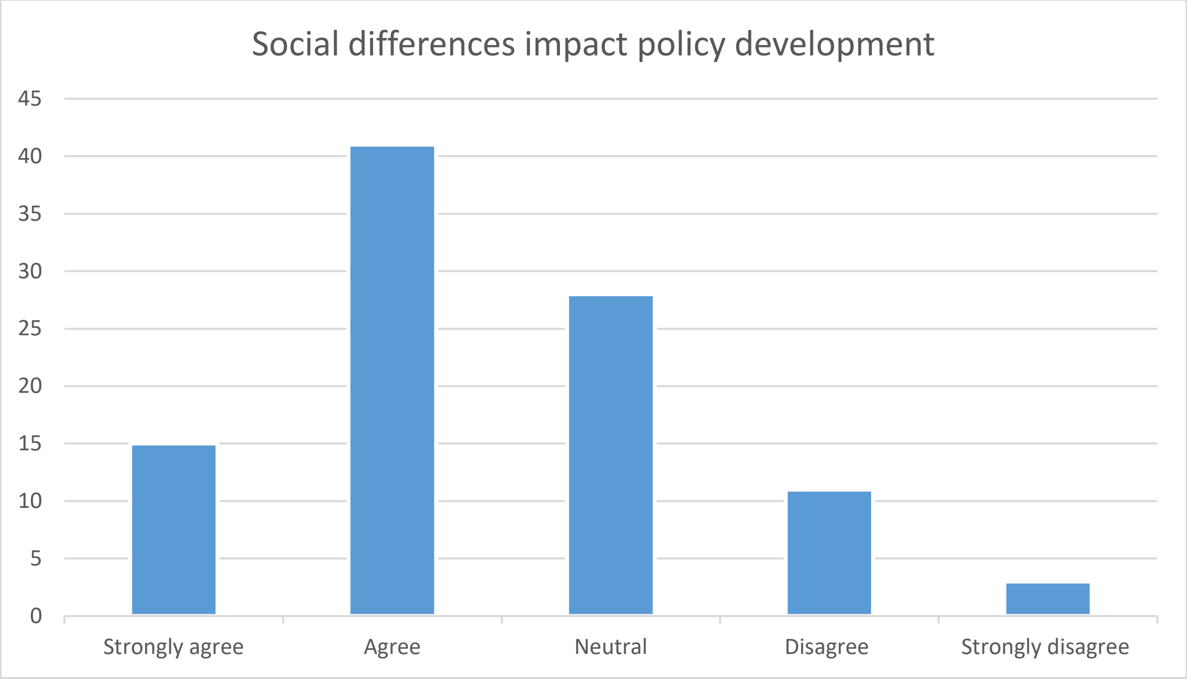


Figure 4.47: Social differences impact policy development (Overview-UK)

The participants agree that economic (See figure 4.45), political (See figure 4.46), and social differences (See figure 4.47) in/amongst the countries have an impact on policy development. This makes it hard for the policy developers to bring all the countries to agree to a unified mechanism. In responding to the questionnaire the participants have highlighted the types of economic, political and social differences they believe to play a vital role in policy development (See figure 4.48-4.50).

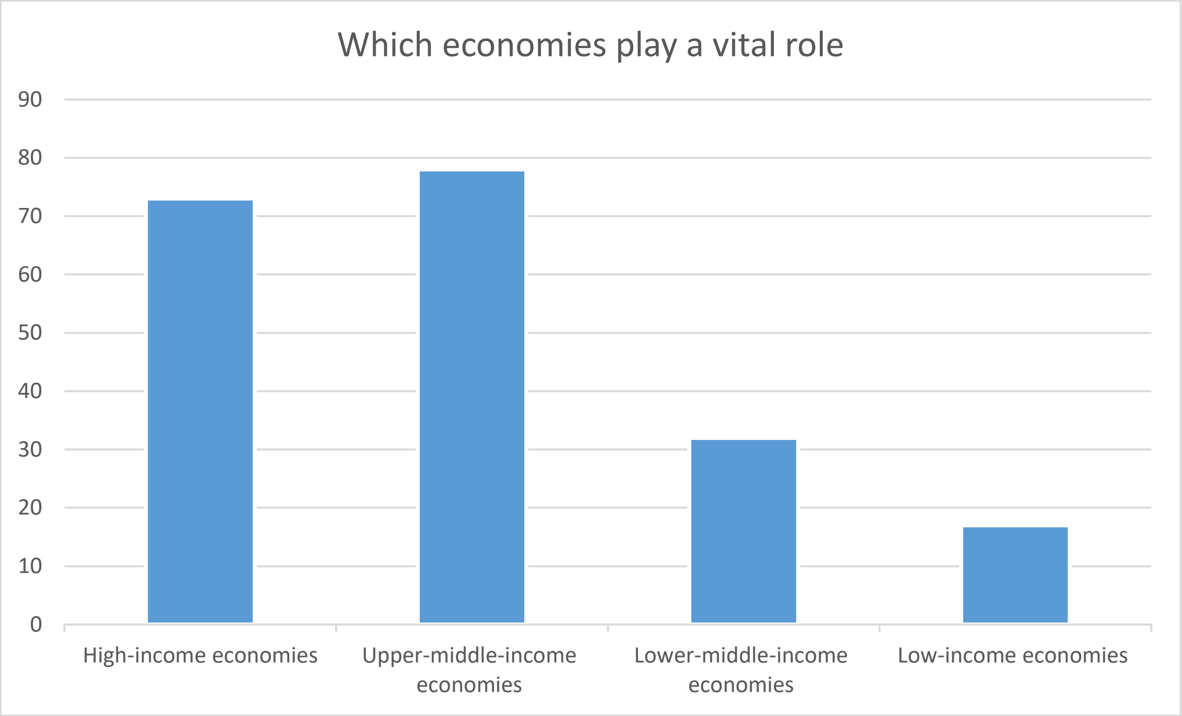


Figure 4.48: Which economies play a vital role (Overview-UK)

The majority concur high income and upper-middle-income countries play a vital role (See figure 4.48). There are key stages in the policymaking process and are described as identifying policymaker aims, identifying the policies to achieve those aims, selecting a policy measure, identifying the necessary resources, implementing and post-implementation evaluation of the policy. These stages are time-consuming, costly, and demanding in resources. Therefore, it is fair to say that the policymaking process is driven by the economic stability and the availability of resources in the country.

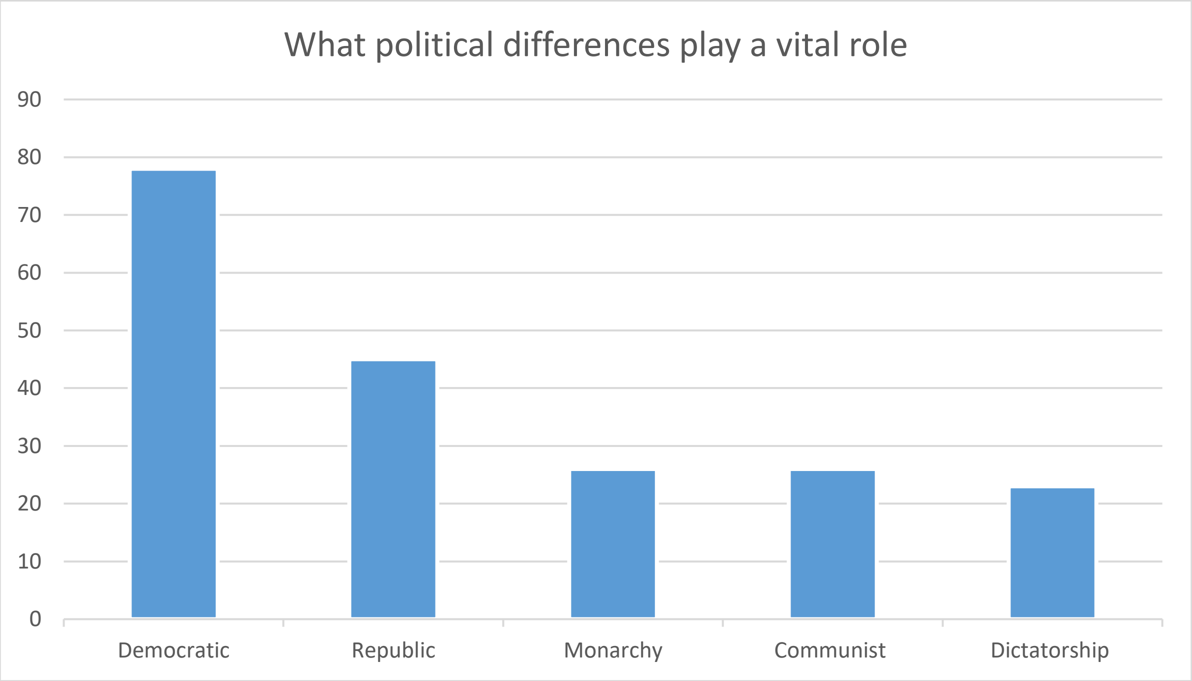


Figure 4.49: What political differences play a vital role (Overview-UK)

The majority have chosen a democratic political system (See figure 4.49), in preference to others because of the public influence in the process of policy development and encompass consensus and collective responsibility for their actions. The adherence to these norms contributes to developing trustworthiness and cordiality between organisations and creates a conducive environment for policy development.

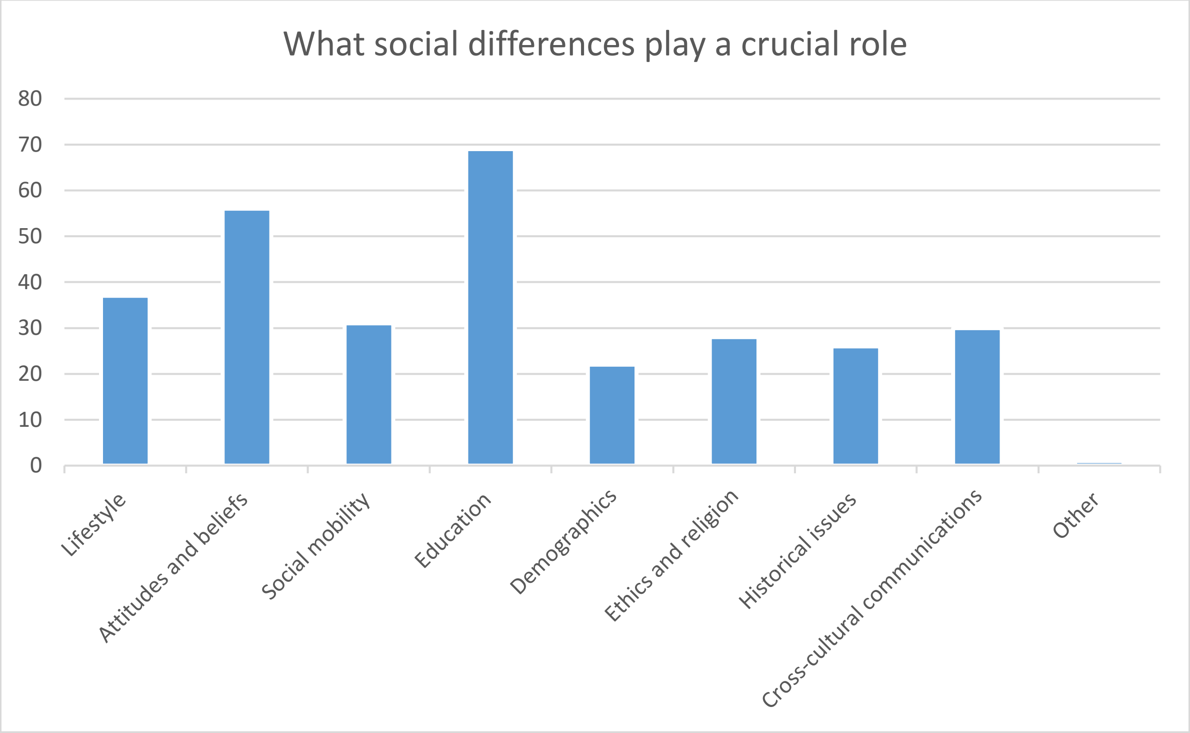


Figure 4.50: What social differences play a crucial role (Overview-UK)

Concerning the question on social differences, the majority see the importance of education and attitude and beliefs (See figure 4.50), and Familiarity of potential cyber threats, their impact on people and national security contributes to accepting and implementing data privacy and security policies. Therefore, it is important to provide cyber security awareness training at schools and at the organisational level. Self-belief in privacy and respecting privacy of the others are contributory factors discussed under attitude and believes.

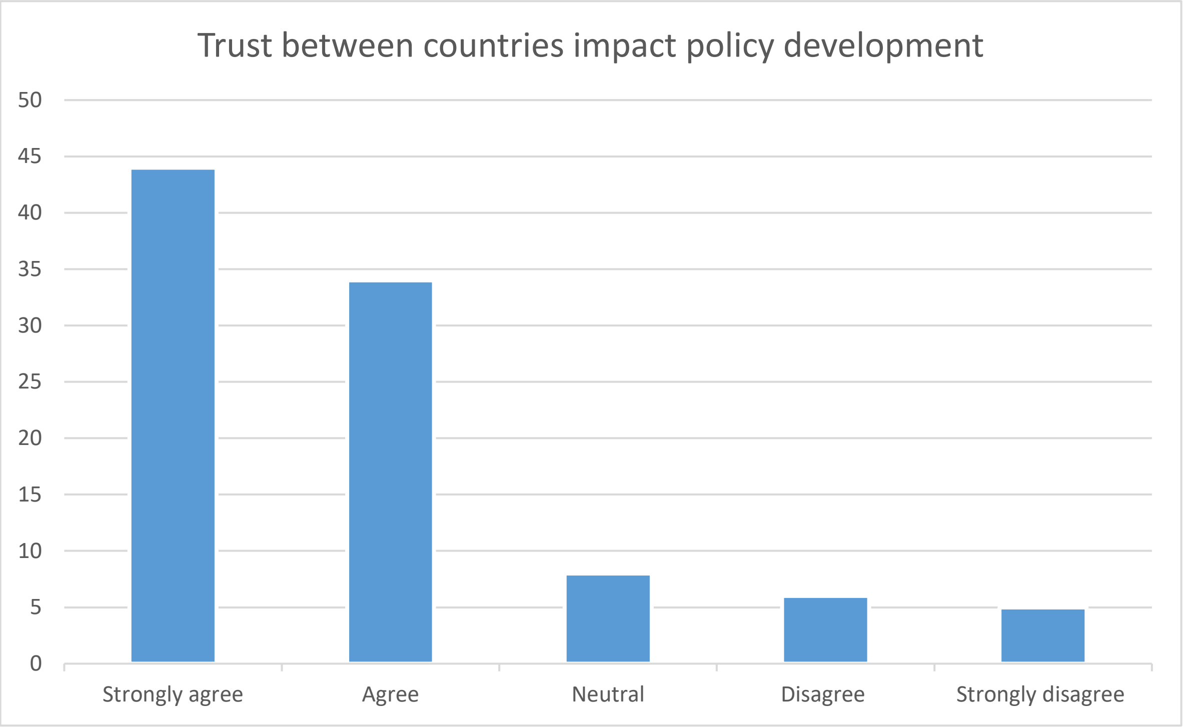


Figure 4.51: Trust between countries impact policy development (Overview-UK)

The participants have highlighted the importance of trust between countries to the highest level. 44 strongly agree, 34 agree, 8 neutral, 6 disagree and 5 strongly disagree (See figure 4.51). The number of participants who have disagreed is considerably law. As highlighted by the participants having trust between countries would help the process of developing regional level and global level data protection mechanism.

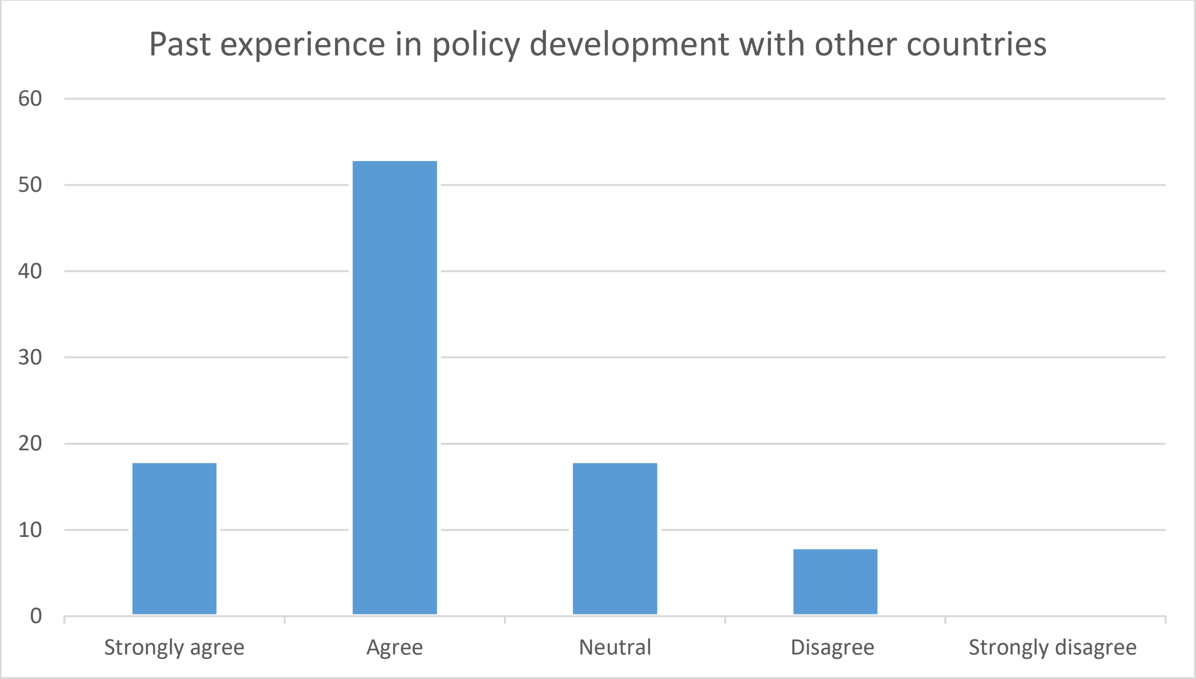


Figure 4.52: Past experience in policy development with other countries useful (Overview-UK)

According to the participants past experience in policy development with other countries is also useful in bringing countries together. In developing a global level data protection mechanism, the countries can make use of the lessons they learned in previous negotiations. 18 strongly agree, 53 agree, 18 neutral, 8 disagree, and most importantly, no one has disagreed with the idea of having past experience in developing policies with other countries (See figure 4.52).

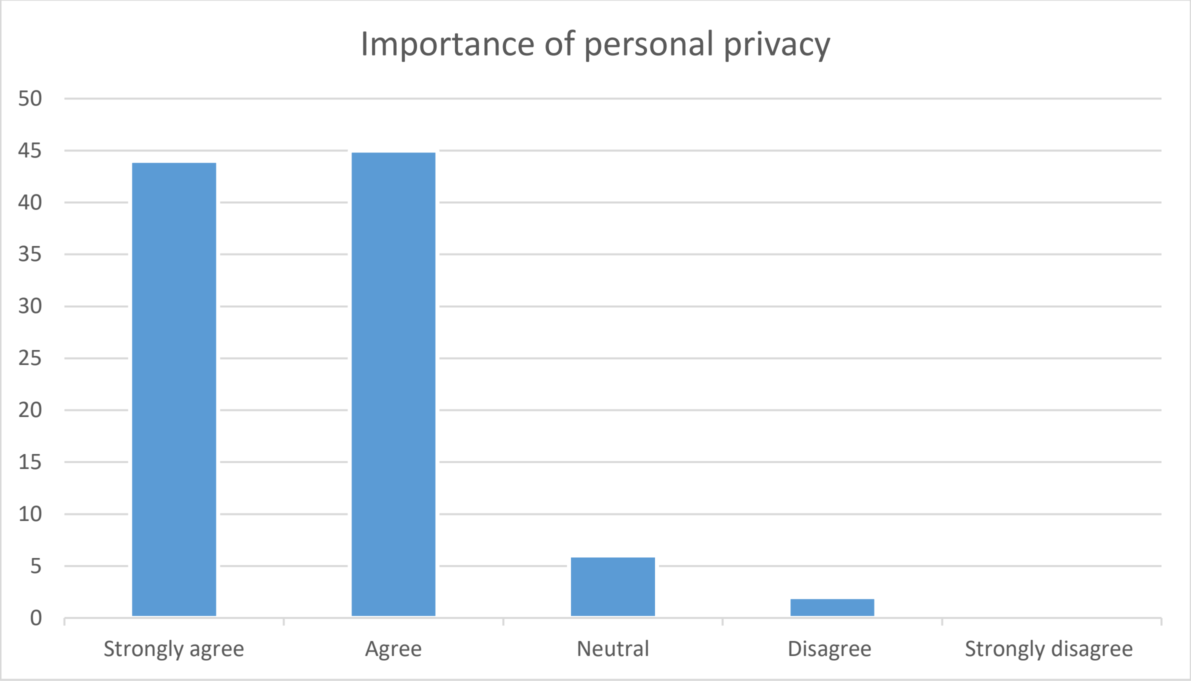


Figure 4.53: Importance of personal privacy (Overview-UK)

A significant amount of participants have indicated the importance of personal privacy and its importance in accepting a global level data privacy and security policy (See figure 4.53).

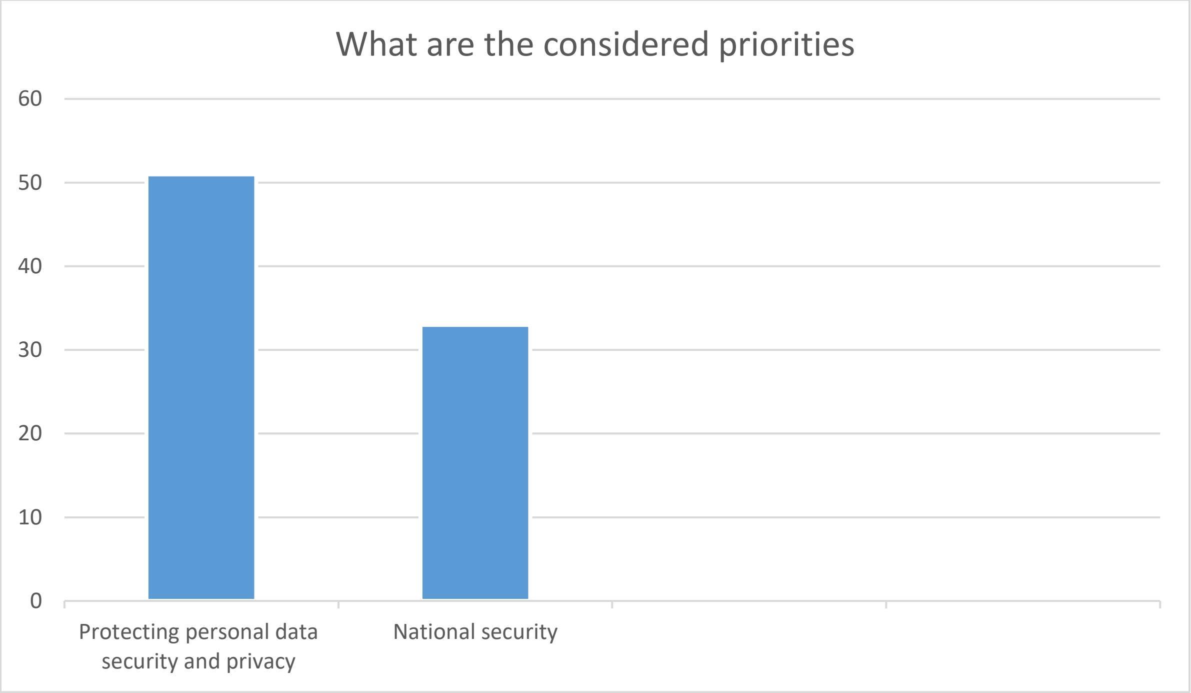


Figure 4.54: What are the considered priorities (Overview-UK)

Either the importance of protection of personal data security and privacy or protection of national security is not considered by the majority (See figure 4.54). However, in a personal data breach incidence, the potential effect on personal privacy and national security cannot be discounted; the likely repercussions will be felt right across the groups as well as the community alike.

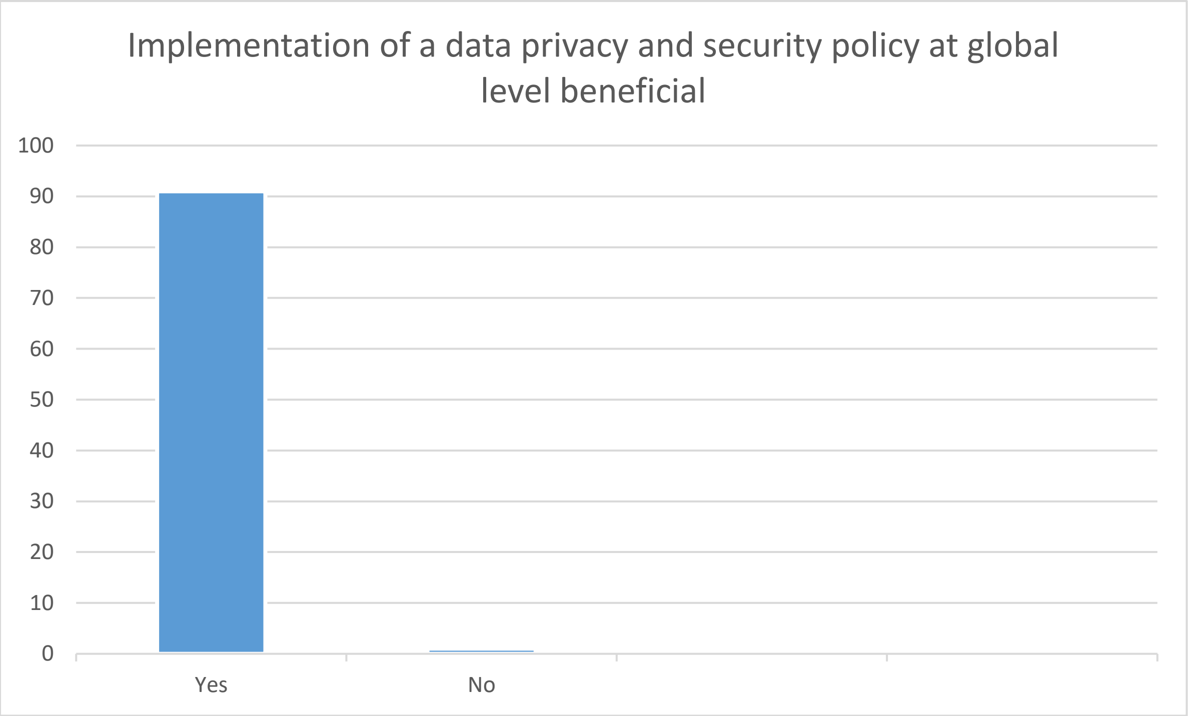


Figure 4.55: Implementation of a data privacy and security policy at global level beneficial (Overview-UK)

Despite the challenges and barriers countries face in developing policies, the message from the respondents is clear. It is a compelling need to have a global level data protection mechanism, with the endorsement of 83 percent of the respondents (See figure 4.55). In the case of UK, they do have a data protection mechanism at the national level and regional level. However, they strongly believe having a global level data protection will help to protect the privacy of the individual to a greater extent.

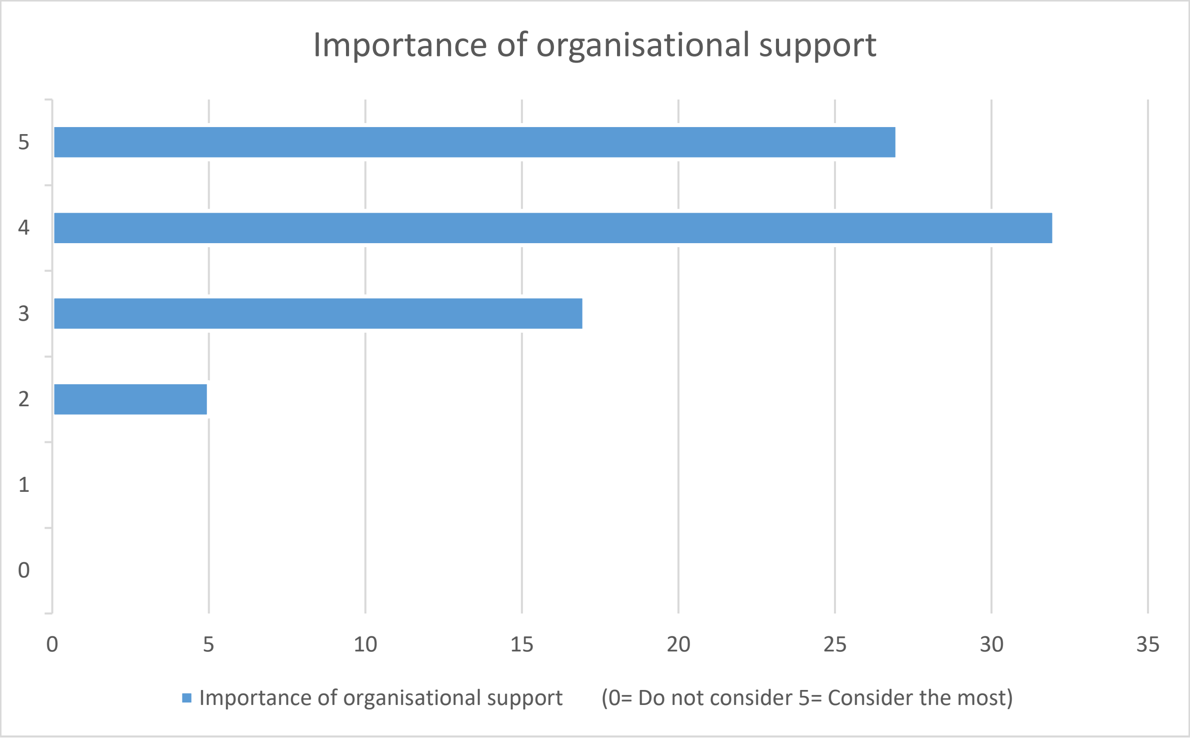


Figure 4.56: Importance of organisational support (Overview-UK)

A significant amount of participants have indicated that organisation support needs to be considered, and it is important in accepting a global level data privacy and security policy.

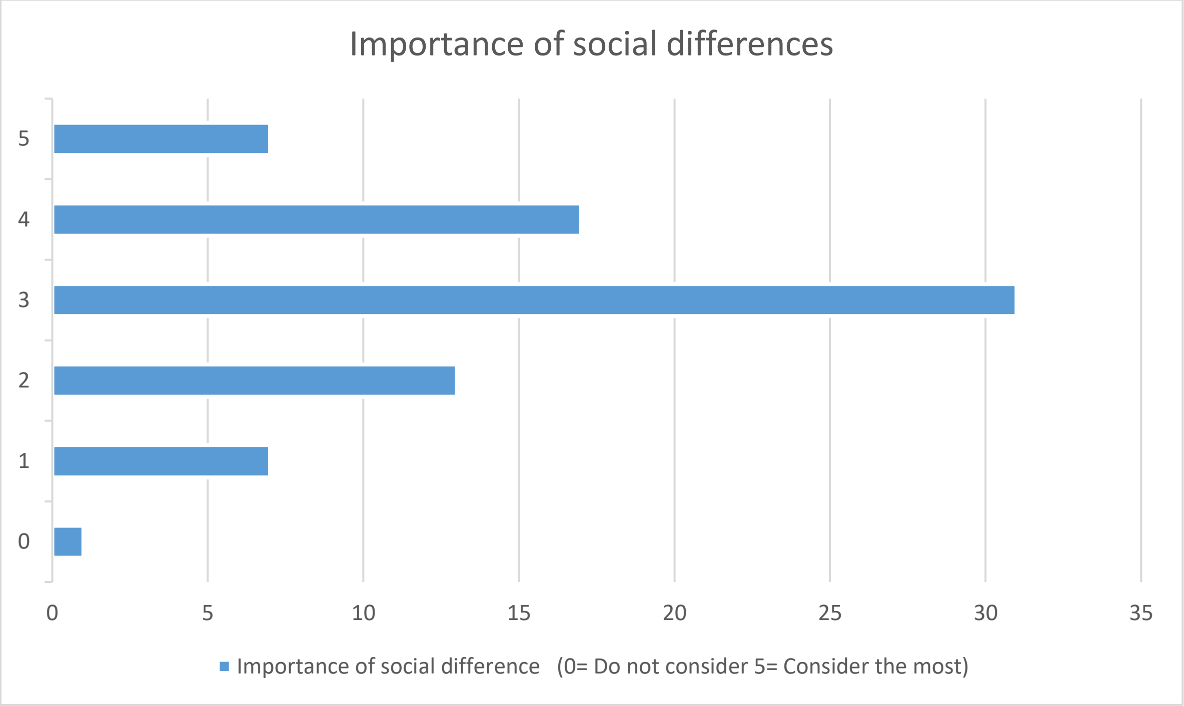


Figure 4.57: Importance of social differences (Overview-UK)

The majority of participants have indicated that social differences need to be considered, and it is important in accepting a global level data privacy and security policy.

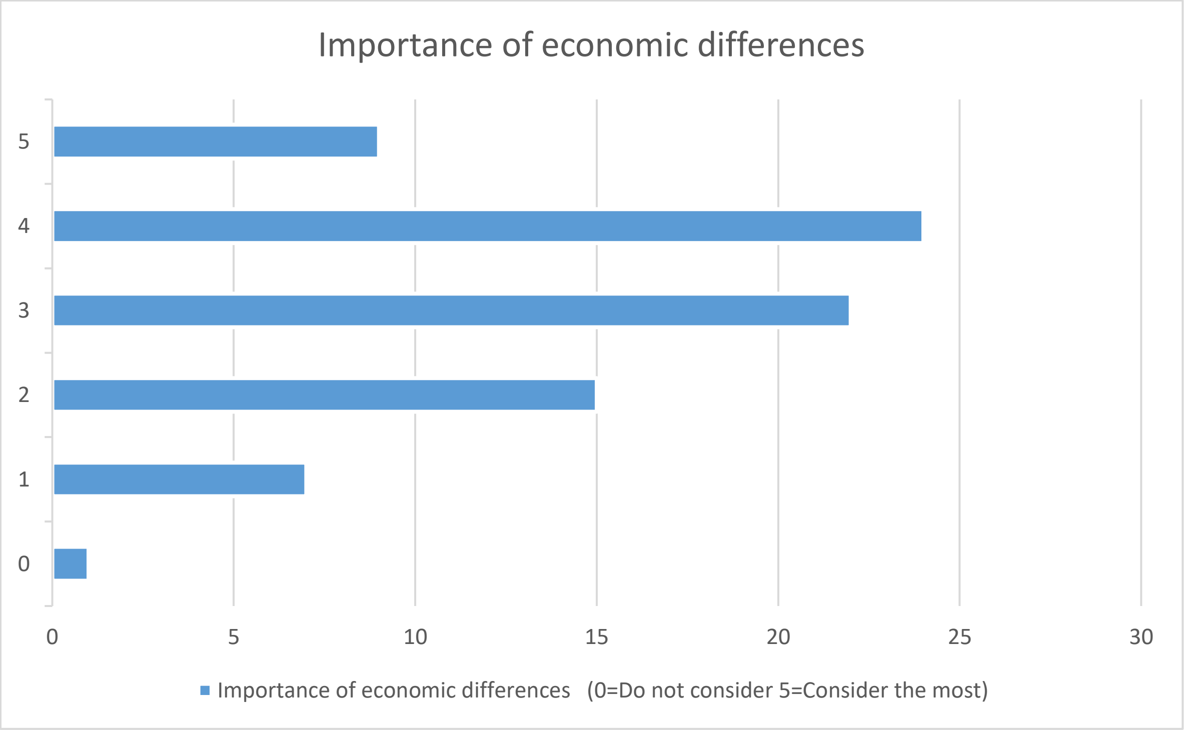


Figure 4.58: Importance of economic differences (Overview-UK)

The majority of participants have indicated that economic differences need to be considered, and it is important in accepting a global level data privacy and security policy.

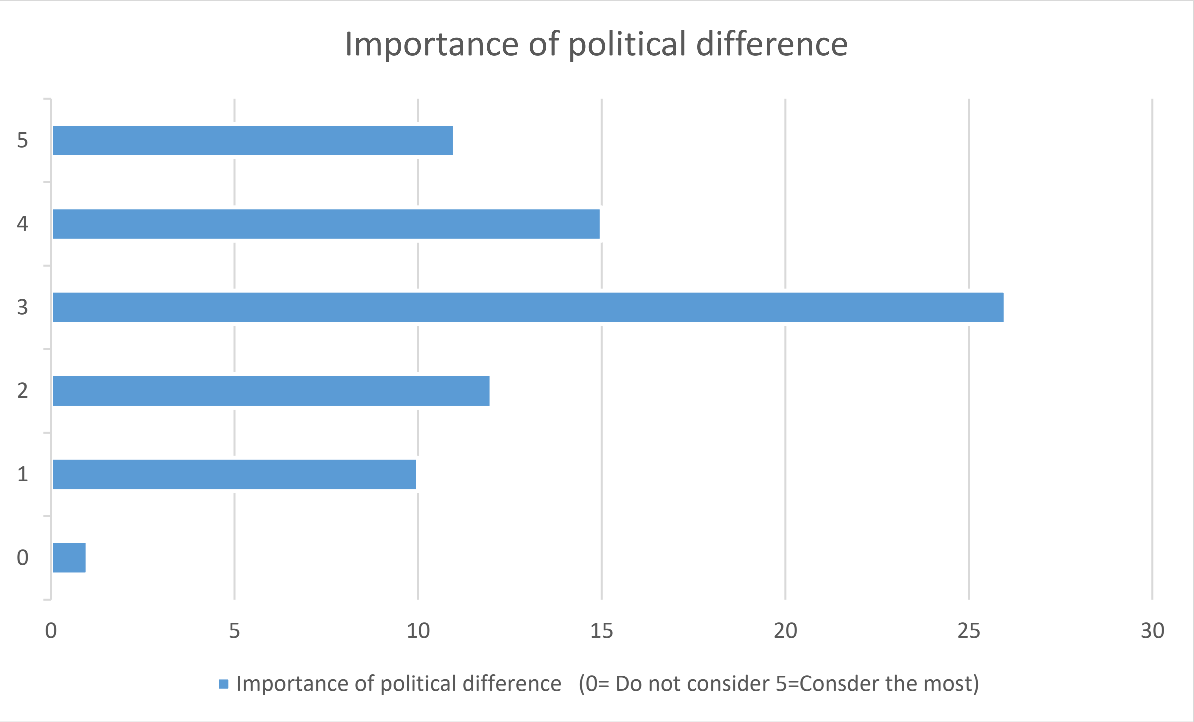


Figure 4.59: Importance of political difference (Overview-UK)

The majority of participants have indicated that political differences need to be considered, and it is important in accepting a global level data privacy and security policy.

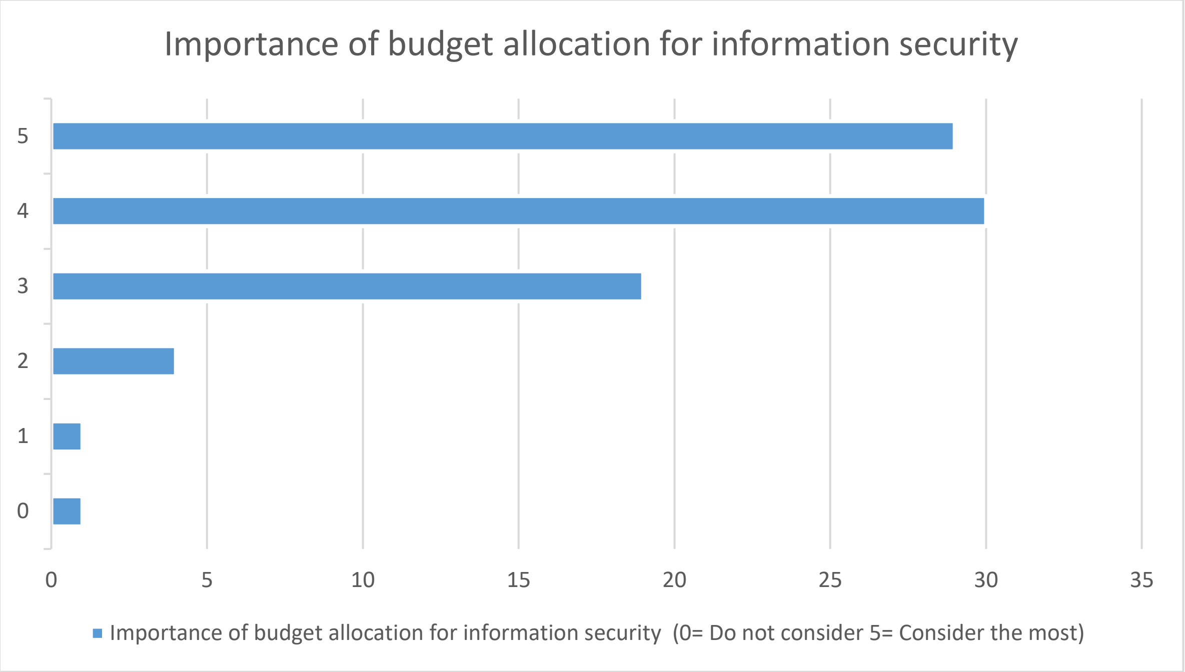


Figure 4.60: Importance of budget allocation for information security (Overview-UK)

A significant amount of participants have indicated the importance of budget allocation for information security needs to be considered, and it is important in accepting a global level data privacy and security policy.

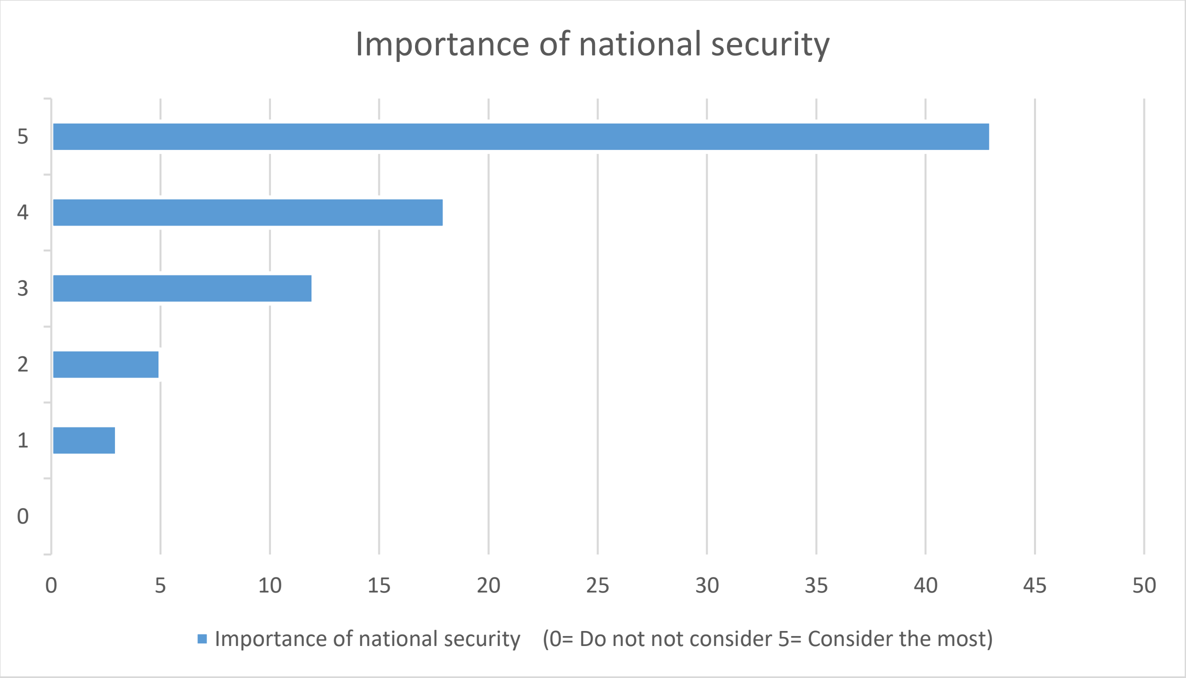


Figure 4.61: Importance of national security (Overview-UK)

A significant amount of participants have indicated that national security needs to be considered, and it is important in accepting a global level data privacy and security policy.

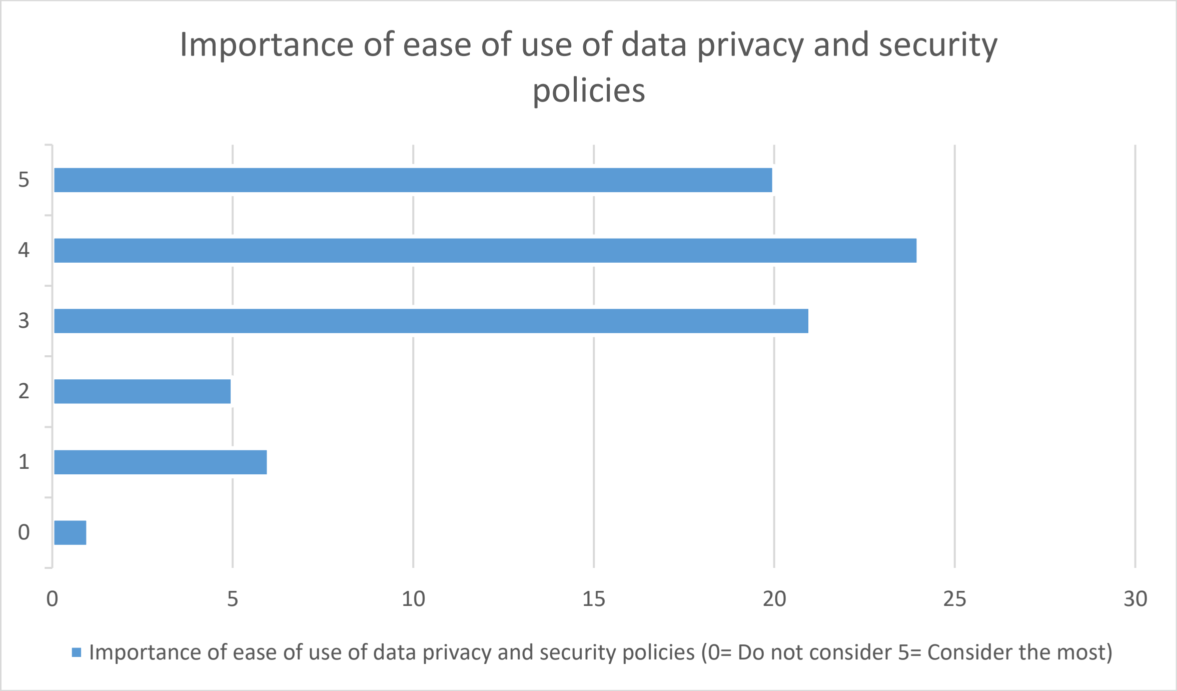


Figure 4.62: Importance of ease of use of data privacy and security policies (Overview-UK)

A significant amount of participants have indicated the ease of use of data privacy and security policies needs to be considered, and it is important in accepting a global level data privacy and security policy.

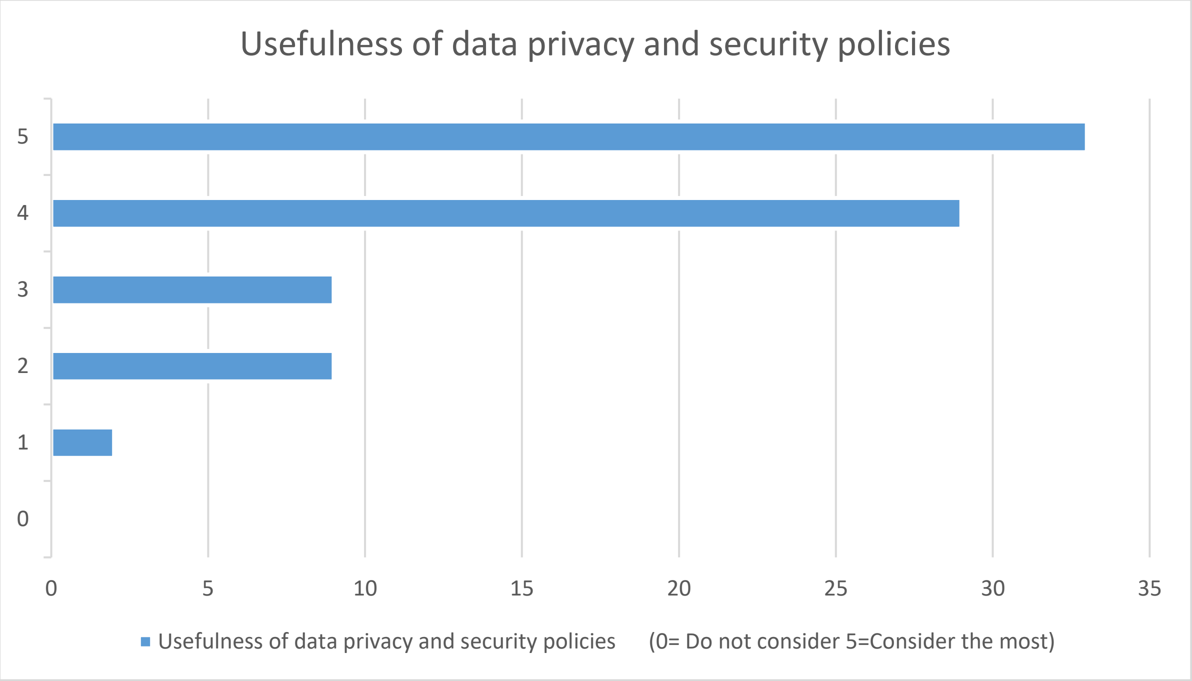


Figure 4.63: Usefulness of data privacy and security policies (Overview-UK)

A significant amount of participants have indicated the need to consider the usefulness of data privacy and security policies and its importance in accepting a global level data privacy and security policy.

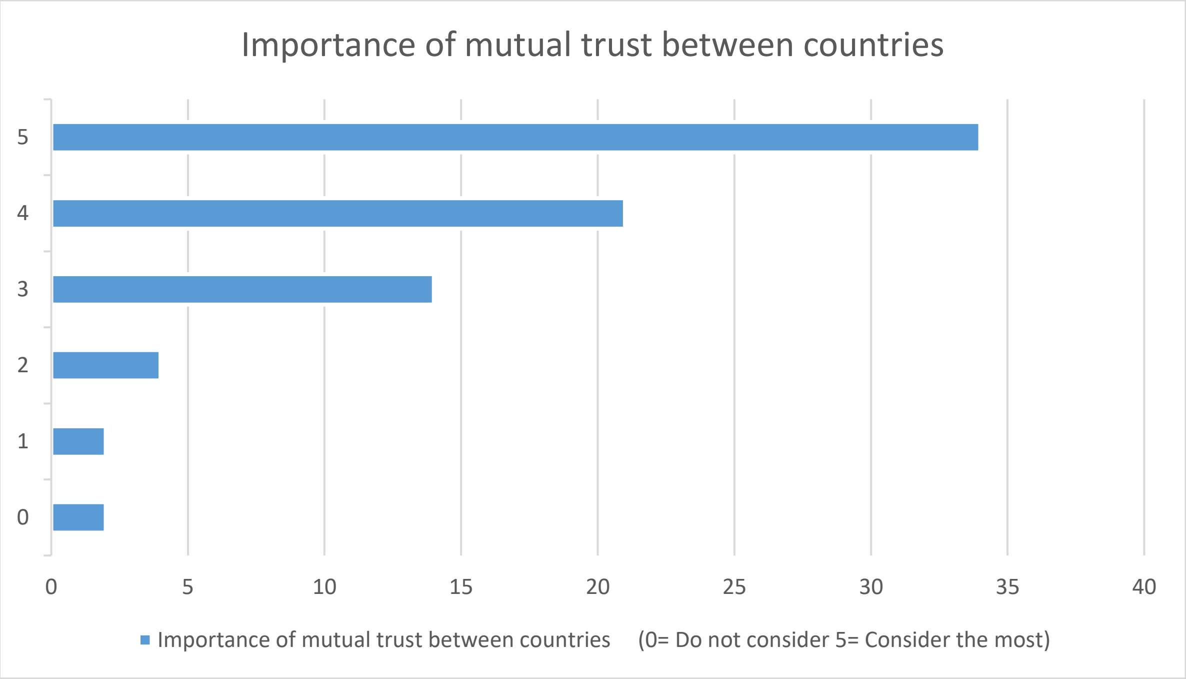


Figure 4.64: Importance of mutual trust between countries (Overview-UK)

A significant amount of participants have indicated the importance of mutual trust between countries and its importance in accepting a global level data privacy and security policy.

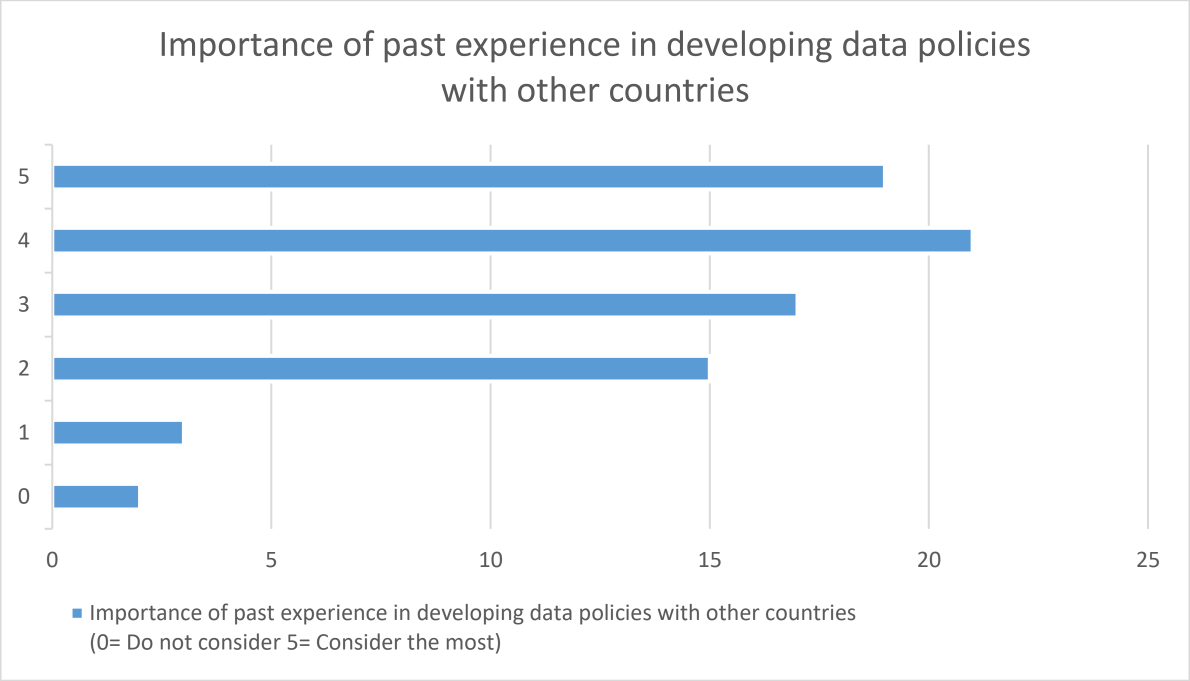


Figure 4.65: Importance of past experience in developing data policies with other counties (Overview-UK)

The majority of participants have indicated the importance of past experience in developing data policies with other counties and its importance in accepting a global level data privacy and security policy.

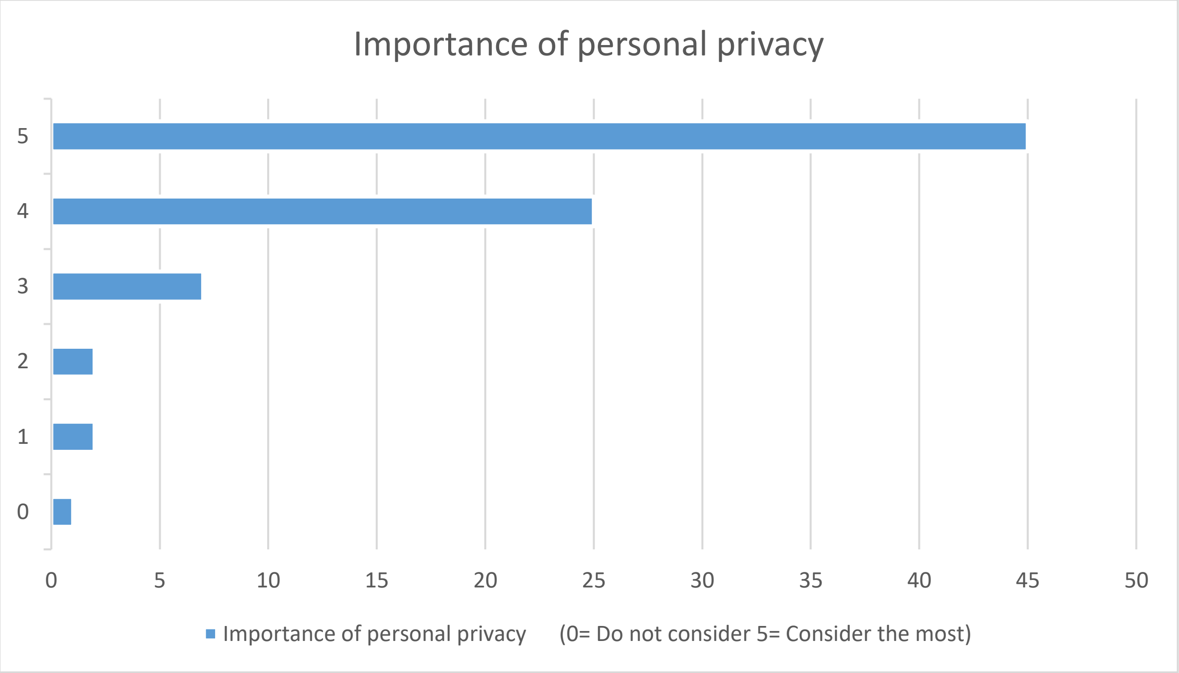


Figure 4.66: Importance of personal privacy (Overview-UK)

A significant amount of participants have indicated the importance of personal privacy and its importance in accepting a global level data privacy and security policy.

In summary, in accepting a global level data protection mechanism, the notable factors the participants would consider are organisational support, budget allocation, economical differences, personal privacy, national security, ease of use of data privacy and security policies, usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure 4.56-4.66).

4.3 Other countries - Overview

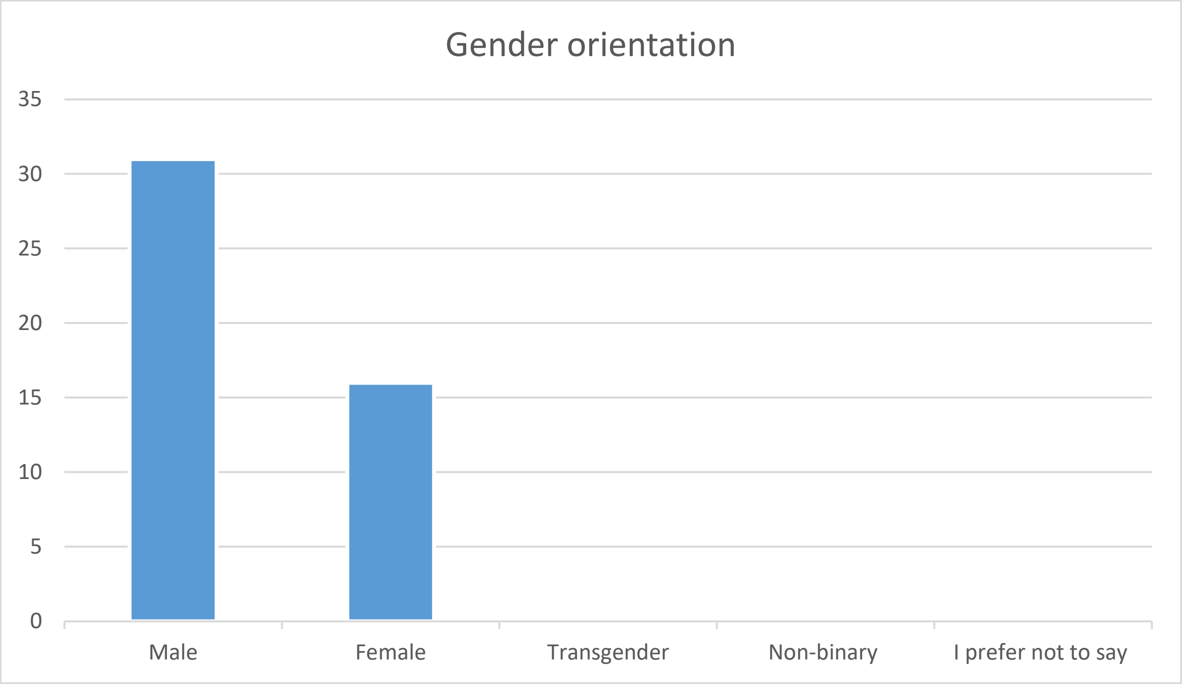


Figure 4.67: Gender orientation (Overview-Other)

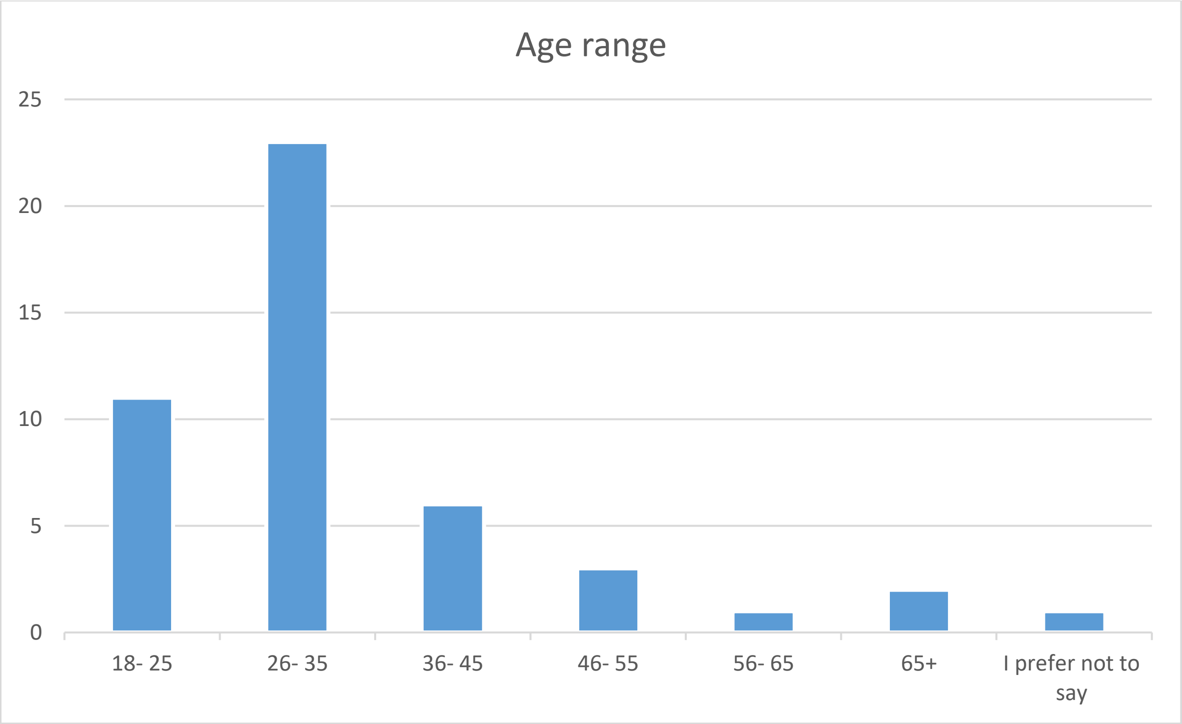


Figure 4.68: Age range (Overview-Other)

This analysis is based on the responses received from the participants outside the United Kingdom and Sri Lanka. The 47 participants consisted of 31 males and 16 females (See figure 4.67). All within 18-65+ age range made up of varying age range groups, 11 of 18-25, 23 of 26-35, 6 of 36-45, 3 of 46-55, 1 of 56-65, and 2 of 65+ range (See figure 4.68). One of the participants preferred not to disclose the age (See figure 4.68).

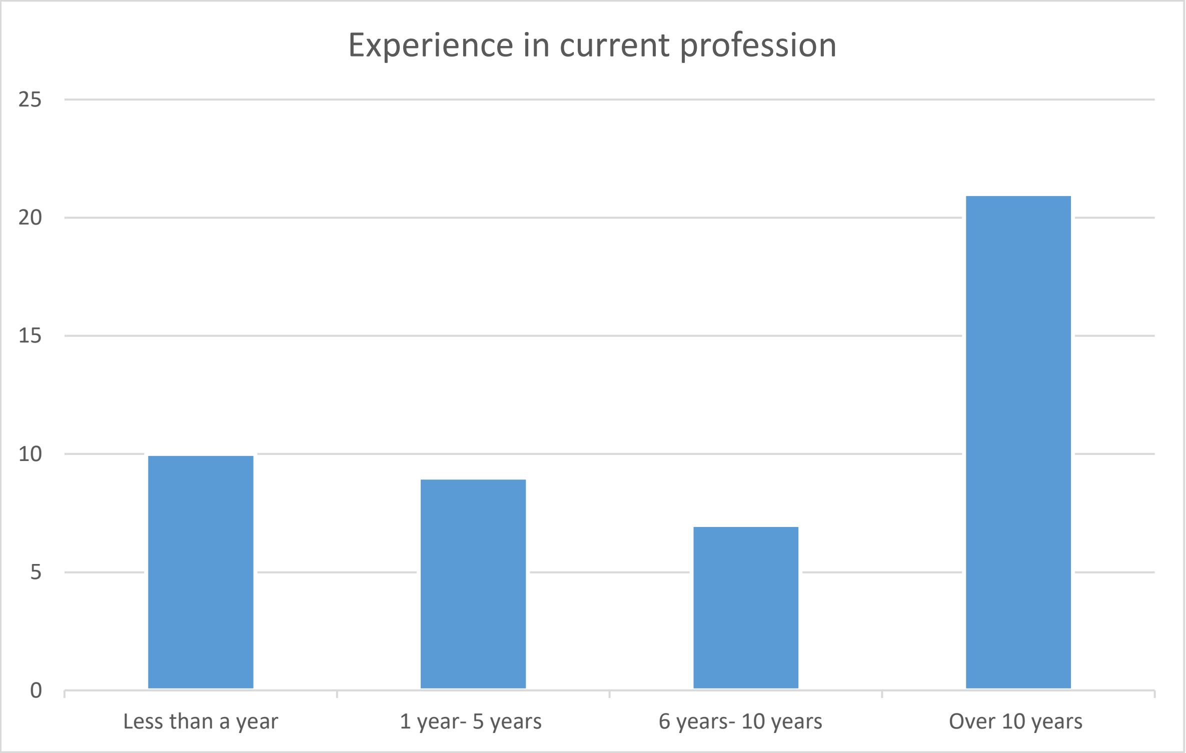


Figure 4.69: Experience in current profession (Overview-Other)

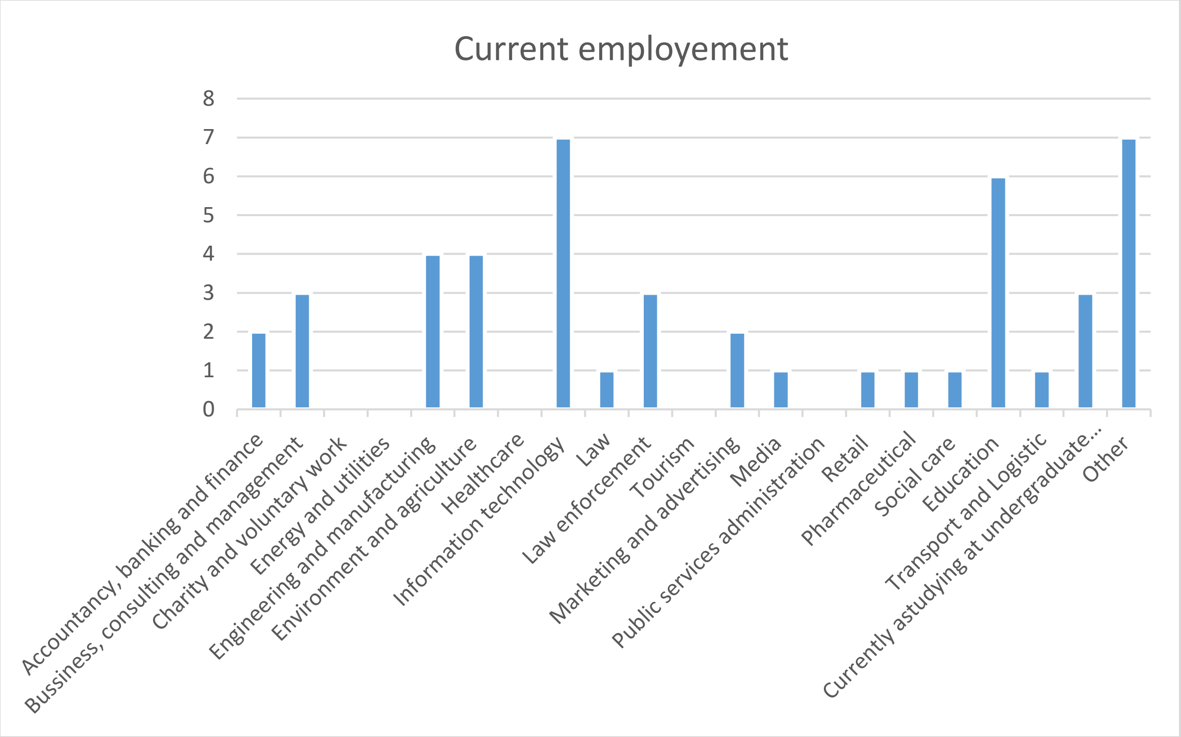


Figure 4.70: Current employment (Overview-Other)

The participants represented different industries (See figure 4.70) with less than a year to over 10 years in employment (See figure 4.69). It appears that most of the participants have working experience of more than 10 years. The diversity amongst the participants based on the gender, age, experience and the current employment is important to conduct an in-depth analysis.

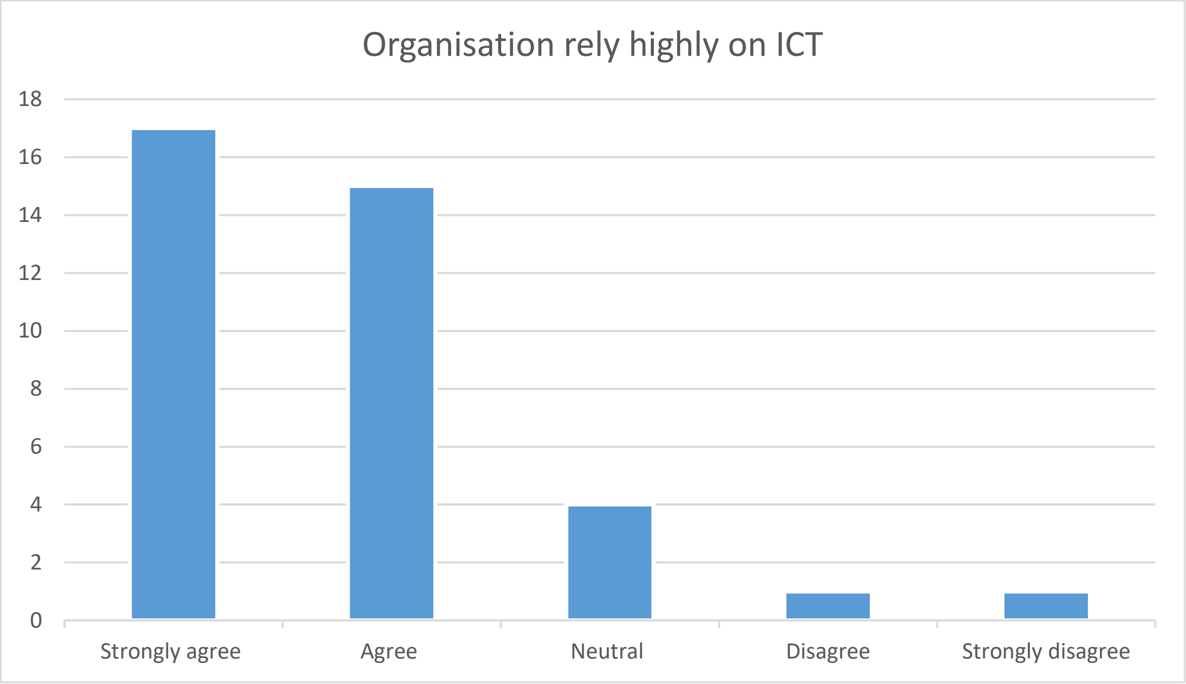


Figure 4.71: Organisation rely highly on ICT (Overview-Other)

Out of the 47 respondents, 32 were employed in a technology reliance working environment, 4 were unaware of reliance on technology because of the nature of the work assigned to them, only 2 marked 'disagree' on ICT (See figure 4.71). This indicates that a majority of the participant from other countries worked in an environment with high reliance on ICT.

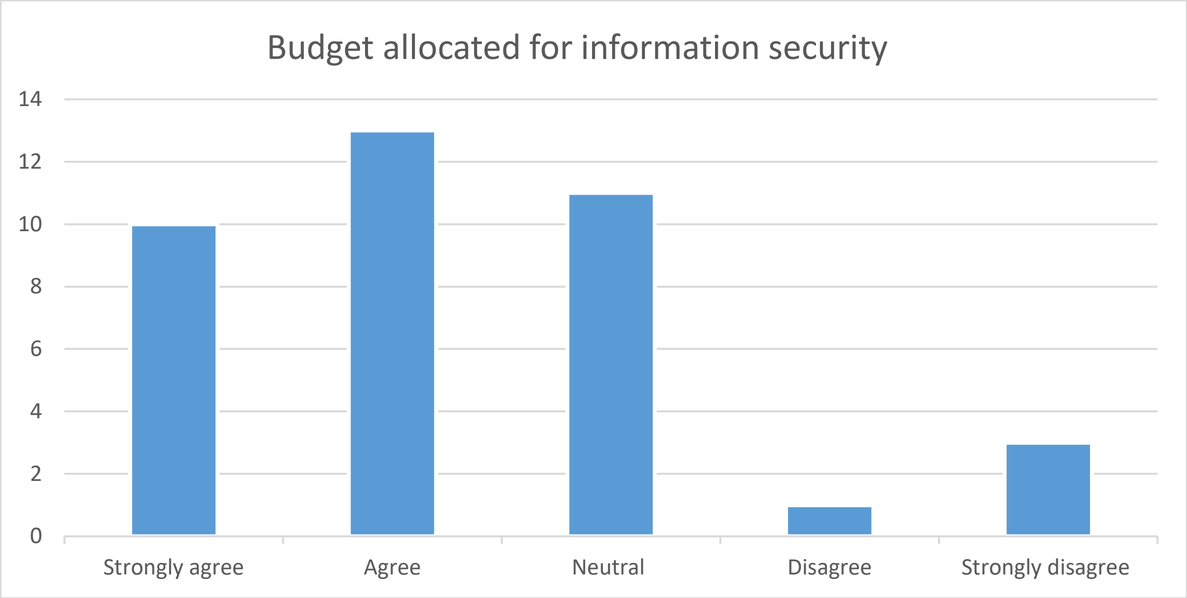


Figure 4.72: Budget allocated for information security (Overview-Other)

23 out of the 47 indicated that their organisations had an allocated budget for information security, and 11 did not express an opinion either way, and according to the 4 disagreed, their organisations had no budget allocation for information security (See figure 4.72). Compared to the high reliance on technology, the budget allocation seems to be relatively low. This could be because of their economic status or due to ongoing issues such as conflicts, natural disasters and social problems with in countries they might not have sufficient funds to allocate to information security. This is why it is important to encourage developed countries who have the resources to support developing/less developed countries is important.

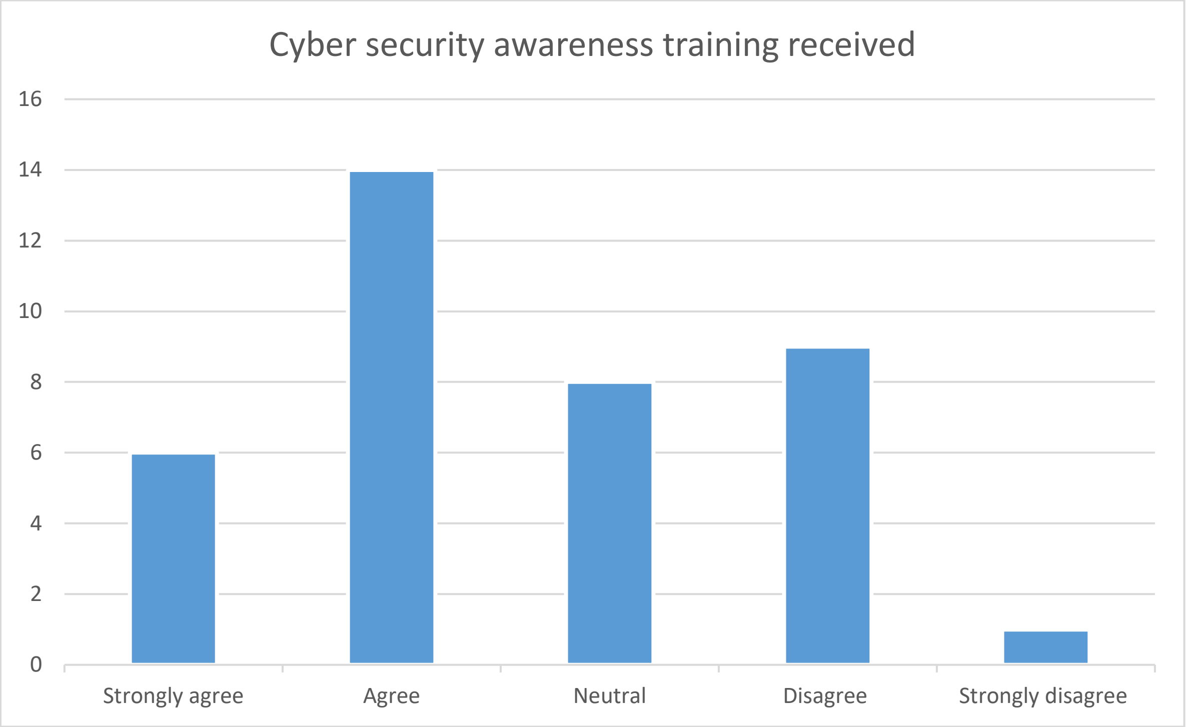


Figure 4.73: Cyber security awareness training received (Overview-Other)

Some of the participants inferred the inadequacy of the regular security awareness training received. Only 20 participants had received regular cyber security awareness training, whilst 8 neither agreed nor disagreed, and 10 participants had not (See figure 4.73). The lack of cyber security awareness training could be due to a lack of resources.

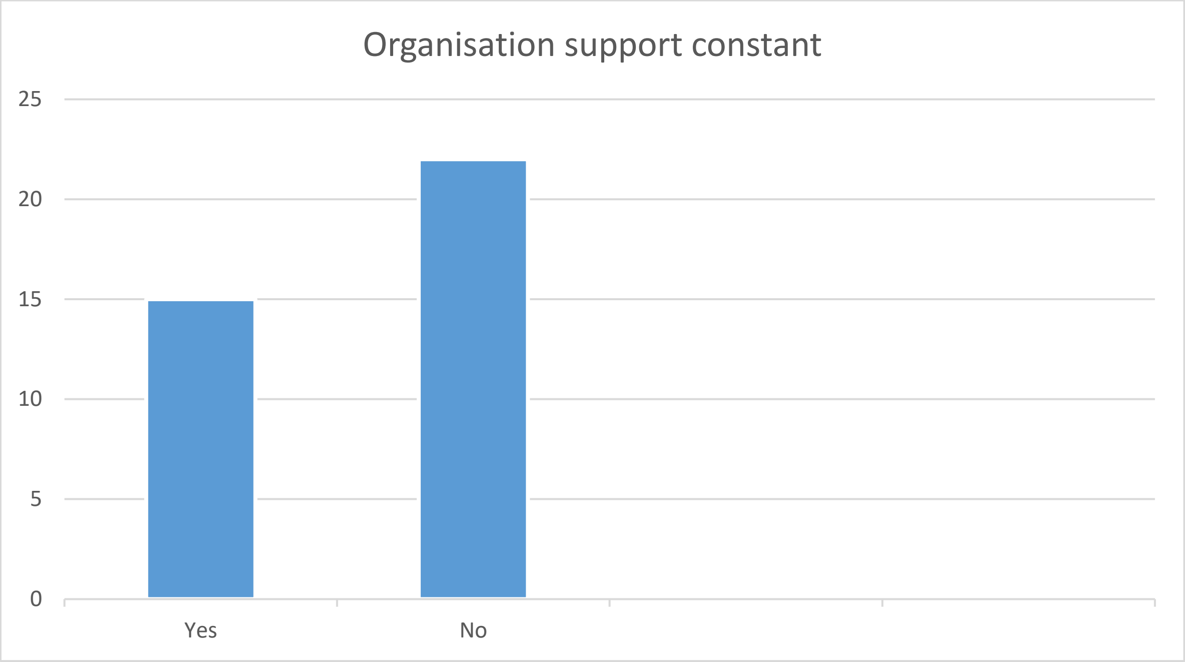


Figure 4.74: Organisation support constant (Overview-Other)

Except for the 15 who did, 22 participants had not received support from the organisation to protect personal information (See figure 4.74). This clearly indicated the disparity between high reliance on technology and the insufficient level of the allocated budget and organisational support to protect personal information.

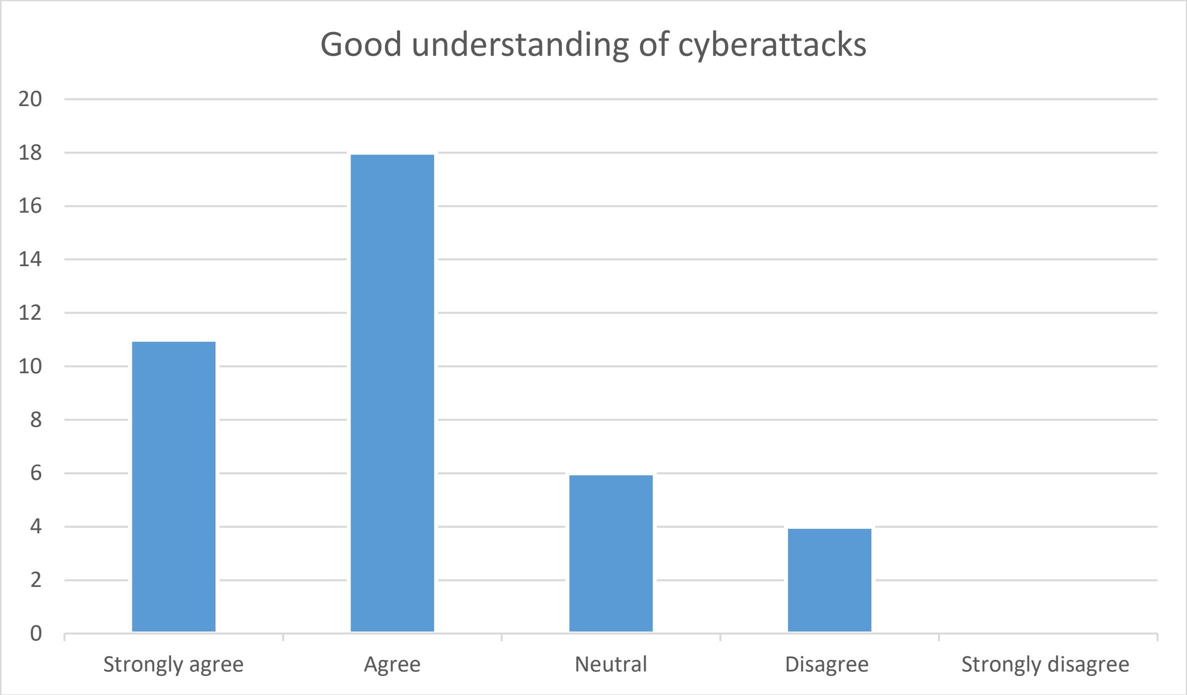


Figure 4.75: Good understanding of cyberattacks (Overview-Other)

Despite the lack of security awareness training, 29 participants claimed to possess a high understanding of the impact of cyber-attacks on the public and the organisation, 6 not expressed an opinion either way, and only 4 claimed to have no understanding (See figure 4.75). It is reasonable to assume that individuals take their own initiative to make themselves aware of the cyber threats happening around them and their impact on them and society.

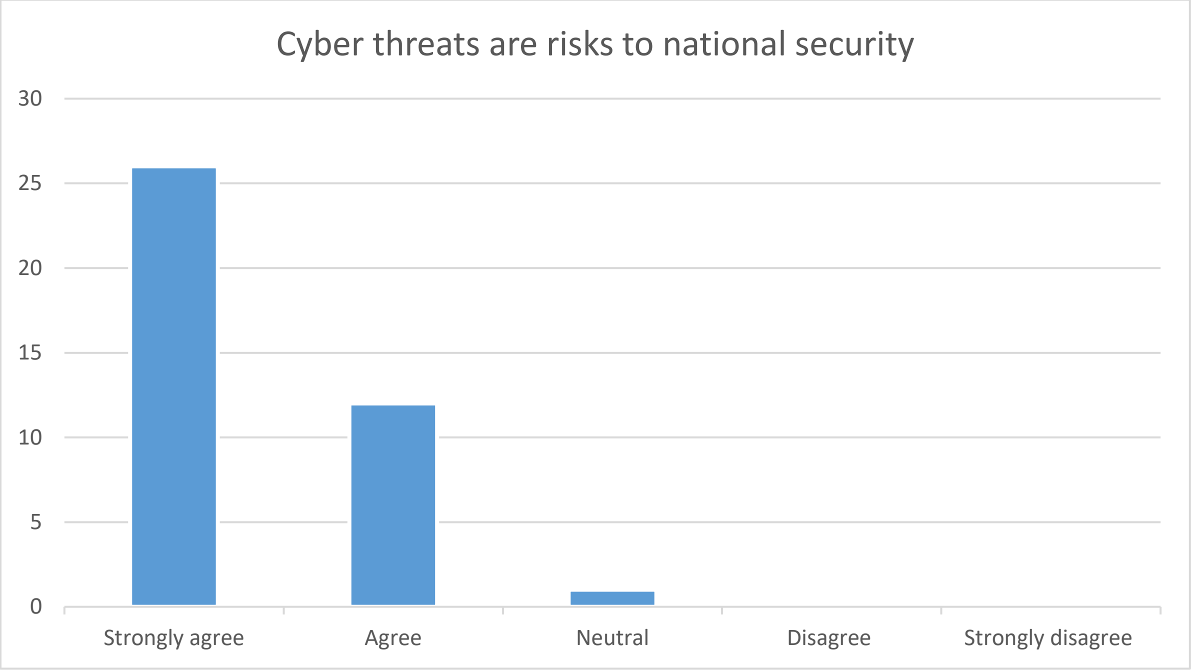


Figure 4.76: Cyber threats are risks to national security (Overview-Other)

Furthermore, 81 percent of the participants appear to be familiar with potential threats to national security from cyber-attacks (See figure 4.76). In general, understanding cyber threats and their impact on national security make people act responsibly to minimise end-user errors, and their views would count towards accepting and implementing a national, regional, and global level mechanism.

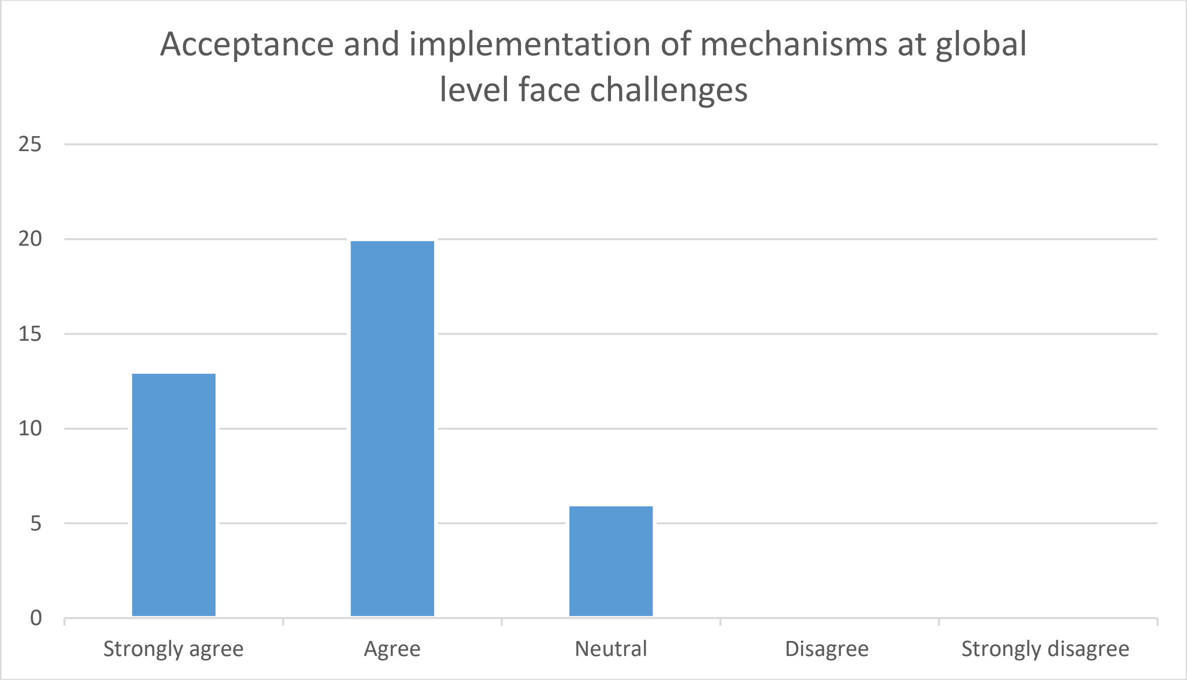


Figure 4.77 Acceptance and implementation of mechanisms at global level face challenges (Overview-Other)

A significant majority has highlighted that acceptance and implementation of mechanisms at the global level face challenges (See figure 4.77). Understanding the barriers that the countries face would help in overcoming the challenges and bring countries together.

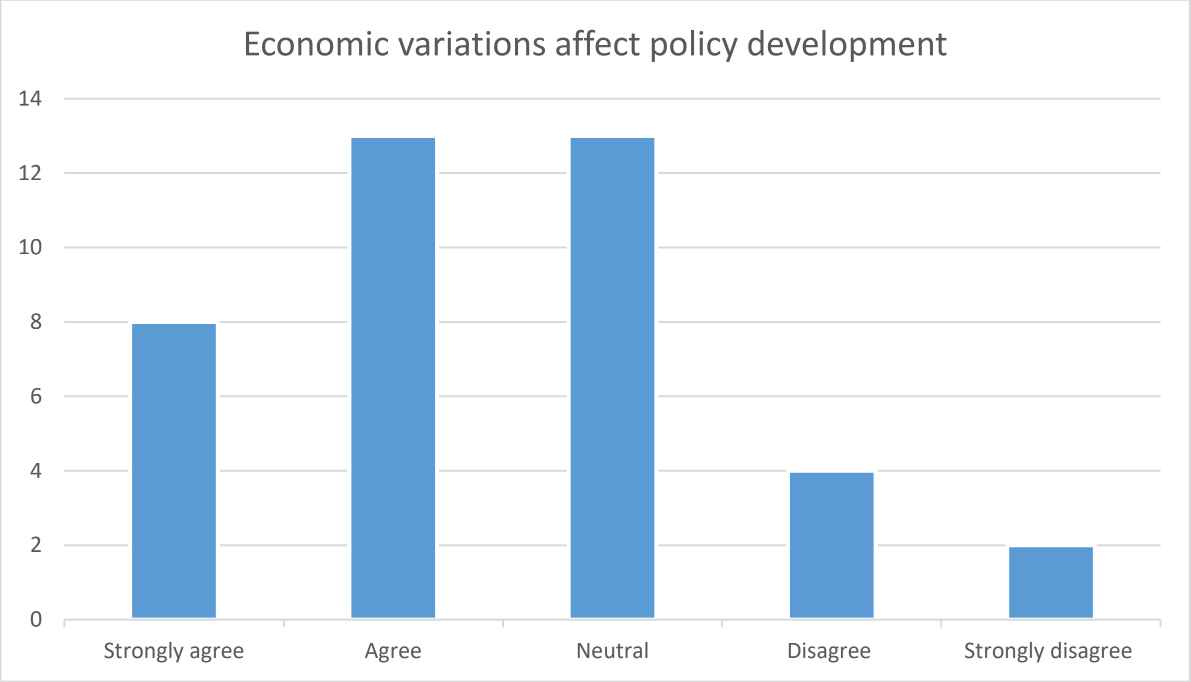


Figure 4.78: Economic variations affect policy development (Overview-Other)

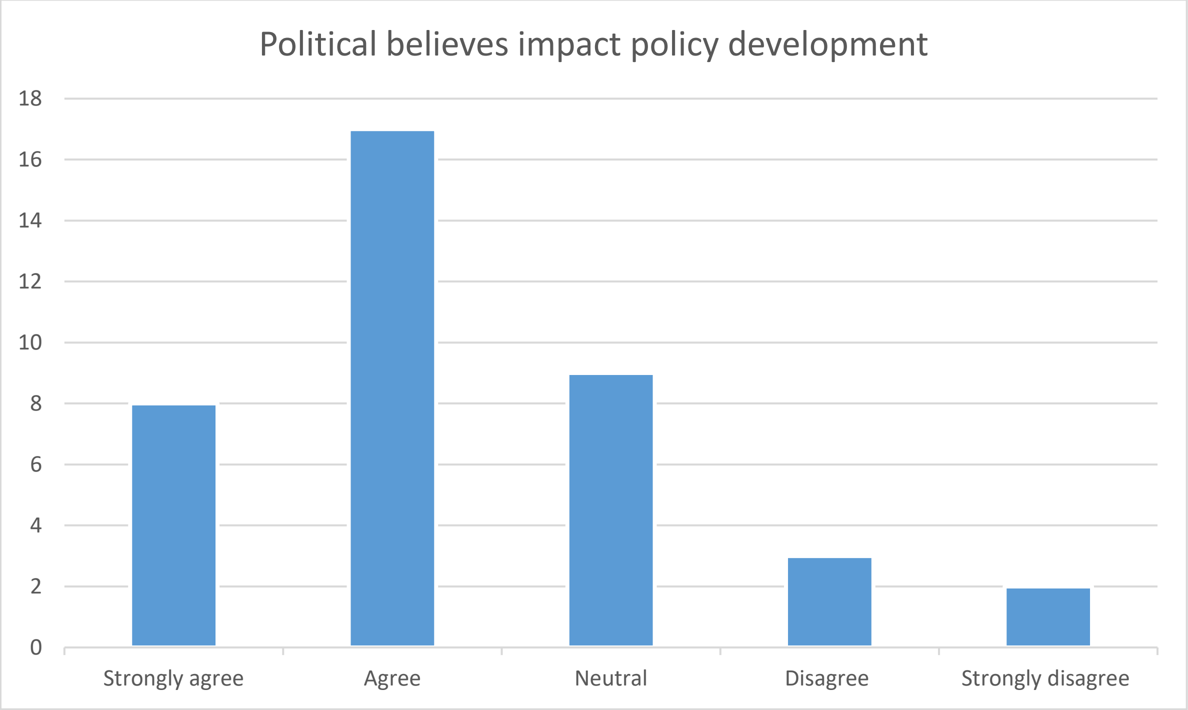


Figure 4.79: Political differences impact policy development (Overview-Other)

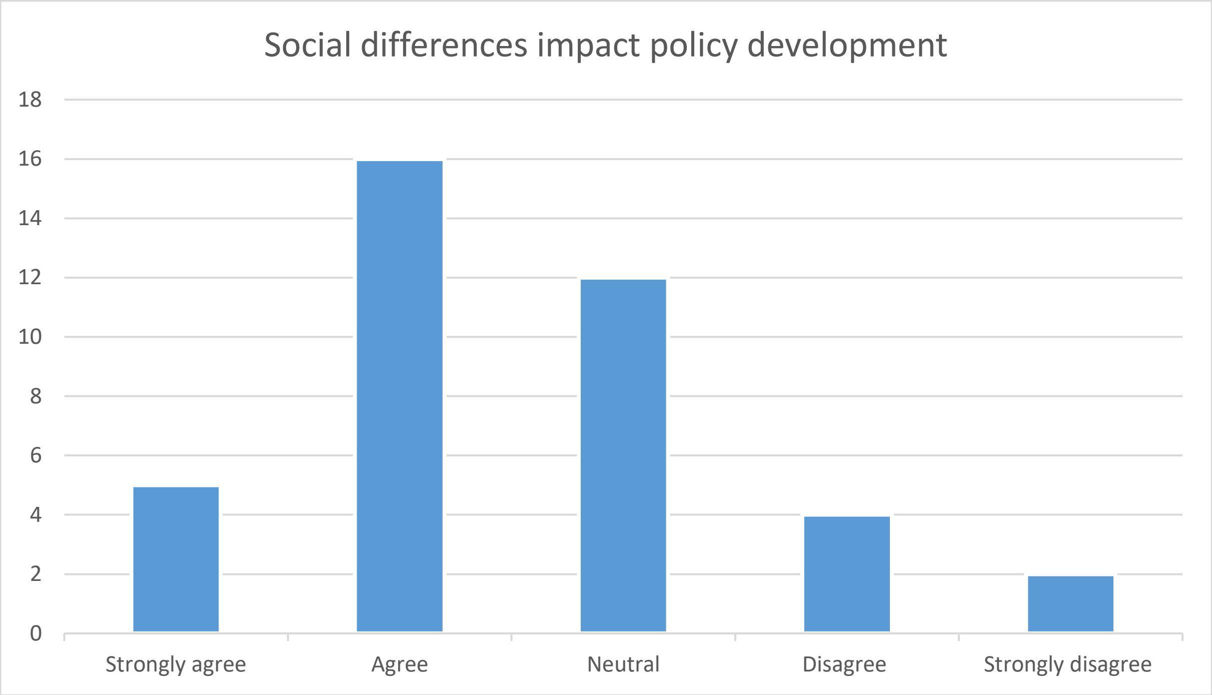


Figure 4.80: Social differences impact policy development (Overview-Other)

The participants have highlighted the impact of economic (See figure 4.78), political (See figure 4.79) and social differences (See figure 4.80) through their responses. Understanding of these differences would help to find a way to support those countries and to eliminate the challenges. Because differences between countries hinders the progress of collective actions at the regional and global level.

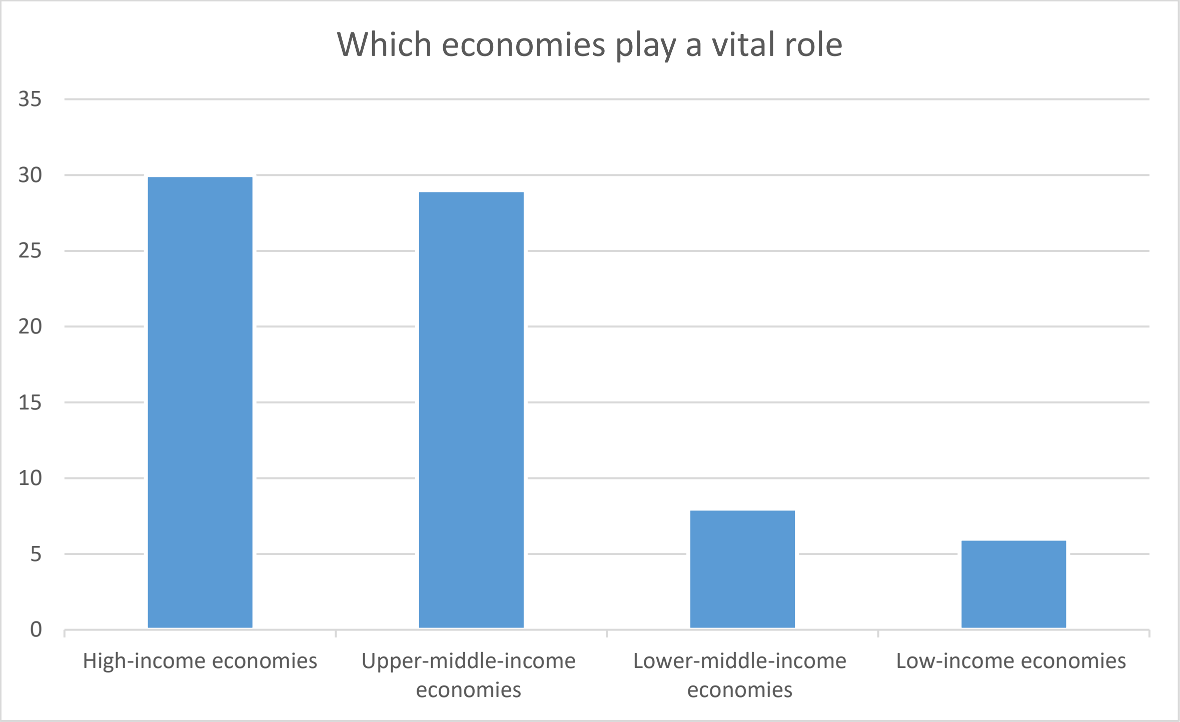


Figure 4.81: Which economies play a vital role (Overview-Other)

In the questionnaire, the responses of the majority state that the high income and upper-middle-income countries play a vital role in the policymaking process (See figure 4.81). There are key stages in the policymaking process and are described as identifying policymaker aims, identifying the policies to achieve those aims, selecting a policy measure, identifying the necessary resources, implementing and post-implementation evaluation of the policy. These stages are time-consuming, costly, and demanding in resources. Therefore, it is fair to say that the policymaking process is driven by the economic stability and the availability of resources in the country.

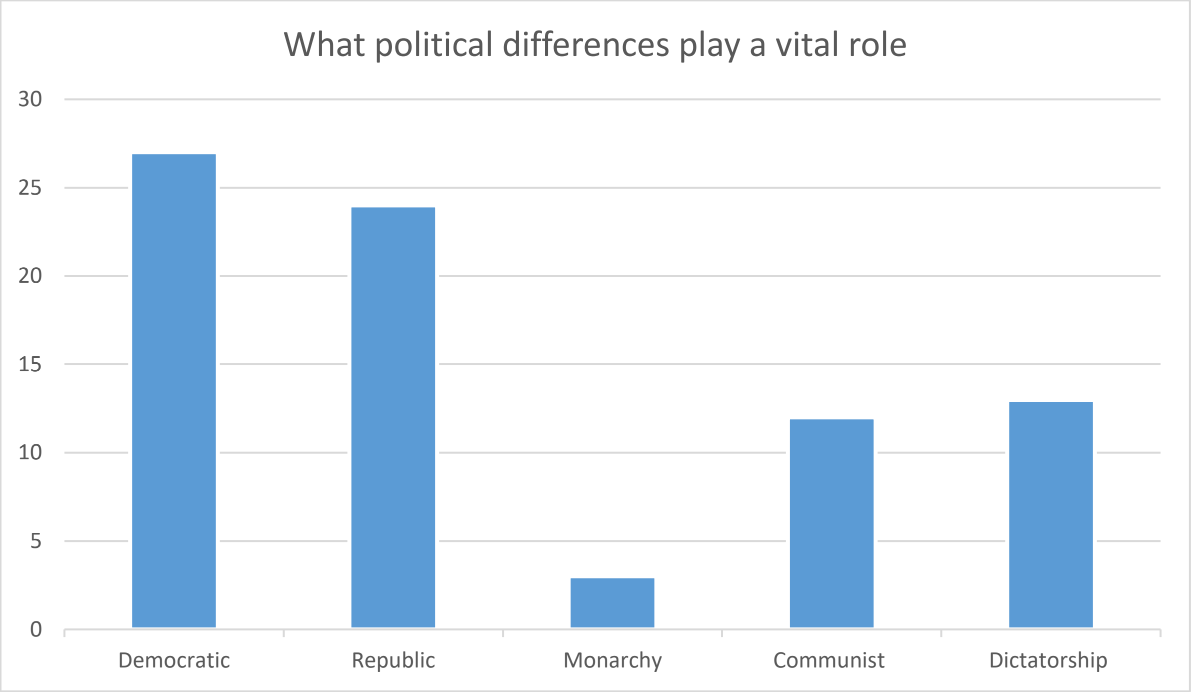


Figure 4.82: What political differences play a vital role (Overview-Other)

The majority chooses democratic and republican political systems (See figure 4.82) in preference to others because of the influence of the public voice in the process of policy development and encompass consensus and collective responsibility for their actions. The adherence to these norms contributes to developing trustworthiness and cordiality between organisations and creates a conducive environment for policy development. In a Republican system, the people and their elected representatives hold power, and they take decisions in accordance with constitutional norms. That leads to the assumption that the elected representatives seek legal assurance from the governments and the organisations involved in collecting, sharing, and retaining personal information that they would not compromise people’s privacy for any given reason.

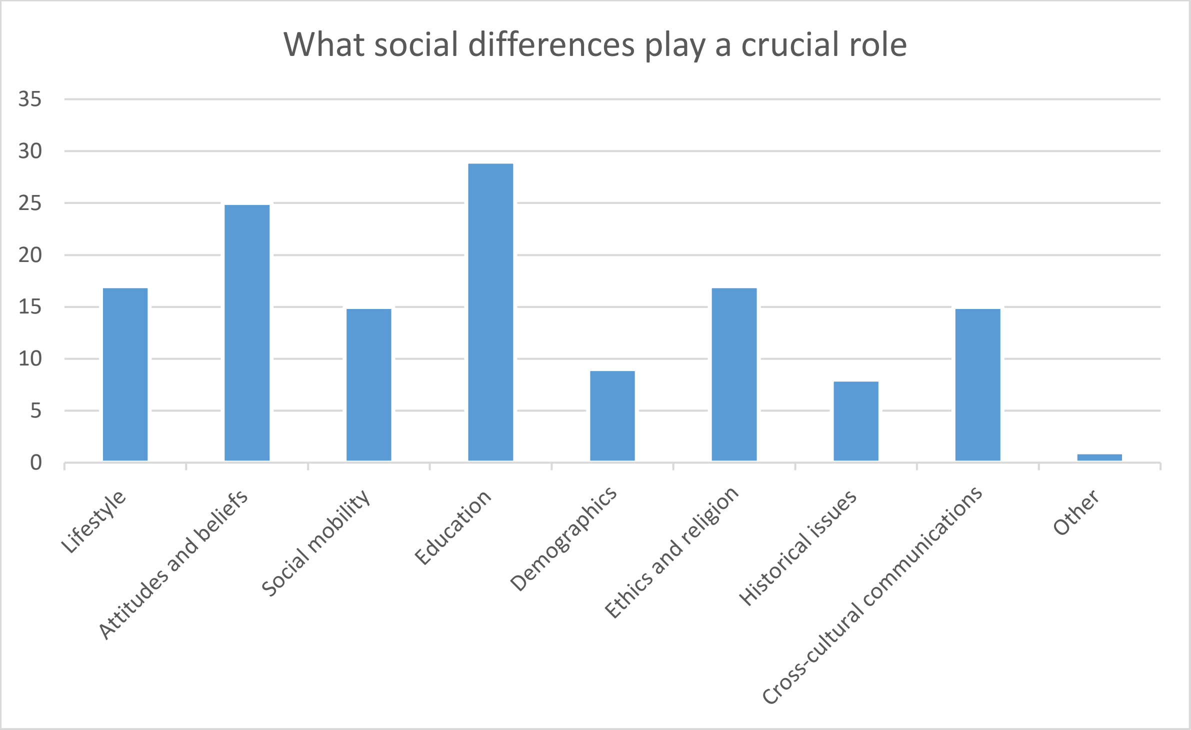


Figure 4.83: What social differences play a crucial role (Overview-Other)

The response to the social differences listed in the questionnaire, majority has highlighted the importance of education and attitudes and beliefs (See figure 4.83). Familiarity with potential cyber threats and their impact on people and national security contributes to accepting and implementing data privacy and security policies. Therefore, it is important to provide cyber security awareness training at schools and at the organisational level. Self-belief in privacy and respecting the privacy of others are also contributory factors discussed under attitude and beliefs.

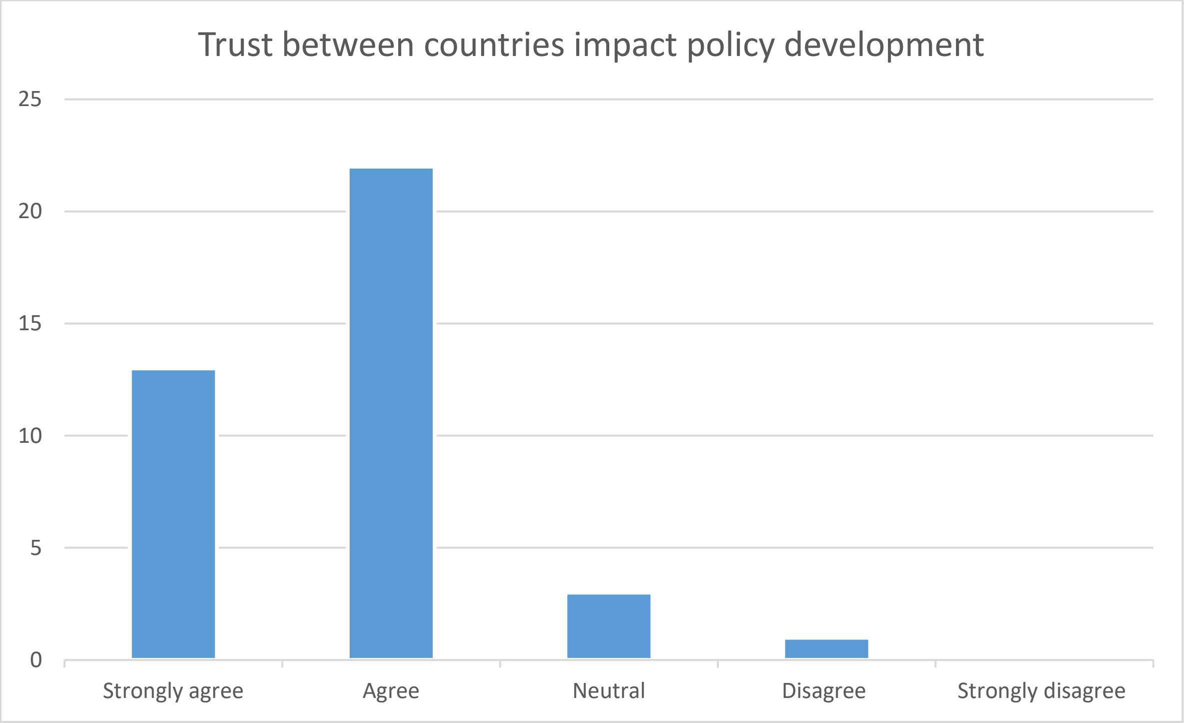


Figure 4.84: Trust between countries impact policy development (Overview-Other)

The majority of the participants from countries except Sri Lanka and the UK has also believed that trust between countries impacts policy development. This idea has been endorsed by 35 participants all together from other countries (See figure 4.84). Even though trust appears to be an important factor, due to the differences amongst countries, developing and maintaining trust for a long time is difficult. However, having trust will give each other the confidence to work together in the regional and global environment.

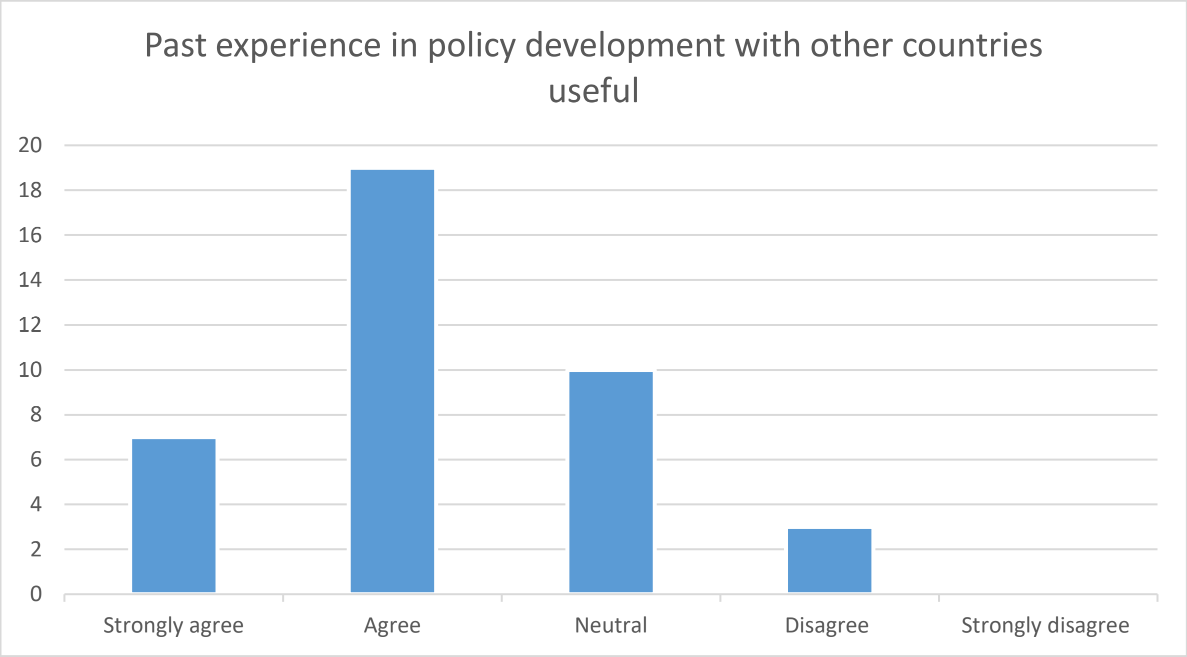


Figure 4.85: Past experience in policy development with other countries useful (Overview-Other)

A significant number has also highlighted the usefulness of having past experience in policy development. 7 strong agree, 19 agree, 10 neutral, 3 disagree, and notably, no one strongly disagree (See figure 4.85). Past experience in developing policies would come handy when it comes to drafting, developing and negotiating policies.

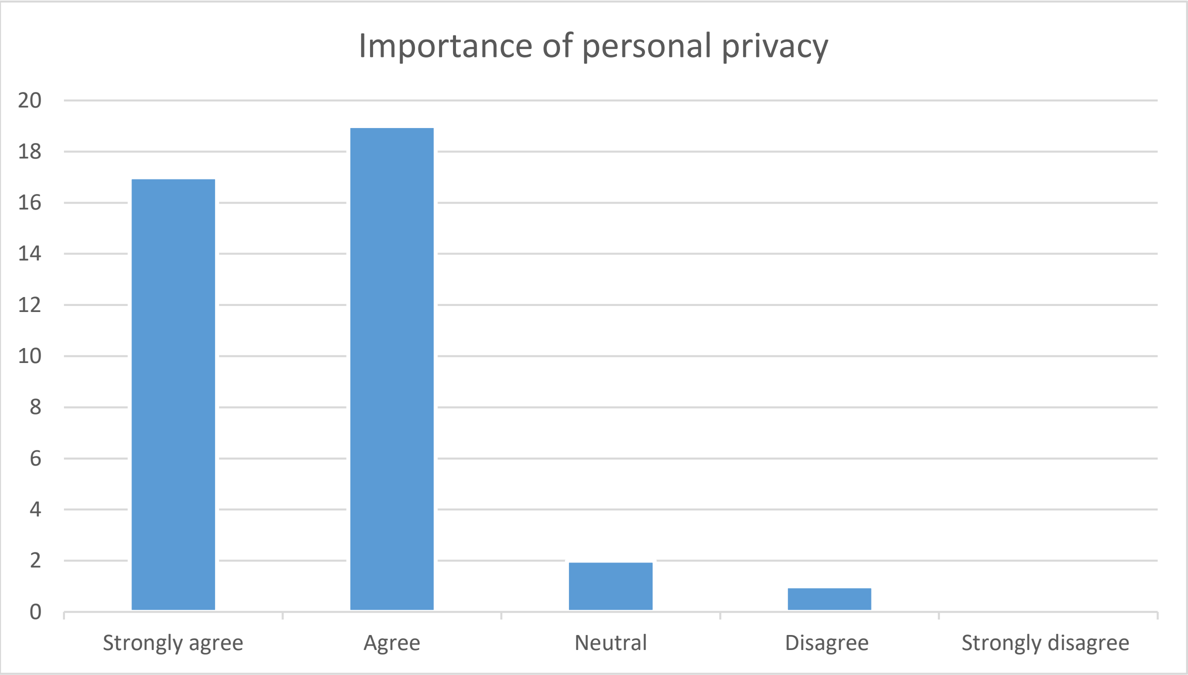


Figure 4.86: Importance of personal privacy (Overview-Other)

A significant amount of participants have indicated the importance of personal privacy and its importance in accepting a global level data privacy and security policy (See figure 4.86).

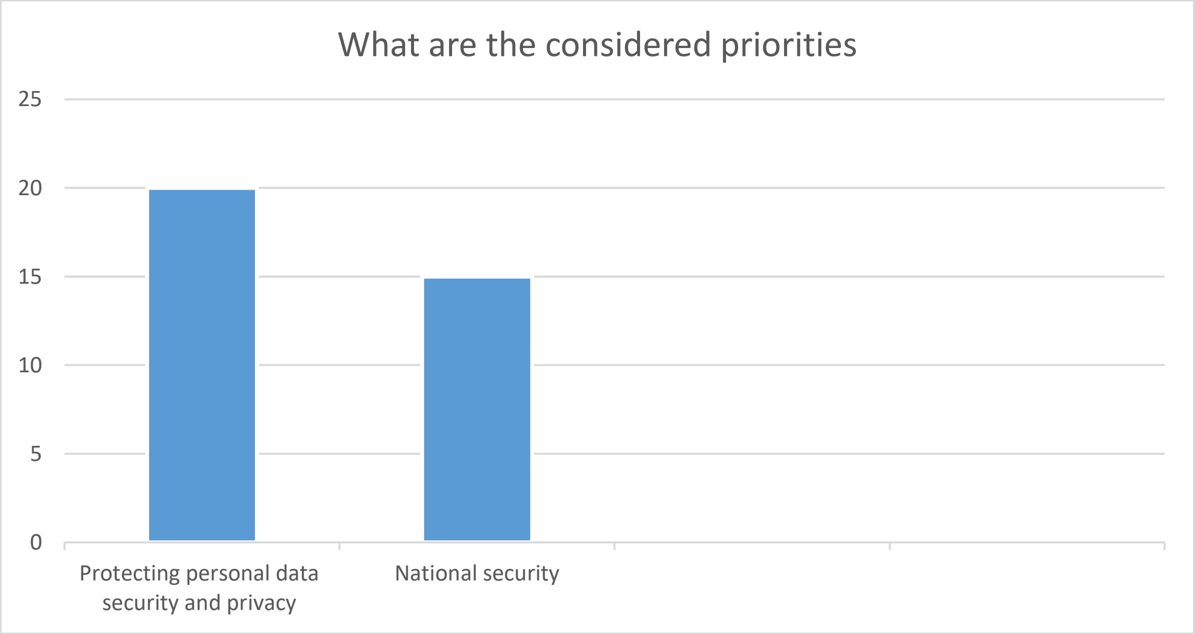


Figure 4.87: What are the considered priorities (Overview-Other)

The majority of the respondents give priority to the protection of personal data security and privacy when accepting and implementing a global data privacy and security policies whilst not discounting national security, and a lesser number believes in national security (See figure 4.87).

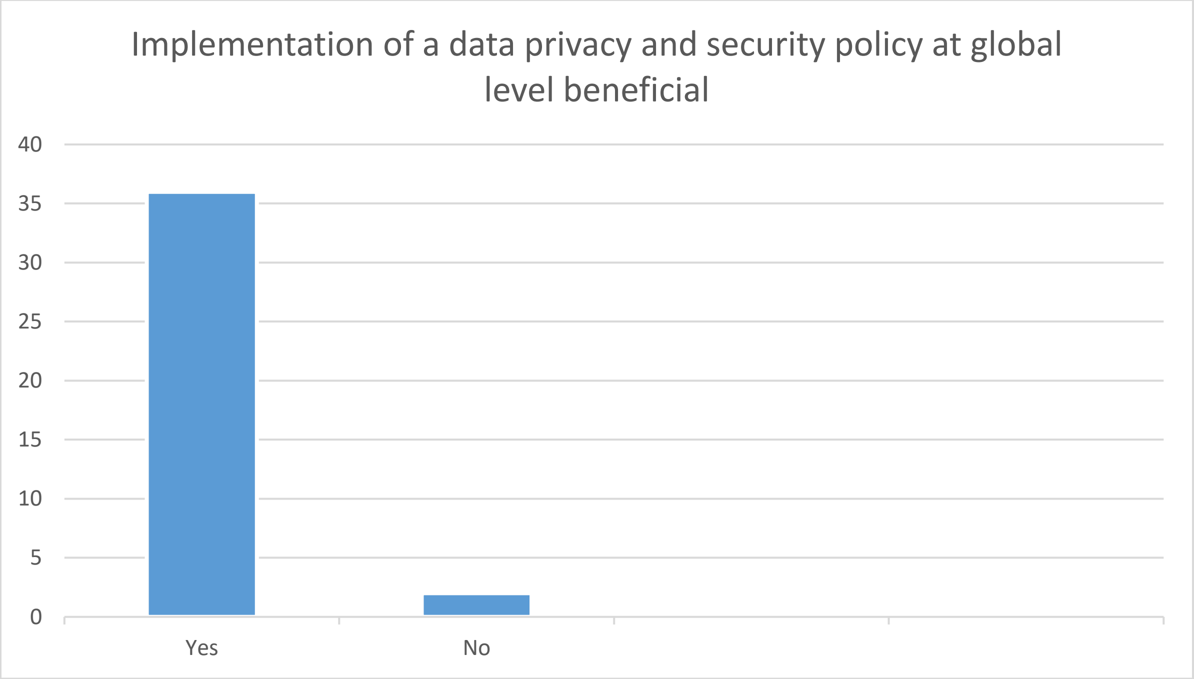


Figure 4.88: Implementation of a data privacy and security policy at global level beneficial (Overview-Other)

The message from the respondents is clear. It is a compelling need to have a global level data protection mechanism, with the endorsement of 77 percent of the respondents (See figure 4.88). This shows that despite the prevailing challenges and differences amongst the countries, participants do strongly believe that it is important to have a global level data protection mechanism to protect their personal privacy and national security of the country.

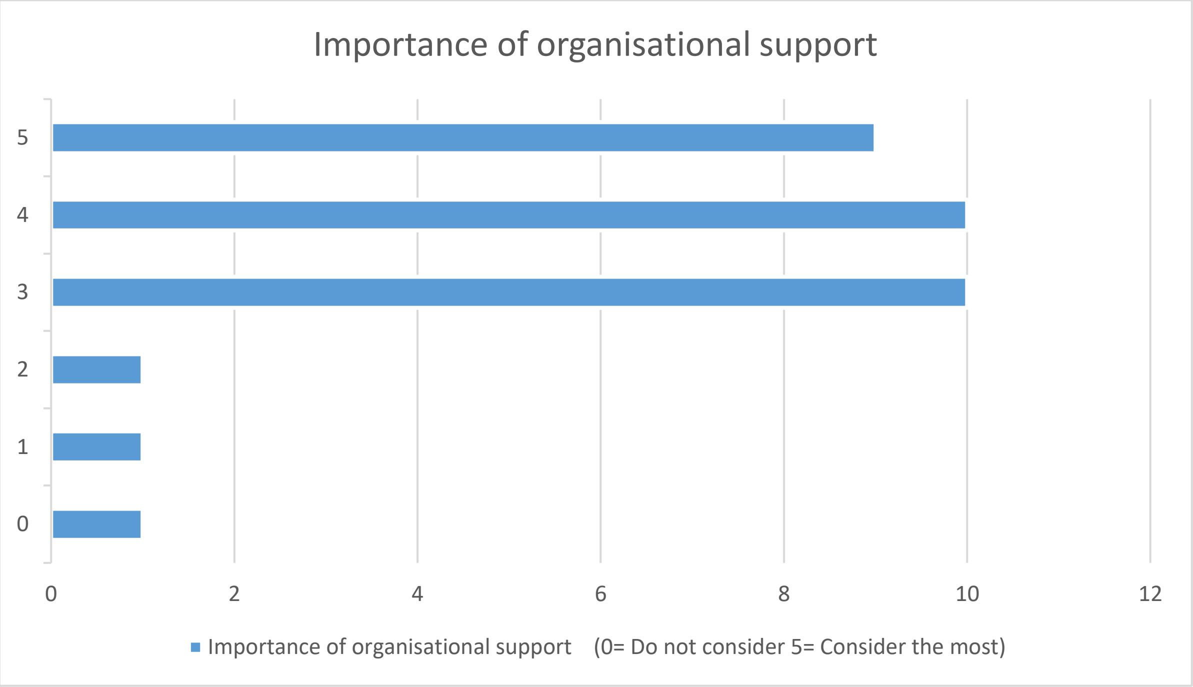


Figure 4.89: Importance of organisational support (Overview-Other)

The majority of participants have indicated that organisation support needs to be considered, and it is important in accepting a global level data privacy and security policy.

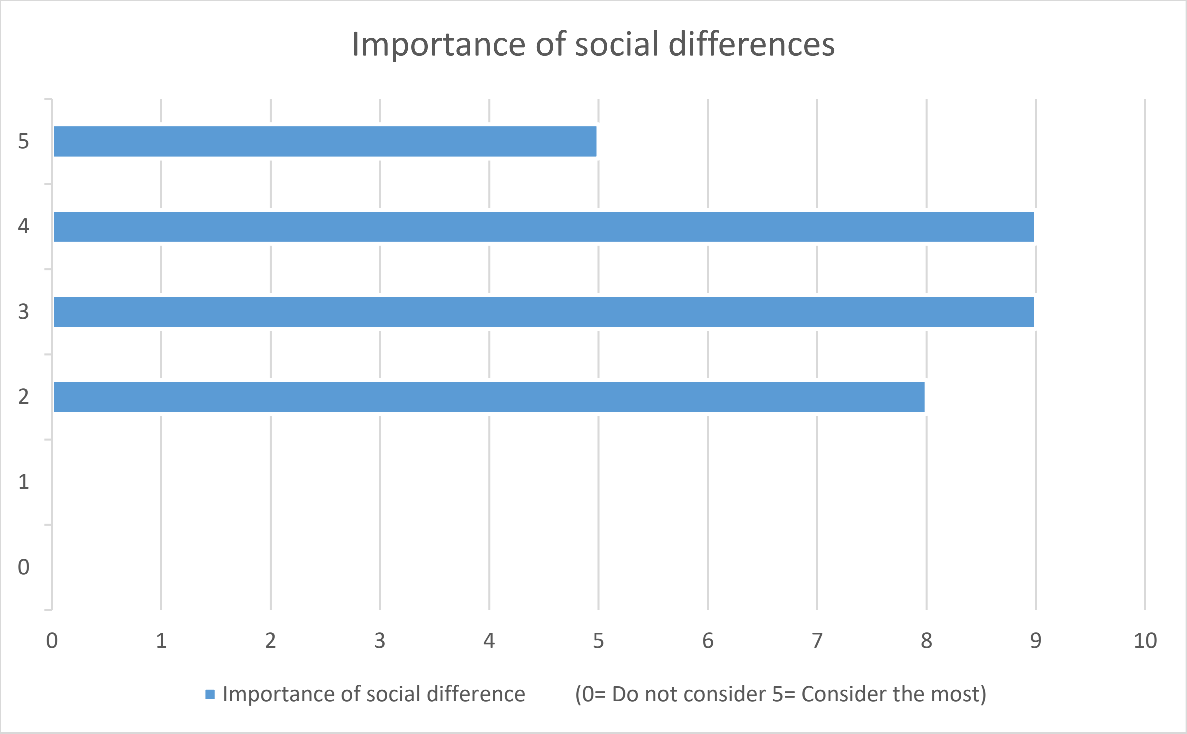


Figure 4.90: Importance of social differences (Overview-Other)

The majority of participants have not indicated that social differences need to be considered, and it is important in accepting a global level data privacy and security policy.

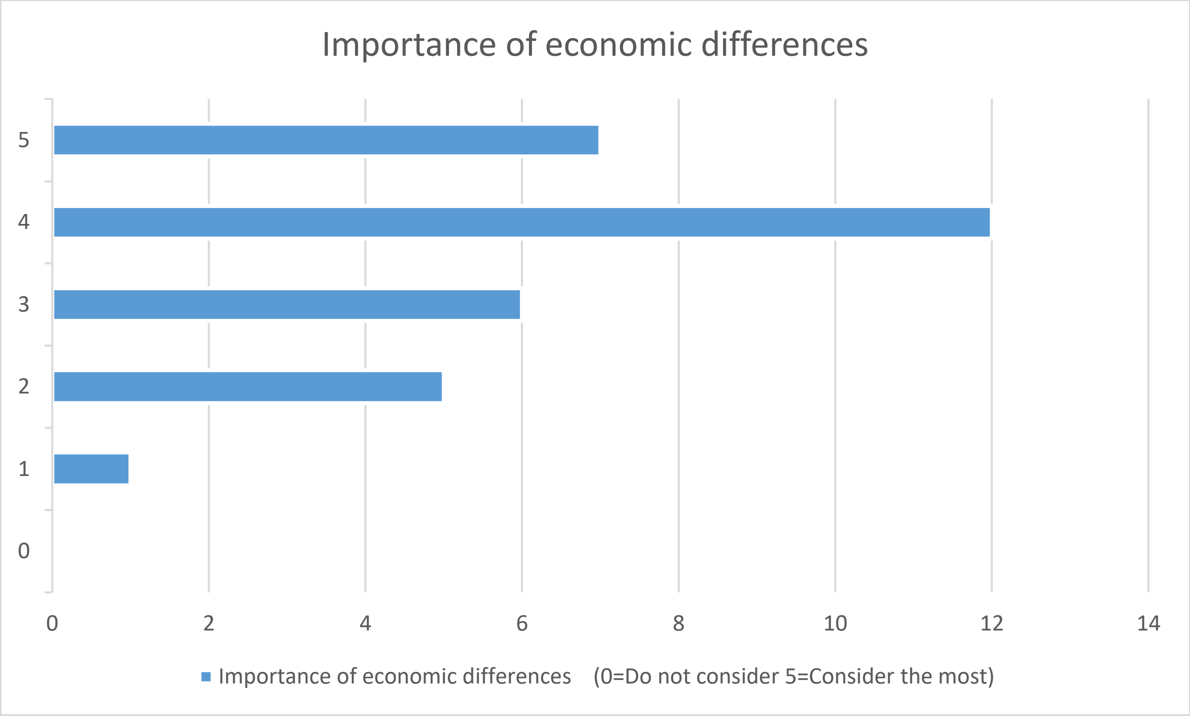


Figure 4.91: Importance of economic differences (Overview-Other)

The majority of participants have indicated that economic differences need to be considered, and it is important in accepting a global level data privacy and security policy.

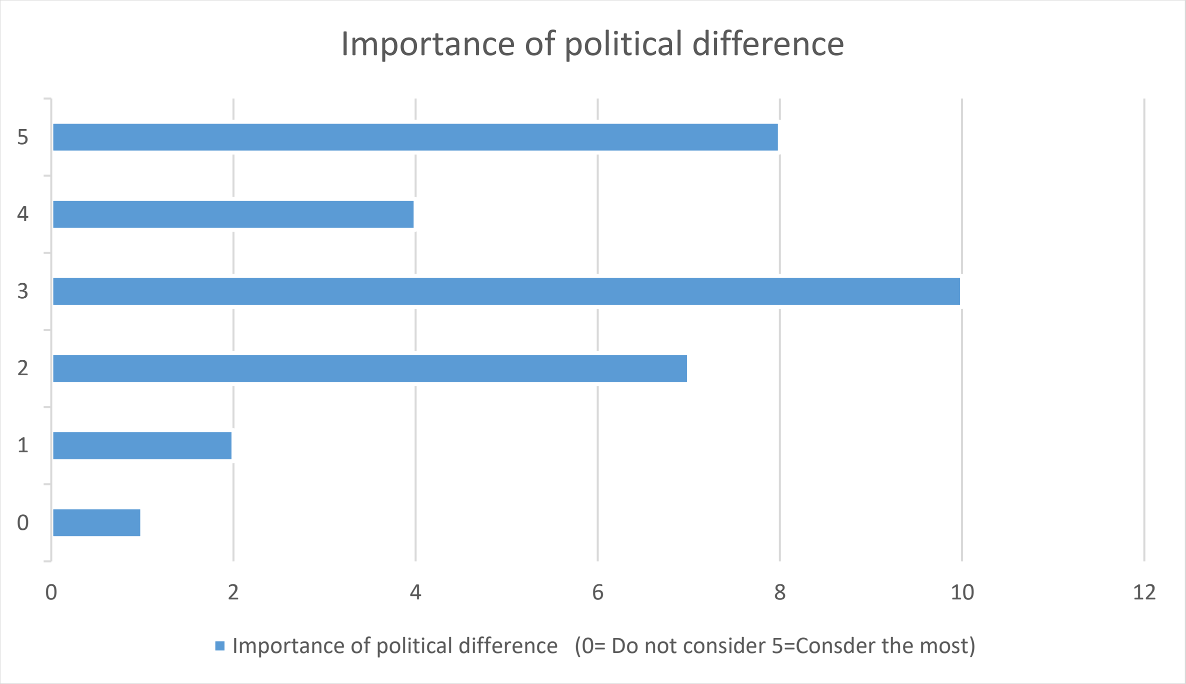


Figure 4.92: Importance of political difference (Overview-Other)

The majority of participants have not indicated that political differences need to be considered, and it is important in accepting a global level data privacy and security policy.

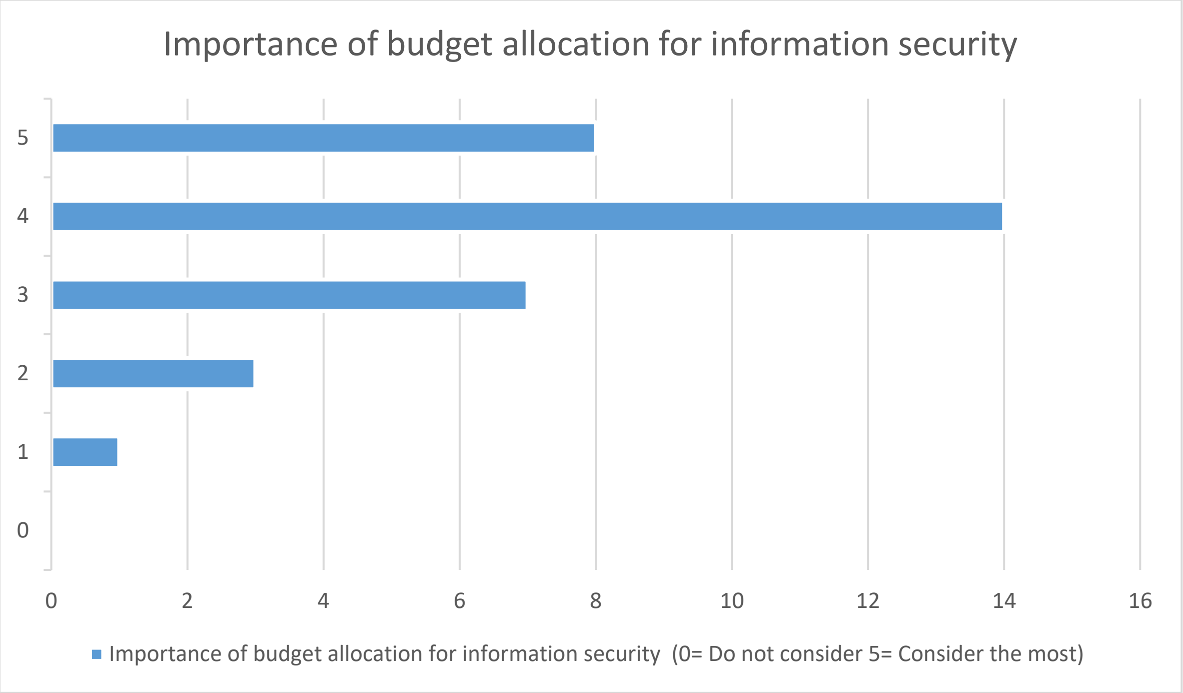


Figure 4.93: Importance of budget allocation for information security (Overview-Other)

The majority of participants have indicated the importance of budget allocation for information security needs to be considered, and it is important in accepting a global level data privacy and security policy.

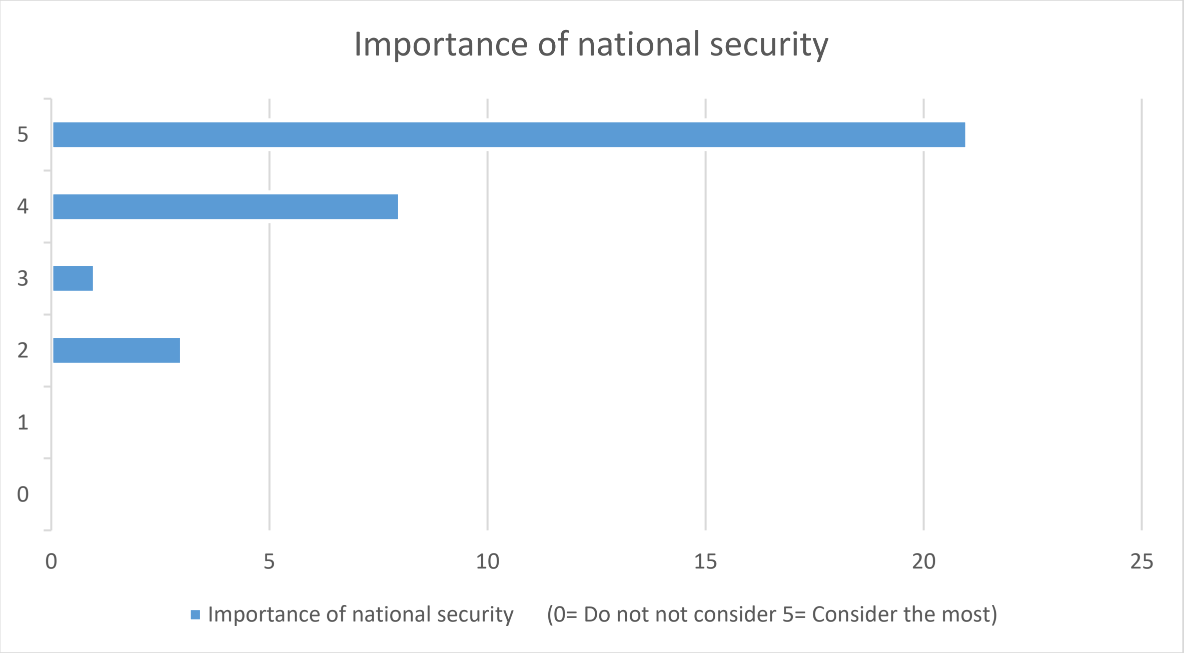


Figure 4.94: Importance of national security (Overview-Other)

A significant amount of participants have indicated that national security needs to be considered, and it is important in accepting a global level data privacy and security policy

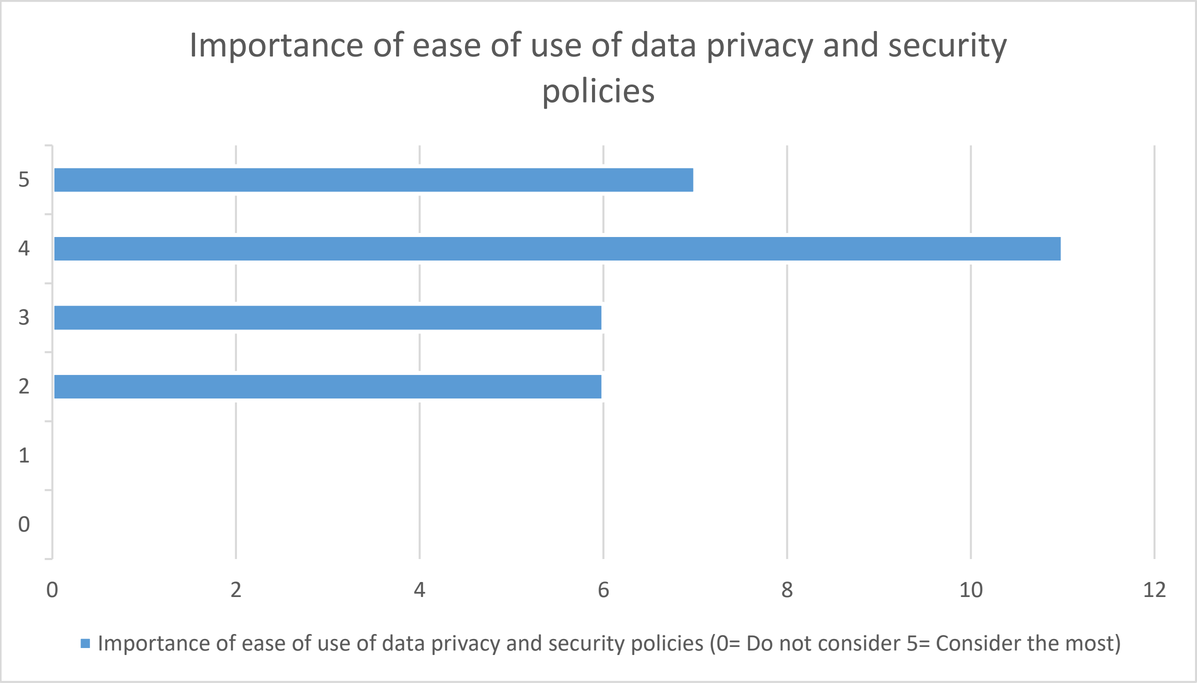


Figure 4.95: Importance of ease of use of data privacy and security policies (Overview-Other)

The majority of participants have indicated the ease of use of data privacy and security policies needs to be considered, and it is important in accepting a global level data privacy and security policy.

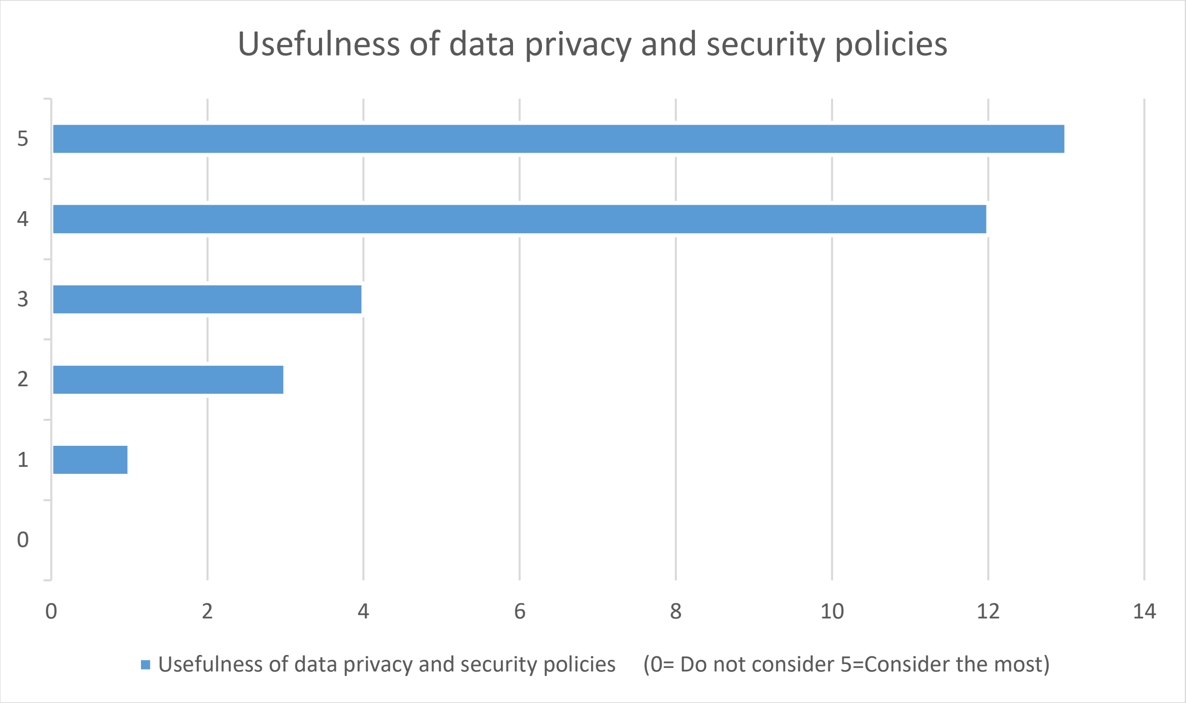


Figure 4.96: Usefulness of data privacy and security policies (Overview-Other)

The majority of participants have indicated the need to considered the usefulness of data privacy and security policies and its importance in accepting a global level data privacy and security policy.

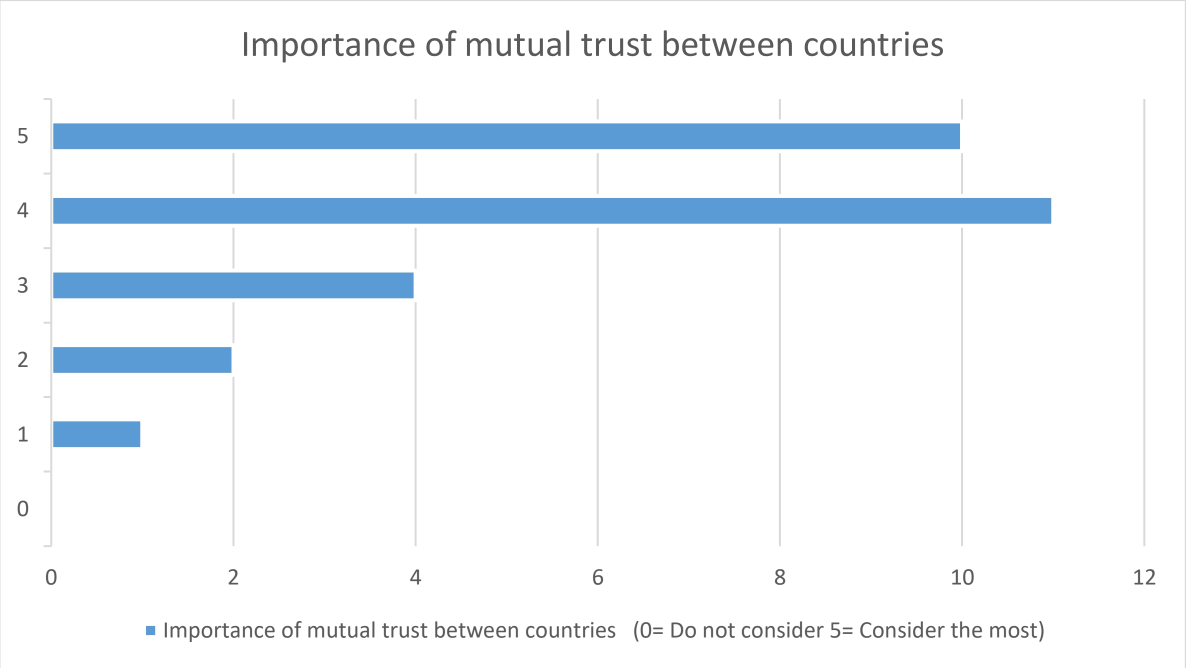


Figure 4.97: Importance of mutual trust between countries (Overview-Other)

The majority of participants have indicated the importance of mutual trust between countries and its importance in accepting a global level data privacy and security policy.

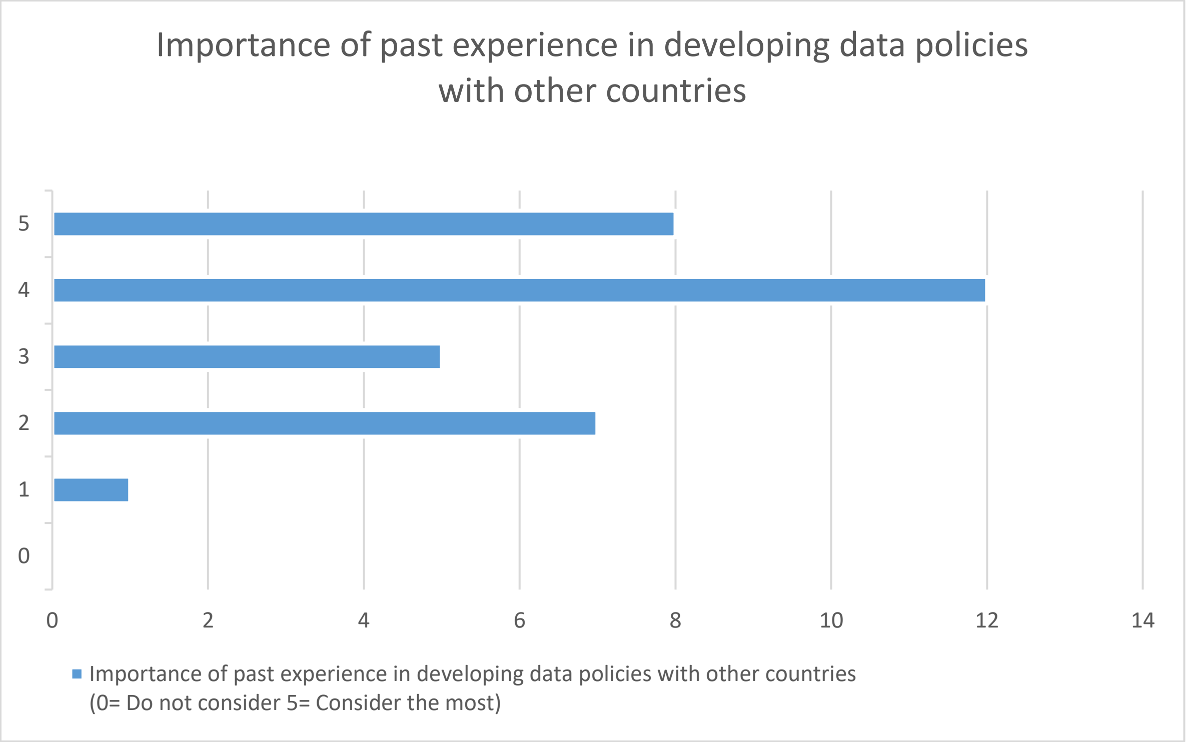


Figure 4.98: Importance of past experience in developing data policies with other counties (Overview-Other)

The majority of participants have indicated the importance of past experience in developing data policies with other counties and its importance in accepting a global level data privacy and security policy.

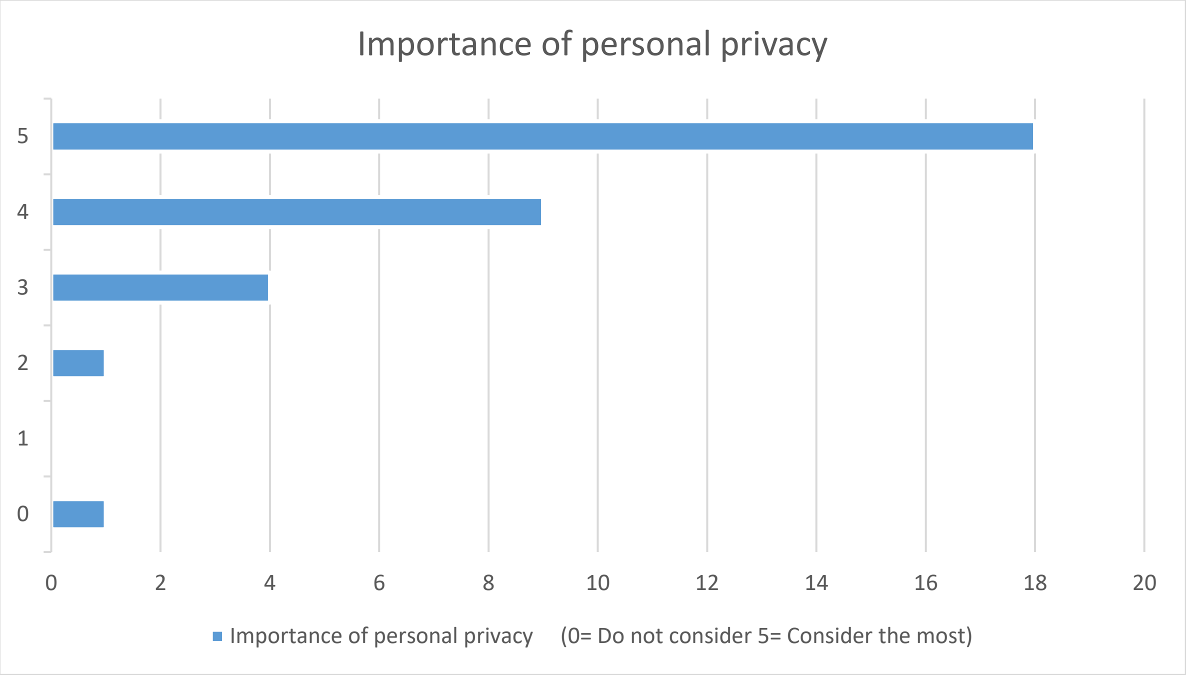


Figure 4.99: Importance of personal privacy (Overview-Other)

A significant amount of participants have indicated the importance of personal and its importance in accepting a global level data privacy and security policy.

In summary, in accepting a global level data protection mechanism, the notable factors the participants would consider are organisational support, budget allocation, economical differences, personal privacy, national security, ease of use of data privacy and security policies, usefulness of data privacy and security policies, mutual trust between countries, previous experience with other countries in developing policies (See figure 4.89-4.99). The marked difference in the responses show that the participants from other countries do not consider the importance of Social (See figure 4.90) and Political differences (See figure 4.92) in accepting and implementing a global level data protection mechanism

This chapter contains the overall analysis of the responses carried out by the researcher to get an understanding of the factors relevant to each country and form a realistic impression of their reliance on ICT, understanding of the cyber threats, assistance received from the organisations, and the training they received. Over and above, the researcher also managed to identify the factors that would influence acceptance and implementation of a data protection mechanism. Researcher’s analysis of the factors covering age, gender, work experience and the type of the employment recorded in annexe D and annexe E.

CHAPTER FIVE

ANALYSIS

This chapter consists of a comparative analysis of the survey undertaken by the researcher to get an understanding of influential factors in the acceptance and implementation of global data security policies of nations, with a special focus on the United Kingdom (UK) and Sri Lanka (See annexe A). These two countries were chosen for their status, the UK high-income country (World Bank, 2020), and Sri Lanka, a lower middle-income country (World Bank, 2020). The researcher distributed a questionnaire to a large sample of randomly selected population on behalf of government organisations and private organisations in UK and Sri Lanka.

The purpose of the survey questionnaire was to collect opinions and perceptions of participating individuals about the challenges faced by the countries in accepting and implementing global data privacy and security policy. The rationale behind each question is outlined in annexe B. The confidentiality of the findings, and the participants were a priority consideration in the data collection process, and the findings were used for the intended purpose only. In the analysis, the responses received from each country were divided into categories, and further broken down into sub-categories based on gender, age range, experience in the industry, and the status of their current profession. The identified factors paved the way for the researcher to develop the Policy Acceptance Model (See figure 5.26) based on the Technology Acceptance Models. In this chapter, the researcher made references to selected TAM models (See 5.5) and highlighted the variables used in Policy Acceptance Model (See table 5.8).

Overall, there were 76 participants from Sri Lanka, 110 from the UK, and 47 participants from other countries. The total number from both countries was made up of 140 male participants, 91 females and 1 non-specified gender category. The participants represented all age groups, 79 between 18-25; 98 between 26-35; 29 between 36-45; 9 between 46-55; 5 between 56-65; 10 in the 65+ range; 2 not revealed. Participants are from different industries, and another sub-group consists of both undergraduate students and/or postgraduate students. In the research's view, survey samples gathered from a cross-section of professionals add value, and help the researcher get a clear understanding of the overall picture of organisational level awareness of the key factors for consideration in accepting and implementing a data protection mechanism. Another category to focus on is those in employment for one year to over 10 period, and their impressions and understanding of policy issues will provide a good indication of their attitudes and beliefs in the privacy and security of their working environment.

5.1 Overview

The overall number of respondents employed in the industry adds up to 191, of which 145 (76 percent) know they are in a technology reliance working environment; 22 (12 percent) do not know because of the nature of the work assigned to them; 6 (3 percent) disagree on the ICT. Of the 42 undergraduate or postgraduate level students, 32 (76 percent) are employees in a technology reliance working environment; 2 (5 percent) unaware due to the nature of the work assigned to them; 2 (5 percent) 'disagree' on ICT. At the country level, 72 percent of Sri Lankan participants, 82 percent of UK participants, and 68 percent other nationals employed in industry, and those studying at undergraduate and postgraduate level are in a technology reliance working environment. The observation here is the majority have a high reliance on ICT.

Out of 191 respondents, 112 (59 percent) employed in the industry show that their organisations have budget allocation for information security, and 43 (23 percent) did not express an opinion either way, and according to 16 (8 percent) no budget allocation for information security. At individual country level, 58 percent of Sri Lankan participants (See figure 4.6), 65 percent of UK participants (See figure 4.39) agreed there was funding allocation for information security, and only 50 percent of the other participants (See figure 4.72) have indicated that their organisations had an allocated budget for information security.

In comparison to other countries, organisations in the UK and Sri Lanka have a satisfactory level of funds allocated for information security. This indicates that Sri Lanka, despite being classified as a lower-middle-income country (World Bank, 2020), and the UK as a high-income bracket (World Bank, 2020), both have committed high-level funding towards information security. That means both countries seem to have a good understanding of the importance of allocating financial resources to support information security. The crucial factor is the provision of a satisfactory level of financial resources necessary for training and equipment for creating a safer working environment.

The responses received from those in employment in the industry sector of Sri Lanka, the UK, and other countries, show that overall, despite the satisfactory level of resources allocated for information security, security awareness training they received was inadequate (See figure 5.1). Only 86 participants (45 percent) received regular cybersecurity awareness training; 48 (25 percent) uncertain; 37 participants (19 percent) significantly had no cybersecurity awareness training.

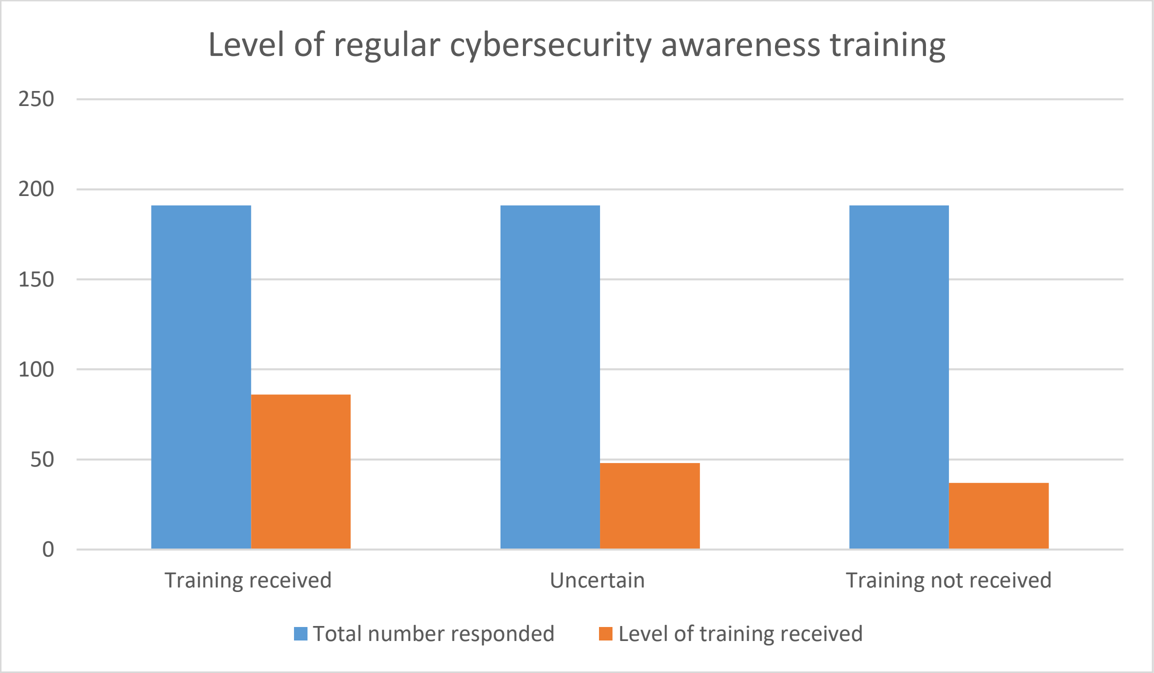


Figure 5.1: Level of regular cybersecurity awareness training (Overview)

However, the analysis shows that the students currently studying at undergraduate or postgraduate level received regular security awareness training to a satisfactory level. From a total of 42 participants, 23 (55 percent) received regular cybersecurity awareness training, 9 (21 percent) not commented, 3 (7 percent) had none. At the country level, the participants from the industry and those still studying, only 40 percent from Sri Lanka (See figure 4.7), 54 percent from the UK (See figure 4.40), and 43 percent from other countries (See figure 4.73) received regular cybersecurity awareness training. The reliance on technology and funding commitments is high in both Sri Lanka and the UK. However, whilst the UK participants received an appreciative level of regular cyber security awareness training, Sri Lankan participants did so to a lesser degree. The participants from other countries did not receive a satisfactory level of regular cybersecurity awareness training, presumably due to lack of funding.

In terms of support for the protection of personal information, overall, 86 participants (45 percent) did not receive support from the organisation; only 74 (39 percent) did (See figure 5.2). At the individual country level, only 35 percent of Sri Lankan participants (See figure 4.8), 47 percent of the UK (See figure 4.41), and 32 percent of the participants in other countries (See figure 4.74) employed in industry and the students currently studying at undergraduate or postgraduate level have received support from the organisation to protect personal information. The significance of these numbers is even though the participants in the UK have received regular cybersecurity awareness training, when it comes to organisational support there is a percentage discrepancy. That could be interpreted as even the organisation has provided the awareness training, going beyond that there has been no more support in terms of installing endpoint protection software and secure web gateways, implementing patch assessment tool to ensure the operating systems and applications are up to date, device control strategies to identify and control the use of removable storage devices and most importantly to implement a data protection policy that guides employees on how to keep personal data secure. Providing security awareness training will not serve the purpose of protecting the privacy of people. Therefore, it is extremely important for organisations to focus on the above-listed aspects as well.

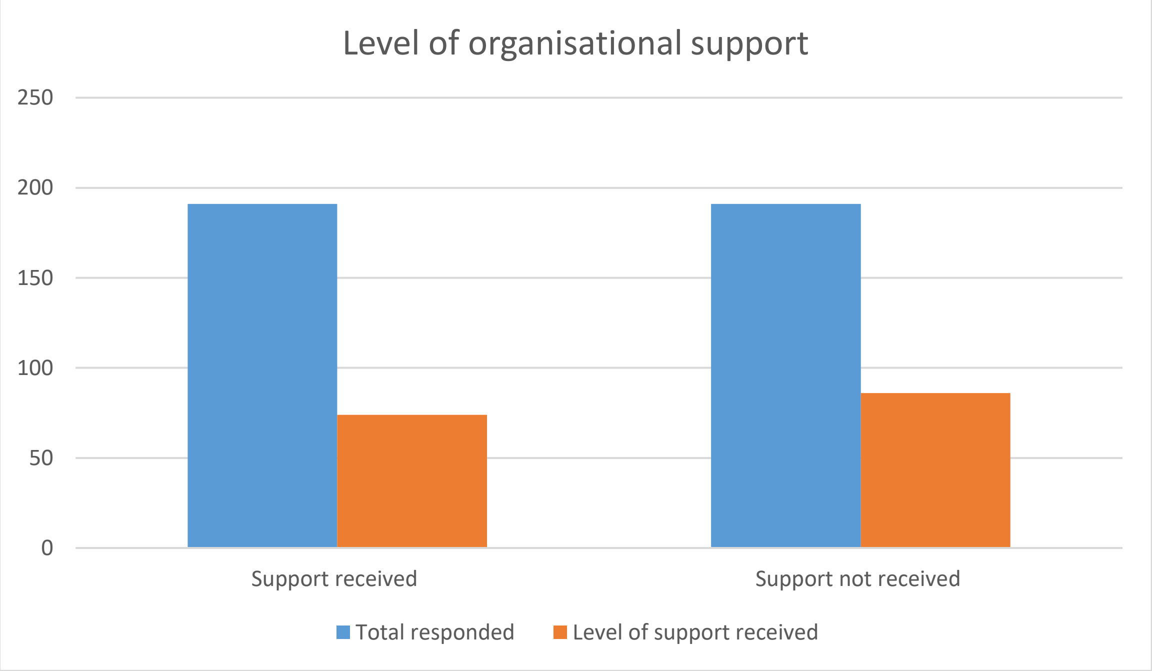


Figure 5.2: Level of organisational support (Overview)

Despite the security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation (See figure 5.3). To the question about understanding of the impact of cyber-attacks on the public and the organisation, overall response of 116 (50 percent) participants in the industry is affirmative, 37 (16 percent) no opinion; 18 participants (8 percent) have no understanding.

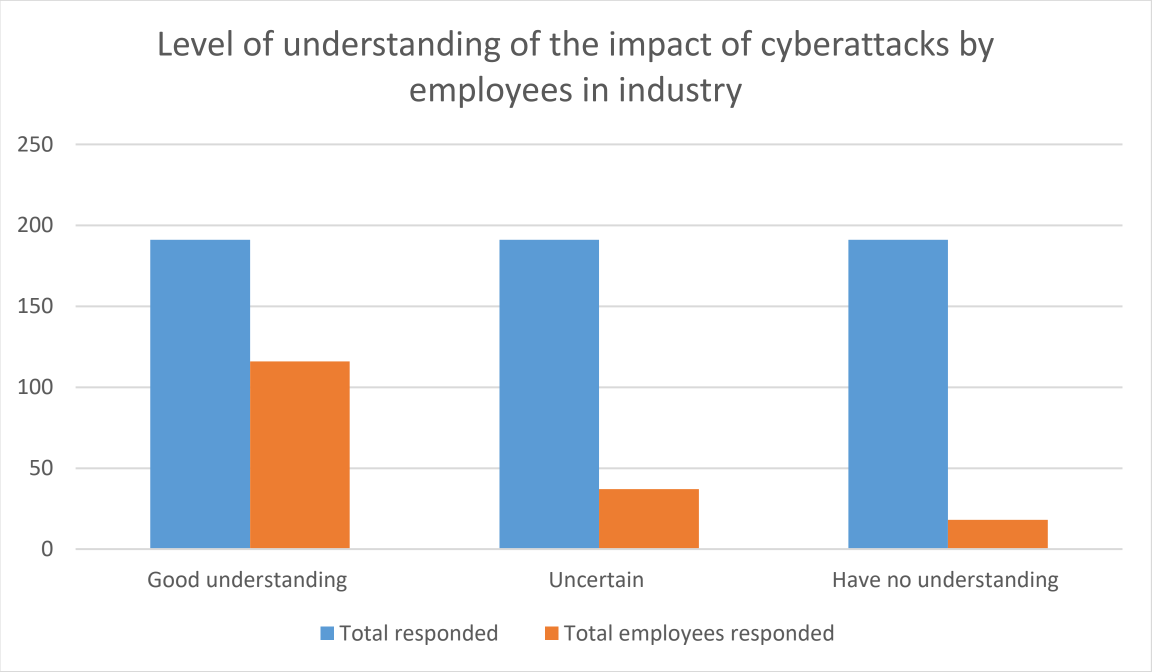


Figure 5.3: Level of understanding of the impact of cyberattack by employees in industry (Overview)

According to the respondents studying at undergraduate and postgraduate level, 28 (67 percent) do understand the impact of cyber-attacks on the public and the organisations; 6 (14 percent) not specified; 3 participants (7 percent) do not (See figure 5.4).

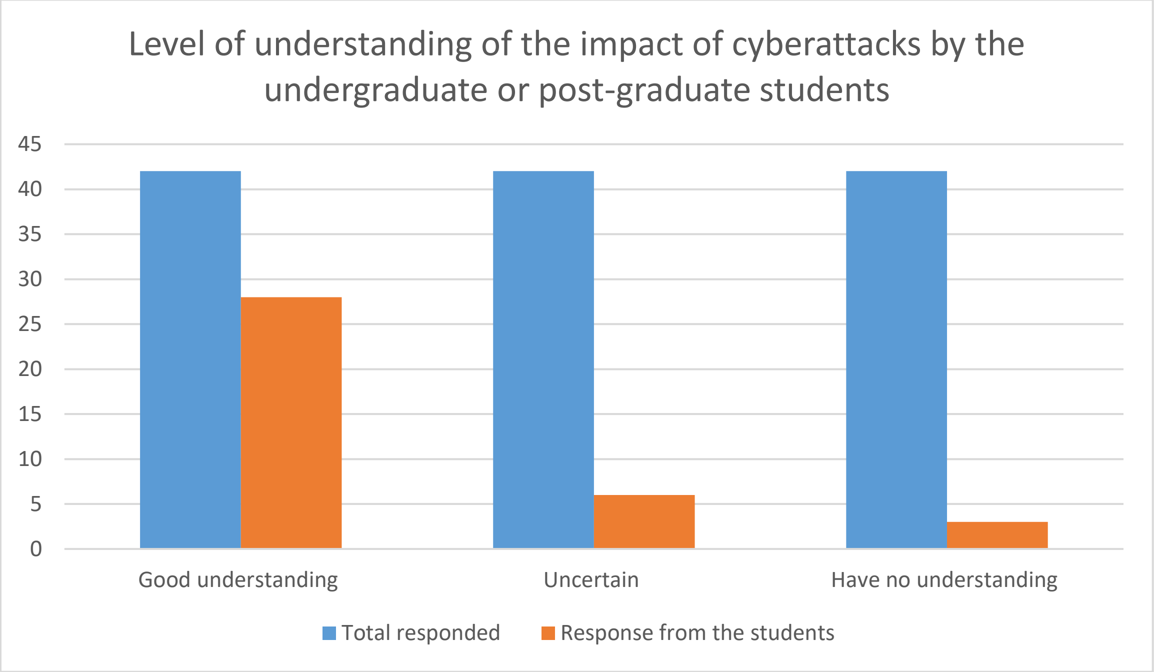


Figure 5.4: Level of understanding of the impact of the cyberattacks by the undergraduate or post-graduate students (Overview)

This indicates that the participants from the industry and those studying have a good understanding of the impact of cyber-attacks. At the individual country level, 63 percent from Sri Lanka, 62 percent from the UK, and 62 percent from other countries affirmed their high level of understanding of cyber of the impact of cyber-attacks on the public and the organisation. Despite the level of training from the organisational level, the individuals are motivated to update their knowledge about the ongoing threats and understand the impact of cyber attacks on the public and the organisations. This knowledge is extremely important for them to be actively involved in taking the necessary steps to protect themselves and the others around them.

Overall, there is a high awareness of potential threats to national security amongst the participants from the industry. Also, a representative sample of 158 (83 percent) of participants from the industry shows a high awareness of potential threats to national security from cyber-attacks. 32 of the participants from undergraduate and postgraduate level students (76 percent) realise the potential threats to national security from cyber-attacks. At the individual country level, together, the total number of participants from industry and undergraduate and postgraduate level students is made up of 83 percent from Sri Lanka, 81 percent from the UK, and 81 percent from other countries. The prominent factor is the high level of understating of potential threats to national security from cyber-attacks amongst these groups. The reasonable assumption to make is the benefits and effectiveness of regular training in security awareness received and, self-learning enabled them to understand the impacts of cyber-attacks to become aware of potential threats to national security from cyberattacks.

Responses to social differences: the majority employed in industry and education recognises the importance of education and attitude and beliefs. The awareness of potential cyber threats and their impact on people and national security figure prominently in the acceptance and implementation of data privacy and security policies. Therefore, the provision of cybersecurity awareness training and education at school and at the organisational level cannot be underestimated. Self-belief in privacy and respect one's own are considered contributory factors which have been discussed earlier previously under attitude and believes.

At the national state level, the majority of the participants from Sri Lanka understand the importance of education (See figure 4.17); and those in the United Kingdom (See figure 4.50) and other countries (See figure 4.83) recognise both education, and attitude and beliefs as equally important. In the Sri Lankan context, the participants give more consideration to education as it offers better prospects, but their organisations failed to provide regular security awareness training and support to protect personal information. The participants from other countries face similar challenges. However, United Kingdom participants recognise the importance of education as much as regular security awareness training they receive. However, the inadequacy of organisational level support to protect individual privacy remains a widely mentioned issue, and those deprived of support aim to build their knowledge through digital skill development courses, and supplement security awareness training.

According to the overall responses received, the majority both in industry and education agree that high income and upper-middle-income countries play a vital role in policy making. Individual country-level statistics support that view. The participants from Sri Lanka (See figure 4.15), the United Kingdom (See figure 4.48) and other countries (See figure 4.81) agree that high income and upper-middle-income countries play a vital role in policy making, and their perceptions are presumably driven by their acceptance of the importance of funding and affordability.

Overall, the majority of those in industry and those in education favour a democratic political system which in practice play an important part in accepting and implementing data privacy and security policies. However, the preferences differ at the individual country level. The majority of Sri Lankan (See figure 4.16) and United Kingdom participants (See figure 4.49) in industry and in education although opt for the democratic political system, the participants from other countries (See figure 4.82) choose both democratic, as well as the republican system as each play an influencing role in the acceptance and implementation of data privacy and security policies.

The majority of participants from the industry, and undergraduate and postgraduate level students do not see the relevance of either importance of protection of personal data security and privacy or the protection of national security in accepting and implementing global data privacy and security policies (See figure 4.21, 4.54 and 4.87). However, at the individual country level (Sri Lanka, UK and Other), all participants from the industry and the students recognise and place the importance of protection of personal data security and privacy above that of national security. This suggests that cultural values embedded in societies are likely to have influenced the participants to have made that decision.

In general, participants from the industry and the student participants echo the need to have a global level data protection mechanism, and 81 percent of the participants tends to agree. Also, at the individual country level, 78 percent of both groups from Sri Lanka, 83 percent from the United Kingdom, and 77 percent from other countries seem to agree. The survey statistics give a clear indication of consensus on the urgent need for a global level data protection mechanism encompassing unified rules across the world to ensure perpetrators will be brought to justice.

The message arising from the survey sample is the set of distinct factors that should be considered in accepting and implementing a global level data privacy and security policy. Overall, the participants from the industry focus on factors such as organisational support, budget allocation, social differences, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience in developing policies with other countries, but political differences not counted as a factor for consideration.

The student participants at the undergraduate and postgraduate level identify only a limited number of factors such as organisational support, funding, personal privacy, national security, the usefulness of data privacy and security policies and mutual trust between countries. The variation from the norm here is the omission of social, economic, political differences, ease of use of data privacy and security policies, and previous experience in developing policies with other countries.

At the national level, those in employment and the students from Sri Lanka (See figure 4.23-4.33), the United Kingdom (See figure 4.56-4.66), and other countries (See figure 4.89-4.99) place emphasis on factors such as organisational support, financial support, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience in developing policies with other countries. However, the majority omits the importance of Social and Political differences in accepting and implementing a global level data protection mechanism, a prominent factor emanating from the analysis of the survey sample.

5.2 Gender

5.2.1 Male

Overall, 109 males from both Sri Lanka and the UK, all within 18-65+ age range, and in employment for less than one year to over 10 years in the industry.

At the national level, 80 percent of the participants from Sri Lanka, and 81 percent from the UK work in a technology reliance working environment. It shows that the participants from both countries have a high reliance on technology. 54 percent of the participants from Sri Lanka (See annexe figure D.4), and 65 percent from the UK (See annexe figure E.4) agree that their organisations allocated budget for information security, but given the high reliance on technology, the level of funding is relatively low in both countries.

According to the participants from both countries, they receive regular security awareness training funded by the organisations, and 51 percent of participants from Sri Lanka (See annexe figure D.5), and 60 percent from the UK agree (See annexe figure E.5). Despite the level of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 71 percent from Sri Lanka, and 66 percent from the UK possess a good level of understanding of cyber threats. Given the high reliance on technology, it is important for the participants to be familiar with potential cyber threats, and supposedly regular awareness training received by them contributed to the increased understanding. In the case of provision of organisational support to protect personal information, only 40 percent of the participants from Sri Lanka (See annexe figure D.6), and 53 percent from the UK (See annex figure E.6) received organisational support. Given high reliance on technology, the organisational support received by the participants from Sri Lanka and the UK believes to be relatively low.

To the survey question on social differences, the majority of the participants from Sri Lanka select both education and, attitudes and beliefs (See annexe figure D.17), whereas a majority from the UK select only the importance of education (See annexe figure E.17). On economic differences, the majority from both countries select high income and upper-middle income countries, and on different political systems, the majority opts for a democratic political system. The distinct factor to emerge from the survey in respect of accepting and implementing a global data privacy and security policy is the majority of male participants from both countries make no reference to either the importance of protection of personal data security and privacy or protection of national security (See annexe figure D.20 and E.20).

The message from the male respondents from both countries is clear. There is a need to have a global level data protection mechanism, and this has been echoed by 86 percent of the male participants in Sri Lanka and 80 percent from the UK. The common factors to have emerged are organisational support, budget allocation, social differences, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience in developing policies in collaboration with other countries.

5.2.2 Female

Overall, 75 females from both Sri Lanka and the UK, all within 18-65+ age range, and in employment for less than one year to over 10 years in the industry.

At the national level, 68 percent of the participants from Sri Lanka (See annexe figure D.35), and 83 percent from the UK (See annexe figure E.35) work in a technology reliance working environment. It shows that the participants from both countries have a high reliance on technology. 68 percent of the participants from Sri Lanka (See annexe figure D.36), and 57 percent from the UK (See annexe figure E.36) agree that their organisations allocated budget for information security, but given the high reliance on technology, the level of funding is relatively low in the UK.

According to the participants from both countries, the regular security awareness training they received was inadequate (See figure 5.5). Only 30 percent of participants from Sri Lanka (See annexe figure D.37) and only 40 percent of participants from the UK (See annexe figure E.37) received regular cybersecurity awareness training.

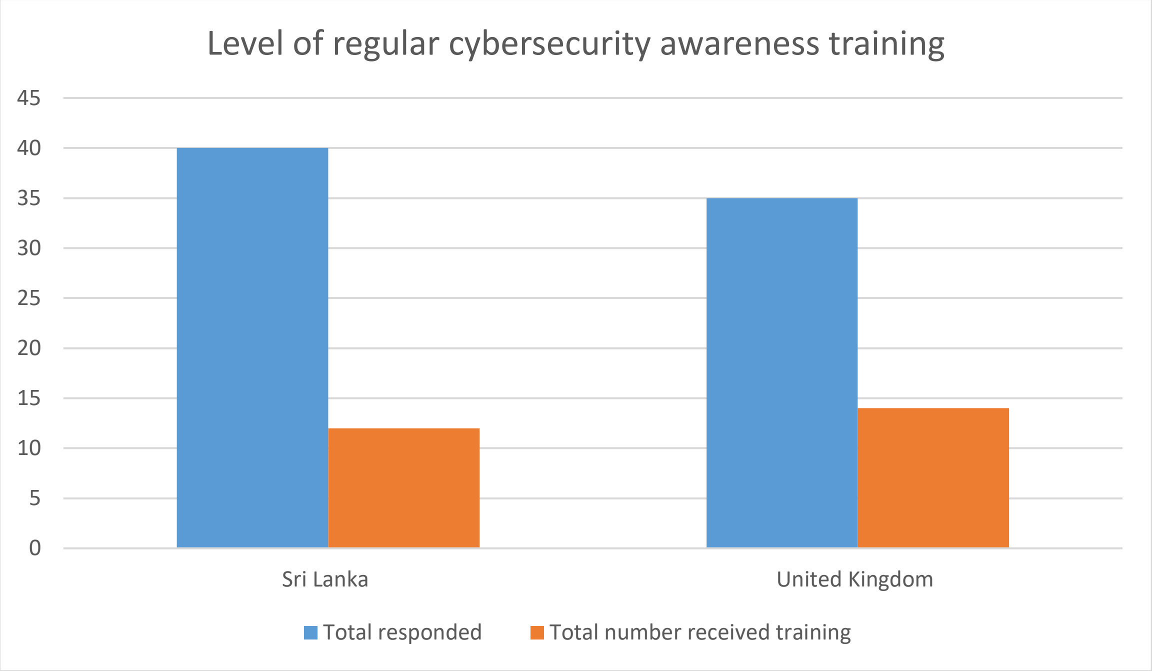


Figure 5.5: Level of regular cybersecurity awareness training (Female)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 55 percent from Sri Lanka (See annexe figure D.39) and 51 percent from the UK (See annexe figure E.39) possess a good level of understanding of the impact of cyber threats on the public and the organisation. This shows that even not having received cybersecurity awareness training, the participants appear to have been proactive in self-learning to keep their knowledge up to date. As for providing organisational support to protect personal information, only 28 percent of the participants from Sri Lanka (See annexe figure D.38), and only 34 percent from the UK (See annexe figure E.38) received organisational support (See figure 5.6).

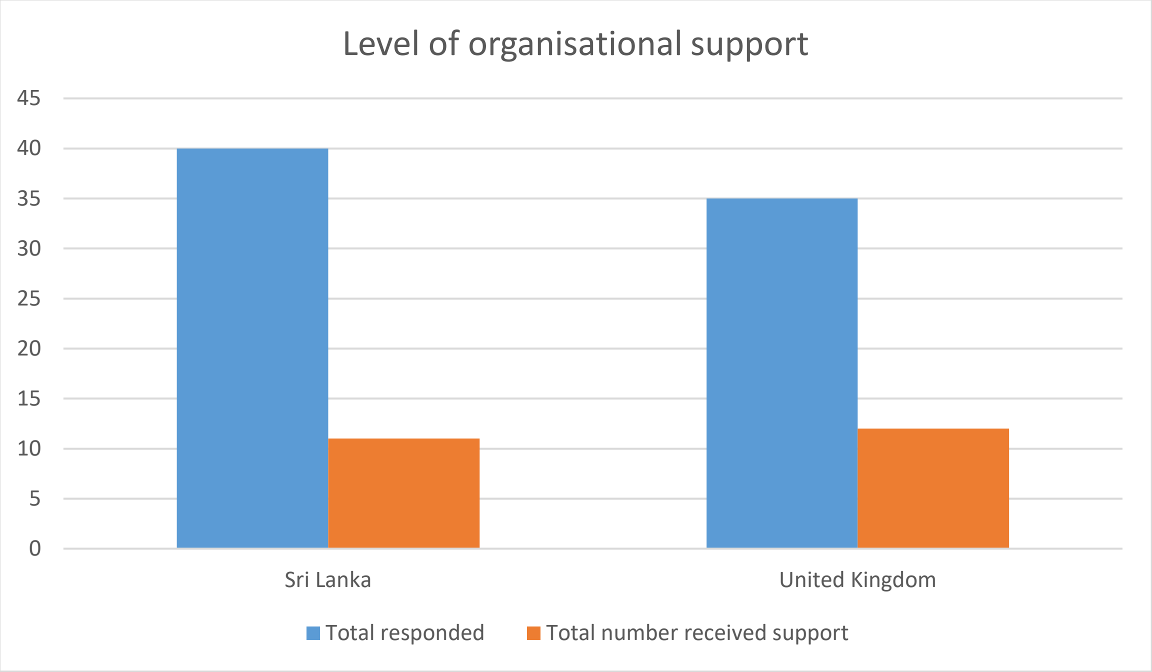


Figure 5.6: Level of organisational support (Female)

This shows that although the reliance on technology is high and a budget had been allocated for information security, the participants from both countries received neither regular cybersecurity awareness nor organisational support to protect personal information.

To the survey question on social differences, the majority of the participants from Sri Lanka select only the importance of education (See annexe figure D.49); whereas the majority from the UK select both education and attitude and beliefs (See annexe figure E.49). On economic differences, the majority from both countries select high income and upper-middle-income countries, and on different political systems, the majority opts for a democratic political system. The distinct factor to emerge from the survey in respect of accepting and implementing a global data privacy and security policy, majority of female participants from the UK recognise the importance of protection of personal data security and privacy (See annexe figure E.52), and those from Sri Lanka make no reference to any (See annexe figure D.52).

The message from the female respondents from both countries is clear (See table 5.1). There is a need to have a global level data protection mechanism, and this has been echoed by 75 percent of the female participants in Sri Lanka (See annexe figure D.53) and 89 percent from the UK (See annexe figure E.53). The common factors to have emerged are organisational support, budget allocation, economic differences, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies. In addition, participants from the UK agree with the importance of social differences and the importance of ease of use of data privacy and security policies.

Table 5.1: Gender based responses

	Male	**Female**
Reliance of technology	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT
Budget allocation	Both countries have an allocated budget	Both countries have an allocated budget
Regular security awareness training	Provision of security awareness training adequate in both countries	Provision of security awareness training inadequate in both countries
Understanding of the impact of cyber-attacks on the public and the organisation	High level of understanding amongst the participants from both countries	High level of understanding amongst the participants from both countries
Organisational level support to protect personal information	Lack of organisational support in Sri Lanka.	Lack of organisational support in both countries

	UK participants received a satisfactory level of organisational support	
Social differences	Importance of education emphasised by the majority of the participants both in Sri Lanka and the UK	Importance of education emphasised by the majority of the participants both in Sri Lanka and the UK
Economic differences	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries
Political differences	The majority prefers the democratic political system	The majority prefers the democratic political system
Need for global level data protection mechanism	The majority from both countries agree	The majority from both countries agree
Commonly agreed factors that should consider in developing a global level data protection mechanism	Organisational support, budget allocation, social differences, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other	Organisational support, budget allocation, economic differences, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See

	countries in developing policies (See annexe figure D.22-32 and E.22-32).	annexe figure D.54-64 and E.54-64).

5.3 Age range

5.3.1 18-25

Overall, 68 participants responded from both Sri Lanka and the UK, 40 males, 27 females and 1 non-binary person, all with employment in the industry for less than a year to over 10 years.

Overall, the participants aged between 18-25 have a high reliance on technology in their working environment. 86 percent of the participants in Sri Lanka, and 83 percent in the UK work in a high technology reliance environment. 77 percent of the participants from Sri Lanka (See annexe figure D.68), and 61 percent from the UK agree that their organisations allocated a budget for information security (See annexe figure E.68). Even though the majority finds that their organisations provide funding, in the UK, the level of funding allocated is relatively low, despite the high reliance on technology.

According to 64 percent of the participants from Sri Lanka, the organisations provide a satisfactory level of regular security awareness training (See annexe figure D.69). However, except for the 48 percent of the participants from the UK who received relevant training, the training the rest received was inadequate (See annexe figure E.69). Despite the level of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 61 percent of the participants from the UK and 68 percent from Sri Lanka agree.

According to 27 percent of the participants from Sri Lanka (See annexe figure D.70) and 39 percent from the UK (See annexe figure E.70), the organisations did not provide support towards protection of personal information (See figure 5.7). The distinct factor is the participants from the United Kingdom did not receive either security awareness training or support from the organisation to protect personal information, despite the high reliance on technology.

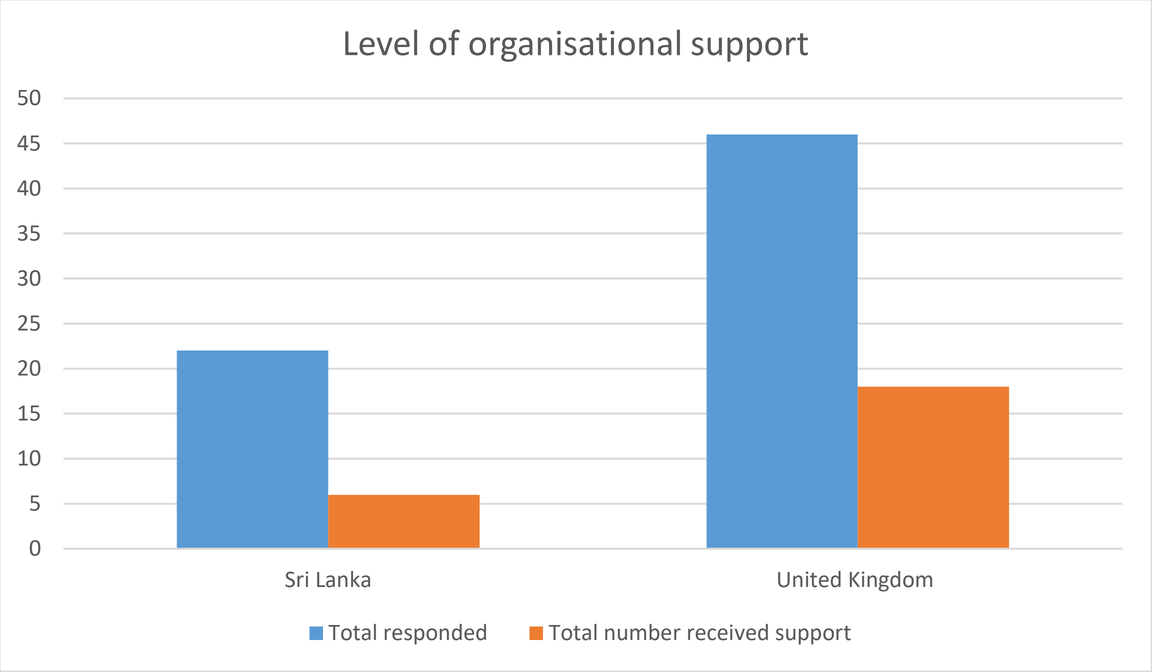


Figure 5.7: Level of organisational support (18-25)

To the survey question on social differences, the majority of the participants from Sri Lanka select both education and lifestyles (See annexe figure D.81), and the majority of the UK participants did not select any (See annexe figure E.81). However, the majority from both countries gives similar responses to both economic and political differences. The majority from both countries agree that the high-income and upper-middle-income countries play a vital role in the process of policy development, and their choice is a democratic political system in preference to others. The participants from both countries do not consider either protecting personal data security and privacy or national security are important factors in the acceptance and implementation of global data privacy and security policies (See annexe figure D.84 and E.84).

The message from the age 18-25 respondents is clear (See table 5.2). 72 percent of the participants from Sri Lanka and 70 percent from the UK agree with the need to have a global level data protection mechanism. The common factors identified by the participants are organisational support, organisational support, budget allocation for information security, personal privacy, national security, the usefulness of data privacy and security policies and mutual trust between countries. In addition, participants from Sri Lanka agree with the importance of economic differences, ease of use of data privacy and security policies, and previous experience in developing policies in collaboration with other countries. However, social differences, political differences have not drawn the attention of participants from both countries.

5.3.2 26-35 years

Overall, 75 participants responded from both Sri Lanka and the UK, 42 males and 33 females, all with employment in the industry for less than a year to over 10 years.

Overall, the participants aged between 26-35 have a high reliance on technology in their working environment. 68 percent of the participants in Sri Lanka, and 77 percent in the UK, work in a high technology reliance environment. 50 percent of the participants from Sri Lanka (See annexe figure D.100), and 71 percent from the UK (See annexe figure E.100) agree that their organisations allocated a budget for information security. Even though the majority finds that their organisations provide funding, in Sri Lanka, the level of funding allocated is relatively low, despite the high reliance on technology.

Only 25 percent of the participants from Sri Lanka received a satisfactory level of regular security awareness training (See annexe figure D.101), but despite training received, 58 percent of the participants have a high understanding of the impact of cyber-attacks on the public and the organisation (See annexe figure D.103). Whereas in the UK, 69 percent have received an adequate level of regular security awareness training (See annexe figure E.101), and 58 percent indicate a high understanding of the cyber-attacks (See annexe figure E.103). In Sri Lanka, participants might have enhanced their understanding of cyber-attacks through self-learning in the absence of sufficient training available to them. In contrast, even the participants from the UK received training, the understanding of cyberattacks amongst them is considerably low. This suggests that training alone will not help; self-learning also play a crucial factor in increasing knowledge and understanding of cyberattacks. Also, only 35 percent of the participants from Sri Lanka (See annexe figure D.102) and only 49 percent from the UK (See annexe figure E.102) received support from the organisation to protect personal information.

This indicates that the participants from the UK, although received regular security awareness training they have no support from organisations to protect personal information. Whereas in Sri Lanka, despite the high level of reliance on technology, the participants claim they received neither regular training nor support from the organisation to protect personal information.

In response to the social differences, the majority from both countries recognise the importance of education and, the majority from Sri Lanka also recognises the importance of attitude and beliefs (See annexe figure D.113). Interestingly, the majority from both countries also select both economic and political differences, and they also agree that the high income and upper-middle-income countries play a vital role in the process of policy development, and democratic political systems are chosen in preference to others. The participants from both countries also accept the importance of the protection of personal data security and privacy above the protection of national security when accepting and implementing global data privacy and security policies (See annexe figure D.116 and E.116).

The message from age 26-35 respondents is clear (See table 5.2). 83 percent of the participants from Sri Lanka (See annexe figure D.117) and 70 percent from the UK (See annexe figure E.117) agree with the need to have a global level data protection mechanism. The common factors identified by the participants are economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies and previous experience with other countries in developing policies. In addition, participants from Sri Lanka agree with the importance of organisational support, budget allocation for information security, and participants from the UK agree with the importance of social differences and mutual trust between countries. However, political differences have not drawn the attention of participants from both countries.

5.3.3 36-45 years

Overall, 23 participants responded from both Sri Lanka and the UK, 14 males and 9 females, all with employment in the industry for less than a year to over 10 years.

Overall, the participants aged between 36-45 have a high reliance on technology in their working environment. 71 percent of the participants in Sri Lanka (See annexe figure

D.131), and 88 percent in the UK (See annexe figure E.131), work in a high technology reliance environment. 86 percent of the participants from Sri Lanka (See annexe figure D.132) and 75 percent from the UK (See annexe figure E.132) agree that their organisations allocated a budget for information security.

In both Sri Lanka and the UK, 57 percent and 56 percent respectively agree that despite the satisfactory level of resources allocated for information security, regular security awareness training received was adequate.

Despite the level of security awareness training, 71 percent of the participants from Sri Lanka and 75 percent from the UK claims a high understanding of the impact of cyber-attacks on the public and the organisation. The participants have a relatively higher understanding of the impact of cyber-attacks, and the enhanced understanding of cyber-attacks can be attributable to self-learning.

In addition, only 43 percent of the participants from Sri Lanka (See annexe figure D.134), and 63 percent from the UK (See annexe figure E.134) received support from the organisation to protect personal information. This indicates that the participants from Sri Lanka received regular security awareness training but no support from organisations to protect personal information. Whereas in the UK, participants received both training and support.

In respect of social differences, the majority of the participants from both countries select both education, and attitude and beliefs. In addition, the majority from Sri Lanka recognises the importance of ethnicity and religion (See annexe figure D.145), and those from the UK highlight the importance of lifestyle (See annexe figure E.145). The majority from both countries agrees that the high income and upper-middle-income countries play a vital role in the policy development process. In response to the political differences, the majority of the participants from the UK prefer a democratic political system (See annexe figure E.147), whilst those from Sri Lanka select none (See annexe figure D.147). The participant from both countries recognise the importance of protection of personal data security and privacy above the protection of national security for acceptance and implementation of global data privacy and security policies (See annexe figure D.148 and E.148)

The message from age 36-45 respondents is clear (See table 5.2). 71 percent of the participants from Sri Lanka (See annexe figure D.149) and 94 percent from the UK (See annexe figure E.149) agree with the need to have a global level data protection mechanism. The common factors identified by the participants are organisational support, budget allocation for information security, social differences, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy. In addition, participants from the UK recognise the importance of political differences, mutual trust between countries and previous experience in developing policies with other countries.

5.3.4 46+ years

Overall, amongst 18 responses received from both Sri Lanka and the UK, 13 male and 5 female participants, all employed in industry for 1-5 years and over 10 years. All the participants aged over 46 have a high reliance on technology. 67 percent of the participants from Sri Lanka (See annexe figure D.164), and 83 percent from the UK (See annexe figure E.163, E,195 and E.227) work in a high technology reliance environment. 50 percent of the participants from Sri Lanka (See annexe figure D.165), and only 25 percent from the UK (See annexe figure E.164, E.196 and E.228) agree that their organisations allocated budget for information security (See figure 5.8).

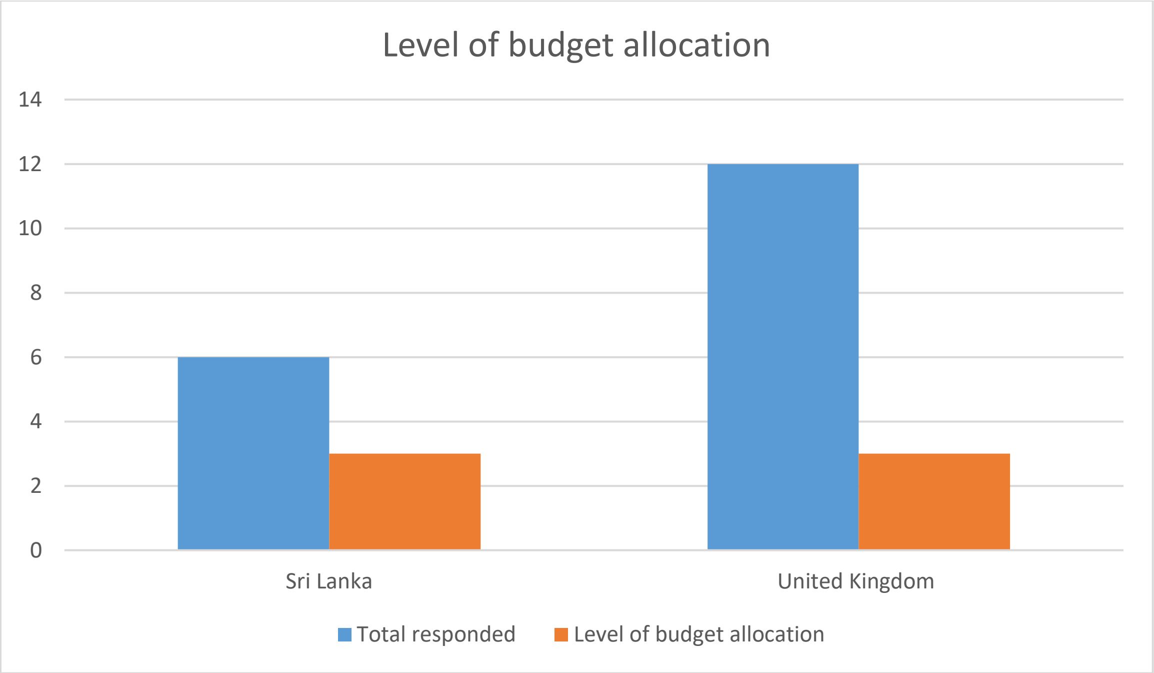


Figure: 5.8: Level of budget allocation (46+ years)

In the UK, the level of funding allocated is relatively low, despite the high reliance on technology. Due to lack of funding allocated, especially in the UK, only 33 percent (See annexe figure E.165, E.197 and E.229) received regular security awareness training (See figure 5.9). However, in Sri Lanka, despite the satisfactory level of funding, only 33 percent of the participants (See annexe figure D.166) received training (See figure 5.9).

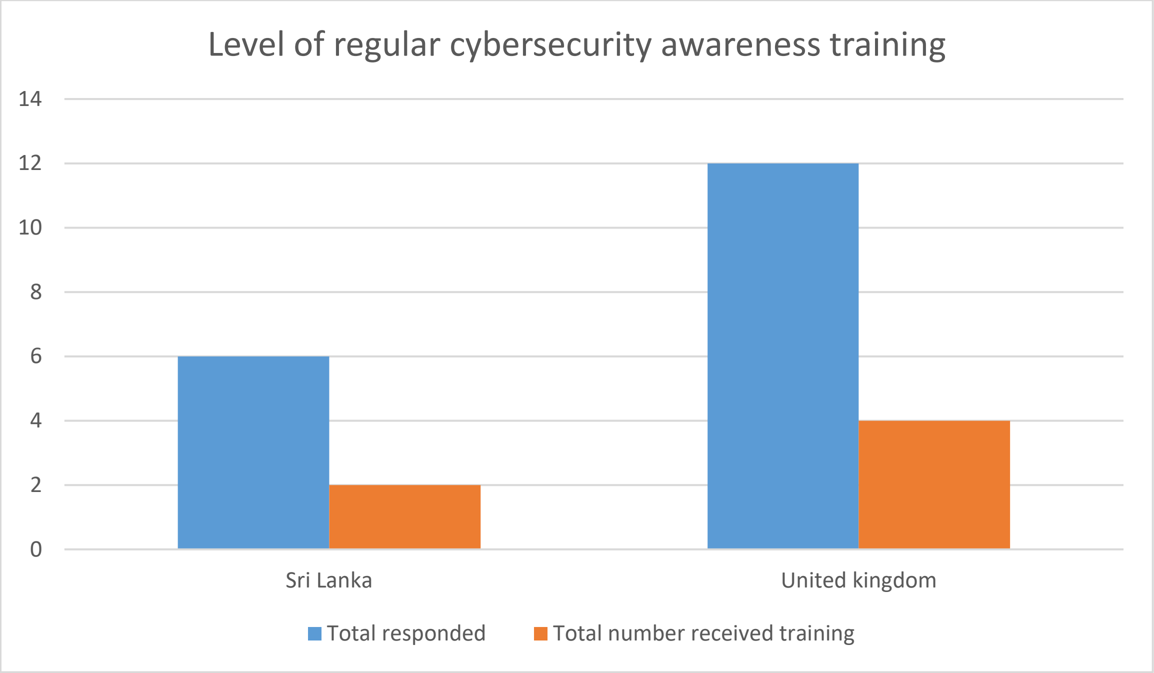


Figure 5.9: Level of regular cybersecurity awareness training (46+ years)

In the UK, given the high level of ICT reliance, there is no satisfactory level of budget allocation and training. However, 50 percent of the participants (See annexe figure E.166, E.198 and E.230) received support from the organisation to protect personal information, but only 33 percent of the participants did in Sri Lanka (See annexe figure D.167)

67 percent of the participants from Sri Lanka (See annexe figure D.168) and 58 percent from the UK (See annexe figure E.167, E.199 and E.231) claim to have a high understanding of the impact of cyber-attacks on the public and the organisation, in contrast to the level of security awareness training received. Supposedly, the participants have a relatively higher understanding of the impact of cyber-attacks than the security

awareness training they received, and the enhanced understanding of cyber-attacks can be attributable to self-learning.

On social differences, the majority of the participants from both countries recognise the importance of education, and the majority from the UK recognise the importance of lifestyle, and attitude and beliefs as well (See annexe figure E.177, E.209 and E.241). The majority from both countries agrees that the high income and upper-middle-income countries play a vital role in policy development. They also select a democratic political system in preference to others. For accepting and implementing global data privacy and security policies, the participants from Sri Lanka agree with the importance of protection of national security (See annexe figure D.181), whereas those from the UK (See annexe figure E.180, E.212 and E.244) select the importance of protection of personal data security.

The message from the age 36-45 respondents is clear (See table 5.2). 83 percent of the participants from Sri Lanka (See annexe figure D.182) and 92 percent of the participants from the UK (See annexe figure E.181, E.213 and E.245) agree with the need to have a global level data protection mechanism. The common factors identified by the participants are organisational support, political differences, national security, ease of use of data privacy and security policies, the usefulness of data privacy, mutual trust between countries, personal privacy. In addition, participants from Sri Lanka agree with the importance of budget allocation, social differences, economic differences, and previous experience with other countries in developing policies.

Table 5.2: Age based responses

	18-25	**26-35**	**36-45**	**46+**
Reliance on technology	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT
Budget allocation	Both countries have an	Both countries have an	Both countries have an	In Sri Lanka, the budget allocated is at

	allocated budget	allocated budget	allocated budget	a satisfactory level, but not so in the UK.
Regular security awareness training	Provision of security awareness training: adequate in Sri Lanka; inadequate in the UK	Provision of security awareness training: inadequate in Sri Lanka; adequate in the UK	Provision of security awareness training adequate in both countries	Provision of security awareness training inadequate in both countries
Understanding of the impact of cyber-attacks on the public and the organisation	High level of understanding amongst the participants from both countries	High level of understanding amongst the participants from both countries	High level of understanding amongst the participants from both countries	High level of understanding amongst the participants from both countries
Organisational level support to protect personal information	Lack of organisational support in both countries.	Lack of organisational support in both countries.	Lack of organisational support in Sri Lanka. UK participants received a satisfactory level of organisational support.	Lack of organisational support in Sri Lanka. UK participants received a satisfactory level of organisational support.

Social differences	The majority from Sri Lanka recognises the importance of education and lifestyle, but no selection from the majority from the UK	Importance of education emphasised by the majority of participants both in Sri Lanka and the UK	Importance of education, and attitude and beliefs emphasised by majority of participants both in Sri Lanka and the UK	Importance of education emphasised by the majority of participants both in Sri Lanka and the UK
Economic differences	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries
Political differences	The majority prefers the democratic political system	The majority prefers the democratic political system	Unspecified by the majority	The majority prefers the democratic political system
Need for global level data	The majority from both countries agree	The majority from both countries agree	The majority from both countries agree	The majority from both countries agree

protection mechanism				
Commonly agreed factors that should consider in developing a global level data protection mechanism	Organisational support, budget allocation for information security, personal privacy, national security, the usefulness of data privacy and security policies and mutual trust between countries (See annexe figure D.86-96 and E.86-96)	Economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies and previous experience with other countries in developing policies (See annexe figure D.118-128 and E.118-128)	Organisational support, budget allocation for information security, social differences, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy (See annexe figure D.150-160 and E.150-160)	Organisational support, political differences, national security, ease of use of data privacy and security policies, the usefulness of data privacy, mutual trust between countries, personal privacy (See annexe figure D.183-193, E.182-192, E.246-256 and E.214-224)

5.4 Experience in the industry

5.4.1 Less than a year in employment

From Sri Lanka and the UK altogether, there were 61 participants and 36 out of them were male, 24 females and 1 non-binary. At the individual country level, in Sri Lanka, there were 16 participants and 7 out of them were males and 9 females, and in the UK, there were 45 participants and 29 out of them were males, 15 females and 1 non-binary. The age range of these participants was 18-35.

At the individual country level, 81 percent from Sri Lanka and 80 percent from the UK work in a technology reliance working environment. This indicates a majority of those who have been working in an organisation for less than a year has had a high reliance on ICT.

In terms of budget allocation, 63 percent from Sri Lanka and 69 percent from the UK indicated that their organisations have an allocated budget for information security. However, considering the reliance on technology in the UK and Sri Lanka, it is apparent that even though the reliance is high, the allocation of budget is comparatively low.

In Sri Lanka, the participants note that despite the satisfactory level of resources allocated for information security, regular security awareness training received was inadequate. Only 50 percent of the participants received regular cybersecurity awareness training (See annexe figure D.198). According to 56 percent of the participants from Sri Lanka (See annexe figure D.200) have a high understanding of the impact of cyber-attacks on the public and the organisations. Whereas 58 percent of the UK participants received regular security awareness training (See annexe figure E.261), and 62 percent with a high understanding of the impact of cyber-attacks on the public and the organisation (See annexe figure E.263). Also, only 44 percent of the participants from Sri Lanka (See annexe figure D.199), and only 40 percent from the UK (See annexe figure E.262) received support from the organisation to protect personal information (See figure 5.10).

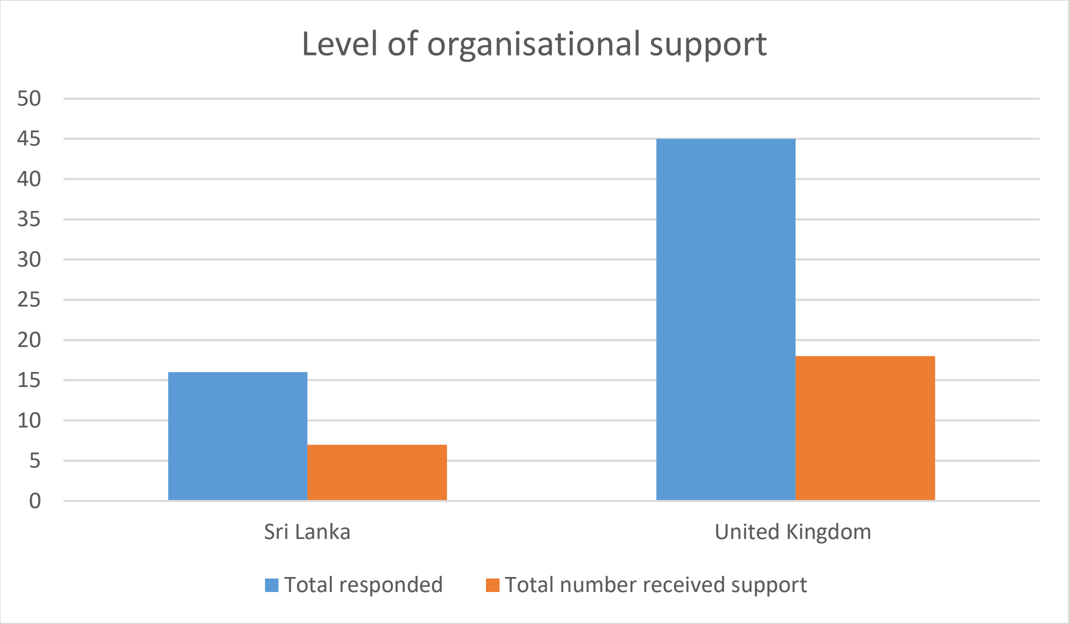


Figure 5.10: Level of organisational support (Less than a year in employment)

At the country level, both in Sri Lanka and the UK, according to the participants, the reliance on technology is high. Sri Lankan participants did not receive a sufficient level of either security awareness training or organisational support to protect personal information, but UK participants although received regular training, they did not receive support from the organisation to protect personal information.

In response to the social differences, the majority of Sri Lankan participants recognise the importance of both education and lifestyle (See annexe figure D.210), and the majority of the UK participants only consider the importance of education (See annexe figure D.273). On the question of economic differences, the majority from both Sri Lanka and the UK agree with the premise that high income and upper-middle-income countries play a vital role in policy development and on political differences question, the majority choose democratic political system. Sri Lanka and the UK are geographically and regionally far apart, and in terms of economic capacity, they are at different levels, yet on the question of economic and political differences, there seems to be a similarity in the responses given by the participants.

Sri Lankan participants agree with the supposition that protecting personal data security and privacy, and national security are both important in accepting and implementing global data privacy and security policies (See annexe figure D.213), and those from the

UK consider the importance of protection of personal data security and privacy only (See annexe figure E.276).

69 percent of Sri Lankan respondents with less than one year in industry (See annexe figure D.214), and 78 percent from the UK (See annexe figure E.277) support the need for having a global level data protection mechanism. To that end, the participants from both countries hold similar views about specific factors that need to be considered in accepting and implementing a global level data protection mechanism (See table 5.3). The key factors identified include organisational support, funding provisions, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, previous experience in developing policies with other countries. However, participants from the UK adds to the list the importance of consideration to political differences, social differences, mutual trust between countries, which was not given prominence by Sri Lankan participants.

5.4.2 1-5 years in employment

From Sri Lanka and the UK altogether, there were 68 participants and 37 out of them were male and 31 females. At the individual country level, in Sri Lanka, there were 32 participants and 12 out of them were males and 20 females, and in the UK, there were 36 participants and 25 out of them were males and 11 females. The age range of these participants was 18- 65+. However, there are no participants in the age range 56-65.

At the individual country level, 63 percent from Sri Lanka (See annexe figure D.228) and 89 percent from the UK (See annexe figure D.291) work in a technology reliance working environment. This indicates that the majority of those who have been working in an organisation for 1-5 years have had a high reliance on ICT, and a high reliance on technology significantly amongst the participants from the UK.

In terms of budget allocation, 62 percent from Sri Lanka and 61 percent from the UK indicated that their organisations had an allocated budget for information security. However, considering the reliance on technology in the UK, it is apparent that even though the reliance is high, the allocation of budget is comparatively low.

In Sri Lanka, the participants claim that despite the satisfactory level of resources allocated for information security, regular security awareness training received was inadequate. Only 34 percent of the participants received regular cybersecurity awareness training (See annexe figure D.230), and 56 percent of the participants (See annexe figure D.232) appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. Whereas 58 percent of the UK participants (See annexe figure E.293) received regular security awareness training, and 67 percent with a high understanding of the impact of cyber-attacks on the public and the organisation (See annexe figure E.295).

Also, only 22 percent of Sri Lankan participants (See annexe figure D.231) had received support from the organisations towards the protection of personal information, but a higher percentage of the participants from the UK, 53 percent received organisational support (See annexe figure E.294). At the country level, both in the UK and Sri Lanka, according to the participants, the reliance on technology is high. Sri Lankan participants did not receive a sufficient level of either security awareness training or organisational support to protect personal information, but UK participants received both regular training, and support from the organisation to protect personal information.

In response to the social differences, the majority from both Sri Lanka and the UK has highlighted the importance of education and attitude and beliefs. On the question of economic differences, the majority from both Sri Lanka and the UK agree with the premise that high income and upper-middle-income countries play a vital role in policy development and on political differences question, the majority choose democratic political system. Sri Lanka and the UK are geographically and regionally far apart; on the question of social, economic and political differences, there seems to be a similarity in the responses given by the participants. Furthermore, participants from Sri Lanka and the UK consider the importance of the protection of personal data security and privacy only.

75 percent of Sri Lanka respondents with 1-5 years in industry (See annexe figure D.246), and 83 percent from the UK (See annexe figure E.309) support the need for having a global level data protection mechanism. To that end, the participants from both countries hold similar views about specific factors that need to be considered in accepting and implementing a global level data protection mechanism (See table 5.3). That includes organisational support, budget allocation, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies. However, participants from the UK adds to the list

the importance of consideration to political difference, which was not given prominence by Sri Lankan participants.

5.4.3 6-10 years in employment

From Sri Lanka and the UK altogether, there were 21 participants and 12 out of them were male and 9 females. At the individual country level, in Sri Lanka, there were 12 participants and 6 out of them were males and 6 females, and in the UK, there were 9 participants and 6 out of them were males and 3 females. The age range of these participants was 18- 45+.

At the individual country level, 83 percent from Sri Lanka (See annexe figure D.260) and 67 percent from the UK (See annexe figure E.323) work in a technology reliance working environment. This suggests that the majority of those in employment in an organisation for 6-10 years had a high reliance on ICT, and notably, the participants from Sri Lanka have a high reliance on technology. In terms of budget allocation, 58 percent from Sri Lanka and 56 percent from the UK agree that their organisations have an allocated budget for information security. However, given the high level of reliance on technology in both countries, the budget allocation is relatively low and is a notable factor in Sri Lanka.

In Sri Lanka, the participants agree that despite the satisfactory level of resources allocated for information security, regular security awareness training received was inadequate (See figure 5.11). In Sri Lanka, only 42 percent of the participants (See annexe figure D.262) received regular cybersecurity awareness training (See figure 5.11). However, despite the lack of security awareness training, 75 percent of the participants from Sri Lanka (See annexe figure D. 264) have a high understanding of the impact of cyber-attacks on the public and the organisation. In the UK only 44 percent of the participants (See annexe figure E.325) received regular security awareness training (See figure 5.11). However, 56 percent of the participants (See annexe figure E.327) appears to have a high understanding of the impact of cyber-attacks on the public and the organisation.

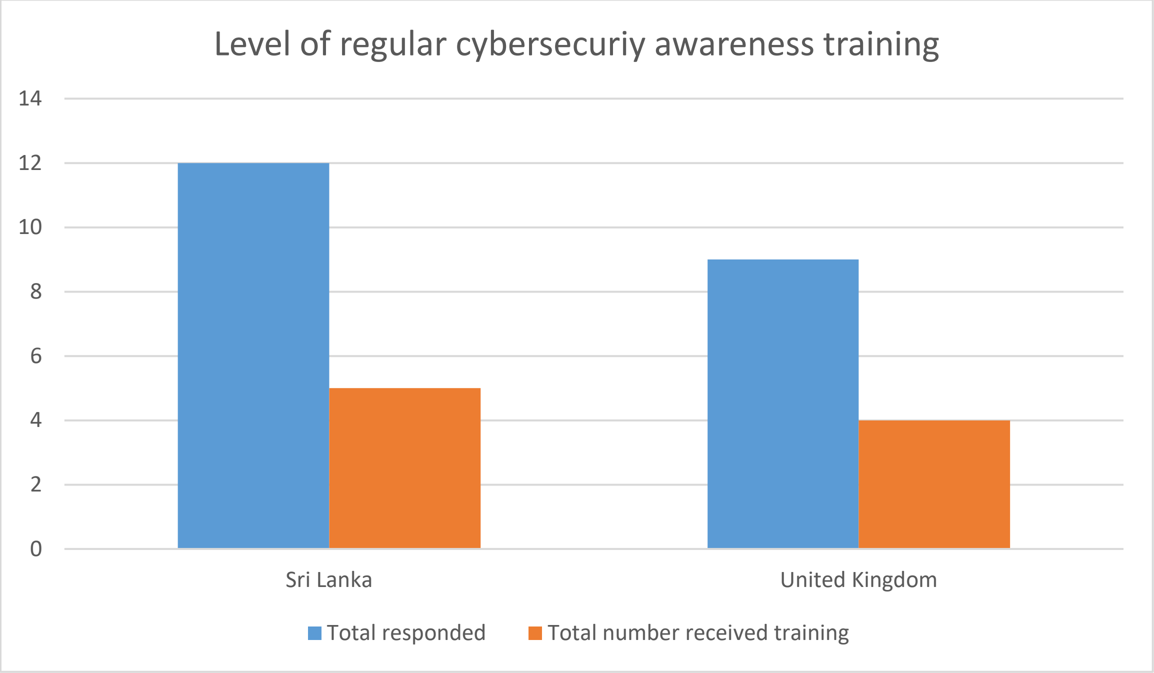


Figure 5.11: Level of cybersecurity awareness training (6-10 years in employment)

In addition to the lack of security awareness training provided by the organisations in both countries, in Sri Lanka, only 33 percent of the participants (See annexe figure D.263) had received support from the organisation to protect personal information, whilst only 44 percent of the participants in the UK (See annexe figure E.326) did receive organisational support (See figure 5.12).

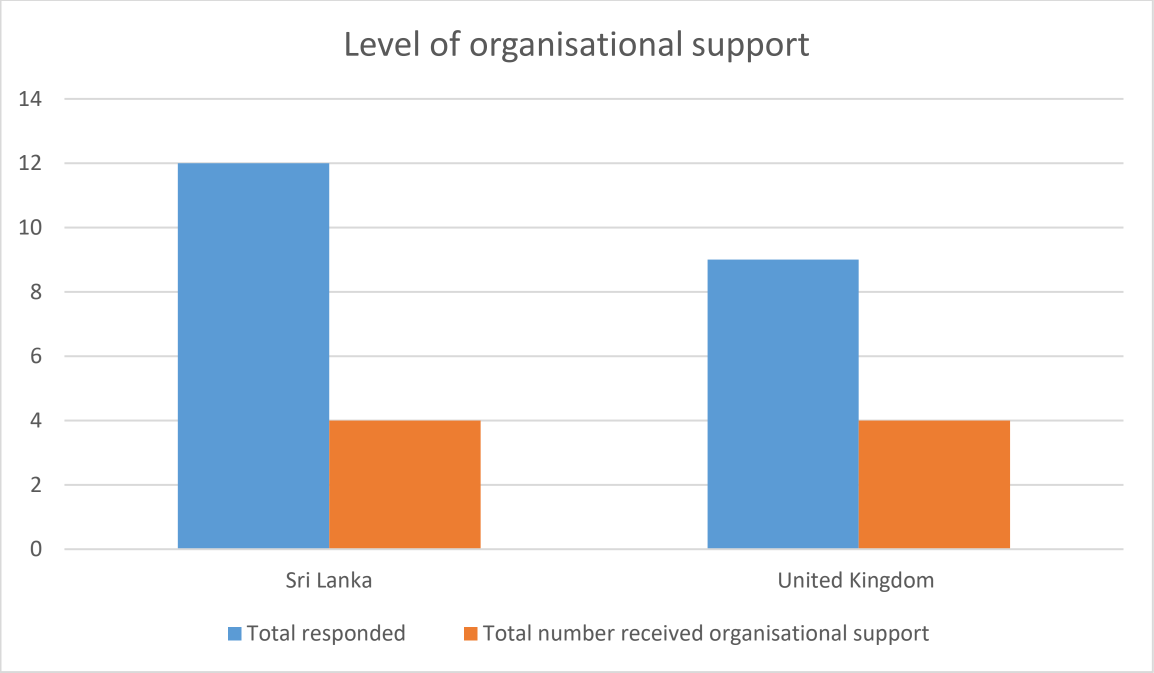


Figure 5.12: Level of organisational support (6-10 years in employment)

At the country level, both in the UK and Sri Lanka, according to the participants, the reliance on technology is high. However, both Sri Lankan and UK participants did not receive a sufficient level of either security awareness training or organisational support to protect personal information (See figure 5.11 and 5.12). The question then arises as to why the organisations did not support their employees although a budget had been allocated, and reliance on technology was high. However, there is a necessity for training and a supporting system for organisations in order to minimise any human errors.

In response to the social differences, the majority of Sri Lankan participants recognise the importance of both education and attitude and beliefs (See annexe figure D.274), and the majority of the UK participants only consider the importance of education (See annexe figure E.236). On the question of economic differences, the majority from both Sri Lanka and the UK agree with the premise that high income and upper-middle-income countries play a vital role in policy development and on political differences question, the majority choose democratic political system. Sri Lanka and the UK are geographically and regionally far apart, and in terms of economic capacity, they are at different levels, yet on the question of economic and political differences, there seems to be a similarity in the responses given by the participants. Sri Lankan participants agree with the supposition that national security is important in accepting and implementing global data privacy and security policies, and those from the UK has not considered any.

83 percent of Sri Lankan respondents with 6-10 years in industry (See annexe figure D.278), and 100 percent from the UK (See annexe figure E.341) support the need for having a global level data protection mechanism. To that end, the participants from both countries hold similar views about specific factors that need to be considered in accepting and implementing a global level data protection mechanism (See table 5.3). The key factors identified include organisational support, budget allocation, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies. In addition, participants from the UK agree with the importance of political differences, social differences in developing policies in collaboration with other countries, but not the participants from Sri Lanka. However, economic differences, ease of use of data privacy and security policies and previous experience with other countries in developing policies have not drawn the attention of the participants from both countries.

5.4.4 Over 10 year in employment

From Sri Lanka and the UK altogether, there were 35 participants and 24 out of them were male and 11 females. At the individual country level, in Sri Lanka, there were 15 participants and 10 out of them were males and 5 females, and in the UK, there were 20 participants and 14 out of them were males and 6 females. The age range of these participants was 18- 65+.

At the individual country level, 80 percent from Sri Lanka (See annexe figure D.292) and 80 percent from the UK (See annexe figure E.355) work in a technology reliance working environment. This indicates a majority of those who have been working in an organisation for over 10 years have had a high reliance on ICT.

In terms of budget allocation, 60 percent from Sri Lanka (See annexe figure D.293) and 55 percent from the UK (See annexe figure E.356) have indicated that their organisations have an allocated budget for information security. However, considering the reliance on technology in both countries, it is apparent that even though the reliance is high, the allocation of budget is comparatively low.

In Sri Lanka and the UK, the participants note that despite the satisfactory level of resources allocated for information security, regular security awareness training received was inadequate (See figure 5.13). Only 40 percent of the participants (See annexe figure D.294) received regular cybersecurity awareness training in Sri Lanka. According to 73 percent of the participants from Sri Lanka (See annexe figure D.296) have a high understanding of the impact of cyber-attacks on the public and the organisations. Whereas in the United Kingdom, only 40 percent of the participants (See annexe figure E.357) received regular security awareness training and 55 percent with a high understanding of the impact of cyber-attacks on the public and the organisation (See annexe figure E.359).

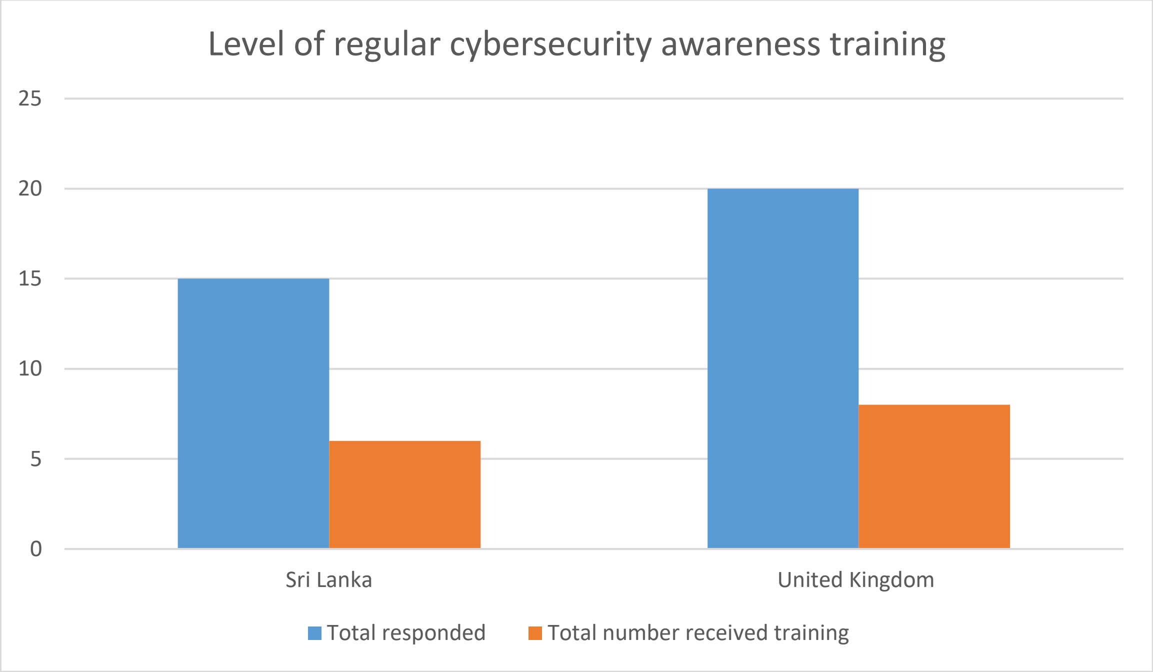


Figure 5.13: Level of regular cybersecurity awareness training (Over 10 year in employment)

In addition to the lack of security awareness training provided by the organisations, both in Sri Lanka and the UK, only 50 percent of the participants had received support from the organisation to protect personal information (See annexe figure D.295 and E.358). At the country level, both in Sri Lanka and the UK, according to the participants, the reliance on technology is high. However, both Sri Lankan and UK participants did not receive a sufficient level of either security awareness training or organisational support to protect personal information.

In response to the social differences, the majority of UK (See annexe figure E.369) and Sri Lankan participants recognise the importance of both education, and attitude and beliefs, and only the Sri Lankan participants have recognised the lifestyle in addition (See annexe figure D.306). On the question of economic differences, the majority from both Sri Lanka and the UK agree with the premise that high income and upper-middle-income countries play a vital role in policy development. In respect of political differences, the majority of UK participants selected democratic and republic political systems (See annexe figure E.371), whereas the majority of participants from Sri Lanka selected none (See annexe figure D.308). Sri Lanka and the UK are geographically and regionally far apart, and in terms of economic capacity, they are at different levels, yet on the question of economics, there seems to be a similarity in the responses given by the participants. Sri Lankan and UK participants agree with the supposition that protecting personal data security and privacy is important in accepting and implementing global data privacy and security policies.

100 percent of UK respondents (See annexe figure E.373) with over 10 years in the industry, and 85 percent from Sri Lanka (See annexe figure D.310) support the need for having a global level data protection mechanism. To that end, the participants from both countries hold similar views about specific factors that need to be considered in accepting and implementing a global level data protection mechanism (See table 5.3). The key factors identified include organisational support, economic differences, political differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies. However, participants from Sri Lanka also recognise the importance of considering social differences, but those from the UK made no reference to this at all.

Table 5.3: Responses based on the experience in employment

	Less than one year	**1- 5 years**	**6-10 years**	**Over 10 years**
Reliance on technology	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT
Budget allocation	Both countries have an allocated budget	Both countries have an allocated budget	Both countries have an allocated budget	Both countries have an allocated budget
Regular security	Provision of security	Provision of security	Provision of security	Provision of security

awareness training	awareness training: inadequate in Sri Lanka; adequate in the UK	awareness training: inadequate in Sri Lanka; adequate in the UK	awareness training inadequate in both countries	awareness training inadequate in both countries
Understanding of the impact of cyber-attacks on the public and the organisation	High level of understanding amongst the participants from both countries	High level of understanding amongst the participants from both countries	High level of understanding amongst the participants from both countries	High level of understanding amongst the participants from both countries
Organisational level support to protect personal information	Lack of organisational support in both countries.	Lack of organisational support in Sri Lanka. UK participants received a satisfactory level of organisational support	Lack of organisational support in both countries.	Satisfactory level of organisational support received by the participants in both countries.
Social differences	Importance of education emphasised by the majority of the participants both in Sri Lanka and the UK	Importance of education, and attitudes and beliefs emphasised by majority of participants both in Sri Lanka and the UK	Importance of education emphasised by the majority of the participants both in Sri Lanka and the UK	Importance of education, and attitudes and beliefs emphasised by majority of participants both in Sri Lanka and the UK

Economic differences	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries
Political differences	The majority prefers the democratic political system	The majority prefers the democratic political system	The majority prefers the democratic political system	Unspecified by the majority
Need for global level data protection mechanism	The majority from both countries agree	The majority from both countries agree	The majority from both countries agree	The majority from both countries agree
Commonly agreed factors that should consider in developing a global level data protection mechanism	Organisational support, budget allocation, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, previous	Organisational support, budget allocation, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust	Organisational support, budget allocation, personal privacy, national security, the usefulness of data privacy and security policies and mutual trust between and previous experience with other countries in developing	Organisational support, economic differences, political differences, personal privacy, national security, ease of use of data privacy and security policies, the

	experience with other countries in developing policies (See annexe figure D.215-225 and E.278-288)	between countries previous experience with other countries in developing policies (See annexe figure D.247-257 and E.310-320)	policies (See annexe figure D.279-289 and E.342-352)	usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See annexe figure D.311-321 and E.374-384)

5.5 Industries

5.5.1 Accountancy, banking, and finance sector

The participants from both Sri Lanka (See annexe figure D.325) and the UK (See annexe figure E.388) work in accountancy, banking, and finance sectors have 100 percent reliance on technology. 88 percent of the participants from both countries accept that their organisations have an allocated budget for information security (See annex figure D.326 and E.389); also, 75 percent received adequate regular security awareness training funded from the allocated budget (See annexe figure D.327 and E.390). 75 percent of the participants from Sri Lanka (See annexe figure D.329) and 63 percent from the UK (See annexe figure E.392) claim a satisfactory level of understanding of the impact of cyber-attacks on the public and the organisation. In addition, 75 percent of the participants from both countries received support from the organisation to protect personal information (See annexe figure D. 328 and E.391). This means that those employed in this sector received regular training and support from the organisation.

In response to the survey component on social differences, the majority from Sri Lanka recognises the importance of education, lifestyle and attitude and beliefs (See annexe figure D.338), whereas the majority from the UK recognises the importance of education, and attitude and beliefs only (See annexe figure E.401). In addition, the majority from Sri Lanka agree that both high income and upper-middle-income countries play a vital role in policy development (See annexe figure D.339), but those from the UK specify upper-middle-income countries only(See annexe figure E.402). Sri Lankan participants in employment in this sector select both the democratic and the republican style political system (See annexe figure D.340), while those from the UK choose only the democratic political system (See annexe figure E.403). The participants from Sri Lanka recognise the importance of the protection of personal data security and privacy when accepting and implementing global data privacy and security policies (See annexe figure D.341), while those from the UK only recognise the importance of protecting national security (See annexe figure E.404).

Those working in the accountancy, banking and finance sectors show an emphatic message on the need to have a global level data protection mechanism, with 75 percent from Sri Lanka (See annexe figure D. 342) and 100 percent from the UK (See annexe figure E.405) in agreement. The common factors that the participants have identified (See table 5.4) as appropriate are organisational support, budget allocation, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between the countries. Also, added to that, the participants from Sri Lanka recognise the importance of previous experience in developing policies with other countries, while those from the UK place emphasis on the political differences. However, the majority of the participants from both countries make no reference to the importance of social differences, economic differences, and the ease of use of data privacy and security policies.

5.5.2 Business, consultancy, and management sector

These participants from both Sri Lanka and the UK are working in the Business, consultancy, and management sectors. The survey shows that 67 percent from Sri Lanka (See annexe figure D.357), and 71 percent from the UK (See annexe figure E.420) have a high reliance on technology in their working environment. Also, the same proportion from each country accepts that their organisations have an allocated budget for information security.

50 percent of the participants from Sri Lanka (See annexe figure D.359) received regular cyber security awareness training, while 71 percent of the participants from the UK (See annexe figure E.422) had claimed that the level of resources allocated for information security was satisfactory and regular security awareness training was adequate.

The survey responses suggest that the understanding of the impact of cyber-attacks on the public and the organisations are high amongst the participants from both Sri Lanka and the UK and, from each country, 50 percent (See annexe figure D.361) and 71 percent (See annexe figure E.424) respectively support that assessment. Also, 66 percent of the participants from Sri Lanka (See annexe figure D.360), and 43 percent from the UK (See annexe figure E.423) received support from the organisation to protect personal information. A percentage of the participants from Sri Lanka claim that they received a minimal level of regular training, however a percentage says the organisational support they received is high.

In respect of the survey question on social differences, the majority from Sri Lanka recognise the importance of education and lifestyle (See annexe figure D.370) while the majority from the UK recognises the importance of education, and attitude and beliefs (See annexe figure E.433). In addition, the majority from Sri Lanka agrees that high-income countries play a vital role in policy development (See annexe figure D.371), and the participants from the UK agree both high income and upper-middle-income countries play a vital role in policy development (See annexe figure E.434).

Furthermore, the majority from both countries favours a democratic political system in preference to others (See annexe figure D.372 and E.435). In accepting and implementing global data privacy and security policies, the participants from Sri Lanka recognise the importance of protection of national security (See annexe figure D.373), and those from the UK focus on the importance of protection of personal data security and privacy (See annexe figure E.436). UK citizens seem less concerned about national security than the risks to privacy. That sense of feeling and the concerns could be attributable to the unpredictable nature of Cyber related threats.

The clear indication from 83 percent of the participants from Sri Lanka (See annexe figure D.374) and 100 percent from the UK (See annexe figure E.437) employed in the business, consultancy and management sector is their recognition of the need to have a global level data protection mechanism. The common factors considered by the participants are (See table 5.4) organisational support, budget allocation, economic differences, personal privacy, national security, the ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience in developing policies with other countries. In addition, participants from Sri Lanka recognise the importance of social differences, and intriguingly majority of the participants from both countries make no reference to the importance of political differences.

5.5.3 Education sector

There is a high reliance on technology amongst the participants employed in the education sector, according to 59 percent of the participants from Sri Lanka (See annexe figure D.389) and 100 percent from the UK. In terms of funding , 59 percent from Sri Lanka and 87 percent from the UK (See annexe figure E.452) agree that their organisations allocated a budget for information security.

Participants from Sri Lanka finds the regular security awareness training they received was inadequate; only 47 percent has received training (See annexe figure D.391) despite the satisfactory level of resources allocated for information security. Despite the lack of security awareness training, 59 percent of the participants (See annexe figure D.393) understand the impact of cyber-attacks on the public and the organisation. 60 percent of the participants in the UK received regular cybersecurity awareness training (See annexe figure E.454), and 73 percent have a high understanding of the impact of cyber-attacks (See annexe figure E.456). Also, 73 percent of the participants from the UK (See annexe figure E.455) received support from the organisation to protect personal information; in contrast, only 41 percent in Sri Lanka received support (See annexe figure D.392), even though the level of the funding allocated through the budget was satisfactory.

In respect of the survey question on social differences, the majority from both Sri Lanka and the UK recognise the importance of education (See annexe figure D.402), and the majority from the UK also recognises the importance of lifestyle, and attitude and beliefs (See annexe figure E.465). Similarly, the majority from both countries agree on economic and political differences. The majority from both countries accept that both high income and upper-middle-income countries play a vital role in policy development (See annexe figure D.403 and E.466). They also choose a democratic political system in preference to others (See annexe figure D.404 and E.467). The participant from both countries recognises the importance of the protection of personal data security and privacy above the protection of national security in respect to accepting and implementing global data privacy and security policies.

Those employed in the education sector, 88 percent from Sri Lanka (See annexe figure D.406) and 93 percent from the UK (See annexe figure E.469) accept the need to have a global level data protection mechanism. The common factors that the participants agree with and accept are (See table 5.4), organisational support, budget allocation, personal privacy, national security, the ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust in developing policies with other countries with previous experience. It is only the UK participants who recognise the importance of social, political and economic differences.

5.5.4 Healthcare sector

The participants who responded to the survey question in this section work in the healthcare sector. The reliance on technology amongst the participants from both Sri Lanka and the UK is high, 60 percent (See annexe figure D.421) and 83 percent (See annexe figure E.484), respectively. On the provision of funding, 60 percent from Sri Lanka (See annexe figure D.422) and 83 percent from the UK (See annexe figure E.485) indicate that their organisations allocated a budget for information security.

The participants from Sri Lanka feel the regular security awareness training received was inadequate; only 40 percent received training (See annexe figure D.423), despite the satisfactory level of resources allocated for information security. But despite the lack of security awareness training, 60 percent of the participants claim to have a high understanding of the impact of cyber-attacks on the public and the organisation (See annexe figure D.425). Whereas in the UK, 83 percent of the participants received regular cyber security awareness training (See annexe figure E.486), and 50 percent have a high understanding of the impact of cyber-attacks (See annexe figure E.488). The statistical figures show the imbalance between the level of training received and the low level of understanding of cyber threats amongst the UK participants. The participants from both countries have not received support from the organisation to protect personal data (See figure 5.14). Only 33 percent of the participants from the UK and only 20 percent from Sri Lanka received support. The reasons behind this increased awareness amongst the participants must be self-learning, and the regular training and support received from the organisation.

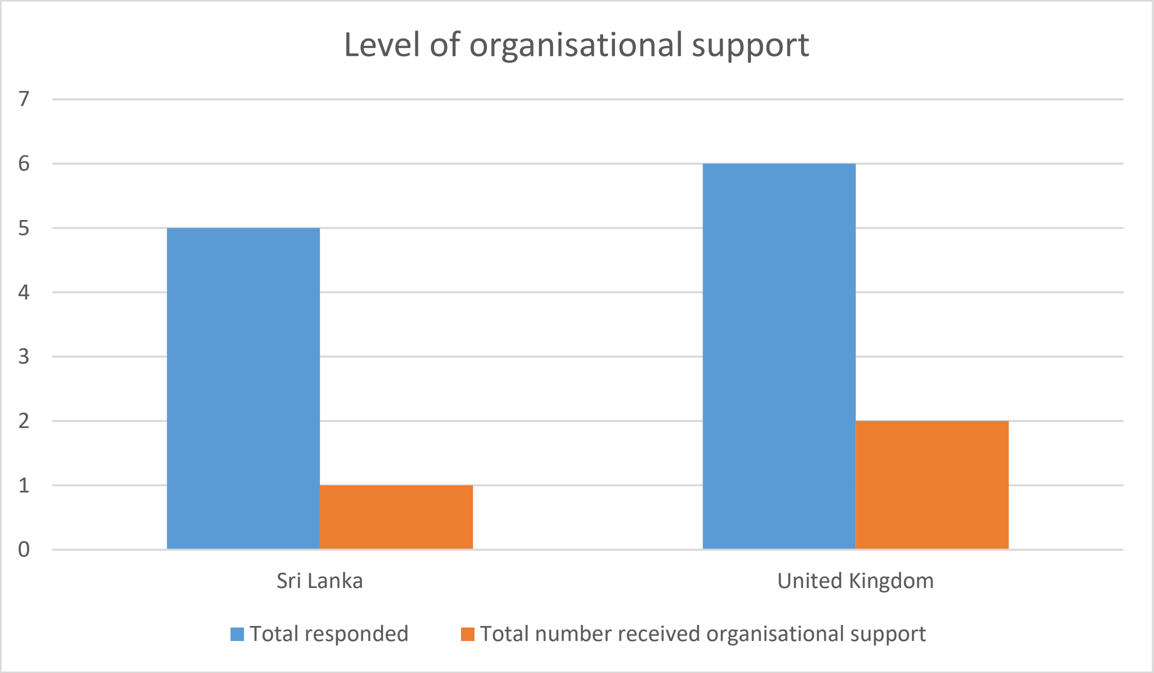


Figure 5.14: Level of organisational support (Healthcare sector)

In response to the question of the social differences, the majority from both Sri Lanka and the UK recognise the importance of education and attitude and beliefs (See annexe figure D.434 and E.497), and in addition, the majority from Sri Lanka also recognises the importance of lifestyle (See annexe figure D.434). Adding to that, the majority from both countries give similar responses to economic differences also. The majority from both countries show that the high income and upper-middle-income and lower-middle-income countries play a vital role in policy development. Unlike the participants in other industries, the majority of the participants from the UK choose democratic, republic, communist and dictatorship political systems (See annexe figure E.498), whilst those from Sri Lanka prefers only the democratic political system (See annexe figure D.435). The participants from the UK emphasises the importance of protection of personal data security and privacy in accepting and implementing global data privacy and security policies (See annexe figure E.500); however, in contrast, in the eyes of the participants from Sri Lanka, it does not appear to be a factor for consideration (See annexe figure D.437).

The message from those who are in the healthcare sector is clear (See table 5.4). 80 percent from Sri Lanka (See annexe figure D.438) and 100 percent from the UK (See annexe figure E.501) have highlighted the need to have a global level data protection mechanism. The common factors that have been highlighted by the participants are organisational support, budget allocation, economic differences, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies. In addition, only the participants from the UK have highlighted the importance of social, political and ease of use of data privacy and security policies.

5.5.5 Information security sector

The participants responded to this section work in the information security sector. There is a high reliance on technology amongst the participants from both Sri Lanka, 86 percent, and 92 percent of those from the UK, respectively. In terms of funding, 71 percent from Sri Lanka, and 69 percent from the UK show that their organisations had a budget allocation for information security.

71 percent of the participants from Sri Lanka (See annexe figure D.455) agree that the regular security awareness training received was adequate; and 71 percent claims to have a high understanding of the impact of cyber-attacks on the public and the organisation (See annexe figure D.457). Whereas in the UK, only 39 percent of the participants received regular cybersecurity awareness training (See annexe figure E.518). However, 62 percent claims a high understanding of the impact of cyber-attacks (See annexe figure E.520), but the participants from both countries received no support from the organisation to protect personal data (See annexe figure D.456 and D.519). What is apparent is that, even though the reliance on technology and budget allocation is high in the United Kingdom, the participants have not received either training or support from the organisation.

In respect of the question on social differences, the majority from both Sri Lanka and the UK recognise the importance of education, and in addition (See annexe figure D.466 and E.529), the majority from the UK recognise the importance of attitude and beliefs (See annexe figure E.529). Furthermore, the majority from both countries accept that the upper-middle-income countries, and in addition, those from the UK also accept that high-income economies play a vital role in policy development. In respect of political differences, the majority from Sri Lanka select the republic political system (See annexe figure D.468), while the majority from the UK opts for the democratic political system (See annexe figure E.531). Both countries neither selected the importance of protection of personal data security and privacy nor protection of national security in the process of accepting and implementing global data privacy and security policies (See annexe figure D.469 and E.532)

The message from those working in the information security sector is clear (See table 5.4). 71 percent from Sri Lanka (See annexe figure D.470) and 85 percent from the UK (See annexe figure E.533) accept the need to have a global level data protection mechanism. Both countries recognise national security as a common factor for consideration. The additional factors considered by the participants from the United Kingdom are, such as organisational support, budget allocation, social differences, economic differences, personal privacy, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience in developing policies with other countries.

5.5.6 Media sector

The participants employed in the media sector, both from Sri Lanka and the UK, have a high reliance on technology reliance amongst them, 100 percent (See annexe figure D.485), and 80 percent (See annexe figure E.548) respectively from both countries. In terms of funding allocation, 50 percent from Sri Lanka (See annexe figure D.486) and 60 percent from the UK (See annexe figure E.549) agree that their organisations have an allocated budget for information security. This represents comparatively a low budget allocation relative to the high level of ICT reliance.

The participants from both countries find that given the satisfactory level of resources allocated for information security, the regular security awareness training received is inadequate (See figure 5.15). Only 40 percent of the participants in the UK received training (See annexe figure E.550), and the participants from Sri Lanka received no training (See annexe figure D.487).

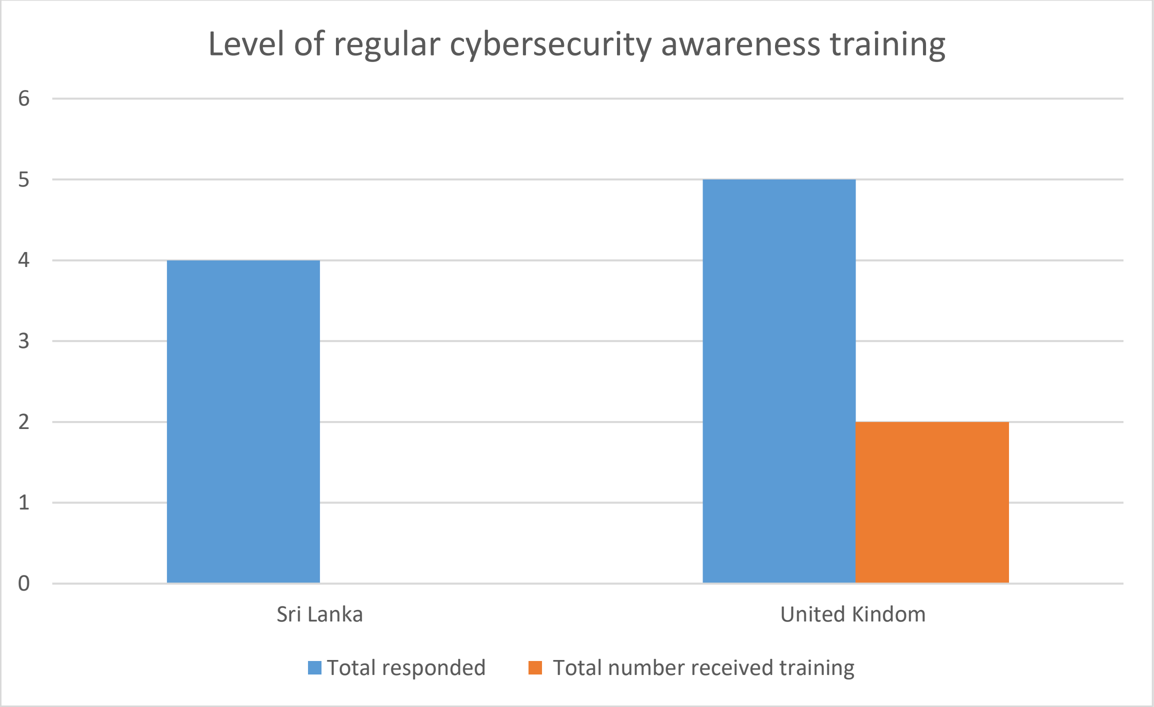
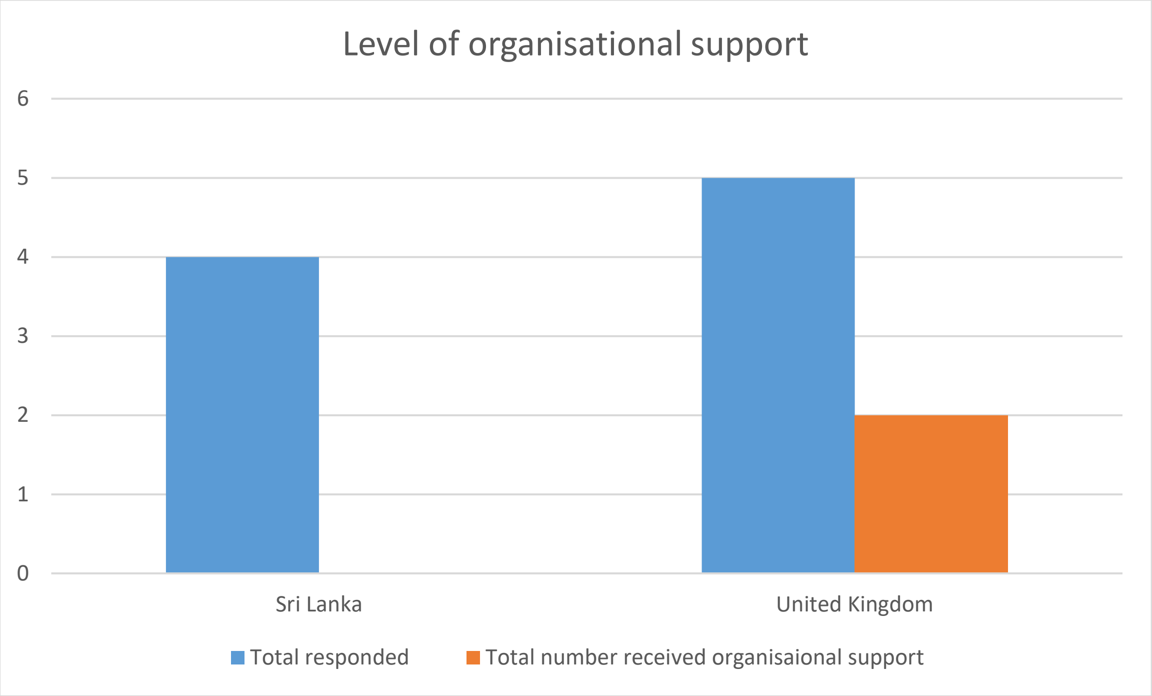


Figure 5.15: Level of regular cybersecurity awareness training (Media Sector)

Despite the lack of security awareness training, 100 percent of the participants from Sri Lanka (See annexe figure D.489) and 60 percent of the participants from the UK (See annexe figure E.552) agree they have a high understanding of the impact of cyber-attacks on the public and the organisation. Only 40 percent of the participants from the UK (See annexe figure E.551) received support from the organisation to protect personal information, but none of the participants from Sri Lanka did (See annexe figure D.488) (See figure 5.16).



5.16: Level of organisational support (Media sector)

This shows that even though the understanding of cyber threats features high amongst the participants from both countries, there is a lack of training and support training and support from the organisation.

In respect of social differences, the majority from Sri Lanka recognises the importance of lifestyle, education and attitude and beliefs, social mobility, demography, and historical issues (See annexe figure D.498), whereas a majority from the UK do not consider any of the factors (See annexe figure E.561). Furthermore, the majority from both countries believe that the upper-middle-income countries play a vital role in policy development (See annexe figure D.499 and E.562). On political differences, the majority from Sri Lanka select both democratic and monarchist political systems (See annexe figure D.500) whilst the majority from the UK (See annexe figure E.563) select the democratic political system. The majority of participants from the UK recognises the importance of protection of national security (See annexe figure E.564), and the majority from Sri Lanka recognises that both protection of personal data security and privacy and protection of national security are important in accepting and implementing global data privacy and security policies (See annexe figure D.501).

There is a clear message from those employed in the media sector (See table 5.4); 100 percent of the participants from both countries (See annexe figure D.502 and E.565) accept the need to have a global level data protection mechanism. The common factors considered by the participants are, organisational support, budget allocation, social differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience in developing policies with other countries. The participants from Sri Lanka emphasise the economic and political differences as well.

Table 5.4: Employment based responses (Continued)

	Accountancy, banking and finance sector	**Business, consultancy and management sector**	**Education sector**
Reliance on technology	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT
Budget allocation	Both countries have an allocated budget	Both countries have an allocated budget	Both countries have an allocated budget
Regular security awareness training	Provision of security awareness training: adequate in both countries	Provision of security awareness training: inadequate in Sri Lanka; adequate in the UK	In Sri Lanka, inadequate security awareness training; in the UK, a satisfactory level of training provided
Understanding of the impact of cyber-attacks on	High level of understanding amongst the	High level of understanding amongst the	High level of understanding amongst the

the public and the organisation	participants from both countries	participants from both countries	participants from both countries
Organisational level support to protect personal information	Satisfactory level of organisational support received by the participants in both countries	Lack of organisational support in the UK. Sri Lankan participants received a satisfactory level of organisational support	Lack of organisational support in Sri Lanka. UK participants received a satisfactory level of organisational support
Social differences	Importance of education and attitude and beliefs emphasised by majority of the participants both in Sri Lanka and the UK	Importance of education emphasised by the majority of the participants both in Sri Lanka and the UK	Importance of education emphasised by the majority of the participants both in Sri Lanka and the UK
Economic differences	The majority from both Sri Lanka and the UK give prominence to upper-middle-income countries	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries

Political differences	The majority prefers the democratic political system	The majority prefers the democratic political system	The majority prefers the democratic political system
Need for global level data protection mechanism	The majority from both countries agree	The majority from both countries agree	The majority from both countries agree
Commonly agreed factors that should consider in developing a global level data protection mechanism	Organisational support, budget allocation, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between countries (See annexe figure D.343-353 and E. 406-416)	Organisational support, budget allocation, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See annexe figure D.375-385 and E.438-448)	Organisational support, budget allocation, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See annexe figure D.407-417 and E.470 and E.480)

Table 5.4: Employment based responses

	Healthcare sector	**Information security sector**	**Media sector**
Reliance of technology	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT	Participants from both countries extensively rely on ICT
Budget allocation	Both countries have an allocated budget	Both countries have an allocated budget	Both countries have an allocated budget
Regular security awareness training	Provision of security awareness training: inadequate in Sri Lanka; adequate in the UK	Provision of security awareness training: inadequate in the UK; adequate in Sri Lanka	Provision of security awareness training: inadequate in both Sri Lanka and in the UK
Understanding of the impact of cyber-attacks on the public and the organisation	High level of understanding amongst the participants from both countries	High level of understanding amongst the participants from both countries	High level of understanding amongst the participants from both countries
Organisational level support to protect personal information	Lack of organisational support in both countries.	Lack of organisational support in both countries.	Lack of organisational support in both countries.

Social differences	Importance of education, and attitude and beliefs emphasised by majority of the participants both in Sri Lanka and the UK	Importance of education emphasised by the majority of the participants both in Sri Lanka and the UK	Unspecified by the majority
Economic differences	The majority from both Sri Lanka and the UK give prominence high income, upper-middle-income and lower-middle-income countries	The majority from both Sri Lanka and the UK give prominence to upper middle-income countries	The majority from both Sri Lanka and the UK give prominence to upper middle-income countries
Political differences	The majority prefers the democratic political system	Unspecified by the majority	The majority prefers the democratic political system
Need for global level data protection mechanism	The majority from both countries agree	The majority from both countries agree	The majority from both countries agree
Commonly agreed factors that should consider in developing a global level data	Organisational support, budget allocation, economic differences, personal privacy,	National security (See annexe figure D.471-481 and E.534-544)	Organisational support, budget allocation, social differences, personal privacy, national security,

protection mechanism	national security, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See annexe figure D.439-449 and E.502-512)		ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See annexe figure D.503-513 and E.566-576)

5.5.7 Other participants from different industries in Sri Lanka

Table 5.5: Public services and administration and Tourism based responses

	Public services and administration	**Tourism**
Reliance of technology	Participants extensively rely on ICT (See annexe figure D.517)	Participants extensively rely on ICT (See annexe figure D.549)
Budget allocation	Have an allocated budget (See annexe figure D.518)	Have an allocated budget (See annexe figure D.550)
Regular security awareness training	Inadequate security awareness training (See annexe figure D.519)	Inadequate security awareness training (See annexe figure D.551)

Understanding of the impact of cyber-attacks on the public and the organisation	High level of understanding amongst the participants (See annexe figure D.521)	High level of understanding amongst the participants (See annexe figure D.553)
Organisational level support to protect personal information	Lack of organisational support (See annexe figure D.520)	Lack of organisational support (See annexe figure D.552)
Social differences	Importance of education, and attitude and beliefs emphasised by the majority (See annexe figure D.530)	Importance of social mobility emphasised by the majority (See annexe figure D.562)
Economic differences	The majority give prominence high income and upper-middle-income countries (See annexe figure D.531)	The majority give prominence high income and upper-middle-income countries (See annexe figure D.563)
Political differences	The majority prefers the democratic political system (See annexe figure D.532)	The majority prefers the republic political system (See annexe figure D.564)
Need for global level data protection mechanism	Majority agree (See annex figure D.534)	Majority agree (See annex figure D.566)
Commonly agreed factors that should consider in developing a global	Organisational support, budget allocation, social differences, political differences, economic differences, personal privacy,	Organisational support, economic differences, personal privacy, national security, ease of use of data privacy and

level data protection mechanism	national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies and previous experience with other countries in developing policies (See annexe figure D.535-545)	security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See annexe figure D.567-577)

5.5.8 Other participants from different industries in the United Kingdom

Table 5.6: Charity and Voluntary work based responses

	Charity and voluntary work
Reliance of technology	Participants extensively rely on ICT (See annexe figure E.580)
Budget allocation	Have an allocated budget (See annexe figure E.581)
Regular security awareness training	Security awareness training received inadequate (See annexe figure E.582)
Understanding of the impact of cyber-attacks on the public and the organisation	Lack of understanding amongst the participants (See annexe figure E.584)
Organisational level support to protect personal information	Lack of organisational support (See annexe figure E.583)

Social differences	Importance of education, lifestyle and attitude and beliefs emphasised by the majority (See annexe figure E.593)
Economic differences	The majority give prominence upper-middle-income countries (See annexe figure E.594)
Political differences	The majority prefers the democratic political system (See annexe figure E.595)
Need for global level data protection mechanism	The majority agree (See annexe figure E.597)
Commonly agreed factors that should consider in developing a global level data protection mechanism	Budget allocation, social differences, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies and mutual trust between countries (See annexe figure E. 598-608)

5.5.9 Currently studying at undergraduate or postgraduate level

From Sri Lanka and the UK, there were 39 participants altogether, 22 male and 16 females, and 1 non-binary. At the country level, all 6 participants from Sri Lanka were females, whereas from the UK, a total of 33 participants, 22 males, 10 females and 1 non-binary; all between 18-45 age range.

100 percent from Sri Lanka (See annexe figure D.581) and 76 percent from the UK (See annexe figure E.612) employed in a technology reliance working environment, which indicates that the majority of those currently studying at undergraduate or postgraduate level have a high reliance on ICT.

In terms of funding, 100 percent from Sri Lanka (See annexe figure D.582) and 58 percent from the UK (See annexe figure E.613) agree that their organisations have an allocated budget for information security. However, only 17 percent of the participants from Sri Lanka (See annexe figure D.584) and 46 percent of the participants in the UK (See annexe figure E.615) received support from the organisation to protect personal information (See figure 5.17). The responses were received from participants with part-time/full-time/voluntary/internship experience.

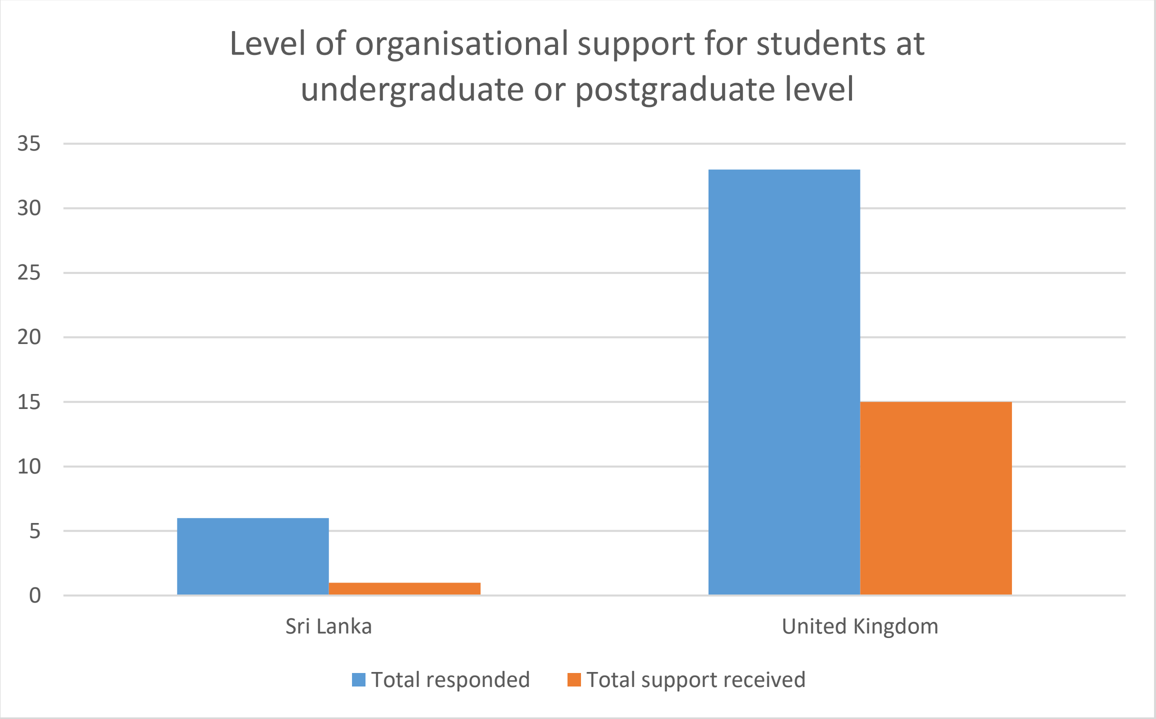


Figure 5.17: Level of organisational support for students at undergraduate or postgraduate level

The participants from Sri Lanka claims that the regular security awareness training they received was inadequate. Only 33 percent of the participants received regular cybersecurity awareness training (See annexe figure D.583); however, 67 percent of the participants (See annexe figure D.585) have a high understanding of the impact of cyber-attacks on the public and the organisation. Whereas 61 percent of the participants from the UK received regular security awareness training (See annexe figure E.614), and 67 percent have a high understanding of the impact of cyber-attacks on the public and the organisation (See annexe figure E.616). In effect, even though the participants from Sri Lanka received no regular training, they have a good understanding of cyber-attacks.

In respect of the survey component social differences, the majority from both Sri Lanka (See annexe figure D.594) and the UK (See annexe figure E.625) made no reference to the importance of any social differences. On the economic differences, the majority from both Sri Lanka and the UK agree that the high income and upper-middle-income countries play a vital role in policy development (See annexe figure D.595 and E.626), and on political differences, the majority selected democratic political system (See annexe figure D.596 and E.627). Furthermore, in accepting and implementing global data privacy and security policies, participants from both Sri Lanka and the UK made no account of the importance of either protecting personal data security and privacy or national security (See annexe figure D.597 and E.628).

There is an encouraging message from the respondents currently studying at the undergraduate and postgraduate levels (See table 5.7). 67 percent of the participants from Sri Lanka (See annexe figure D.598) and 73 percent of the participants from the UK (See annexe figure E.629) accept the need to have a global level data protection mechanism. The common factor identified by the participants are organisational support, budget allocation, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience in developing policies with other countries. In addition, participants from Sri Lanka also consider the importance of political differences, and participants from the United Kingdom opt for economic differences. However, the social differences component was not considered by the majority of the participants from either country.

Table 5.7: Undergraduate and postgraduate level based responses

	Currently studying at undergraduate and postgraduate level
Reliance of technology	Participants from both countries extensively rely on ICT
Regular security awareness training	Provision of security awareness training: inadequate in Sri Lanka; adequate in the UK
Understanding of the impact of cyber-attacks on the public and the organisation	High level of understanding amongst the participants from both countries

Social differences	Unspecified by the majority
Economic differences	The majority from both Sri Lanka and the UK give prominence high income and upper-middle-income countries
Political differences	The majority prefers the democratic political system
Need for global level data protection mechanism	The majority from both countries agree
Commonly agreed factors that should consider in developing a global level data protection mechanism	Organisational support, budget allocation, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See annexe figure D.599-609 and E. 630-640)

In the above section, the researcher analysed the responses received from the participants and identified the factors that the participants have considered useful in developing a global level data protection mechanism. Having considered the factors emphasised by the majority of the participants, the researcher embarked on developing the Policy Acceptance Model using Technology Acceptance Models.

5.6 Technology Acceptance Models

TAM is an information systems theory that illustrates how the users are inclined to accept and use a particular technology (Surendran, 2012). The theory explains that an intention to accept a certain technology and its actual use is predicted by the person's perceptions of the usefulness and ease of use of a specific technology (Portz at el., 2019). The Technology Acceptance Models had been applied widely in a variety of domains to understand and to predict user behaviour such as voting, dieting, family planning, donating blood, women's occupational orientations, breast cancer screening, transport mode preferences, the use of birth control pills, education, consumer purchase behaviours, and computer usage (Taherdoost, 2017, P.961). In this research, the researcher has used components from the existing Technology Acceptance Models (TAM), namely TAM by Fred D. Davies (1989) (Surendran, 2012) (See figure 5.18), the final version of TAM (Venkatesh and Davis, 1996) (See figure 5.19), TAM 2 (Venkatesh and Davis (2000) (See figure 5.20), the Unified Theory of Acceptance and Use of Technology (UTAUT) (2003) (Alwahaishi and Snasel, 2013, P.25-39) (See figure 5.21), TAM (Mc Farland and Hamilton, 2006) (See figure 5.22) and TAM 3 (Venkatesh and Bala, 2008) (See figure 5.23) in developing Policy Acceptance Model.

5.6.1 Technology Acceptance Model (TAM) (1989)

This model sets out a number of factors that influence the user to make decisions on how and when to use the technology. TAM explains the user motivation in three factors; perceived usefulness, perceived ease of use, and attitude toward use. These beliefs are regarded as essential determinants for assessing users' acceptance of technology and their attitudes towards adopting a particular system (Taherdoost, 2017, P.962). In this TAM model, the attitude towards using is governed by the perceived usefulness and perceived ease of use, and it defines the criteria for accepting or rejecting a specific system. In addition, several external variables will affect perceived usefulness and perceived ease of use.

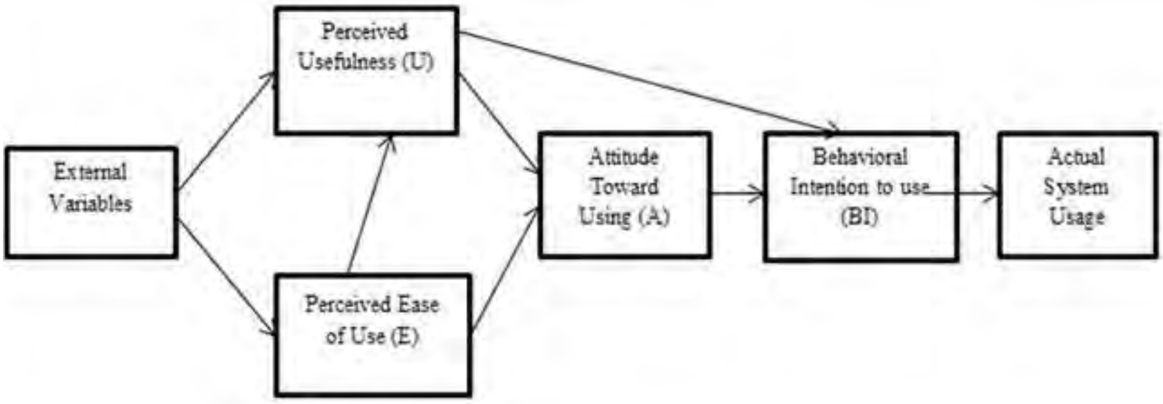

Perceived Usefulness (U)
External Variables
Attitude Toward Using (A)
Behavioral Intention to use (BI)
Actual System Usage
Perceived Ease of Use (E)

Figure 5.18: Technology Acceptance Model (TAM) by Davis (1989) (Surendran, 2012)

5.6.2 The final version of Technology Acceptance Model (1996)

Venkatesh and Davis created the final version of their Technology Acceptance Model (Venkatesh and Davis, 1996) and found that both perceived usefulness and perceived ease of use have a direct influence on behaviour intention. However, the attitudes factor had been omitted from the TAM Model due to its insignificant role in the users' behaviour, and by omitting the attitude factor, they have highlighted that perceived usefulness and perceived ease had a direct effect on behavioural intention, and further concluded that the users might perhaps resort to the use of technology even in the absence of a positive attitude.

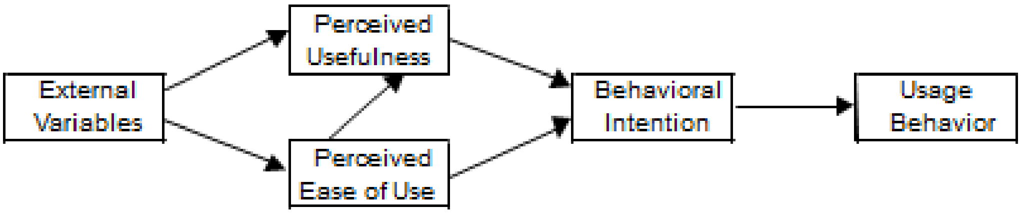


Figure 5.19.: The final version of Technology Acceptance Model by Venkatesh and Davis (1996) (Lai, 2017)

5.6.3 Technology Acceptance Model 2 (2000)

TAM2 was developed with the intention to identify the reasons for finding specific systems useful from different perspectives (Venkatesh and Davis, 2000). Venkatesh and Davis extended the original TAM model to explain perceived usefulness and usage intentions in terms of subjective norms, job relevance, output quality, image, result demonstrability experience, voluntariness, and perceived ease of use. The attitude was omitted from the TAM2 as well.

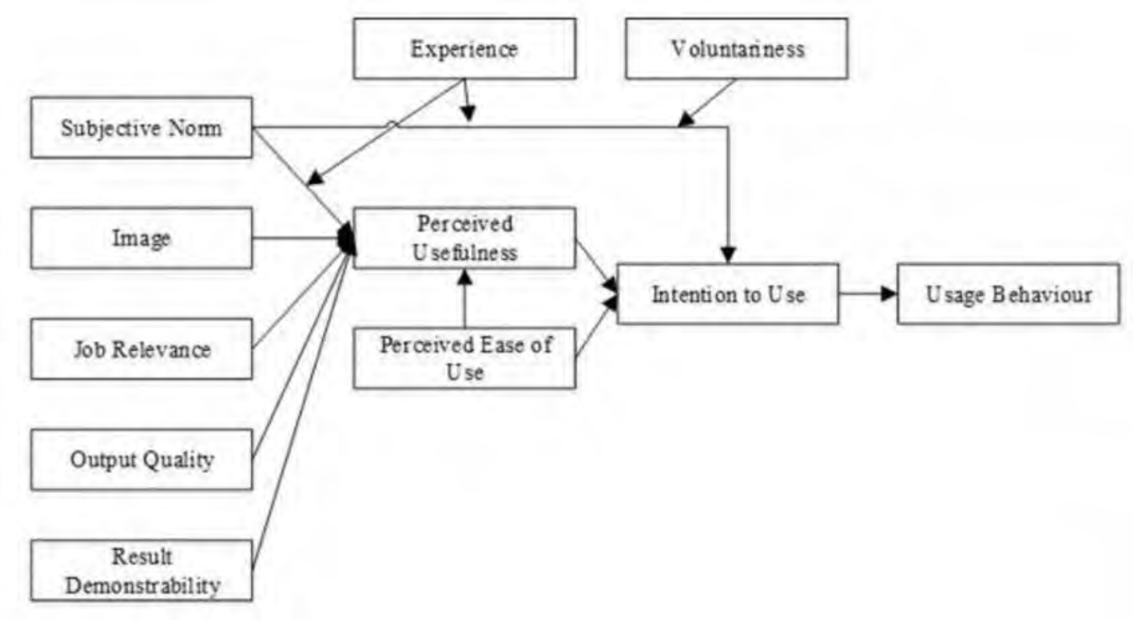


Figure 5.20: Technology Acceptance Model 2 by Venkatesh and Davis (2000) (Venkatesh and Davis, 2000, P.188)

5.6.4 The Unified Theory of Acceptance and Use of Technology (UTAUT) (2003)

In their attempt to integrate user acceptance models, Venkatesh et al. formulated the Unified Theory of Acceptance and the Use of Technology (UTAUT) (Alwahaishi and Snasel, 2013, P.25-39). This model explains behavioural intention using performance expectancy, effort expectancy, social behaviour, facilitating conditions, gender, age, the voluntariness of Use and Experience. The UTAUT has been adopted by some studies in healthcare Wang, Liu, Y. and Liu, H. 2020).

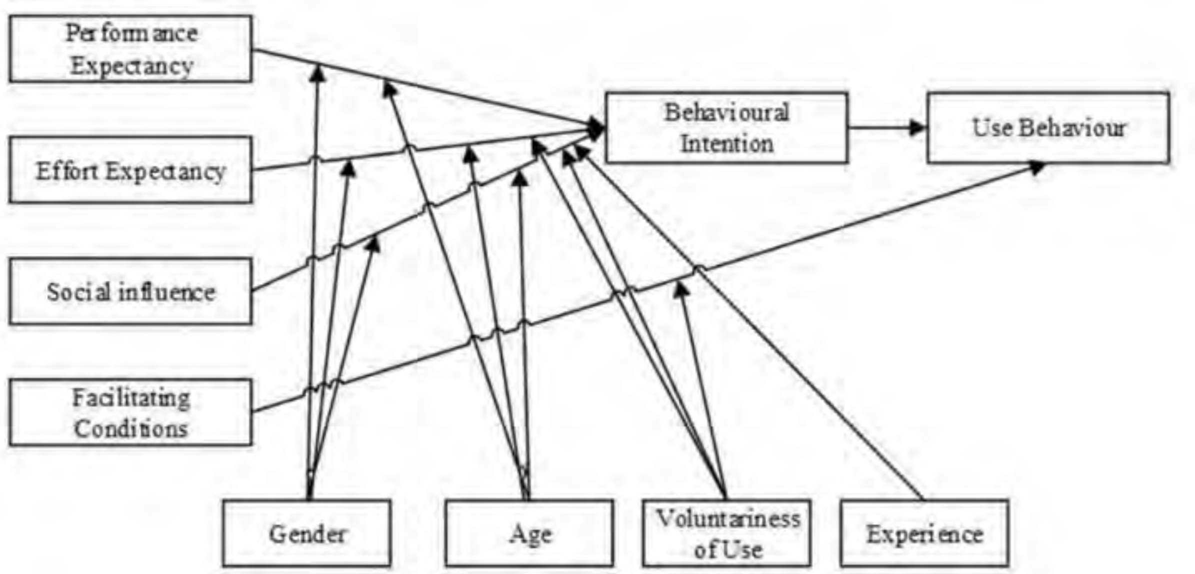


Figure 5.21: The Unified Theory of Acceptance and Use of Technology (UTAUT) by Venkatesh et al., (2003) (Alwahaishi and Snasel, 2013, P.25-39)

5.6.5 Technology Acceptance Model (2006)

McFarland and Hamilton made changes to the TAM model (McFarland and Hamilton 2006). This model explains computer efficacy, perceived ease of use, perceived usefulness and system usage using other's use, system quality, organisational support, prior experience, anxiety, and task structure.

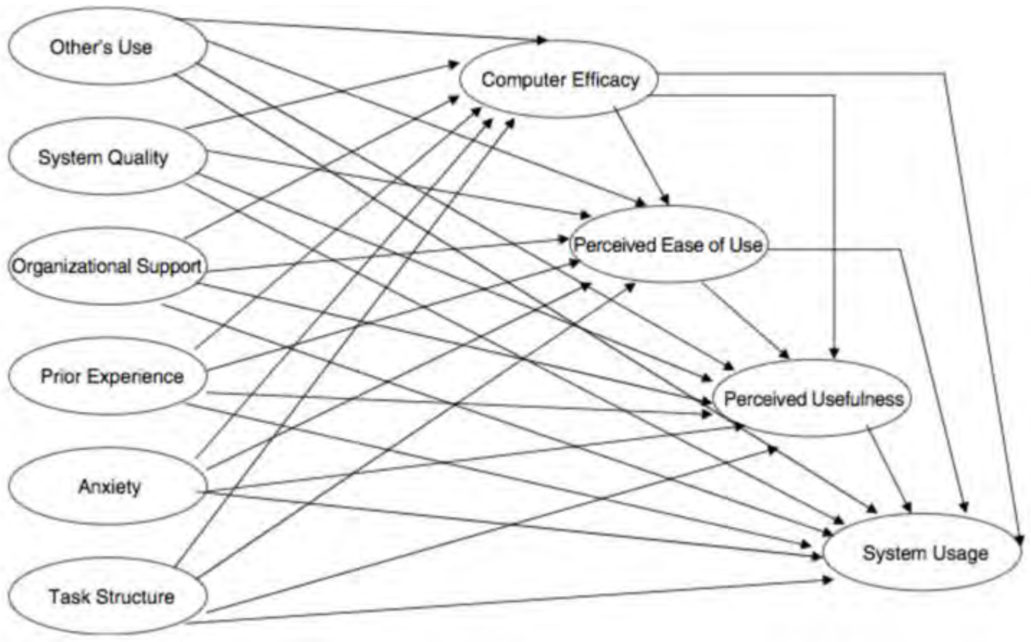


Figure 5.22: Technology Acceptance Model by Mc Farland and Hamilton (2006) (McFarland and Hamilton, 2006, P.433)

5.6.6 Technology Acceptance Model 3 (2008)

Venkatesh and Bala combined TAM2 and the model of the determinants of perceived ease of use and developed an integrated model of technology acceptance known as TAM3.

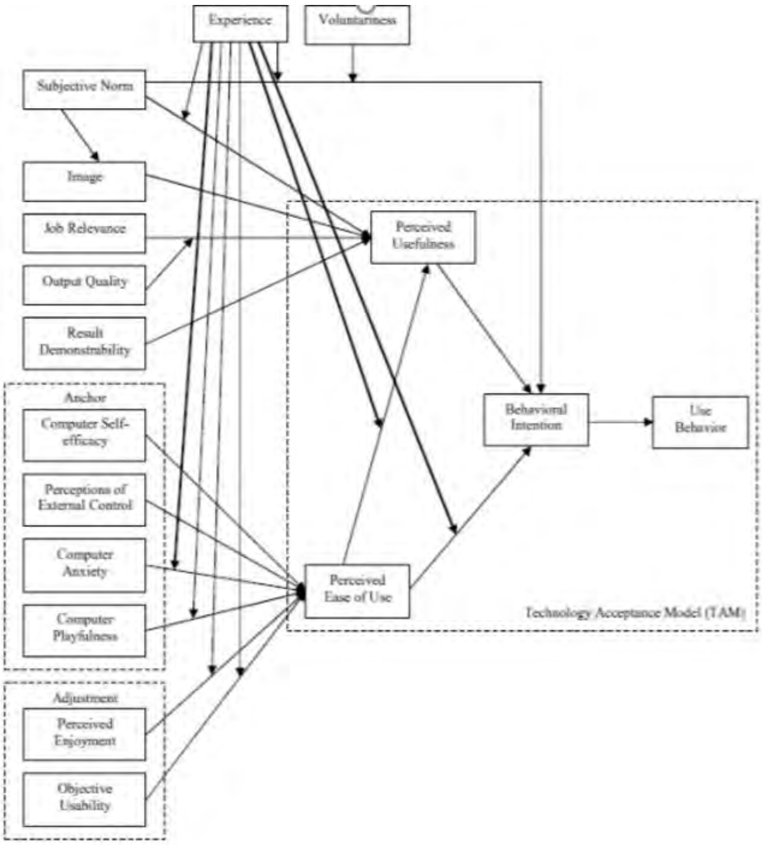


Figure 5.23: Technology Acceptance Model 3 by Venkatesh and Bala. (Venkatesh and Bala, 2008, P.280)

Available publications show that TAM has been applied to different sectors. One refers to the investigation of the adoption by the banks, and acceptance by the bank customers of internet banking in the sultanate of Oman, which is authored by Bassam Khalil Hamdan Tabsh under the supervision of Dr Jason Williams (Tabsh, 2012). Also, there had been others, Alice M. Johnson had used the TAM as a basis for studying factors that might motivate organizations to invest (or not to invest) in information security (Johnson, 2005), Sek et al had used TAM in the prediction of User Acceptance and Adoption of Smart Phone for Learning (Sek et al., 2010), and Rauniar et al had used TAM in their paper titled social media usage: an empirical study on Facebook (Rauniar et al., 2013).

Furthermore, Zhou et al. developed a new model based on TAM called Online Shopping Acceptance Model (OSAM) to assess the behaviour in online shopping (Zhou, Dai and Zhang, 2007). Ervasti and Helaakoski have developed a model based on TAM and TPB to get an understanding of the adaptation of mobile services (Ervasti and Helaakoski, 2008), Muller-Seitz et al. (2009) used the Technology Acceptance Model to assess the acceptance of Radio Frequency Identification (RFID) (Muller-Seitz et al. 2009).

Building on the original version of TAM, the researchers have made attempts to modify the TAM by adding new variables to it. Moon and Kim (2001) has added a new variable called playfulness to study the acceptance of the world wide web (Tan, and Chung, N.D); Van der Heijden (2000) added two new variables perceived entertainment value and perceived presentation attractiveness to TAM, after analysing the individual acceptance and usage of the website (Surendran, 2012); also, Chau and Hu (2002) had combined peer Influence with Technology Acceptance Model (Surendran, 2012).

5.7 Policy Acceptance Model

Pierce, at el. wrote a paper on the topic, Extending The Technology Acceptance Model: Policy Acceptance Model (PAM), introducing the PAM (See figure 5.24), and it is designed for the analysis and evaluation purposes of people’s attitudes toward the upcoming health care reform based on the responses received from the 72 participants (Pierce, at el. 2014, P.129). PAM was developed by adding two variables (age and ethnicity) to the TAM model developed by Davis in 1989. This model suggests that age and ethnicity have an effect on perceived usefulness and the perceived ease of use of health care reform. Prior to developing the model, a quantitative survey was designed and distributed to a diverse population in the United States, and the survey results were used to investigate and identify the trends amongst people of various ages and ethnic groups (Pierce, at el. 2014, P.133-134).

Pierce, at el. have used perceived ease of use and perceived usefulness in PAM, believing that both were significant factors in predicting acceptance. Also, they had considered attitudes and emphasised that a positive attitude would increase the willingness to accept of the policy. Pierce, at el. Also believe that the theory behind this model could be used as a framework that would be applicable to studies looking into introducing or modifying the policies (Pierce, at el. 2014, P.133). However, the researcher believes that if this model is to be applied to developing new policies, there are many other external factors that should be considered. That emphasises the need for future research on additional variables that would bring about uniformity in policy acceptance and implementation.

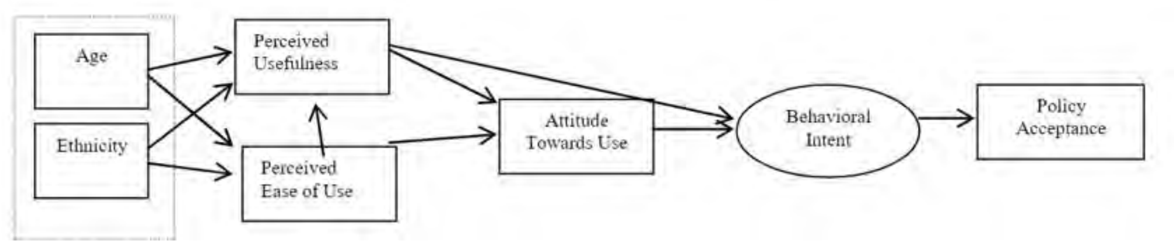


Figure 5.24: Research Model Policy Acceptance Model (Pierce at el., 2014, P.135)

In this research, in developing the policy acceptance model, the researcher referred to existing Technology Acceptance Models (TAM), which includes TAM by Fred D. Davies (1989) (Surendran, 2012) (See figure 5.18), the final version of TAM (Venkatesh and Davis, 1996) (See figure 5.19), TAM 2 (Venkatesh and Davis (2000) (See figure 5.20), the Unified Theory of Acceptance and Use of Technology (UTAUT) (2003) (Alwahaishi and Snasel, 2013, P.25-39) (See figure 5.21), TAM (Mc Farland and Hamilton, 2006) (See figure 5.22) and TAM 3 (Venkatesh and Bala, 2008) (See figure 5.23). In this research, the researcher will extract the key concepts such as Organisational support, Perceived usefulness, Perceived ease of use, Political differences, Social differences, Economic differences, Attitudes, Prior experiences in developing a Policy Acceptance Model (See table 5.8).

Table 5.8: Review Table

	TAM (Davis, 1989)	Final version of TAM (Venkatesh and Davis, 1996)	TAM-2 (Venkatesh and Davis, 2000)	The unified theory of Acceptance and Use of Technology (Venkatesh et al., 2003)	TAM (McFarland and Hamilton 2006)	TAM3 (Venkatesh and Bala, 2008).	The researcher, 2020
Dependency on ICT							✓
Security awareness							✓
Organisational support					✓		
Information security budget							✓
Social differences	✓	✓					
Economic differences	✓	✓					
Political differences	✓	✓					

Prior experience			✓		✓	✓	
Trust							✓
Privacy							✓
National Security							✓
Perceived ease of use	✓	✓	✓		✓	✓	
Perceived usefulness	✓	✓	✓		✓	✓	
Organisational support					✓		
Attitude	✓						

Prior to the analysis of the survey outputs, the researcher developed a Policy Acceptance Model (See figure 5.25) by drawing on the literature review, and it consists of two stages, the pre-adaptation and the adaptation stage. In the pre-adaptation stage, the focus will be on external factors likely to affect the decision-making process. The adaptation stage will focus on real need assessment to develop a data privacy and security policy. In the pre-adaption stage, factors such as attitude, dependency on ICT, perceived risks of not having global data security, information security budget, security awareness, organisational support, social and economic differences, cyber maturity, political differences, and language come for consideration based on the literature reading.

In the adaption stage, privacy, national security, perceived usefulness of global data security policies, perceived ease of use of global data security policies, intention to ratify and implement and use of global data security policies were key factors identified for consideration. The trust between countries is another important factor considered in the adaption stage. If there are issues relating to trust, cyber diplomacy will be a good tool to bring all the parties together and enhance trust between them. However, cyber diplomacy on its own will not be enough to build trust; also, such as historical, political, and social factors will have a significant role to play in enhancing trust between countries. Having previous experience in policy development is also an influential contributory factor in building trust between the nations. Working together means building mutual trust and respect, and it would help develop consensus amongst the nations without disruptive conflicts. The intent to ratify global data security policies and, to implement and use global data security policies are included in the first model under the decision to adapt. However, in developing the second model, the researcher considered the intent to develop policies and, the implementation and use of the policies under the adaptation of global-level data protection mechanism.

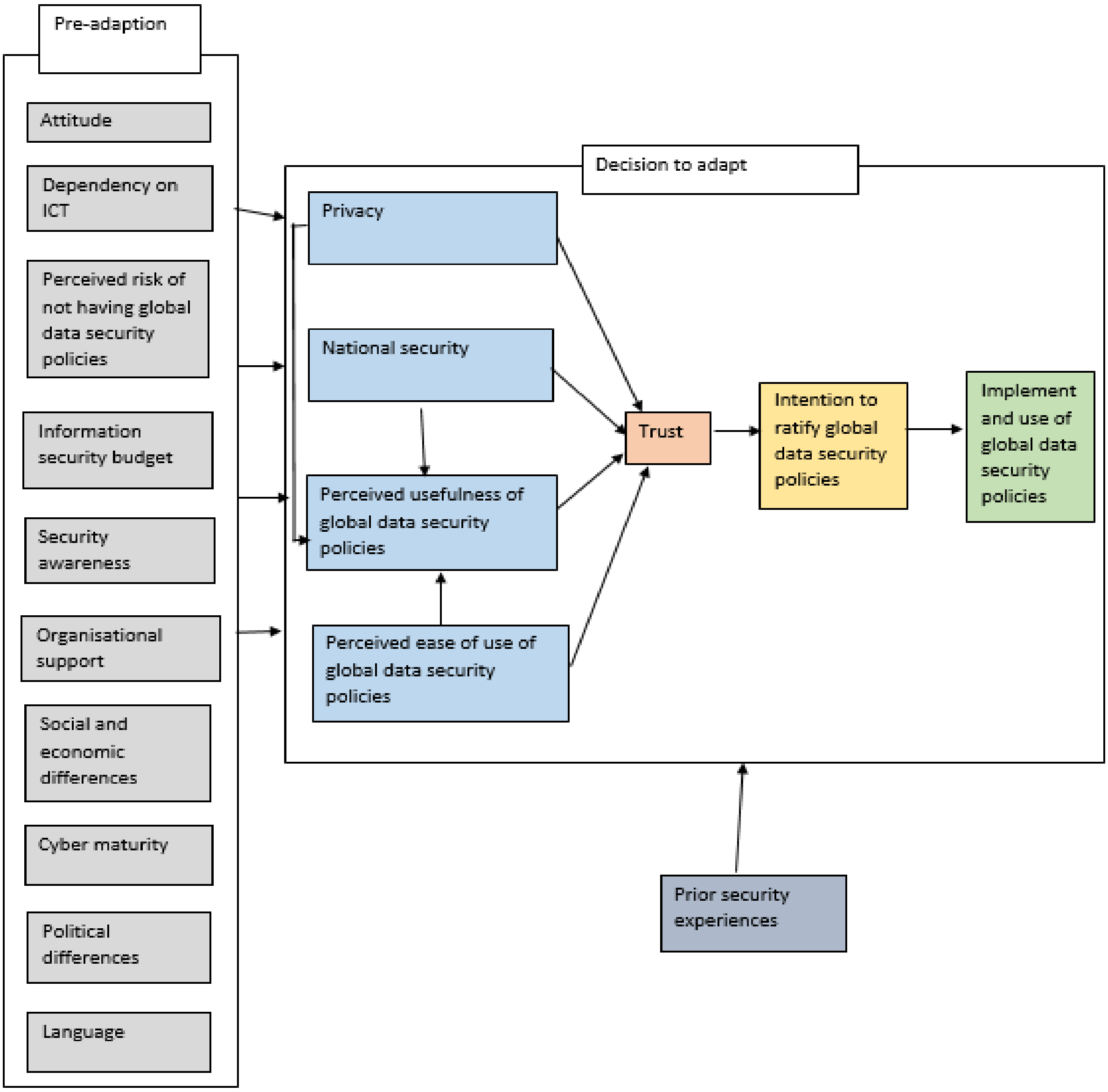

Pre-adaption
Attitude
Dependency on ICT
Perceived risk of not having global data security policies
Information security budget
Security awareness
Organisational support
Social and economic differences
Cyber maturity
Political differences
Language
Decision to adapt
Privacy
National security
Perceived usefulness of global data security policies
Perceived ease of use of global data security policies
Trust
Intention to ratify global data security policies
Implement and use of global data security policies
Prior security experiences

Figure 5.25: Policy Acceptance Model developed based on the literature review (The researcher, 2021)

The survey questions were developed reflecting the factors identified by extracting materials from the literature review. The questionnaire and the justification for the choice of questions are annotated in annexes A and B. After having analysed the questionnaire, the researcher produced the second model (see figure 5.26). The statistical data analysis from the survey give sufficient information of participant's perceptions of the key factors in the survey questionnaire and enables the researcher to make reasonable assumptions on which to develop the model.

The ease of use and perceived usefulness are the most important determining factors in the use of the system. The perceived usefulness is defined as the probability of using a model to enhance and protect personal privacy, and the perceived ease of use can be defined as the degree to which the user expects the model to be less complicated. In the light of the advancement of technologies and the rising number of threats, the speed of accepting and implementing a global level data protection mechanism by the countries depends on a number of factors such as attitude, risk of not having a global data security, dependency on ICT, information security budget, security awareness, organisational support, Economic differences and cyber maturity.

In taking decisions to adapt a global privacy mechanism, trust, privacy, national security, perceived usefulness, perceived ease of use and prior information security experience become crucially important. When developing a global level data protection mechanism, trust is considered a major factor, and it ensures that the common interest is served free of a hidden agenda. If the countries believe that a legal mechanism has the potential to protect citizen's privacy and national security, there is a high tendency to accept and implement a global level data protection mechanism. Prior experience in negotiating information security policies does not directly influence the decision-making process to accept and implant a global level data protection mechanism. However, it can be considered as a supplementary factor which would help countries in negotiating and developing effective policies that would serve the purpose.

Overall, the dependency on technology is high amongst the participants from Sri Lanka, UK, and others. Even though there is a lack of training and organisational support, there is a high understanding of the impact of cyber-attacks on the public and organisations. Given the awareness of the extent of the threats amongst the participants, the majority of them recognise the importance of having a global level data protection mechanism. Furthermore, the majority of the participants also recognise the importance of organisational support, budget allocation, and economic differences. However, the majority has skipped social and political differences, therefore it was removed from figure 5.26. In response to the question on social differences, the majority from all the countries recognised the importance of attitudes and beliefs, and education. In researcher's view, without an adequate level of education, undertaking training would have been difficult.

Based on these observations, the researcher redesigned the factors considered for the pre-adaption section, in figure 5.26. The next step in the decision-making stage for adaption of a policy model, the majority of the participants from all the countries find all the factors set out in figure 5.25 satisfactory, hence no changes made in figure 5.26.

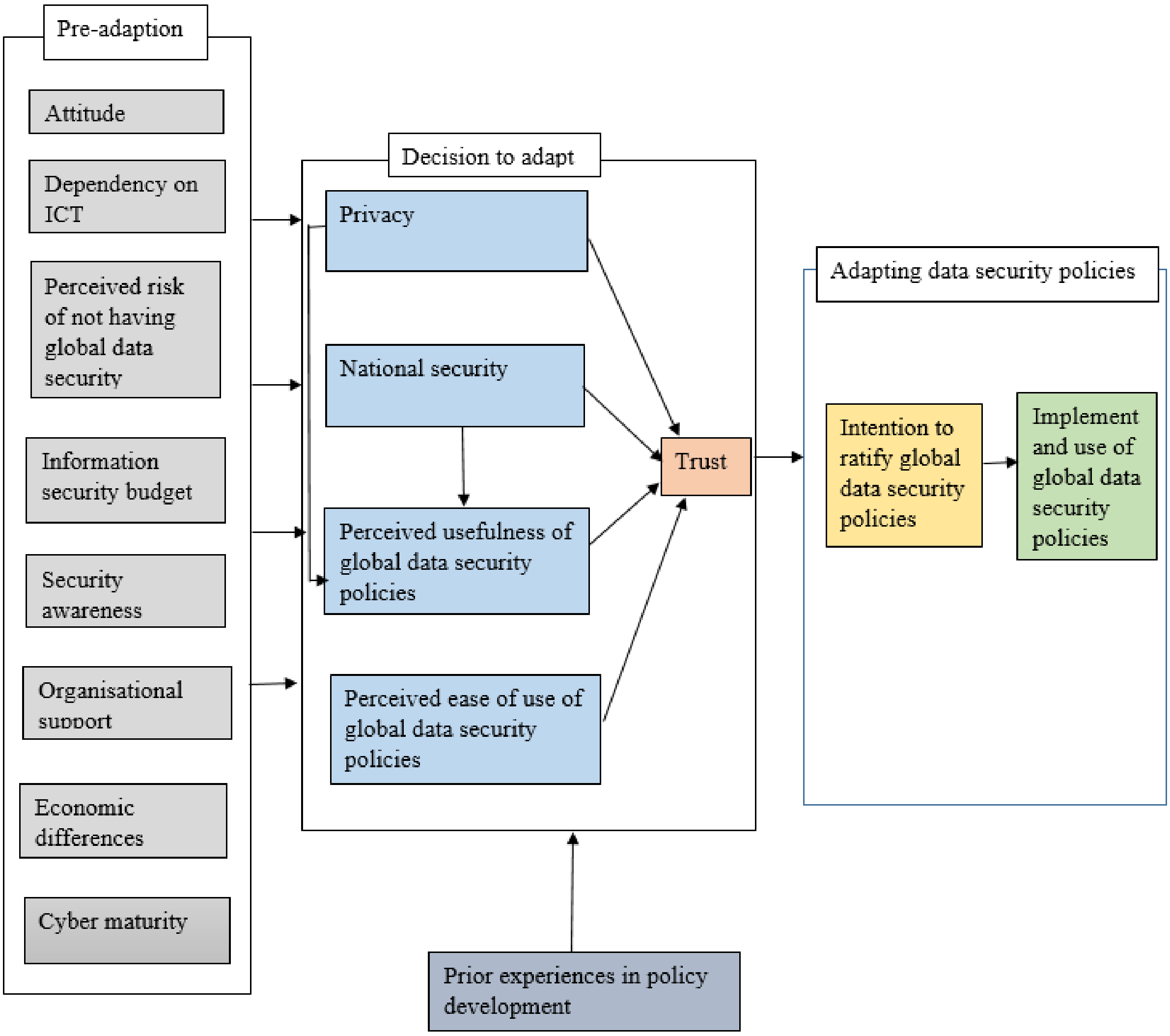

Pre-adaption
Attitude
Dependency on ICT
Perceived risk of not having global data security
Information security budget
Security awareness
Organisational support
Economic differences
Cyber maturity
Decision to adapt
Privacy
National security
Perceived usefulness of global data security policies
Perceived ease of use of global data security policies
Trust
Adapting data security policies
Intention to ratify global data security policies
Implement and use of global data security policies
Prior experiences in policy development

Figure 5.26: Policy Acceptance Model based on the literature and survey responses (The researcher, 2021)

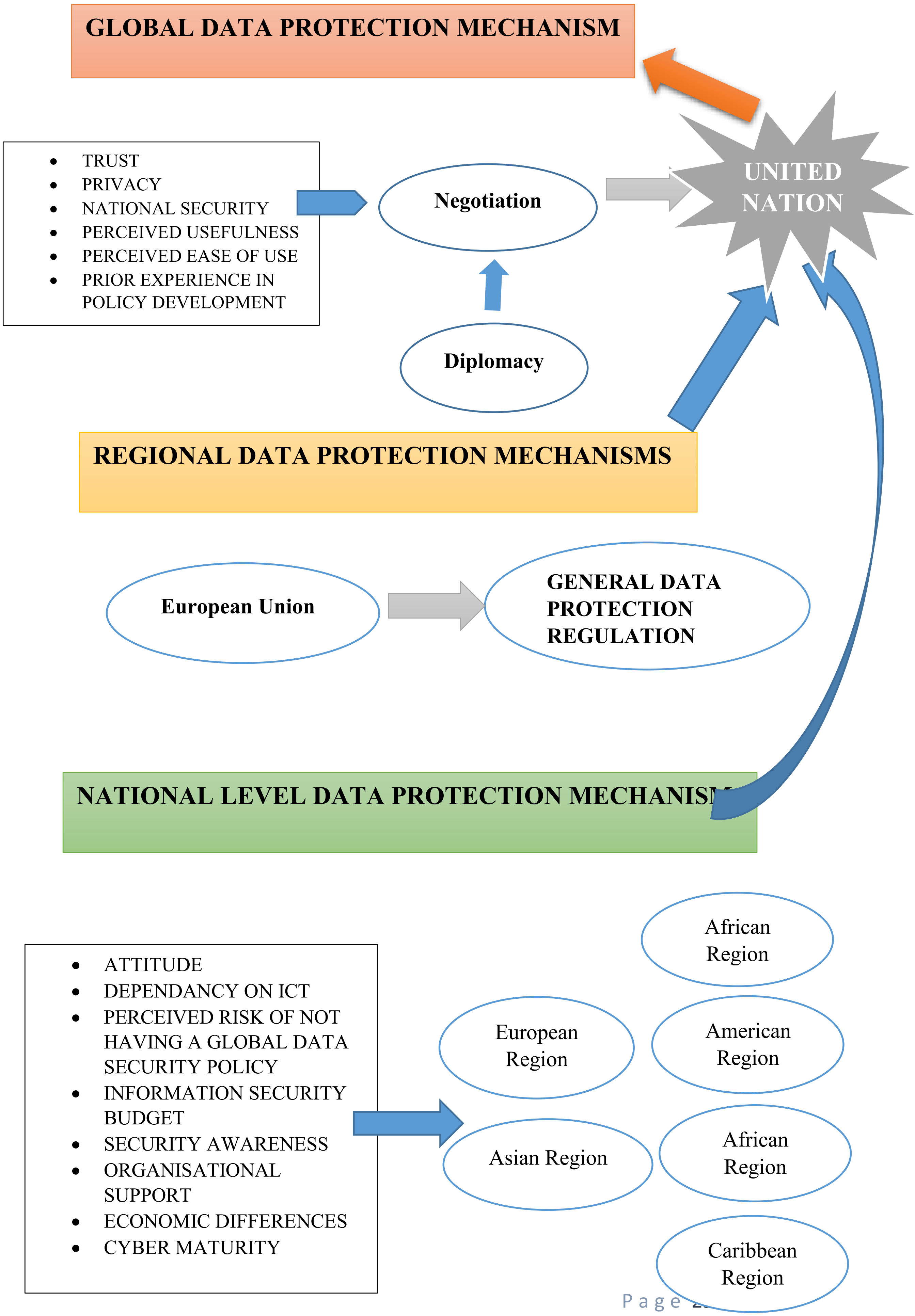
In the pre-adaptation stage, each country (the countries) would have begun to develop a data protection mechanism that meets their national needs, focusing on the factors outlined in the pre-adaptation phase. To move forward, each country would undertake a self-assessment of the resources available and extra support required, if any, for the acceptance and implementation phase. There will be challenges that some countries would face, and they would need support to overcome them and request further assistance from other countries under the auspicious of the UN, which should play a coordinating role with countries who have 'know-how' in policy development techniques and procedures.

The next is the decision-making phase, whether to adapt policies based on the parameters outlined in the model developed by the researcher. The 'decision to adapt' should be driven by meeting the key criteria set out in the model. This process undoubtedly will be long drawn, time consuming and cumbersome. It follows a sequential roadmap until an agreed version is presented for approval and and ratification.

The pre-drafting of the final version consists of participatory discussions, consultations, considerations, perusals, consensus, and collective appraisal before the first draft will become available for review. The purpose of doing so is to ensure fullest participation, transparency, accountability, clarity, viability, consistency, appropriateness, credibility, validity, and most of all not seen to be controversial in any way. The extent of preparatory work could be cumbersome and not without obstacles, and these are the challenges the countries would face until finally approved.

Once the policy is signed, it goes through ratification to become a legally binding mechanism. The final stage is the adaptation.The policies developed on international platforms need further ratification by individual countries before it becomes law. It is the responsibility of the countries to apply the law to individuals and organisations. Therefore, the agreed version is presented for approval by the appropriate authorities in each country, whether it is the government/parliament (in a democratic political system) or the constitutional body (a constitution governed republic).

This proposed Policy Acceptance Model will be an influencing tool for decision making and developing data protection mechanisms that could be adapted by the states in developing national and regional data protection mechanisms. This cooperation and convergence in the policy development process will help embed trust between the nations at the global level, identify the disparities between countries, and reach consensus in developing a global data protection mechanism. In this study, the researcher's focus is not on the last stage which is intended to cover the adaptation of data security policies. Therefore, the model developed by the researcher will allow the future academic/scholars to take up further research work that would complement what has been done and presented by the researcher in this dissertation.



GLOBAL DATA PROTECTION MECHANISM

- TRUST
- PRIVACY
- NATIONAL SECURITY
- PERCEIVED USEFULNESS
- PERCEIVED EASE OF USE
- PRIOR EXPERIENCE IN POLICY DEVELOPMENT

Negotiation

Diplomacy

UNITED NATION

REGIONAL DATA PROTECTION MECHANISMS

European Union

GENERAL DATA PROTECTION REGULATION

NATIONAL LEVEL DATA PROTECTION MECHANISM

- ATTITUDE
- DEPENDANCY ON ICT
- PERCEIVED RISK OF NOT HAVING A GLOBAL DATA SECURITY POLICY
- INFORMATION SECURITY BUDGET
- SECURITY AWARENESS
- ORGANISATIONAL SUPPORT
- ECONOMIC DIFFERENCES
- CYBER MATURITY

African Region

European Region

American Region

Asian Region

African Region

Caribbean Region

Figure 5.27: Summary diagram

In this chapter, the researcher analysed the collected responses and developed a Policy Acceptance Model based on the Technology Acceptance Models. In the pre-adaptation stage, the respondents had highlighted the importance of attitude, dependency on ICT, perceived risks in the absence of a global data protection mechanism, information security budget, security awareness, organisational support, economic differences, and cyber maturity. In deciding to adapt, the respondents had paid particular attention to privacy, national security, the usefulness of data privacy and security policies, perceived ease of use, trust and prior experience, mutual trust between countries and previous experience with other countries in developing policies. This model is not written in stone; the flexibility allows the addition of new parameters to the model, in line with anticipated advancements in technology. However, the researcher remains optimistic that the current model would serve as an enabling framework to make progress towards accepting and implementing a global level data protection mechanism, which would help achieve the desired outcome to protect the privacy of citizens and the security of the nation.

CHAPTER SIX

CONCLUSION

The world is faced with unprecedented challenges from cybercriminals, the reality of increasing cyber related threats became a major concern for the intelligence and security services and, in the wake of cyberthreats spreading beyond borders, the need to find solutions became a high priority. The cyberspace related threats are stealth in nature, and the enemy is characteristically invisible, difficult to trace, and dangerous, and that made taking urgent action to protect people and the nations a necessity. Against that background, security experts started searching for ways to counteract the threats arising from vulnerabilities associated with cyberspace and effective measures to protect the security of the citizens and that of the nation.

It appears paradoxically coincidental that this research study to formulate a privacy protection policy framework began in an environment of an unprecedented pandemic and increased demand for digital surveillance. The deployment of sophisticated digital systems for gathering and processing personal data by the government and the permissible organisations during pandemic raised privacy concerns. In the light of the increased reliance on technologies, and the higher risk factors to the privacy of the individuals, inevitably brought to the forefront the need to find solutions to the challenges faced by the organisations and the security services. Against that background, the need to develop a global level policy framework to fill the gaps in the existing legislation became an urgent necessity.

The invention of the internet was the foundation of modern communication systems, and the advancements in technology-enabled the nations to become closer together in the digital world. The pace of technology evolutionary phase stepped up to an unimaginable magnitude the world has seen in decades, and that has provided immense opportunities. Over time, the digital systems have become commonly used consumer items whether at home or in the workplace and they have become integrated into user lifestyles. Amongst the array of available digital systems, telecommunication, Big Data, the Internet of Things, machine learning, artificial intelligence, robotics, satellite, and drone technologies, were meant to serve specific purposes in different circumstances, with immense benefits to the world. Most used by the public at large are telecommunication and the Internet of Things through which they interact with people, government, and organisations. However, the extensive use of the internet and the e-communication systems has exposed the users to the greatest risks at the hands of the perpetrators who have the know-how and capacity to get unauthorised access to personal accounts and information, and consequently the user becoming the victims of cybercrime (See annexes C.5 and C.8). They are the challenges and concerning issues that need addressing and finding solutions to protect the individuals and the state from becoming victims to cyber criminals.

6.1 Introduction and deployment of IoTs and technologies

The anticipation is that the IoTs with a direct connection to the network, bypassing any physical involvement of the user, will lead to expansion of the connected devices and a substantial increase in the volume of data generated by the humans to around 2.3 zettabytes per day (See figure 1.3). The data so collected is categorised as Big Data, and the privacy experts believe that the generation of large volume of data contributes to exacerbating the risks factors and challenges associated with innovative technologies. The speedy transmission of data (Big Data) in this way comes under scrutiny requiring accuracy in handling, processing, and transparency in the usage, and the onus is on the organisations to obtain prior consent from the data subject. The failure to do so will create public concerns about the misuse of personal information, mistrust in the system itself, and tarnish the reputation of the data gathering entities, and end up having complex unpleasant disputes between the organisation and their clients. The responsibility for data security and data breaches at any point in the process and accountability for the consequences of noncompliance with regulations governing data protection rest with the collecting institutions.

The IoT devices may remain constantly connected to the 5G networks when transferring large volumes of data over the internet and will create challenges to the protection of the privacy of the user. For instance, the UK and US became suspicious about the proposed installation of key elements of the Huawei 5G network and raised concerns about the risks associated with its capability to intercept the flow of traffic and clandestinely monitor information passing through. The outcome was the limiting and barring of installation of hardware to prevent risks to national security. However, the Chinese company, Huawei made strong representations to respective nations claiming that the accusations and propaganda mounted against their company and products were without foundation and had no credibility. Such disputes do not create a conducive environment to engage in negotiations to reach consensus on developing global policies; therefore, to make progress, it is important to set aside refutable allegations and contentious issues that are likely to hinder progress and follow a collaborative approach devoid of misgivings and prejudices to achieve the common objective.

Modern technologies opened exciting opportunities beneficial to the individual, but the relationship between innovative modern technology and personal data should come under close examination for potential privacy and security risks. The suggestion is to incorporate concepts such as Privacy-by-Design, encryption, anonymization and pseudonymization into the law to mitigate emerging risks. Also, the organisations should participate in the risk evaluation process and when seeking to identify the origins of the risks, and to make a balance judgement. This process encapsulates the need to develop a framework for data protection mechanism for acceptance and implementation at global level, beneficial for all with a special focus on the most vulnerable individuals.

When introducing and deploying new devices or technologies, the primary focus should be on transparency and prior consent, but the collection, processing and retention should also be limited to a minimum. In addition, the focus should also be on risk assessments, security measures in force prior to deployment of devices, constant monitoring, and evaluating the equipment during the recommended usable lifespan. The risk assessment process should concentrate on the devices, networks, and the users who are the most vulnerable and affected by data breaches, and the process itself must be meaningful and effective with clearly defined criteria to avoid breaches at source. Also, the consumers should have an overview of the purpose of use, procedures, and the reasons if used for commercial purposes, with an opt-out clause allowing the consumer to accept or decline the terms for collecting, processing, and storing their personal information. The market research organisations and the advertising agencies if failed to disclose required information will tarnish their reputations with the loss of customer trust and faith in their products. The disclosure of customer preferences and location data for financial gains should come under restrictions, and likewise, the access to data by the government and law enforcement agencies unless in exceptional circumstances such as national security concerns.

6.2 Policy initiatives related to development and deployment of new devices and technologies

The IoT manufacturers continue to introduce a variety of devices to meet the increasing demand, and the consumers, including state institutions and organisations have taken advantage to deploy an array of high-technology devices for various purposes. The wide-scale deployment of IoTs have become popular as observed during the prevailing COVID-19 pandemic. The popularity of IoTs and their use in a wide also increase the risk implications, therefore undertaking a risk assessment prior to deployment of any IoT device is crucial to prevent privacy and security breaches, although some take preventive measures to avoid them.

In the current context of COVID-19, it is incumbent on respective governments to have in place a document setting out IoT security guidelines and a proper testing procedure/mechanism before permitting free-for-all deployment of any device. Put into perspective, for instance, the use of drones and CCTV cameras and threats from unauthorised persons (scammers) have drawn the attention of the governments. The most conspicuous amongst the challenges are device malfunction/failure, loss of user control, left unattended with power on or even on standby mode. Also, there are growing concerns about the prolonged use of new technologies to track and trace people movements and monitor their behaviour, as well as the continued use of surveillance measures beyond the pandemic period without conditional limitations. It is the responsibility of the governments and policy-making bodies to stress the need to give precedence to privacy and security considerations at the initial stage of innovation and deployment of technologies and promote similar norms at the national and global level.

Also, Data Protection Authorities should conduct assessments on the functionality of connected devices and their data processing activities. The industrial institutions, researchers and professional academics should extend their support to the government/s to adopt robust security standards for devices constantly connected to the peripherals and continuously in use uninterrupted. Personal Privacy legislations should remain periodically under review, at least annually, and the policies should updated regularly to reflect the additions of new technologies into the market. It is important that the authorities responsible for consumer affairs pay attention to the functionality of the connected devices, remain vigilant, and flag up any potential harm to the consumers. This step-by-step approach to safeguarding personal privacy has its advantages and merits consideration for incorporating into the policy framework.

6.3 The key findings of the study

As individuals, we all face challenges and take risks when we use IoTs and modern technologies indoors and outdoors, and we rely on Wi-Fi, Bluetooth technology, and the internet. In doing so, we use high technology integrated smart devices, such as smart televisions, laptops, mobile phones, satellite television systems, technology-aided driving, and many more. These human habits are here to stay, even becoming intense as technology-dependent lifestyles drive the world forward. The higher the extent of the use of smart things, the higher the risks but the reality of the challenges and the risks have not sunk in deep enough, not enough to avoid data privacy breaches.

The threats posed by the cybercriminals and the unethical use of personal data are the critical challenges of modern times, and given these are global issues, an in-depth assessment of all aspects of privacy issues seems the appropriate way forward to find global solutions, starting at national, regional, and finally global level. The researcher believes that it is important to have unified purposeful data protection mechanisms produced collectively by the nations to overcome security and privacy challenges and prevent data breach perpetrators escape with impunity (See figure 5.27).

The intensive literature review helped the researcher to determine the key findings and understand the strengths, weaknesses, and limitations in existing privacy policies and lapses in privacy regulations in developing and developed countries. The key observation was that many nations had at least a draft data protection mechanism in place at the national level. Chapter two (See table 2.1-2.14) contains a list of the relevant countries. There are also a few nations in each region without any type of data protection mechanism at the national level, and the common challenges they face, the researcher discussed in chapter 2 (See figure 2.4). That leaves other regions, including those in South Asia, without a visible approach to developing a meaningful data protection mechanism at the regional level. The General Data Protection Regulation (GDPR) developed by the EU at the regional level remains the only credible, meaningful regulatory framework available as a resource. However, the increasing volume of data generated has prompted a debate on the need to revisit the GDPR. The researcher believes that there is a need to develop a 'Big Data' friendly data protection mechanism and, the researcher presented the case for doing that in a publication as indexed in annexe C.9.

It is fair to say that the lack of data protection mechanisms at the national level is hindering progress towards developing regional data protection mechanisms, and in turn will obviously hold up progress towards developing a global level data protection mechanism. Currently most nations have individually developed data protection mechanisms matching GDPR, and that sets a benchmark for the other nations. Therefore, it is crucially important that the developed nations support the ones that are struggling, at least to produce a draft data protection mechanism. Also, the existence of meaningful data protection mechanisms at the national level will create a conducive environment for facilitating constructive dialogue between the nations to produce a unified regional mechanism.

The absence of a universal data protection mechanism at the global level indicates a clear gap, to address that weakness and find a way forward, the appropriate and effective route to take is collaboration through diplomacy under the auspicious of the UN. That would provide an open forum for the participating nations to reach consensus through meaningful dialogue with the aim of ensuring rigidity in the application of a data protection mechanism at the global level. There are ambiguities in the existing data protection mechanisms and flaws in the application of the law. Also, differences in opinion, misgivings, mistrust, and lack of faith between the nations give rise to undue disputes; therefore, there is a need to take a resolute approach to resolve them and to give added impetus to developing a consensus-based data protection mechanism.

The key findings of the survey undertaken by the researcher underscore the prominence of key issues of concern. They may not be common at the national or regional level and may be variable on the capacity, and social and political background of each nation in the first instance. The key factors identified reflect personal perceptions taken as a representative sample of a cross-section of the population. The prominent factors are demography, the makeup of the community, economic status, level of education, employment status, influential capacity, awareness of the issues, the working environment, the attitudes of the citizens, political establishment, considered relevant and important in the policy development process. The analysis of these factors underlines the benefits of having a conceptually sound policy model that guides the policymakers who can use it as an aid to produce a privacy protection strategy at the national and regional level as the first step, leading to the establishment of a global level as the last stage. The researcher delineated a set of research questions meant to achieve the research aim.

6.4 The research questions and its contribution to the research aims

The (researcher's) first research question was whether each nation had committed to protect personal privacy. The literature review suggests that amongst the countries, there is a good understanding of the importance of protecting personal privacy, and most of them are in the process of revisiting their current data protection mechanisms. It is also the case that many of them used GDPR as a model to upgrade and bring their data protection mechanisms to the current standard (See sections 2.7 and 2.9).

The second research question was whether the national data privacy and security policies in South Asian and European regions are robust enough to protect the personal privacy of the citizens. The European region countries have a standardised, robust data protection mechanism at the national level, as well as adequate data protection mechanisms at the regional level (See section 2.7.6). However, the South Asian region countries seem to have made little progress in developing data protection mechanisms at the national level. Some countries have draft data protection mechanisms, and some have none in any meaningful way (See section 2.9) However, the existing draft mechanisms show that these countries have taken GDPR into account when developing/revisiting their current data protection mechanisms, and they provide a level of data protection similar that in the European region.

The researcher then embarked on exploring the extent to which the South Asian data privacy and security policies meet the adequacy of the GDPR. The available literature clearly suggests that the current data protection mechanisms in the South Asian region meet the adequacy of the GDPR (See section 2.9). In parallel to the requirements set out in the GDPR, the data protection mechanisms in the South Asian region do flag up broadly individual rights, data subject consent compulsory for processing information, data sharing limited to the countries having an adequate level of data protection mechanisms and mandatory data breach notifications. However, although the countries are bound by the requirement to send a notification following a data breach, the time duration varies from one country to another. In an incident of failure to protect personal data, the value of the fine and the punishment also varies from one country to another. In addition, although the GDPR stipulates the requirement for appointing a Data Protection Officer, not all countries have considered it as a requirement. However, despite minor regulatory differences between GDPR and GDPR inspired legal mechanisms in the South Asian region, the existing data protection mechanisms seem sufficient to protect data subject's personal privacy.

The researcher narrowed down the area further to develop the research question with the aim to ascertain what the data privacy and security policies in Sri Lanka and the UK were and the challenges faced in accepting and implementing policies by countries. Sri Lanka, despite being a developing country, has a draft data protection mechanism pending approval from the parliament (See section 2.10.1). The United Kingdom, on the other hand, is a developed country, and it developed its own version of the Data Protection Act 2018, but following the BREXIT transition process, the modified version of the EU GDPR became integrated into the UK legal system named, 'UK GDPR' with effect from January 2021 (See section 2.10.2).

The researcher, having gone through a thorough literature search on the development of data protection mechanisms, sought to identify the challenges faced by the countries in developing data protection mechanisms. The identified factors are listed in chapter 2 (See section 2.12). The researcher then used the identified factors to develop the research questionnaire (See annexe A), which aimed to ascertain the accuracy and timeliness of the barriers referred to in the literature and seek the public opinion of the importance of developing a global level data protection mechanism and the factors for consideration in developing one.

The researcher also pondered on whether there was a need to revisit the current data protection mechanisms to address the privacy risks associated with evolving technologies and Big Data. The researcher strongly believes that there should be flexibility in the data protection mechanism to allow adjustments deemed necessary in respect of emerging technologies, also a requirement to review current policies at least once a year to keep up with the challenging demands of advanced technology. It is important to frequently update and maintain legal mechanisms to avoid policy implementation failures due to outdated mechanisms (See annexe C.9).

Taking account of the effects of the COVID-19 pandemic, the researcher sought to determine the extent to which the available data security policies addressed privacy and security challenges associated with surveillance measures deployed during the prevailing state of the pandemic. Since the onset of digitalisation, the development of modern devices and technologies gathered pace, and their deployment proved to be effective in maintaining the living standards of the people. However, whilst digitalisation became the thing of the future, the onset of the COVID-19 pandemic and the increased use of technologies brought privacy and data protection to the forefront of public concerns. The modern high-tech devices and advanced technologies generated large volumes of data during the collection process, and the collected data was processed and stored by the organisations for commercial use and research purposes. There are potential immediate, medium, and long-term privacy issues associated with generating Big Data and the deployment of new technologies. The researcher discussed the current mechanisms in use, such as data minimisation, data anonymization, data masking, purpose limitation, and privacy by design to protect collected data and emphasised the importance of taking uniform and collective decisions to develop a global level data protection framework to protect the privacy of people in post-COVID-19. The researcher discussed these issues in detail in annexe C.12.

Different countries used technology in alternative ways to track and trace (identify) positive cases and to mitigate the risks of transmission of the pandemic. Annexe C.10 and C.11 contain an in-depth discussion on the use of modern technologies. The generation of large volumes of data has given rise to new security and privacy challenges; hence, the demand for immediate and long-term solutions has grown. The researcher analysed the issues and outlined the suggested solutions in annexe C.12.

This research study aimed to identify the barriers the countries faced with developing privacy policies and, to develop an appropriate Policy Acceptance Framework. The delineated research questions and the responses received helped the researcher identify the prevailing status in the development of national level data protection mechanisms, the regional level cooperation, and the barriers faced by countries. Guided by the information gathered through the literature search, the researcher compiled a questionnaire, and taking stock of the analysis of the responses, the researcher flagged up the import parameters to be considered in developing a global level data protection mechanism. The researcher used the results derived from the analysis to develop the Policy Acceptance Model (See section 5.6).

6.5 The main contribution of the study

The Policy Acceptance Model developed by the researcher (See figure 5.26) is a hybrid version based on Technology Acceptance Models developed by Fred D. Davies (1989), Venkatesh and Davis (1996), Venkatesh and Davis (2000), Venkatesh et al. (2003) McFarland and Hamilton (2006), and Venkatesh and Bala (2008). TAM models set out several factors that would influence the decision-making process, and the user to decide on how and when to use technology. In developing the policy acceptance model, the researcher drew on several aspects/areas of previous models and also took into consideration extra factors such as dependency on technology, security awareness, information security budget, trust, privacy, national security (See table 5.8). The factors influencing acceptance and implementation of a global level data protection policies are complex and not limited to a certain country or a region. Therefore, to make the model meaningful and appropriate in the current and evolving environment of modern technology, the researcher decided to integrate into the model other factors specified in the responses to the survey questionnaire.

In developing the model, in the preadaptation stage, the researcher took account of the factors such as attitude, dependency on ICT, Perceived risk of not having global data security policy, information security budget, security awareness, organisational support, economic differences, and cyber maturity. The factors considered in the Decision to adapt stage were privacy, national security, perceived usefulness, perceived ease of use, prior experience and trust. This model developed by the researcher is unique in nature because of the parameters used to highlight the risks, human perceptions, evolving IoT dependent lifestyles, so on.

Pierce, at el. extended the Technology Acceptance Model and introduced Policy Acceptance Model (PAM) (See figure 5.24) for the analysis and evaluation purposes of people's attitudes toward the upcoming health care reform. PAM was developed by adding two variables (age and ethnicity) to the TAM model developed by Davis in 1989 (See figure 5.18). Pierce, at el. claimed that the theory behind this model could be used as a framework that would be applicable to studies looking into introducing or modifying the policies. However, given the modern trends in the evolution of modern technology and user preferences in, the researcher believed that factors other than age and ethnicity should be considered when accepting and implementing a global level data protection mechanism. The survey responses received from the participants show agreement by highlighting the factors they believed to be important in developing a global level data protection mechanism, which conforms to the researcher's thoughts.

The Policy acceptance model developed by the researcher addresses a wide range of factors, in fact wider than those considered in the past, and it offers flexibility to incorporate emerging factors, amend, and delete any from the current model to meet different scenarios. Therefore, the researcher feels satisfied that the model, as it stands, is appropriate and consistent with the requirements for developing a data protection framework at the global level.

The procedure followed throughout the research is consistent with the aim to develop a Policy Acceptance Model for the acceptance and implementation of data protection mechanisms at the global level. Literature reading provided sufficient materialistic substance that enabled the researcher to get a clear view of the gaps in the enhancement of technology and misfit of current data protection mechanisms, and that met the objectives of research questions 1-3 (See section 1.4). The potential conflict between the need to deploy new technologies and the difficulties in law enforcement faced by the countries reduce their ability to provide adequate security and privacy to their citizens. Therefore, the identified challenges enabled to address the research questions 4-6 (See section 1.4). It suggests that there is a need to revisit current mechanisms, and the researcher remains convinced that the policy acceptance model developed by the researcher would be an enormously useful tool that will influence countries to revisit their current mechanisms and to update them, and this addressed the aim of this research.

The researcher is satisfied that the developed model will do exactly that and serve as an influencing tool encompassing appropriate benchmarks for developing a model for safeguarding privacy rights of the citizens and security of the nations, and the added benefit of inclusion of flexibility allows modifications and to the accommodation of any evolving modern technologies or devices.

6.6 Limitations or weaknesses of the study and recommendations for future research

The literature search pointed to contradicting information on data privacy and security policies, and it was a challenge that affected the progress of the literature review. An unknown number of countries are in the process of reviewing and modernising their legal mechanisms to protect personal privacy in the climate of evolving technologies. That, in a way, has inundated literature published in the previous years. It was a matter of selecting the most appropriate articles to ensure the quality of the research outputs.

The researcher could have conducted interviews with state officials, Ministers, lawyers, and activists directly/indirectly having an influence in the process of developing policies and keeping abreast of policy developments. However, the researcher found getting access to high profile personnel to get an interview hard, even impossible, but had the researcher been successful in getting an interview with personnel familiar with or involved with policy development, it would have been feasible to have obtained their views of the challenges they faced from their own perspective.

The researcher's focus for this research study limited to the South Asian region only. The researcher recommends that future research should focus on other Asian regions and do a comparative analysis of data protection mechanisms with a view to assessing similarities and dis-similarities between data protection mechanisms. A similar approach should apply to other regions as well, and at least like-minded states grouped together should endeavour to develop a regional level data protection mechanism.

The future researchers can also apply the Policy Acceptance Model developed by the researcher and evaluate the feasibility of applying the model to other regions in the world, and if deemed necessary, the researchers can add or disregard any variables associated with regional differences or technological differences.

The literature review led to major differences amongst the countries in terms of social, economic, and political grounds. Therefore, to apply one model to all the countries is difficult in practice, and this presents a limitation to the unanimity of developing a global level data protection mechanism. However, such obstacles could be removed through negotiations to soften any obtrusive impact and sustain the momentum.

In this research, the researcher has not concentrated on the ratification and implementation phases. Therefore, the identification of the challenges in the ratification and implementation of the policy, based on this framework, should be the focus for future research, or a researcher. In the light of evolving technologies, there is space available within the framework to add emerging parameters associated with situations of unforeseen circumstances like the COVID-19 pandemic, and the national/regional differences.

The researcher believes that the UN, by taking this framework as the model, should influence member nations to take the initiative to develop national and regional level data protection mechanisms and become a signatory to an institutionally binding unified force under the UN umbrella. The researcher believes that diplomacy would be the most appropriate route to bring all concerned together and move forward with developing a global level data protection mechanism a reality. Falling short of that aim, it is incumbent on future researchers to explore other avenues to consolidate the findings of this research study, but the researcher remains optimistic about achieving the goal, a worldwide data protection mechanism for the benefit of all the nations.

BIBLIOGRAPHY

Adonis A. A. (2020) *International Law on Cyber Security in the Age of Digital Sovereignty*. [Online]. Available at: https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/ (Accessed 12 April 2020)

Agrawal, R. (2020) *The Pandemic Is Enabling Big Brother- India's new contact tracing app leads to concerns over privacy, security, and surveillance* [Online]. Available at: https://foreignpolicy.com/2020/05/07/india-coronavirus-pandemic-big-brother-contact-tracing-mobile-app/ (Accessed: 20 May 2020)

Ainsworth, Q. (2021) *How many questions to include in an online survey* [Online]. Available at: https://www.jotform.com/blog/how-many-questions-should-a-survey-have/ (Accessed: 27 September 2021)

Ajayi, O. V. (2017) *Primary Sources of Data and Secondary Sources of Data* [Online], PhD thesis, Benue state university, Makurdi. Available at https://www.researchgate.net/publication/320010397_Primary_Sources_of_Data_and_Secondary_Sources_of_Data [Accessed: 15 May 2021]

Akpi, A. (2019) *Positivist Explanation and the emergence of Spatial Science* [Online]. Available at https://www.researchgate.net/publication/333853435_Positivist_Explanation_and_the_emergence_of_Spatial_Science [Accessed: 15 Feb 2021]

Albrecht, J. P. (2016) 'How the GDPR Will Change the World', *European Data Protection Law Review*, Volume (2-Issue 3), [Online]. Available at: DOI https://doi.org/10.21552/EDPL/2016/3/4 (Accessed: 13 February 2020)

Alkoofi, H. (2021) *Bahrain - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/bahrain-data-protection-overview (Accessed: 2 September 2021)

Altman, M. et al. (2018) 'Practical approaches to big data privacy over time', *International Data Privacy Law*, Volume (8, Issue 1) P.29–51 [Online]. Available at: https://doi.org/10.1093/idpl/ipx027 (Accessed: 15 February 2020)

Alwahaishi, S. and Snasel, V. (2013) 'Modeling the Determinants Affecting Consumers' Acceptance and Use of Information and Communications Technology', *International Journal of E-Adoption*, Volume 5(2) [Online]. Available at https://www.researchgate.net/publication/257921834_Modeling_the_Determinants_Affecting_Consumers%27_Acceptance_and_Use_of_Information_and_Communications_Technology (Accessed 15 June 2020)

Ameen, D. (2020) *Maldives - Data Protection Overview* [Online]. Available at https://www.dataguidance.com/notes/maldives-data-protection-overview (Accessed: 5 November 2020)

Amnesty International (2020) *Amnesty gives cautious welcome to UK government U-turn on contact tracing app* [Online]. Available at: https://www.amnesty.org.uk/press-releases/amnesty-gives-cautious-welcome-uk-government-u-turn-contact-tracing-app (Accessed: 3 July 2020)

Anderson-Fortson, C. E. (2016) 'Cyber Security and the Need for International Governance' The National Law Review, Volume XI, Number 238 [Online]. Available at https://www.natlawreview.com/article/cyber-security-and-need-international-governance (Accessed: 13 September 2019)

Antwi, S. K. and Hamza, K. (2015) 'Qualitative and Quantitative Research Paradigms in Business- Research: A Philosophical Reflection'*, European Journal of Business and Management,* Volume 7(3) [Online]. Available at: https://core.ac.uk/download/pdf/234626233.pdf [Accessed: 4 March 2020]

Arceo, A. D. and Alcocer, G A. (N.D) *Mexico: Data Protection Law and Regulations 2021* [Online]. Available at: https://iclg.com/practice-areas/data-protection-laws-and-regulations/mexico (Accessed: 23 November 2021)

Arena, P.(2009) 'Review of Andrew Kydd, Trust and Mistrust in International Relations' , *Journal of Conflict Studies*. Volume 29, Available at: https://www.erudit.org/en/journals/jcs/1900-v1-n1-jcs29/jcs29br06.pdf (Accessed: 13 July 2020)

Arora, S. K. (2021) *What is Data Analysis? Methods, Techniques & Tools* [Online]. Available at https://hackr.io/blog/what-is-data-analysis-methods-techniques-tools#:~:text=1.-,Qualitative%20Analysis,%2C%20standard%20outcomes%2C%20and%20more [Accessed: 17 June 2021].

Ascher, W. A. (2005) *The Frog Principle: The Loss of Freedom in America*. *Google book* [Online]. Available at: https://books.google.co.uk/books?id=6CXmZX0izuMC&printsec=frontcover&dq=the+frog+principles:+the+loss+of+freedom&hl=en&sa=X&ved=0ahU (Accessed 3 January 2020)

Aston, B. (2018) *Data Protection within the Digital Age* [Online] Available: https://afrisig.org/2018/11/28/data-protection-within-the-digital-age/ (Accessed at: 8 October 2019)

Author unknown. (2015) *Digital Privacy: Issues and Challenges in Bhutan* [Online]. Available at https://kuenselonline.com/digital-privacy-issues-and-challenges-in-bhutan/ (Accessed: 23 January 2018)

Baer, M. (2018) Bhutan: From Pre-Tech to One of the Most Wired Countries [Online]. Available at: https://www.fels.upenn.edu/recap/posts/1523 (Accessed: 23 January 2022)

Bagley, Andrew and Brown, Justin, (2015) Limited Consumer Privacy Protections Against the Layers of Big Data, Santa Clara High Technology Law Journal Volume 31 (4). Available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1599&context=chtlj (Assessed: 25 August 2019)

Balboni, P. (2018) *The New Surinamese Privacy And Data Protection (SPDP) Law* [Online]. Available at: https://www.paolobalboni.eu/index.php/2018/05/15/the-new-surinamese-privacy-and-data-protection-spdp-law/ (Accessed: 13 May 2020)

Bannelier, K. et al, (2019) 'Cyberspace debris' in Pawlak, P. and Biersteker, T (ed.) *Guardian of the galaxy: EU cyber sanctions and norms in cyberspace*, *Paris: European Union Institute for Security Studies* [Online]. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf (Accessed: 15 October 2019)

BBC. (2018) *Should we worry about Huawei?* [Online]. Available at: https://www.bbc.co.uk/news/business-46465438 (Accessed: 12 January 2019)

BBC. (2018) *Huawei: The rapid growth of a Chinese champion in five charts* [Online]. Available at: https://www.bbc.co.uk/news/business-46480208 (Accessed:16 January 2019)

Beal, D., Rueda-Sabater, E., and Santo, T. E., (2012) Comparing Socioeconomic Development Across Nations [Online]. Available at: https://www.bcg.com/publications/2012/public-sector-globalization-comparing-socioeconomic-development (Accessed: 12 November 2020)

Bentotahewa, V. Hewage, C. and Williams, J. (2020) 'Big Data in the wake of Data Protection Laws – Asian Perspective', *South Asian Journal* [Online]. Available at http://southasiajournal.net/big-data-in-the-wake-of-data-protection-laws-asian-perspective/ (Accessed: 15 June 2021)

Bentotahewa, V., Hewage, C. and Williams, J. (2020) *Do Privacy Rights Override #COVID19 Surveillance Measures?* [Online] Available at: https://www.infosecurity-magazine.com/next-gen-infosec/privacy-rights-covid19/ (Accessed: 22 February 2021)

Bentotahewa, V. and Hewage, C. (2020) *Challenges and Obstacles to Application of GDPR to Big Data* [Online] Available at: https://www.infosecurity-magazine.com/next-gen-infosec/challenges-gdpr-big-data/ (Accessed: 23 February 2021)

Berry, L. (2017) *Data Protection Law an E-Business and E-Government Perception* [Online]. Available at https://silo.tips/download/data-protection-law-an-e-business-and-e-government-perception (Accessed: 2 August 2019)

Bevitt, A., Retzer, K and Łopatowska, J. (N.D) *Dealing with data breaches in Europe and beyond* [Online]. Available at: https://uk.practicallaw.thomsonreuters.com/6-505-9638?transitionType=Default&contextData=(sc.Default)&firstPage=true (Accessed: 3 July 2020)

Birnbaum, M. (2019) *Poland detains employee of Chinese tech giant Huawei on spying charges* [Online]. Available at: https://www.washingtonpost.com/world/europe/poland-detains-employee-of-chinese-tech-giant-huawei-on-spying-charges/2019/01/11/ac148e42-15a0-11e9-90a8-136fa44b80ba_story.html?utm_term=.ac80177bf106 (Accessed: 13 January 2019)

Broadhurst, R. and Grabosky, P. (2005) *Cyber-Crime: The Challenge in Asia*. Google book [Online]. Available at: https://books.google.co.uk/books/about/Cyber_crime.html?id=O7HEwAEACAAJ&redir_esc=y (Accessed: 16 June 2019)

Brogan, C. (2019) *Anonymising personal data 'not enough to protect privacy', shows new study* [Online] Available at: https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/ (Accessed: 15 November 2019)

Burgess, J. and Northage, A. (2018) *The 'security principle' under GDPR and personal data breaches* [Online]. Available at: https://www.walkermorris.co.uk/publications/our-series-of-guides-to-the-eu-general-data-protection-regulation-round-up-of-the-latest-guidance-on-gdpr-2/the-security-principle-under-gdpr-and-personal-data-breaches/ (Accessed: 15 March 2020)

Burgess, M. (2020) *What is GDPR? The summary guide to GDPR compliance in the UK* [Online]. Available at https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (Accessed: 20 May 2020)

Burgos, C. and Pehlivan, C. (2020) Data Protected – Spain [Online]. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---spain (Accessed: 18 August 2020)

Burkevics, A. (N.D) Latvia - Data Protection Overview [Online]. Available at: https://www.dataguidance.com/notes/latvia-data-protection-overview (Accessed: 5 September 2020)

Burman, A. (2020) *Privacy and Promote Growth?* [Online]. Available at https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217 (Accessed: 12 August 2020)

Cadete, L. (2017) *What is a pilot study?* [Online]. Available at https://s4be.cochrane.org/blog/2017/07/31/pilot-studies/ (Accessed: 15 August 2021)

Calzon, B. (2021) *Your Modern Business Guide To Data Analysis Methods And Techniques* [Online]. Available at https://www.datapine.com/blog/data-analysis-methods-and-techniques/ [Accessed: 18 April 2021]

Chisenga, S. (2021) *Zambia - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/zambia-data-protection-overview (Accessed: 23 August 2021)

Cleland J. A (2017) 'The qualitative orientation in medical education research', *Korean J Medicine Education,* Volume (2) [Online]. Available at DOI: 10.3946/kjme.2017.53. [Accessed: 23 November 2020]

Cloen, T. (2020) South Asia: The road ahead in 2020 [Online]. Available at https://www.atlanticcouncil.org/commentary/feature/south-asia-the-road-ahead-in-2020/#India (Accessed: 12 May 2020)

Clough, J. (2014) 'A world of Difference: The Budapest Convention on cybercrime and the challenges of Harmonisation' *Monash University Law Review*, Volume 40(3) [Online]. Available at https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf (Accessed: 13 March 2020)

Cohen, J. (2020) *Cambodia - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/cambodia-data-protection-overview

Court of Justice of the European Union. (2021) *General Data Protection Regulation (GDPR): the Court specifies the conditions for the exercise of the national supervisory authorities' powers with respect to the cross-border processing of data. Court of Justice of the European Union- Press release. Luxemburg* [Online]. Available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-06/cp210103en.pdf (Accessed: 5 August 2021)

Consumers International. (2018) *The state of data protection rules around the world A briefing for consume organisations*. *Consumers International* [Online]. Available at: https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf (Accessed: 5 May 2019)

Council of Europe. (N.D) Budapest Convention and related standards [Online]. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 17 March 2020)

Council of EU. (2020) *EU imposes the first ever sanctions against cyber-attacks* [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ (Accessed 6 August 2021)

Council on foreign relations. (N.D) U.S. Relations With China (1949-2021) [Online]. Available at: https://www.cfr.org/timeline/us-relations-china (Accessed: 14 March 2021)

Croatian Data Protection Agency, (N.D) *National legislation- Act on the implementation of the General Data Protection Regulation* [Online]. Available at: https://azop.hr/national-legislation/ (Accessed: 29 January 2021)

Cuihong, C. (2015) 'Cybersecurity in the Chinese Context', *China Quarterly of International Strategic Studies*, Vol. 1, No. 3, P. 471–496. Available at: DOI: 10.1142/S2377740015500189 (Accessed: 13 May 2019)

Dabbagh, A. A. (2021*) Iraq - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/iraq-data-protection-overview (Accessed: 3 August 2021)

Data Guidance, (N.D) *Morocco* [Online]. Available at: https://www.dataguidance.com/jurisdiction/morocco (Accessed: 2 April 2019)

Data Guidance, (N.D) The Gambia [Online]. Available at: https://www.dataguidance.com/jurisdiction/gambia (Accessed: 12 January 2021)

Data Guidance. (N.D) *Madagascar* [Online]. Available at: https://www.dataguidance.com/jurisdiction/madagascar (Accessed: 14 May 2021)

Data Guidance, (2020) *Republic of Congo: Personal Data Protection Law published in Official Journal* [Online]. Available at: https://www.dataguidance.com/news/republic-congo-personal-data-protection-law-published (12 April 2021)

Data Guidance, (N.D) *Yemen* [Online]. Available at: https://www.dataguidance.com/jurisdiction/yemen (23 November 2020)

Data Guidance, (N.D) *Jordan* [Online]. Available at: https://www.dataguidance.com/jurisdiction/jordan (20 October 2020)

Data Guidance, (N.D) *Lebanon* [Online]. Available at: https://www.dataguidance.com/jurisdiction/lebanon (Accessed: 27 May 2020)

Data Guidance, (2020) *Oman: Latest developments in data protection and cybersecurity* [Online]. Available at: https://www.dataguidance.com/opinion/oman-latest-developments-data-protection-and (Accessed: 14 December 2020)

Data Guidance, (N.D) Kuwait [Online]. Available at: https://www.dataguidance.com/jurisdiction/kuwait (Accessed: 10 February 2021)

Data Guidance, (N.D) *Iran* [Online]. Available at: https://www.dataguidance.com/jurisdiction/iran (Accessed: 27 October 2020)

Data Guidance, (2019) *Guatemala: Data protection thus far* [Online]. Available at: https://www.dataguidance.com/opinion/guatemala-data-protection-thus-far (Accessed: 12 August 2020)

Data Guidance, (N.D) *Ecuador* [Online]. Available at: https://www.dataguidance.com/jurisdiction/ecuador (Accessed: 19 July 2020)

Data Guidance, (N.D) *Haiti* [Online]. Available at: https://www.dataguidance.com/jurisdiction/haiti (Accessed: 29 October 2020)

Data Guidance, (N.D) *Bulgaria* [Online]. Available at: https://www.dataguidance.com/jurisdiction/bulgaria (Accessed: 14 May 2021)

Data Guidance, (N.D) Slovenia [Online]. Available at: https://www.dataguidance.com/jurisdiction/slovenia (Accessed: 23 January 2021)

De Soysa, S. (2017) *The right to privacy and a data protection act: Need of the hour* [Online]. Available at http://www.ft.lk/article/606874/The-right-to-privacy-and-a-data-protection-act:-Need-of-the-hour (Accessed: 3 May 2018)

DeCarlo, M. (N.D) *Inductive and deductive reasoning* [Online]. Available at https://scientificinquiryinsocialwork.pressbooks.com/chapter/6-3-inductive-and-deductive-reasoning/ [Accessed: 15 October 2020]

Deloitte. (2019) *The Asia Pacific Privacy Guide. Deloitte* [Online]. Available at https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-

Deloitte_AP-PrivacyGuide_Interactive-noexp.pdf (Accessed: 12 December 2019)

Deloitte. (2019) *India Draft Personal Data Protection Bill, 2018 and EU General Data Protection Regulation A comparative view. Deloitte* [Online]. Available at https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-india-draft-personal-data-protection-bill-noexp.pdf (Accessed: 20 September 2020)

Deloitte. (2019) *Unity in Diversity; The Asia Pacific Privacy Guide. Deloitte* [Online]. Available at https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-Deloitte_AP-PrivacyGuide_Interactive-noexp.pdf (Accessed: 5 March 2020)

Deloitte, (2017) *Privacy is Paramount- Personal Data Protection in Africa. Deloitte* [Online]. Available at: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf (22 January 2021)

Deloitte, (N.D) The new German Privacy Act [Online]. Available at: https://www2.deloitte.com/dl/en/pages/legal/articles/neues-bundesdatenschutzgesetz.html (Accessed: 13 March 2021)

Deloitte, (N.D) *Brazilian General Data Protection Act* [Online]. Available at: https://www2.deloitte.com/br/en/pages/risk/articles/lgpd.html (Accessed: 23 November 2020)

Desjardins, J. (2019) *How much data is generated each day?* [Online]. Available at https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/ (Accessed: 10 February 2020)

Dhungel, R. (2019) *Cyber Security For National Security* [Online]. Available at https://risingnepaldaily.com/opinion/cyber-security-for-national-security (Accessed: 12 April 2020)

DLA Piper. (2021) *Data protection laws of the world. DLA Piper.* [Online]. Available at https://www.thebackgroundinvestigator.com/file/Data-Protection-Full.pdf (Accessed 3 May 2021)

DLA Piper. (2020) *Data protection laws of the world* [Online]. Available at https://www.dlapiperdataprotection.com/index.html?t=transfer&c=PK (Accessed: 3 January 2021)

DLA Piper, (2021) *Qatar* [Online]. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=QA (Accessed: 20 March 2021)

DLA Piper, (2021) *Chile* [Online]. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=CL (Accessed: 13 October 2020)

Doulah, N. (2020) *Bangladesh - Data Protection Overview* [Online]. Available at https://www.dataguidance.com/notes/bangladesh-data-protection-overview (Accessed: 3 October 2020)

DPO centre. (2018) What is the difference between the DPA 2018 and the GDPR? (and why does it matter?) [Online]. Available at: https://www.dpocentre.com/difference-dpa-2018-and-gdpr/ (Accessed: 14 April 2019)

Dube, H. (2021) *Privacy and personal data protection in Africa A rights-based survey of legislation in eight countries*. *Cathy Chen (APC)* [Online]. Available at: https://www.apc.org/sites/default/files/PrivacyDataProtectionAfrica_CountryReports.pdf (17 October 2020)

Dudovskiy. J. (N.D) *Research Approach* [Online]. Available at https://research-methodology.net/research-methodology/research-approach/#:~:text=Research%20approach%20can%20be%20divided,Abductive%20research%20approach [Accessed: 15 May 2020]

Dudovskiy. J. (N.D) *Abductive reasoning (abductive approach)* [Online]. Available at https://research-methodology.net/research-methodology/research-approach/abductive-reasoning-abductive-approach/ [Accessed: 20 June 2020]

Dudovskiy. J. (N.D) *Inductive Approach (Inductive Reasoning)* [Online]. Available at https://research-methodology.net/research-methodology/research-approach/inductive-approach-2/#:~:text=Inductive%20approach%2C%20also%20known%20in,result%20of%

20observations%5B1%5D.&text=Patterns%2C%20resemblances%20and%20regularities%20in,(or%20to%20generate%20theory) [Accessed: 15 May 2020]

Dudovskiy, J. (N.D) *Data Collection Methods* [Online]. Available at https://research-methodology.net/research-methods/data-collection/#:~:text=Data%20collection%20is%20a%20process,primary%20methods%20of%20data%20collection [Accessed: 14 January 2021]

Dudovskiy, J. (N.D) *Interpretivism (interpretivist) Research Philosophy* [Online]. Available at https://research-methodology.net/research-philosophy/interpretivism/#:~:text=%5B1%5D%20Development%20of%20interpretivist%20philosophy,qualitative%20analysis%20over%20quantitative%20analysis [Accessed: 5 June 2020]

Dudovskiy, J. (N.D) *Bussiness Research Methodology* [Online]. Available at https://research-methodology.net/research-philosophy/pragmatism-research-philosophy/ [Accessed: 3 January 2021]

Dudovskiy, J. (N.D) *Pragmatism Research Philosophy* [Online]. Available at https://research-methodology.net/research-philosophy/pragmatism-research-philosophy/ [Available: 20 August 2020]

Dudovskiy, J. (N.D) *Realism Research Philosophy* [Online]. Available at https://research-methodology.net/research-philosophy/realism/ [Accessed: 14 October 2020]

Edirisingha, P. (2012) *Interpretivism and Positivism (Ontological and Epistemological Perspectives)* [Online]. Available at https://prabash78.wordpress.com/2012/03/14/interpretivism-and-postivism-ontological-and-epistemological-perspectives/ [Accessed: 12 March 2021]

Encyclopedia, (N.D) *Bill of Attainder* [Online]. Available at: https://www.encyclopedia.com (Accessed: 7 June 2019)

Enneifar, I (2021) *Tunisia - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/tunisia-data-protection-overview (Accessed: 27 June 2021)

Ervasti, M. and Helaakoski, H. (2008) 'Adoption of Mobile Services in Finland - Conceptual Model and Application-based Case Study', *ICE-B 2008 - Proceedings of the International Conference on e-Business*, Porto, Portugal, 26-29 July 2008. Available at https://www.researchgate.net/publication/220917747_Adoption_of_Mobile_Services_in_Finland_-_Conceptual_Model_and_Application-based_Case_Study (Accessed 12 June 2020)

Eur-Lex, (2016) *Regulation (EU) 2016/679 of the European parliament and of the council* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434 (12 January 2019)

European Commission. (2020) *Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps* [Online]. Availabel at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043 (23 October 2020)

European Union , (2016) 'Legislative acts', *Official Journal of the European Union. European Union* , [Online]. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Accessed: 15 February 2019)

Fahim, K., Kim, M.J., and Hendrix, S. (2020) *Cellphone monitoring is spreading with the coronavirus. So is an uneasy tolerance of surveillance* [Online]. Available at: https://www.washingtonpost.com/world/cellphone-monitoring-is-spreading-with-the-coronavirus-so-is-an-uneasy-tolerance-of-surveillance/2020/05/02/56f14466-7b55-11ea-a311-adb1344719a9_story.html (17 July 2020)

Finances Online Research Center. (N.D) *97 Big Data Statistics You Must Learn: 2020/2021 Market Share & Data Analysis* [Online]. Available at https://financesonline.com/big-data-statistics/ (Accessed: 2 August 2021)

Formplus Blog. (N.D) *What is Quantitative Data? + [Types & Examples]* [Online] Available at https://www.formpl.us/blog/quantitative-data [Accessed: 2 March 2021]

Fox, C and Lee, D. (2016) *Apple rejects order to unlock gunman's phone* [Online]. Available at: https://www.bbc.co.uk/news/technology-35594245 (Accessed: 7 October 2020)

Gartenberg, C. (2019) *Huawei can't officially use microSD cards in its phones going forward* [Online]. Available at: https://www.theverge.com/2019/5/24/18638539/huawei-microsd-card-sd-association-us-trump-ban (Accessed: 4 June. 2019)

Gerlach, V. (2020) *Data Protected – Netherlands* [Online]. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---netherlands (Accessed: 5 June 2021)

Gervasius, N. (N.D) *Data Protection and Privacy In Namibia: an exploratory study in the context of COVID-19* [Online]. Available at: https://isocnamibia.org/wp-content/uploads/2021/04/Data-Protection-During-COVID-19-Study-in-Namibia.pdf

Goldstein, M. et al., (2018) *How a National Security Investigation of Huawei Set Off an International Incident* [Online]. Available at: https://www.nytimes.com/2018/12/14/business/huawei-meng-hsbc-canada.html (Accessed: 23 December 2018)

Goswami, S. (2021) *Bangladesh to Propose a Privacy Law* [Online]. Available at https://www.bankinfosecurity.asia/bangladesh-to-propose-privacy-law-a-15898 (Accessed 3 March 2021)

Government of Argentina, (2000) *Personal Data Protection Act* [Online]. Available at: http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf

Government of Belize, (2021) *Data Protection Bill, 2021* [Online]. Available at: https://www.nationalassembly.gov.bz/wp-content/uploads/2021/07/Data-Protection-Bill-2021-updated.pdf (16 March 2021)

Government of Bostwana, (2018) *Data Protection Act, 2018* [Online]. Available at: https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf

Government of Denmark, (2018) *The Data Protection Act* [Online]. Available at: https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf (17 March 2021)

Government of Hong Kong (2013*) Personal Data (Privacy) Ordinance* [Online]. Available at: https://www.elegislation.gov.hk/hk/cap486!en.assist.pdf?FILENAME=Assisted%20Monolingual%20PDF%20(English).pdf&DOC_TYPE=K&PUBLISHED=true (3 February 2021)

Government of India, (2019) *The personal data protection bill, 2019* [Online]. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf (Accessed: 22 July 2020)

Government of Japan, (2003) *Act on the Protection of Personal Information Act No. 57 of (2003)* [Online]. Available at: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf (4 April 2021)

Government of Luxemburg, (2018) official gazette of the grand duchy of Luxembourg memorial A [Online]. Available at: https://cnpd.public.lu/dam-assets/fr/legislation/droit-lux/Act-of-1-August-2018-on-the-organisation-of-the-National-Data-Protection-Commission-and-the-general-data-protection-framework.pdf (7 January 2021)

Government of Malaysia, (2010) *Laws of Malaysia Act 709- Personal Data Protection Act 2010* [Online]. Available at: https://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf (28 January 2021)

Government of Pakistan. (2018) *Personal data protection bill* [Online]. Available at: https://moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%20without%20track%20changes.pdf (Accessed: 10 January 2019)

Government of the People's Republic of Bangladesh, (2020) *Digital security act, 2018* [Online]. Available at: https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf (17 August 2020)

Government of Sri Lanka (2021) *Sri Lanka draft Data protection Bill* [Online]. Available at: https://www.dataguidance.com/sites/default/files/sri_lanka_draft_data_protection_bill_2021.pdf (14 May 2020)

Government of Sweden, (2018) *Swedish Code of Statutes* [Online]. Available at: https://www.government.se/4a5a80/contentassets/467ef1335aac404c8840c29f9d02305a/act-containing-supplementary-provisions-to-the-eu-general-data-protection-regulation-sfs-2018218 (Accessed: 25 November 2020)

Government of Thailand, (2019) *Personal Data Protection Act, B.E. 2562 (2019)* [Online]. Available at: https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf (14 January 2021)

Government of Turkey, (N.D) Law on the protection of personal data [Online]. Available at: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf (19 March 2021)

Government of UK. (2016) *National Cyber Security Strategy 2016-2021. Government of UK* [Online]. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Accessed: 5 September 2019)

Government of UK. (2017) *The Queen's speech 2017. Prime minister's office*, London [Online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/620838/Queens_speech_2017_background_notes.pdf (Accessed: 05 January 2020)

Government of United Kingdom, (N.D) *Data protection* [Online]. Available at: https://www.gov.uk/data-protection (Accessed: 23 April 2019)

Government of United Kingdom. (2018) *Data Protection Act 2018* [Online] Available at: https://www.legislation.gov.uk/ukpga/2018/12/enacted/data.xht?view=snippet&wrap=true (Accessed: 13 March 2019)

Government of UK. (2020) *The security of 5G* [Online], Authority of the House of Commons, Available at: https://libguides.scu.edu.au/harvard/government-publications#:~:text=Year%2C%20page%20number)-,References%3A,Year%2C%20Title%20(Report%20No. (Accessed: 24 September 2021)

Greenleaf, G. (2019) ‘Advances in South Asian Data Privacy Laws: Sri Lanka, Pakistan and Nepal’. *Privacy Laws & Business International Report* [Online]. Available at: https:/ssrn.com/abstract=3549055 (Accessed: 22 October 2019)

Greenleaf, G. (2017) ‘Privacy in South Asian (SAARC) States: Reasons for Optimism’, *UNSW Law Research Paper.* No. 18-20. Available at SSRN: https://ssrn.com/abstract=3113158 (Accessed: 15 March 2019)

Griffin, A. (2018) Huawei phone equipment in UK to be dismantled amid fears they could be used by China to spy on people [Online]. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/huawei-5g-phone-masts-equipment-bt-ee-internet-data-chinese-government-a8669076.html (Accessed: 20 January 2019)

Gumbis, J. (2020) Data Protected – Lithuania [Online]. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---lithuania (2 July 2021)

Gunawardana, K, (2018) *Current Status of Information Technology And Its Issues in Sri Lanka* [Online]. Available at https://www.researchgate.net/publication/316383091_Current_Status_of_Information_Technology_And_Its_Issues_in_Sri_Lanka (Accessed 3 Mach 2019)

Hakmeh, J. (2017) *Building a Stronger International Legal Framework on Cybercrime* [Online]. Available at: https://www.chathamhouse.org/2017/06/building-stronger-international-legal-framework-cybercrime (Accessed: 12 December 2020)

Hargittai, E. (1991) Weaving the Western Web Explaining Differences in Internet Connectivity Among OECD Countries, *Telecommunications Policy* [Online]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.79.7637&rep=rep1&type=pdf (Accessed: 3 March 2020)

Healey, J. and Jordan, K T. (2014) *NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow* [Online]. Available at: www.jstor.org/stable/resrep03426. (Accessed 14 April 2019)

Hollis, D. (2021) *A brief primer on international law and cyberspace*. *Carnegie endowment for international peace* [Online]. Available at https://carnegieendowment.org/files/Hollis_Law_and_Cyberspace.pdf (Accessed: 13 July 2021)

Hooker, L. and Palumbo, D. (2018) *Huawei: The rapid growth of a Chinese champion in five charts* [Online]. Available at: https://www.bbc.co.uk/news/business-46480208 (Accessed:16 January 2019)

Hossain, K., et al (2018) *Data Privacy in Bangladesh A Review of Three Key Stakeholders Perspectives* [Online]. Available at: https://www.researchgate.net/publication/329275065_Data_Privacy_in_Bangladesh_A_Review_of_Three_Key_Stakeholders_Perspectives (Accessed: 12 December 2019).

Hounslow, D. (2020) *Japan - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/japan-data-protection-overview (Accessed: 11 December 2020)

Hyde, F. K. (2000) *Recognising deductive processes in qualitative research* [Online]. Available at https://www.emerald.com/insight/content/doi/10.1108/13522750010322089/full/html (Accessed: 4 February 2021)

ICO, (N.D.), About the DPA 2018 (Online). Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/ (Accessed: 15 May 2021)

ICO (N.D) *Binding Corporate Rules at the end of the transition period* [Online]. Available at: https://ico.org.uk/media/for-organisations/documents/2618639/binding-corporate-rules-at-the-end-of-the-transition-period-final-131120.pdf (Accessed: 20 May 2020)

ICO. (N.D) *Overview – Data Protection and the EU* [Online]. Available at: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/ (Accessed: 23 March 2021)

IFEX. (2020) *Pakistan's new draft of data protection law contains 'draconian and anti-democratic' sections* [Online]. Available at https://ifex.org/pakistans-new-draft-of-data-protection-law-contains-draconian-and-anti-democratic-sections/ (Accessed : 10 July 2020)

Ikigai Law. (2019) *Introduction to Digital Security Laws in Nepal, Sri Lanka, and Bangladesh* [Online]. Available at http://www.mdiit.gov.lk/images/Legal_framework_for_proposed_DP_Bill_11th_June_2019_-_revised_FINAL_ver3.pdf (Accessed: 10 January 2020)

International Criminal Court of Justice. (N.D) *Understanding the International Criminal Court* [Online]. Available at https://www.icc-cpi.int/iccdocs/pids/publications/uicceng.pdf (Accessed 20 June 2019)

International the news. (2018) *Huawei rejects Western security fears* [Online]. Available at: https://www.thenews.com.pk/print/407691-huawei-rejects-western-security-fears (Accessed: 14 January 2019)

International Telecommunications Union, Nielsen Online, GfK, local ICT Regulators. (2021) *Internet usage statistics: The Internet Big Picture- World Internet Users and 2021 Population Stats* [Online]. Available at: https://www.internetworldstats.com/stats.htm (Accessed: 18 May 2021)

International Telecommunication Union. (2014) *Understanding cybercrime: Phenomena, Challenges and Legal response* [Online]. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf (Accessed: 17 May 2019)

Internet World Stats (N.D) *Asia* [Online]. Available at: https://www.internetworldstats.com/asia.htm (Accessed: 3 May 2020)

ITU, (2021) *Countries ramp up cybersecurity strategies* [Online]. Available at: https://www.itu.int/en/mediacentre/Pages/pr06-2021-global-cybersecurity-index-fourth-edition.aspx (Accessed: 15 July 2021)

ITU, (N.D) *About International Telecommunication Union* (ITU) [Online]. Available at: https://www.itu.int/en/about/Pages/default.aspx ((Accessed: 15 July 2021)

Johnson, J. (2021) *Number of internet users worldwide from 2009 to 2020, by region (in millions)* [Online]. Available at: https://www.statista.com/statistics/265147/number-of-worldwide-internet-users-by-region/ (Accessed: 15 April 2021)

Johnson, M. A. (2005) *The technology acceptance model and the decision to invest in information security* [Online] Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.108.4895&rep=rep1&type=pdf (Accessed: 16 February 2021)

Kahiani, M. (2020) Kazakhstan - Data Protection Overview [Online]. Available at: https://www.dataguidance.com/notes/kazakhstan-data-protection-overview (Accessed: 27 August 2021)

Karageorgiou, S. (2020) *Data Protected – Greece* [Online]. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---greece (Accessed: 17 December 2020)

Karamagi, R. (2021) *Scientific Research Methods*. Lulu Press [Online]. Available at https://books.google.co.uk/books?id=MzwjEAAAQBAJ&pg=PT17&lpg=PT17&dq=#v=onepage&q&f=false [Accessed: 4 May 2021]

Kark, K., Briggs, B. and Terzioglu, A. (2019) *The future of work in technology* [Online]. Available at: https://www2.deloitte.com/us/en/insights/focus/technology-and-the-future-of-work/tech-leaders-reimagining-work-workforce-workplace.html (Accessed: 2 October 2020)

Katagiri, N. (2021) 'Why international law and norms do little in preventing non-state cyber attacks', *Journal of Cybersecurity*, Volume 7, Issue 1 [Online]. Available at https://doi.org/10.1093/cybsec/tyab009 (Accessed: 13 June 2021)

Kaushik, V. and Walsh A. C. (2019) 'Pragmatism as a Research Paradigm and Its Implications for Social Work Research' *Social Science Journal 2019*, Volume 8(9) [Online]. Available at https://doi.org/10.3390/socsci8090255 [Accessed: 20 March 2020]

Kelion L. (2020) *NHS rejects Apple-Google coronavirus app plan* [Online]. Available at:https://www.bbc.co.uk/news/technology-52441428 (Accessed 2 May 2020)

Kelion, L. (2020) *UK virus-tracing app switches to Apple-Google model* [Online]. Available at: https://www.bbc.co.uk/news/technology-53095336 (Accessed: 28 June 2020)

Kemp, S. (2021) *Digital 2021: Global overview report* [Online]. Available at https://datareportal.com/reports/digital-2021-global-overview-report (Accessed: 16 May 2021)

Kemp, R. (2014) 'Big data and data protection', *Kemp IT Law*, Volume (1. 0) [Online]. Available at: file:///C:/Users/sm77809/Downloads/Big-Data-and-Data-Protection-White-Paper-v1_1-November-2014.pdf (Accessed: 16 March 2020)

Khan, I. et al., (2019) 'Applicability and Appropriateness of Distributed Ledgers 'Consensus Protocols in Public and Private Sectors: A Systematic Review'. *IEEE*, Volume (7) [Online]. Available at: https://ieeexplore.ieee.org/document/8672572 (Accessed: 15 January 2020)

Koch, R. (N.D) *The EU's GDPR only applies to personal data, which is any piece of information that relates to an identifyable person. It's crucial for any business with EU consumers to understand this concept for GDPR compliance* [Online]. Available at: https://gdpr.eu/eu-gdpr-personal-data/ (Accessed 28 March 2020)

Koh, H H. 'International Law in Cyberspace' *Harvard International Law Journal* Volume 54 [Online]. Available at: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers (Accessed on 25 June 2019)

Kraemer, T. (2020) *Afghanistan - Data Protection Overview* [Online]. Available at https://www.dataguidance.com/notes/afghanistan-data-protection-overview (Accessed: 23 December 2020)

Kretzmer, D. (2013) 'The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum', *European Journal of International Law*, Volume 24, Issue 1, Pages 235–282. Available at: https://doi.org/10.1093/ejil/chs087 (Accessed: 15 April 2019)

Ktenas, N. (2021) *Cyprus - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/cyprus-data-protection-overview (Accessed: 23 July 2021)

Kukk, U. (2021) *Estonia - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/estonia-data-protection-overview (Accessed: 10 May 2021)

Kuo, L. (2020) *'The new normal': China's excessive coronavirus public monitoring could be here to stay* [Online]. Available at: https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay ((Accessed: 14 July 2020)

Lai, P. (2017) 'THE LITERATURE REVIEW OF TECHNOLOGY ADOPTION MODELS

AND THEORIES FOR THE NOVELTY TECHNOLOGY', Journal of Information Systems and Technology Management, Volume 14(1) Available at: DOI: 10.4301/S1807-17752017000100002 (Accessed 23 July 2020)

Lancefield, N. (2020) *Drones rules relaxed for police enforcing Covid-19 lockdown* [Online]. Available at: https://www.belfasttelegraph.co.uk/news/uk/drones-rules-relaxed-for-police-enforcing-covid-19-lockdown-39130731.html (Accessed: 26 November 2020)

Lang, F. (2019) *Huawei Discloses Its New OS Name* [Online]. Available at https://interestingengineering.com/huawei-discloses-its-new-os-name (Accessed: 9 July 2019)

Lazar, N (N.D) *Romanian Implementation of the GDPR* [Online]. Available at: https://uk.practicallaw.thomsonreuters.com/w-020-4330?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true (5 February 2021)

Lecher, C. (2019) *Huawei is challenging its US contracting ban as unconstitutional* [Online]. Available at: https://www.theverge.com/2019/5/29/18644040/huawei-government-ban-lawsuit-policy-unconstitutional (Accessed: 2 June 2019)

Lecher, C. and Brandom. R. (2019) *Is Huawei a security threat? Seven experts weigh in* [Online]. Available at: https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g (Accessed: 14 April 2019)

Lee, Y. N. (2021) *U.S.-China relations are 'still deteriorating,' says former U.S. ambassador* [Online] Available at https://www.cnbc.com/2021/06/11/us-china-relations-are-still-deteriorating-says-max-baucus.html (Accessed: 23 July 2021)

Lendman, S. (2018) *China Warns of Escalation Over Huawei Incident* [Online]. Available at: https://stephenlendman.org/2018/12/china-warns-of-escalation-over-huawei-incident/ (Accessed: 13 January 2019)

Leskin, P. (2018) *Here's everything you need to know about Huawei, the Chinese tech giant whose founder's daughter was arrested and could spark an all-out trade war* [Online]. Available at: https://www.businessinsider.com/huawei-meng-wanzhou-trump-china-trade-war-2018-12?r=US&IR=T (Accessed: 12 January 2019)

Levy, D. (N.D) 'Qualitative methodology and grounded theory in property research Pacific Rim' *Property Research Journal*, Volume 12 (4) [Online]. Available at https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.1517&rep=rep1 &type=pdf [Accessed: 5 May 2021]

Li, C. and Lalani, F. (2020) *The COVID-19 pandemic has changed education forever. This is how* [Online]. Available at https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/ (Accessed: 27 May 2021)

Liu, J., Hebenton,B and Jou, S. (2013) 'Handbook of Asian Criminology' Google book [Online]. Available at https://books.google.co.uk/books?id=5QFw0WHPJD8C&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false (Accessed: 12 May 2020)

Lorenzo, S. S. (2021) *Panama - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/panama-data-protection-overview (Accessed: 1

Luo, D. and Wang, Y. (2020) *China - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/china-data-protection-overview (17 February 2021)

Ma, A. (2019) *China sentenced a Canadian man to death in the latest escalation of the countries' feud over Huawei* [Online]. Available at: https://www.businessinsider.com/china-sentences-canadian-robert-schellenberg-to-death-amid-huawei-feud-2019-1?r=US&IR=T (Accessed: 12 February 2019)

Mačák, K (2016) 'Is the International Law of Cyber Security in Crisis?', *8th International Conference on Cyber Conflict,* Available at*:* https://ccdcoe.org/uploads/2018/10/Art-09-Is-the-International-Law-of-Cyber-Security-in-Crisis.pdf (Accessed: 12 March 2020)

Madugalla, K.K. (2016) *Right to Privacy in Cyberspace: Comparative Perspectives from Sri Lanka and other Jurisdictions* [Online]. Available at http://repository.kln.ac.lk/bitstream/handle/123456789/15625/2829.pdf?sequence=1&isAllowed=y (Accessed 27 April 2019)

Makszimov, V. (2020) *Social and economic differences across EU less important for citizens – survey* [Online]. Available at: https://www.euractiv.com/section/economy-jobs/news/social-and-economic-differences-across-eu-less-important-for-citizens-survey/ (Accessed: 12 February 2021)

Marko, R. (N.D) *Austrian Implementation of the GDPR* [Online]. Available at: https://uk.practicallaw.thomsonreuters.com/w-011-7695?originationContext=document&vr=3.0&rs=PLUK1.0&transitionType=DocumentItem&contextData=(sc.Default) (Accessed: 21 February 2021)

Mars, S. D. (2020) *Brexit next steps: The Court of Justice of the EU and the UK* [Online]. Available at: https://commonslibrary.parliament.uk/brexit-next-steps-the-court-of-justice-of-the-eu-and-the-uk/ (Accessed: 22 October 2020)

Matouk Bassiouny and Hennawy, (2020) *Law No. 151 of 2020 Promulgating the Personal Data Protection Law* [Online]. Available at: https://www.acc.com/sites/default/files/program-materials/upload/Data%20Protection%20Law%20-%20Egypt%20-%20EN%20-%20MBH.PDF (15 November 2020)

Maxwell, J. A. (2012) *A Realist Approach for Qualitative Research*. Sage publishers. Available at https://books.google.co.uk/books?id=xIs49CdoNp0C&pg=PA5&lpg=PA5&dq=xAhUOhf0HHQZWCRgQ6AF6BAgFEAM#v=onepage&q&f=false [Accessed: 7 November 2020]

McFarland, D. and Hamilton, D. (2006) 'Adding contextual specificity to the technology acceptance model' *Elsevier*, Volume 22(3). Available at https://www.sciencedirect.com/science/article/abs/pii/S074756320400130X?via%3Dihub (Accessed: 14 March 2021)

McKenzie, B. (2021) *Vietnam: New developments as regards the draft decree on personal data protection* [Online]. Available at: https://insightplus.bakermckenzie.com/bm/attachment_dw.action?attkey=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQJsWJiCH2WAXW59W9rh3JQaAJGkBQphF7&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQbuwypnpZjc4%3D&attdocparam=pB7HEsg%2FZ312Bk8OIuOIH1c%2BY4beLEAe2xOw7OxoJ1U%3D&fromContentView=1 (16 February 2021)

Melnikovas, A. (2018) ‘Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies’ *Journal of Futures Studies*, volume (23(2): 29–4) [Online]. Available at: https://jfsdigital.org/wp-content/uploads/2019/01/03-Melnikovas-Onion-Research-Model.pdf [Accessed; 3 June 2020]

Mencel, A.(2020) *Data Protected – Poland* [Online]. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---poland (Accessed: 19 March 2021)

Mendoza, M. A. (2017) *Challenges and implications of cybersecurity legislation* [Online]. Available at: https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/ (Accessed: 13 October 2020)

Mia, I. B. R. and Habaradas, R. (2020) ‘ASEAN ICT developments: Current state, challenges, and what they mean for SMEs’, *PHILIPPINE Academy of Management E-Journal* Vol.3 – No.1. Available at: https://www.researchgate.net/publication/341368761_ASEAN_ICT_developments_Current_state_challenges_and_what_they_mean_for_SMEs (18 February 2021)

Ministry of information technology & telecommunication, (2020) *Personal data protection bill 2020* [Online].Available at: https://moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%202020%20Updated.pdf (12 May 2021)

Ministry of Justice, (N.D) *Data Protection Act (1050/2018)* [Online]. Available at: https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf

Mishbah, A. B. M. H. (2019) *Bangladesh steps into the data protection regime* [Online]. Available at https://www.thedailystar.net/opinion/human-rights/news/bangladesh-steps-the-data-protection-regime-1726351 (Accessed: 22 May 2019)

Mitchell, J. A. (2018) 'A Review of Mixed Methods, Pragmatism and Abduction Techniques' *The Electronic Journal of Business Research Methods*. Volume 16 (3) [Online]. Available at https://www.researchgate.net/publication/328343822 [Accessed: 19 August 2020]

Molla, M. S. and Nahar, S. (N.D) *Need of Personal Data Protection Laws in Bangladesh: A legal Appraisal* [Online]. Available at https://www.hg.org/legal-articles/need-of-personal-data-protection-laws-in bangladesh-a-legal-appraisal-48450 (Accessed: 12 February 2020)

Moller, M. (2021) *Seychelles - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/seychelles-data-protection-overview

Moniruzzaman, M. (2019) *Personal Data Protection in Bangladesh and GDPR* [Online]. Available at https://bdjls.org/personal-data-protection-in-bangladesh/ (Accessed: 23 September 2020)

Morgan, B (2021) *Status of Data Privacy Laws in the Caribbean* [Online] Available at: https://www.bartlettmorgan.com/2021/02/03/status-of-data-privacy-laws-in-the-caribbean-feb-2021/ (Accessed: 21 April 2021)

Moskwa, W. et al., (2019) *Huawei Arrests in Poland Show How Trump Vs. China Tests Europe* [Online]. Available at https://www.bloomberg.com/news/articles/2019-01-11/poland-detains-huawei-employee-accuses-him-of-spying-for-china (Accessed: 15 January 2019)

Moynihan, H. (2019) *The Application of International Law to Cyberspace: Sovereignty and Non-intervention* [Online] Available at https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/ (Accessed: 28 March 2020)

Mudavanhu, E. (2021) *Lesotho - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/lesotho-data-protection-overview (Accessed: 3 May 2021)

Mudavanhu, E. (2021) *Rwanda - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/rwanda-data-protection-overview (Accessed: 12 April 2021)

Muller-Seitz et al. (2009) 'Customer acceptance of RFID technology: Evidence from the German electronic retail sector', *Journal of Retailing and Consumer Services*, Volume 16(1), P. 31-39 [Online] Available at https://www.researchgate.net/publication/229359169_Customer_acceptance_of_RFID_technology_Evidence_from_the_German_electronic_retail_sector (Accessed: 23 April 2020)

Mysicka, V. (2021) *Slovakia - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/slovakia-data-protection-overview (Accessed: 20 May 2021)

National Information Technology Development Agency (N.D) *Nigeria Data Protection Regulation 2019* [Online]. Available at: Fichet, C. (2020) *Burkina Faso - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/burkina-faso-data-protection-overview (Accessed: 3 March 2021)

National Information Technology Development Agency (N.D) *Nigeria Data Protection Regulation 2019* [Online]. Available at: https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf (23 March 2021)

National Forum of Parliamentarians on Population and Development. (2020) *Nepal's Constitution and Federalism Vision and Implementation* [Online]. Available at https://asiafoundation.org/wp-content/uploads/2020/10/Nepals-Constitution-and-Federalism_Vision-and-Implementation_English.pdf (Accessed: 10 August 2020)

Nepal Law Commission, (2018) *The Privacy Act, 2075 (2018)* [Online]. Available at: https://www.lawcommission.gov.np/en/archives/category/documents/prevailing-law/statutes-acts/the-privacy-act-2075-2018 (7 January 2020)

Neupane, A. and Karki, S (2019) *Nepal: An introduction to the Individual Privacy Act 2018* [Online]. Available at https://www.dataguidance.com/opinion/nepal-introduction-individual-privacy-act-2018 (Accessed: 13 March 2020)

Neupane Law Associates (2019) *Introduction To The Privacy Act 2018* [Online]. Available at https://www.neupanelegal.com/news-detail/introduction-to-the-privacy-act-2018.html (Accessed: 10 June 2019)

Ng, A. (2020) *COVID-19 immunity certificates: Everything to know about this controversial solution* [Online]. Available at: https://www.cnet.com/health/covid-19-immunity-certificates-everything-to-know-about-this-controversial-solution/ (Accessed 29 May 2020)

Ng, A. (2020) *How China uses facial recognition to control human behaviour* [Online]. Available at: https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/ (Accessed: 14 September 2020)

NHS. (N.D). *COVID-19 app support* [Online]. Available at: https://covid19.nhs.uk/ (Accessed: 17 November 2020)

NIS Cooperation Group. (2019) *EU coordinated risk assessment of the cybersecurity of 5G networks*
[Online]. Available at file:///C:/Users/sm77809/Downloads/report__eu_risk_assessment_E4583F51-F351-6B15-A1317185D4FB353A_62132.pdf (Accessed: 20 September 2021)

No author. (N.D) *What Is Realism, and Why Should Qualitative Researchers Care?* [Online]. Available at https://www.sagepub.com/sites/default/files/upm-binaries/44131_1.pdf (Accessed: 3 May 2021)

No author, (2012) *A New Dawn: Privacy in Asia* [Online]. P. 10-13. Available at: https://privacyinternational.org/sites/default/files/2017-12/A%20New%20Dawn_Privacy%20in%20Asia.pdf (Accessed 10 January 2020)

Nomin and Advocates (2021) *Draft law on personal data protection* [Online]. Available at: https://www.nominadvocates.com/upload/files/Client%20note_Draft%20Law%20on%20Personal%20Data_Eng_Final.pdf (18 December 2019)

Nougrères, A. B. (2021) *Uruguay - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/uruguay-data-protection-overview (Accessed: 23 June 2021)

NPEx. (N.D). *NPEx: A National Scale Solution for the COVID-19 Crisis* [Online]. Available at: https://www.npex.nhs.uk/news/200409 (Accessed: 13 August 2020)

OECDiLibrary. (N.D) *Risks and challenges of data access and sharing* [Online]. Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across societies. Available at: https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en (Accessed: 13 May 2021)

OneTrust Technology. (2019) Pakistan: *Revised draft Personal Data Protection Bill v. GDPR* [Online]. Available at https://www.dataguidance.com/opinion/pakistan-revised-draft-personal-data-protection-bill-v-gdpr (Accessed: 3 July 2019)

OneTrust Company News. (2018) *What is the Pakistan Data Protection Bill 2018?* [Online]. Available at https://www.onetrust.com/what-is-the-pakistan-data-protection-bill-2018/ (Accessed: 4 November 2018)

One Trust Data Guidance, (N.D) El Salvador: Assembly passes personal data protection law [Online]. Available at: https://www.dataguidance.com/news/el-salvador-assembly-passes-personal-data-protection (Accessed: 26 June 2021)

Orban, Z. (2020) *Data Protected – Hungary* [Online]. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---hungary (Accessed: 5 April 2021)

Orji, U J. (2018) *Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?* [Online]. Available at: https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf (Accessed: 15 May 2019)

Osborne, C. (2020) *France asks Apple to relax iPhone security for coronavirus tracking app development* [Online]. Available at: https://www.zdnet.com/article/france-asks-apple-to-relax-iphone-security-for-coronavirus-tracking-app-development/ (Accessed: 27 May 2020)

Panakal, D D. (2020) *Pakistan's Data Protection Bill Includes Localization and Registration Provisions* [Online]. Available at:

https://www.natlawreview.com/article/pakistan-s-data-protection-bill-includes-localization-and-registration-provisions (Accessed: 5 July 2020)

Panday, J. (2017) *India's Supreme Court Upholds Right to Privacy as a Fundamental Right—and It's About Time* [Online]. Available at https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time#:~:text=The%20one%2Dpage%20order%20signed,Part%20III%20of%20the%20Constitution (Accessed: 10 August 2018)

Pernik, P. (2014) *Improving Cyber Security: NATO and the EU* [Online]. Available at: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf (Accessed: 16 December 2019)

Peters, A. (2019) *Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime* [Online]. Available at https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/ (Accessed: 05 April 2020)

Pfleeger, L S and Caputo D D. (2012) *Leveraging Behavioral Science to Mitigate Cyber Security Risk* [Online] Available at: https://www.mitre.org/sites/default/files/pdf/12_0499.pdf (Accessed 16 November 2019)

Pierce, at el. (2014) 'Extending The Technology Acceptance Model: Policy Acceptance Model (PAM)', *American Journal of Health Sciences*, Volume 5 (2). Available at https://clutejournals.com/index.php/AJHS/article/view/8963/8951 (Accessed 24 March 2021)

Plantera, F. (2019) *Estonia takes on a major role in cyber diplomacy with a new department for international cooperation* [Online]. Available at https://e-estonia.com/estonia-cyber-diplomacy-international-cooperation/ (Accessed: 14 September 2020)

Polish Investment and Trade Agency, (N.D) *EU Funds* [Online]. Available at: https://www.paih.gov.pl/why_poland/eu_funds (Accessed: 23 June 2021)

Portz, J. D. at el., (2019) 'Using the Technology Acceptance Model to Explore User Experience, Intent to Use, and Use Behavior of a Patient Portal Among Older Adults With Multiple Chronic Conditions: Descriptive Qualitative Study' *Journal* *of Medical Internet Research*, Volume 21 (4). Available at: DOI: 10.2196/11604 (Accessed: 14 September 2021)

Portulans Institute, (N.D) *Performance Overvirew* [Online]. Available at: https://networkreadinessindex.org/ (Accessed: 20 January 2022)

Pradhan, K. (2014) *Nepal* [Online]. Available at https://www.giswatch.org/en/country-report/communications-surveillance/nepal (Accessed: 24 February 2018)

Pradhan, D. (2020) *Nepal - Data Protection Overview* [Online]. Available at https://www.dataguidance.com/notes/nepal-data-protection-overview (Accessed: 14 July 2020)

Privacy International Organisation. (N.D) *Data Protection* [Online] Available at: https://privacyinternational.org/learn/data-protection (Accessed: 16 September 2020)

Privacy International and the Digital Rights Foundation. (2019) *State of Privacy Pakistan* [Online]. Available at https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan (Accessed: 20 February 2020)

Puddu, S. (2020) *Data Protected – Italy* [Online]. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---italy (Accessed: 27 August 2020)

Raghunath, P. (2019) 'Human Security in a Datafying South Asia: Approaching Data Protection', *International Journal of Media Studies*. Vol.(1). Available https://www.efluniversity.ac.in/Journals-Communication/IJMS1_Raghunath

Rauniar, R., Rawski, G., Yang, J. and Johnson, B. (2014). 'Technology acceptance model (TAM) and social media usage: an empirical study on Facebook', *Journal of Enterprise Information Management*, Volume 27 [Online] Available at http://dx.doi.org/10.1108/JEIM-04-2012-0011 (Accessed 3 March 2020)

Revisesociology. (2015) *Positivism and Interpretivism in Social Research* [Online]. Available at https://revisesociology.com/tag/interpretivism/#:~:text=of%20the%20two.-,Positivism,have%20good%20reliability%20and%20representativeness.&text=In%20positivist%20research%2C%20sociologists%20tend,between%20two%20or%20more%20variables [Accessed 23 April 2020]

Robinson, P. H. (2006) *Final Report of The Maldivian Penal Law & Sentencing Codification Project: Text of Draft Code (Volume 1) and Official Commentary (Volume 2)* [Online]. Available at https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1289&context=faculty_scholarship (Accessed 23 January 2019)

Rehman, S. (2020) *Pakistan - Data Protection Overview* [Online]. Available at https://www.dataguidance.com/notes/pakistan-data-protection-overview (Accessed: 23 August 2020)

Reichert, C and Keane, S. (2019) *Huawei OS may be called 'Hongmeng,' but it's reportedly 'far from ready'* [Online]. Available at: https://www.cnet.com/news/calls-to-break-up-amazon-google-facebook-and-apple-get-louder/ (Accessed: 24 June 2019)

Reiff, N. (2019) *Why Huawei Is in the Middle of the U.S. China Trade War* [Online]. Available at: https://www.investopedia.com/why-huawei-is-in-the-middle-of-the-u-s-china-trade-war-4687522 (Accessed: 22 May 2019)

Rengel, A. (2013) *Privacy in the 21st Century*. *Google book* [Online]. P.57. Available at: https://books.google.co.uk/books?id=6dLeAQAAQBAJ&printsec=frontcover&dq=privacy+in+21+cene (Accessed: 28 January 2020)

Republic of Kazakhstan, (2013) *On Personal Data and their Protection* [Online]. Available at: https://adilet.zan.kz/eng/docs/Z1300000094 (Accessed: 24 June 2021)

Republic Of Kenya, (2019) *Kenya gazette supplement* [Online]. Available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf (3 December 2020)

Republic of Kyrgyzstan, (2008) *The law of the Kyrgyz Republic On Personal Data* [Online]. Available at: https://www.legislationline.org/download/id/4220/file/Kyrgyz_Law_personal_data_2008_EN.pdf (12 January 2021)

Republic of Mauritius, (2017) *The Data Protection Act 2017* [Online]. Available at: https://rm.coe.int/dpa-2017-maurice/168077c5b (5 February 2021)

Republic of Philippines. (2012) *Republic Act 10173 – Data Privacy Act of 2012* [Online]. Available at: https://www.privacy.gov.ph/data-privacy-act/ (Accessed: 23 March 2019)

Republic of Singapore, (2012) *Personal Data Protection Act 2012* [Online]. Available at: file:///C:/Users/sm77809/Downloads/Personal%20Data%20Protection%20Act%202012.pdf (18 February 2021)

Republic of Singapore, (2020) *Personal Data Protection (Amendment) Act 2020* [Online]. Available at:

Republic of South Africa, (N.D) *Protection of Personal Information Act (POPI Act)* [Online]. Available at: https://popia.co.za/ (Accessed: 20 April 2020)

Republic of Uzbekistan, (2019) *On personal data* [Online]. Available at: https://lex.uz/docs/4831939 23 January 2020)

Republic of Tajikistan, (2018) *About personal data protection* [Online]. Available at: https://cis-legislation.com/document.fwx?rgn=108952 (Accessed: 23 may 2019)

Republic of Zimbabwe. (N.D) *Cyber security and data protection bill, 2019* [Online]. Available at: https://t3n9sm.c2.acecdn.net/wp-content/uploads/2020/05/Cyber-Security-and-Data-Protection-Bill.pdf (Accessed: 19 April 2020)

Rizo, A T. (2021) *Nicaragua - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/nicaragua-data-protection-overview (Accessed: 3 May 2021)

Rizvi, R. (2020) *UAE - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/uae-data-protection-overview (Accessed: 17 June 2021)

Rosenthal, D. (2020) *Data Protected – Switzerland* [Online]. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---switzerland (Accessed: 18 February 2021)

Saarinen, M. at el., (2019) *Data protection in France: overview* [Online]. Available at: https://www.lw.com/thoughtLeadership/data-protection-in-france-overview (Accessed: 20 September 2020)

Sabbagh, D., Hern, A and Proctor, K. (2020) *UK racing to improve contact-tracing app's privacy safeguards* [Online]. Available at: https://www.theguardian.com/technology/2020/may/05/uk-racing-to-improve-contact-tracing-apps-privacy-safeguards (Accessed: 13 April 2020)

Sabbah, C. (2018) *Pressing Pause: A New Approach for International Cybersecurity Norm Development* [Online]. Available at: https://ccdcoe.org/uploads/2018/10/Art-14-Pressing-Pause.-A-New-Approach-for-International-Cybersecurity-Norm-Development.pdf (Accessed: 17 May 2019)

Safari, B A. (2017) *Intangible privacy rights: How Europe's GDPR will set a new global standard for personal data protection* [Online]. Available at: https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1600&context=shlr (Accessed: 24 March 2020)

SAGE publications, (N.D) *The Selection of a Research Approach* [Online]. Available at: https://us.sagepub.com/sites/default/files/upm-binaries/55588_Chapter_1_Sample_Creswell_Research_Design_4e.pdf [Accessed: 4 December 2020]

Saif, A N M. (2021) 'ICT service exports in South Asia: a cross-country forecasting approach' *International Journal of Business Innovation and Research.* Available at: DOI: 10.1504/IJBIR.2021.10039997

Salazar, M. E. (2021) *Venezuela - Data Protection Overview* [Online] Available at: https://www.dataguidance.com/notes/venezuela-data-protection-overview (Accessed: 28 May 2021)

Sankaran, V. (2021) *Cyberattacks on US are 'here to stay', Biden official warns* [Online]. Available at https://www.independent.co.uk/news/world/americas/cyberattack-us-gigabyte-colonial-pipeline-hack-b1844690.html (Accessed: 12 July 2021)

Santos, A. (2020) *Data Protected – Portugal* [Online]. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---portugal (22 August 2020)

Saunders, M., Lewis, P., and Thornhill, A. (2009) *Understanding research philosophies and approaches* [Online]. Available at https://www.researchgate.net/publication/309102603_Understanding_research_philosophies_and_approaches [Accessed: 10 November 2020]

Schrijver, S. D. and Fraeyenhoven, O. V. (2020) *The Privacy, Data Protection and Cybersecurity Law Review: Belgium* [Online]. Available at: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/belgium (Accessed: 23 December 2020)

Sek, Y. (2010) *Prediction of User Acceptance and Adoption of Smart Phone for Learning with Technology Acceptance Model* [Online]. Available at: http://eprints.utem.edu.my/id/eprint/142/1/Journalv8.pdf (Accessed 13 June 2020)

Shahaab, A. et al., (2020) 'Managing Gender Change Information on Immutable Blockchain in Context of GDPR'. *The Journal of The British Blockchain Association*, Volume (3- Issue 1) [Online]. Available at: https://jbba.scholasticahq.com/article/11592-managing-gender-change-information-on-immutable-blockchain-in-context-of-gdpr (Accessed 23 March 2020)

Shiv, Y. (2020) *Israel - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/israel-data-protection-overview (Accessed: 15 June 2020)

Sirimane, M. (2020) *Sri Lanka: Proposed Bill on Personal Data Protection* [Online]. Available at https://www.dataguidance.com/opinion/sri-lanka-proposed-bill-personal-data-protection (Accessed: 13 April 2020)

Skopik, F. and Pahi, T. (2020) 'Under false flag: using technical artifacts for cyber attack attribution', *Cybersecurity* 3 (8). Available at: https://doi.org/10.1186/s42400-020-00048-4 (23 August 2020)

Smart News, (2018) *Overview of Legal News June – July 2018* [Online]. Available at: https://www.lpalaw.com/wp-content/uploads/2018/08/LPA-CGR-Smart-News-Algeria-Overview-of-Legal-News-JUNE-JULY-2018_V....pdf (3 December 2020)

Smith, C. and Elger, T. (2020) *Critical Realism and Interviewing Subjects* [Online]. Available at https://core.ac.uk/download/pdf/28902322.pdf [Accessed: 15 July 2020]

Sobers, R. (2021) 134 *Cybersecurity Statistics and Trends for 2021* [Online]. Available at https://www.varonis.com/blog/cybersecurity-statistics/ (Accessed: 20 June 2021)

Sobers, R. (2020) *What is Human Generated Data?* [Online]. Available at https://www.varonis.com/blog/what-is-human-generated-data/ (Accessed: 20 June 2020)

Sobh, R. and Perry, C. (2006). 'Research design and data analysis in realism research' *European Journal of Marketing*. Volume 40 (11/12) [Online]. Available at https://www.researchgate.net/publication/228953893_Research_design_and_data_analysis_in_realism_research [Accessed: 10 August 2020].

Soiferman, K. L. (2010) *Compare and Contrast Inductive and Deductive Research Approaches* [Online]. Available at https://files.eric.ed.gov/fulltext/ED542066.pdf [Accessed: 16 July 2020]

Soutullo, J. and Masur, W. (2021) *European Parliament Fact Sheets on the European Union* [Online]. Available at: https://www.europarl.europa.eu/factsheets/en/sheet/181/south-asia (22 August 2021)

Sputnike International. (2018) *China Slams Treatment of Huawei Executive Held in Canada as 'Inhumane'* [Online]. Available at: https://sputniknews.com/asia/201812101070546808hina-meng-inhumane-treatment/ (Accessed: 12 January 2018)

Sputnik International. (2018) *Analyst on Huawei Case: Incident May Have 'Extremely Unpleasant Consequences* [Online]. Available at: https://sputniknews.com/analysis/201812141070672863-canada-pays-us-malleability-huawei (Accessed: 12 January 2019)

Sputnik International. (2018) *Canada Has Chosen "Soft" Scenario for Ending the Huawei Crisis – Scholars* [Online]. Available at:

https://sputniknews.com/analysis/201812131070649707-canada-china-huawei-crisis/ (Accessed: 15 January 2019)

Stainton, H. (2020) *Positivism and Interpretivism: A Simple Explanation* [Online]. Available at https://tourismteacher.com/positivism-and-interpretivism-simple-explanation/#:~:text=However%2C%20a%20positivist%20approach%20is,a%20positivist%20study%20would%20do [Accessed 28 May 2021]

Standing Committee of the National People's Congress, (2016*) Cybersecurity Law of the People's Republic of China [Effective]* [Online]. Available at: http://www.lawinfochina.com/Display.aspx?LookType=3&Lib=law&Id=22826&SearchKeyword=&SearchCKeyword=&paycode= (Accessed: 23 February 2019)

Stanford Encyclopedia of Philosophy. (2019) *The Pragmatic Theory of Truth* [Online]. Available at https://plato.stanford.edu/entries/truth-pragmatic/ [Accessed: 27 June 2021]

Stat counter (N.D) Mobile Vendor Market Share United States Of America [Online]. Available at: https://gs.statcounter.com/vendor-market-share/mobile/united-states-of-america/2018 (Accessed: 13 September 2020)

Stevens, E. (2021) *The 7 Most Useful Data Analysis Methods and Techniques* [Online]. Available at https://careerfoundry.com/en/blog/data-analytics/data-analysis-techniques/ [Accessed: 4 May 2021]

Stokel-Walker, C. (2021) *The battle for control of Afghanistan's internet* [Online]. Available at: https://www.wired.co.uk/article/afghanistan-taliban-internet (Accessed: 17 January 2022)

Streefkerk, R. (2019) *Inductive vs. deductive reasoning* [Online]. Available at https://www.scribbr.com/methodology/inductive-deductive-reasoning/ [Accessed: 18 June 2021]

Subedi, R. (N.D) *Cyber Security Situation in Nepal* [Online]. Available at https://www.enepalese.com/2015/07/32099.html (Accessed 10 October 2020)

Subramaniam, A and Das, S. (2020) *The Privacy, Data Protection and Cybersecurity Law Review: India* [Online]. Available at https://thelawreviews.co.uk/edition/1001546/the-privacy-data-protection-and-cybersecurity-law-review-edition-7 (7 March 2020)

Sun Media Group. (2016) *Privacy and Data Protection Act under compilation* [Online]. Available at https://en.sun.mv/40808 (Accessed 13 February 2018)

Surendran, P. (2012) 'Technology Acceptance Model: A Survey of Literature', *International Journal of Business and Social Research (IJBSR)*, Volume 2 (4) [Online].
Available at: file:///C:/Users/sm77809/Downloads/161-319-1-SM%20(1).pdf (Accessed 28 May 2020)

Sykes, L. (2020) *Bolivia - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/bolivia-data-protection-overview (Accessed: 23 June 2021)

Tabsh, H. K. B. (2012) 'An investigation of the adoption by banks and acceptance by bank customers of internet banking in the sultanate of Oman', PhD thesis, University of Cardiff Metropolitan University, Cardiff. (16 August 2020)

Taherdoost, H. (2017) 'A review of Technology Acceptance and Adoption Models and theories'*, Science Direc*t, Volume 22 [Online]. Available at https://doi.org/10.1016/j.promfg.2018.03.137 (Accessed 20 August 2020)

Talwar Thakore & Associates. (2020) *Data Protected – India* [Online]. Available at https://www.linklaters.com/en/insights/data-protected/data-protected---india#:~:text=India%20is%20not%20a%20party,or%20the%20Data%20Protection%20Directive.&text=India%20has%20also%20not%20yet%20enacted%20specific%20legislation%20on%20data%20protection (Accessed: 20 June 2020)

Tan, F. and Chung, J. (N.D) 'Validating the Extended Technology Acceptance Model: Perceived Playfulness in the Context of Information-searching Websites' , *CORE* [Online] Available at https://core.ac.uk/download/pdf/56361822.pdf (Accessed: 13 January 2021)

Taylor, R. (2020) *Myanmar - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/myanmar-data-protection-overview (Accessed: 24 February 2021)

Taylor, R. (2020) Myanmar - Data Protection Overview [Online]. Available at: https://www.dataguidance.com/notes/myanmar-data-protection-overview#:~:text=Currently%2C%20there%20are%20no%20specific,to%20data%20protection%20in%20Myanmar.&text=In%20addition%2C%20other%20laws%20related,the%20disclosure%20of%20confidential%20information (Accessed: 5 November 2020)

The Australian Strategic Policy Institute, (2017) *Cyber maturity in the Asia–Pacific region 2017*, Australian Strategic Policy Institute, Australia. Available at: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2017-12/ASPI%20Cyber%20Maturity%202017_AccPDF_FA_opt.pdf?hDv5_AxfVWgwCA_q8it1_H1wkH_HwZjb (18 October 2019)

The Editor. (N.D) 'The Rhetoric of Positivism Versus Interpretivism' *MIS Quarterly*, Volume 28(1) [Online]. Available at: file:///C:/Users/sm77809/Downloads/edcommentsv28n1.pdf [Accessed: 18 June 2021)

The electronic Irish Statute Book (eISB) (N.D) *Data Protection Act 2018* [Online]. Available at: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html (Accessed: 13 October 2020)

The global legal group. (2020) *Pakistan: Data Protection Laws and Regulations 2020* [Online]. Available at https://iclg.com/practice-areas/data-protection-laws-and-regulations/pakistan (Accessed: 13 October 2020)

The Guardian. (2019) *China's ambassador accuses Canada of 'white supremacy' in Huawei CFO arrest* [Online]. Available at: https://www.theguardian.com/world/2019/jan/09/china-ambassador-canada-white-supremacy-huawei (Accessed: 15 February 2019)

The morning, (2020) *Data Protection Bill further delayed* [Online]. Available at http://www.themorning.lk/data-protection-bill-further-delayed/ (Accessed 24 January 2020)

The Open University. (N.D) *3.3 Interpretivism* [Online]. Available at https://www.open.edu/openlearn/education-development/education/engaging-educational-research/content-section-3.3 [Accessed: 23 December 2020]

The Republic Of Ghana, (N.D) *Data Protection Act, 2012* [Online]. Available at: https://cybersecurity.gov.gh/documents/Data_Protection_Act_2012.pdf

The Republic of Uganda, (2019) *The Data Protection and Privacy Act, 2019* [Online]. Available at: https://www.nita.go.ug/sites/default/files/publications/Data%20Protection%20and%20Privacy%20Act%20No.%209%20of%202019.pdf (11 February 2021)

The UN privacy policy group. (2020) *Joint Statement on Data Protection and Privacy in the COVID-19 Response* [Online] Available at https://www.un.org/en/coronavirus/joint-statement-data-protection-and-privacy-covid-19-response (Accessed: 5 April 2021)

The Unwanted Witness. (2020). *Statement* [Online]. Available at: https://www.unwantedwitness.org/government-of-uganda-must-respect-human-rights-in-the-use-of-surveillance-technologies-to-fight-coronavirus-says-unwanted-witness-uganda/ (Accessed: 18 August 2020)

The Verge. (N.D) *Huawei vs. Trump: all the news about the Chinese phone maker's messy relationship with the US* [Online]. Available at: https://www.theverge.com/2019/5/21/18634046/huawei-donald-trump-us-trade-war-china-android-google-ban-5g-future (Accessed: 26 May 2019)

The World Bank (2013) *From Transition to Tranformation: The Role of the ICT Sector in Afghanistan* [Online]. Available at https://www.infodev.org/infodev-files/final_afghanistan_ict_role_web.pdf (Accessed: 21 January 2018)

Thimbleby H. (2013) 'Technology and the future of healthcare'. *Journal of public health research,* Volume 2(3) [Online]. Available at https://doi.org/10.4081/jphr.2013.e28 (Accessed: 23 March 2021)

Tovi, M. D. and Muthama, M. N. (2013) 'Addressing the challenges of data protection in developing countries'. *European Journal of Computer Science and Information Technology*, Volume 1(2) [Online]. Available at: https://www.eajournals.org/wp-content/uploads/ADDRESSING-THE-CHALLENGES-OF-DATA-PROTECTION-IN-DEVELOPING-COUNTRIES.pdf (18 November 2019)

Trueman, C N. (2015) *League Of Nations* [Online] Available at: https://www.historylearningsite.co.uk/modern-world-history-1918-to-1980/league-of-nations/ (Accessed: 29 April 2021)

Tseng, K. Y. (2021) *Taiwan: Data Privacy Comparative Guide* [Online]. Available at: https://www.mondaq.com/privacy/1005652/data-privacy-comparative-guide (2 October 2021)

UN. (N.D) *United Nations Charter (full text)* [Online]. Available at https://www.un.org/en/about-us/un-charter/full-text (Accessed: 13 November 2020)

UN. (2018) *The Application of International Law in Cyberspace: State of Play* [Online]. Available at: https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/ (Accessed date 10 March 2019)

UN. (2017) *Civil Society and Disarmament 2017- Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology A Commentary* [Online]. Available at: https://www.un.org/disarmament/wp-content/uploads/2018/04/Civil-Society-2017.pdf (Accessed: 16 May 2019)

UN High-Level Committee on Management, (2018) *Personal data protection and privacy principles* (Online). Available at: https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf (Accessed: 23 January 2021)

UN System Chief Executives Board for Coordination. (N.D) *Personal Data Protection and Privacy* [Online]. Available at: https://unsceb.org/privacy-principles (Accessed: 23 December 2020)

UNCTAD. (2020) *Data Protection and Privacy Legislation Worldwide* [Online]. Available at https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (Accessed: 15 June 2021)

UNCTAD. (N.D) *Bhutan Rapid eTrade Readiness Assessment* [Online]. Available at: https://unctad.org/es/node/27213 (Accessed: 20 January 2022)

UNICEF. (2020) *Children at increased risk of harm online during global COVID-19 pandemic* [Online]. Available at: https://www.unicef.org/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic (Accessed: 18 January 2021).

UNIDIR, (2021) *Sierra Leone- Cybersecurity Policy- Strategy Document* [Online]. Available at: file:///C:/Users/sm77809/Downloads/Sierra_Leone%20(1).pdf (16 February 2021)

University of Southern California. (N.D) *Research Guides* [Online]. Available at https://libguides.usc.edu/writingguide/quantitative [Accessed: 14 May 2020]

Upreti, R A. (2018) *Individual Privacy Act, 2018* [Online]. Available at http://www.pioneerlaw.com/news/individual-privacy-act-2018-2075 (Accessed: 3 January 2019)

US department of states. (2021) *U.S. Security Cooperation With Poland*, Bureau of political-military affairs [Online]. Available at: https://www.state.gov/u-s-security-cooperation-with-poland/ (Accessed: 12 August 2021)

Utzerath, J. et al. (N.D) *Contact tracing apps in China, Hong Kong, Singapore, Japan, and South Korea* [Online]. Available at: https://digital.freshfields.com/post/102g5my/contact-tracing-apps-in-china-hong-kong-singapore-japan-and-south-korea (Accessed: 12 May 2020)

Venkatesh, V and Davis, F. (2000) 'A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies', *Management Science*, Volume 46 (2) [Online] Available at https://www.jstor.org/stable/2634758 (Accessed 20 August 2020)

Venkatesh, V. and Bala, H. (2008) 'Technology Acceptance Model 3 and a Research Agenda on Interventions' *Decision Science*, Volume 39 (2). Available at https://www.docketalarm.com/cases/PTAB/IPR2014-00023/Inter_Partes_Review_of_U.S._Pat._6482520/09-25-2014-Petitioner/Exhibit-1048-Venkatest_and_Bala_2008/ (Accessed: 3 November 2020)

Vincent, J. (2018) *Don't use Huawei phones, say heads of FBI, CIA, and NSA* [Online]. Available at: https://www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears (Accessed: 3 September 2021)

Vincent, J. (2019) *UK and Japanese carriers press pause on Huawei phone launches* [Online]. Available at: https://www.theverge.com/2019/5/22/18635313/huawei-phones-dropped-uk-carrier-ee-5g-mate-20-launch (Accessed: 3 June 2019)

Virtual Collage. (2018) *What are the main differences between GDPR and the Data Protection Act?* [Online]. Available at: https://www.virtual-college.co.uk/resources/the-differences-between-gdpr-and-data-protection (Accessed: 23 January 2020)

Walia, H. and Chakraborty, S (2020) *India: Data protection laws and regulations 2020* [Online]. Available at https://iclg.com/practice-areas/data-protection-laws-and-regulations/india (Accessed: 10 November 2020)

Wall, A. (2018) *GDPR matchup: South Korea's Personal Information Protection Act* [Online]. Available at: https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/ (Accessed: 13 March 2019)

Wang, X., Liu, Y., & Liu, H. (2020). Examining Users' Adoption of Precision Medicine: The Moderating Role of Medical Technical Knowledge. *International journal of environmental research and public health*, Volume 17(3). Available at: https://doi.org/10.3390/ijerph17031113 (Accessed: 22 January 2021)

Ward, A. (2019) *Microsoft says it notified nearly 10,000 customers that they were cyberattack victims.* [Online]. Available at: https://www.vox.com/2019/7/17/20697851/microsoft-russia-iran-north-korea-10000-election (Accessed: 14 April 2019)

Warren, T. (2019) *ARM cuts ties with Huawei, threatening future chip designs* [Online]. Available at: https://www.theverge.com/2019/5/22/18635326/huawei-arm-chip-designs-business-suspension (Accessed: 30 May 2019)

Weissman, C. G. (2015) *What is an IP address and what can it reveal about you?* [Online]. Available at: https://www.businessinsider.com/ip-address-what-they-can-reveal-about-you-2015-5?r=US&IR=T (Accessed: 17 May 2020)

Wilkinson, D. (2020) *Saudi Arabia - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/saudi-arabia-data-protection-overview (Accessed: 23 May 2020)

Wilson, D and Sutton, A. (2004) ‘Watched Over or Over-watched? Open Street CCTV in Australia’, *The Australian and New Zealand journal of criminology*, Volume (37-Number 2). P.211-230 [Online]. Available at: https://core.ac.uk/download/pdf/141439629.pdf (Accessed: 15 March 2020).

Wolford, B. (N.D) *What are the GDPR Fines?* [Online]. Available at https://gdpr.eu/fines/ (Accessed: 15 August 2020)

Woodward, M. (2021) *16 Countries with GDPR-like Data Privacy Laws* [Online] Available at https://securityscorecard.com/blog/countries-with-gdpr-like-data-privacy-laws (Access: 13 August 2021)

World Bank. (2020) *World Bank Country and Lending Groups* [Online]. Available at: https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups (Accessed: 03 March 2019)

World population review, (2021) *Countries Where Porn Is Illegal 2021* [Online] Available at: https://worldpopulationreview.com/country-rankings/countries-where-porn-is-illegal (Accessed: 17 January 2021)

Yannakogeorgos, P. A. (2016) *Strategies for Resolving the Cyber Attribution Challenge*, Air University Press, Alabama. Available at: https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEORGOS_CYBER_TTRIBUTION_CHALLENGE.PDF (12 May 2019)

Young, I. (2018) *The United States is using a presentation Huawei CFO Sabrina Meng Wanzhou gave to HSBC to argue she's guilty of breaching sanctions* [Online]. Available at: https://www.businessinsider.com/powerpoint-proves-huawei-cfo-wanzhou-guilty-says-us-2018-12?r=US&IR=T (Accessed: 13 June 2020).

Yu, Y. (2019) *A Huawei-made operating system: How feasible is it?* [Online]. Available at: https://asia.nikkei.com/Spotlight/Huawei-crackdown/A-Huawei-made-operating-system-How-feasible-is-it2 (Accessed: 8 June 2019)

Yuldashev, N. (2020) *Turkmenistan - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/turkmenistan-data-protection-overview (Accessed: 14 March 2020)

Yuriutomo, I D. (2020) *Indonesia - Data Protection Overview* [Online]. Available at: https://www.dataguidance.com/notes/indonesia-data-protection-overview (Accessed: 16 February 2021)

Zammit, A. J. (2021) *Malta - Data Protection Overview* [Online]/. Available at: https://www.dataguidance.com/notes/malta-data-protection-overview (Accessed: 9 August 2021)

Zhang, D. (2018) Big Data Security and Privacy Protection, *Advances in Computer Science Research*, volume 77. Available at: file:///C:/Users/sm77809/Downloads/25904185.pdf (Accessed: 2 June 2020)

Zarsky, T. (2017) 'Incompatible: The GDPR in the Age of Big Data', Seton Hall Law Review Vol. 47 Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646 (Accessed: 23 May 2020)

Zhou, L., Dai, L., and Zhang, D. (2007) 'Online shopping acceptance model - A critical survey of consumer factors in online shopping', *Journal of Electronic Commerce Research*, Volume 8(1) [Online] Available at https://www.researchgate.net/publication/228889606_Online_shopping_acceptance_model_-_A_critical_survey_of_consumer_factors_in_online_shopping (Accessed: 23 November 2020)

ZICO law (2019) *ASEAN industries series* [Online]. Available at: https://zico.group/wp-content/uploads/resources/asean_insiders/ASEAN_Insiders-PDPA.pdf (15 June 2020

Žukauskas, P., Vveinhardt, J., and Andriukaitienė, R. (2018) 'Philosophy and Paradigm of Scientific Research' *Management Culture and Corporate Social Responsibility* [Online]. Available at DOI: 10.5772/intechopen.70628 [Accessed: 23 August 2020]

ANNEXURE A

Your perspective on challenges faced in accepting and implementing global data security policies.

Personal statement

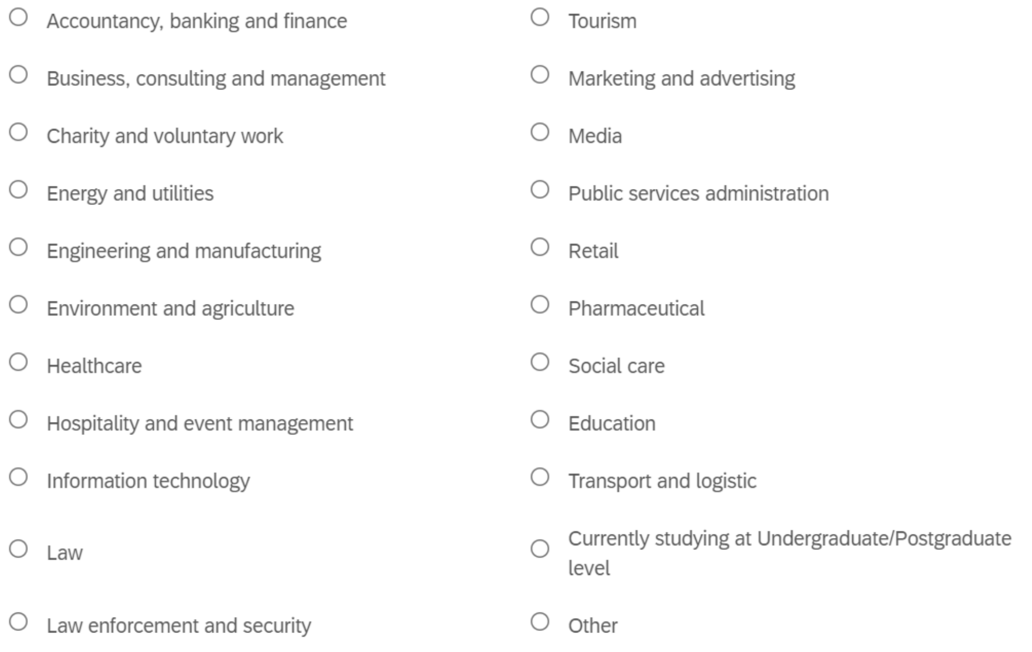
I confirm my acceptance of your invitation to participate in this research on a voluntary basis. I understand that the answers I give will be kept anonymously for the duration of the project and will be stored in the Cardiff Metropolitan University provided OneDrive (Business) storage in encrypted form until December 2023. If you have further questions, please do contact the primary researcher Vibhushinie Bentotahewa by email to v.bentotahewa@outlook.cardiffmet.ac.uk and, use the same email if you wish us to remove your data from the study, at any time before the commencement of the analysis.

Agree □ Disagree □

This questionnaire consists of two sections. First section consists of personal information and second section consists of subject specific questions.

Personal questions

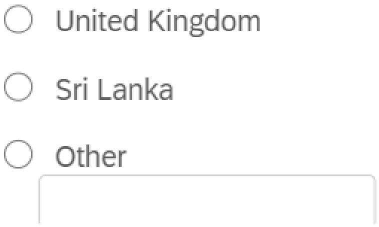
I. Which of the following best describes your current sector of employment



○ Accountancy, banking and finance
○ Business, consulting and management
○ Charity and voluntary work
○ Energy and utilities
○ Engineering and manufacturing
○ Environment and agriculture
○ Healthcare
○ Hospitality and event management
○ Information technology
○ Law
○ Law enforcement and security
○ Tourism
○ Marketing and advertising
○ Media
○ Public services administration
○ Retail
○ Pharmaceutical
○ Social care
○ Education
○ Transport and logistic
○ Currently studying at Undergraduate/Postgraduate level
○ Other

If OTHER, Please specify

II. In which country is your organisation based

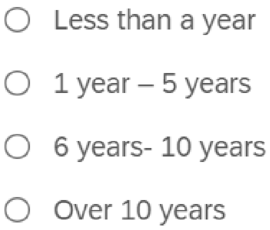


○ United Kingdom

○ Sri Lanka

○ Other

III. Experience in your current profession



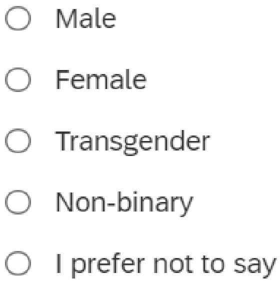
○ Less than a year

○ 1 year – 5 years

○ 6 years- 10 years

○ Over 10 years

IV. What gender do you identify with?



○ Male

○ Female

○ Transgender

○ Non-binary

○ I prefer not to say

V. What age range do you do you fall into?

○ 18-25

○ 26-35

○ 36-45

○ 46-55

○ 56-65

○ 65+

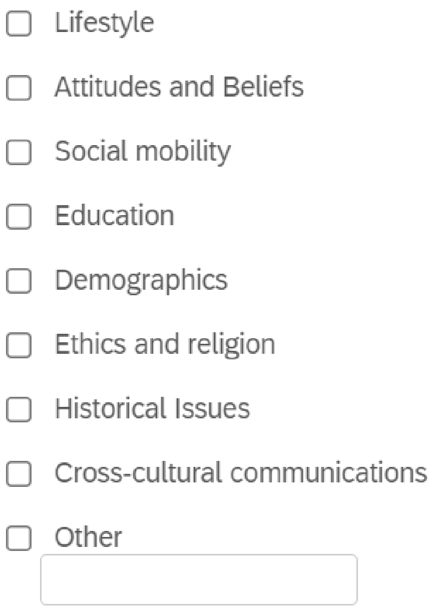
○ I prefer not to say

Subject specific questions

Question	**Strongly agree**	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**	**I do not have an idea**
My organisation relies on technology to run the business.						
My organisation has an allocated budget for information security.						
I regularly do receive security awareness training.						
Do you have a good understanding of cyber-attacks affecting you, general public and organisations across the globe						
Social differences (e.g. Age, Gender and other) play a vital role in accepting and implementing data privacy and security policies.						
Economic differences (e.g. Developed, Developing, Under developed and other) play a vital role in accepting and implementing data privacy and security policies.						
Political differences (e.g. Democratic, Republic, Monarchy, Communist Dictatorship and other) play a vital role in accepting and implementing data privacy and security policies.						
Mutual trust amongst countries is important in accepting and implementing global data privacy and security policies.						

Privacy of individuals is crucial in accepting and implementing global data privacy and security policies, laws and regulations.						
It is useful to have previous experience in policy development with other countries for the purpose of accepting and implementing data privacy and security policies.						
Cyber threats pose potential risks to national security.						
Acceptance and implementation of global data privacy and security policies, laws and regulations faces many challenges.						

I. What social differences play a vital role in accepting and implementing data privacy and security policies? (Not limited to single answer)



□ Lifestyle

□ Attitudes and Beliefs

□ Social mobility

□ Education

□ Demographics

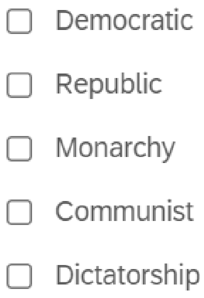
□ Ethics and religion

□ Historical Issues

□ Cross-cultural communications

□ Other

II. Which political differences play a vital role in accepting and implementing data privacy and security policies? (Not limited to single answer)



□ Democratic

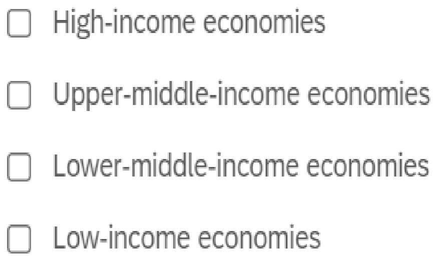
□ Republic

□ Monarchy

□ Communist

□ Dictatorship

III. Which economies play a vital role in accepting and implementing data privacy and security policies? (Not limited to single answer)



□ High-income economies

□ Upper-middle-income economies

□ Lower-middle-income economies

□ Low-income economies

IV. Do you believe it is beneficial to implement a global data privacy and security policy?

Yes □ No □

Give reasons for your answer

…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
……………………

V. Do you receive constant support from the organisation to protect personal information about you and your clients?

Yes □ No □

If YES, Specify the support you received from the organisation

…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
……………………

VI. In accepting and implementing a global data privacy and security policies, what would you consider to be the priority?

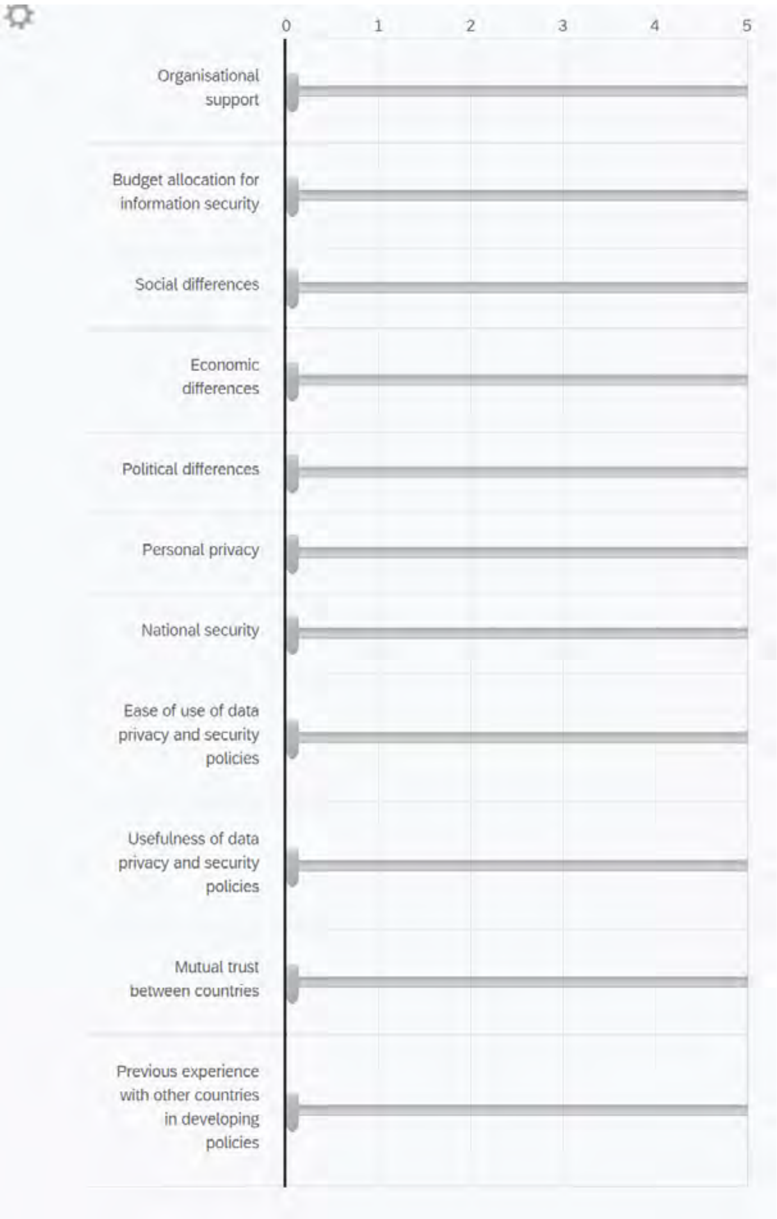
Protecting personal data security and privacy □

National security □

Justify your answers

…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
……………………

VII. If you are to accept and implement a global data privacy and security policies what factors would you consider the most? (0- Do not consider, 5- Consider the most)


0
1
2
3
4
5
Organisational support
Budget allocation for information security
Social differences
Economic differences
Political differences
Personal privacy
National security
Ease of use of data privacy and security policies
Usefulness of data privacy and security policies
Mutual trust between countries
Previous experience with other countries in developing policies

VIII. What other factors would you consider?
……………………………………………………………………………………
……………………………………………………………………………………
……………………………………………………………………………………
……………………………………………………………………………………
…………………………………

Thank you for taking your time to complete this survey.

ANNEXURE B

The purpose of the questionnaire is to collect the perception of the individual about the challenges faced by countries in accepting and implementing global data privacy and security policy. That would allow the researcher to develop the model based on the evaluation of the important parameters identified in the literature review. The rationale behind including each question is shown below.

Question	Concept associated with the question	The purpose of the question	Literature
My organisation relies on technology to run the business.	Dependency on ICT	To understand whether the organisation relies on technology to perform their daily tasks, and if solely not dependent on technology, vulnerability to cyberattacks will be low, and that will determine the benefits of cyber security and staff training.	Concept added to the model by the researcher following a comprehensive literature review.
Do you have a good understanding of cyber- attacks affecting you, general public and organisations across the globe	Security awareness	To get an understanding on whether people realise the overall impact of cyber-attacks and likely losses in the short, medium, and in the long term, and also whether they will actively take part in developing preventive measures to avoid occurrence of such incidents.	Concept added to the model by the researcher following a comprehensive literature review.
I regularly do receive security awareness trainings.	Organisational support (Top management support)	This is to get an idea of what level of support if any is given to the employees by the organisation. The	The TAM by McFarland and Hamilton (2006).

		literature suggests that the computer user has a crucial role to play in protecting their organizational network. That makes the user a key player and should have a good understanding of risks and vulnerabilities, hence should be given regular training to the employees as appropriate.	
My organisation has an allocated budget for information security.	Information security budget	To get an understanding about the cyber security readiness in organisations. Cyber-attacks are unpredictable, and the organisations could be vulnerable and caught unaware. Therefore, organisations should have a separate budget allocation in place to cover replacement of any equipment, enhance their security systems and staff training.	Concept added to the model by the researcher following a comprehensive literature review.
Social differences (e.g. Age, Gender and other) play a vital role in accepting and implementing data privacy and security policies.	Social differences (external variables)	This is to get an understanding of how social differences play a crucial role in accepting and implementing global data security policies. It has been observed that, in Asia, notions of obscenity and pornography/erotica vary widely from country to country. For example, compared to 15	The unified theory of Acceptance and Use of Technology , Technology Acceptance Model (TAM) (Davis,1989), Final version of TAM (Venkatesh and Davis, 1996).

		people in China, Taiwan and Hong Kong, the tolerance level to erotic materials might be higher in Japanese. Islamic countries have a much less tolerant approach to obscene materials. Many have a have a 'zero tolerance' approach where any form of pornography is considered obscene.	
Economic differences (e.g. Developed, Developing, Under developed and other) play a vital role in accepting and implementing data privacy and security policies	Economic differences (external variables)	To get an understanding of how economic differences play a crucial role in accepting and implementing global data security policies. In implementing global data security policies, it is important to consider the economic differences in countries as it would otherwise be very difficult for developing and under developing countries to accept those global data security policies, due to lack of resources to comply with the standards.	Technology Acceptance Model (TAM) (Davis,1989), Final version of TAM (Venkatesh and Davis, 1996).
Political differences (e.g. Democratic, Republic, Monarchy, Communist Dictatorship and other) play a vital role in accepting and implementing data privacy and security policies.	Political differences (external variables)	To get an understanding of how social differences play a crucial role in accepting and implementing global data security policies. When implementing a global data security policy, it is crucial to have a balance	Technology Acceptance Model (TAM) (Davis,1989), Final version of TAM (Venkatesh and Davis, 1996).

		between communist and democratic principles. For instance, China and few other countries refused to ratify the Budapest Convention for two main reasons, one being their non-participation in the drafting process, the other being the belief that it would infringe on their sovereignty.	
It is useful to have previous experience in policy development with other countries for the purpose of accepting and implementing data privacy and security policies.	Prior information security experience (Prior experience)	This is to understand whether the ongoing relations with other countries matter in developing a global data security policy. It would be easier to reach consensus and reach agreements with nations having amicable diplomatic relations amongst them. On the other hand, if they have had a chance to take part in policy implementing dialogues the countries would be able to use that experience in developing a global cyber legislation.	The TAM by McFarland and Hamilton (2006), Extended Technology Acceptance Model (TAM2), (Venkatesh and Davis, 2000) The unified theory of Acceptance and Use of Technology (Venkatesh et al., 2003), TAM3 (Venkatesh and Bala, 2008).
Mutual trust amongst countries is important in accepting and implementing global data privacy and security policies.	Trust	This is to get an understanding whether trust is important in developing a global data security policy. Countries tend to develop good relations with each other based on trust. Therefore, trust is	Concept added to the model by the researcher following a comprehensive literature review.

		crucial in developing global decisions.	
Privacy of individuals is crucial in accepting and implementing global data privacy and security policies, laws and regulations.	Privacy	This is to understand the importance of privacy in implementing and accepting global data security policies. Each and every country particularly interested in protecting privacy of individual and to that end most of the countries have active regulations in place issuing orders and guidelines to protect privacy of people. Therefore, even in developing a global data security policy, the researcher believes that privacy is crucial.	Concept added to the model by the researcher following a comprehensive literature review.
Cyber threats pose potential risks to national security.	National security	This is to understand whether organisations see cyber threats as a national security threat. Originally under national security countries did focus on protection against military attack, however after the 9/11 attack national security is now include non-military dimensions, such as terrorism, economic security, energy security, environmental security, food security, cyber-security etc.	Concept added to the model by the researcher following a comprehensive literature review.
Acceptance and implementation of	Perceived ease of use of	To understand whether people find it	Technology Acceptance

global data privacy and security policies, laws and regulations faces many challenges.	international cyber laws (Perceived ease of use)	challenging to accept and implement global data security policies. If global data policies are not aligned with national data security policies, it would become challenging to accept and implement new policies. Therefore, it is necessary to have a good understanding of social, political and, economic differences in countries before implementing global data security policies.	Model (TAM) (Davis,1989), The TAM by McFarland and Hamilton (2006), Final version of TAM (Venkatesh and Davis, 1996), TAM3 (Venkatesh and Bala, 2008).
Do you believe it is beneficial to implement a global data security policy	Perceived usefulness of international cyber laws (Perceived usefulness)	This is to understand whether people do believe that it is beneficial to have a global data security policy. If having a global data security policy is not considered a priority, it is questionable whether people would be inclined to accept and implement one. In such situations, it is questionable as to how they propose to protect people's privacy especially in cross boarder data transfers.	Technology Acceptance Model (TAM) (Davis,1989), The TAM by McFarland and Hamilton (2006), Final version of TAM (Venkatesh and Davis, 1996), TAM3 (Venkatesh and Bala, 2008).
Do you receive constant support from the organisation to protect personal information about you and your clients?	Organisational support	Privacy is a key priority in data security. Organisations do collect vast amount of personal information using different means, and	The TAM by McFarland and Hamilton (2006).

		that requires companies to have a proper mechanism in place to safeguard such information held by them.	
In accepting and implementing a global data privacy and security policy, what would you consider to be the priority?		According to the researcher, key priority in implementing and accepting a global data security is to ensure national security and the privacy of people. The question is to understand whether the researcher's reading is the majority's opinion.	
What factors would you consider in accepting and implementing a global data privacy and security policy		To gather their personal views based on their knowledge, views and experience.	
It is useful to have a global data privacy and security policy	Attitude	To understand whether people do believe that it is useful to have a global cyber legislation in place. If yes, people will make a positive contribution.	Technology Acceptance Model (TAM) (Davis,1989).

ANNEXURE C.1

Could Huawei jeopardise Five Eyes partnership?

The contents of this document in the form of an opinion paper was submitted to the Cardiff Met symposium-2019.

Bentotahewa, V. Hewage, C. and Williams, J. (2019) Could Huawei jeopardise Five Eyes partnership?, *CardiffMet Symposium*, Cardiff Metropolitan University, Cardiff, 2019.

Huawei is a Chinese based major high-tech company trading in more than 70 countries providing telecommunications services (Leskin, 2018). In the Smartphone circuit, it has surpassed Apple to become the world's second largest smartphone seller and only behind Samsung (Leskin, 2018). In recent months the company has been subjected to a barrage of accusations by the US, and has called for actions to ban Huawei claiming it posed potential security threats (Lecher and Brandom, 2019). Huawei has also come under criticism from the international community.

China's National Intelligence Law and National Cyber Law legally oblige Chinese entities to cooperate with the government, but Huawei has emphatically stated that neither Beijing had any influence over Huawei nor had they received any request from the Chinese government for access to information (Kharpal, 2019, Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice). Huawei has also reaffirmed that it was under no obligation to provide information to the government except paying due taxes, and that it operated as an independent company (Karl, N.D).

Huawei row has gone beyond boundaries, and the US initiated campaign against the company has enticed Australia, New Zealand, Canada, India, Japan, France, Germany and even the Czech Republic express their concerns about security issues (International the news, 2018). Of the Five Eyes nations Australia and the US are the two countries to have banned Huawei from their 5G networks, and similar action is under consideration by Canada and New Zealand (BBC, 2019, Huawei: Which countries are blocking its 5G technology?).

The UK already uses some Huawei equipment in its existing 3G, and 4G network (Griffin, 2018). British Telecom (BT), the largest mobile network provider in the UK with whom Huawei has been in long standing (17years) collaboration partnership, providing Huawei equipment to BT Mobile network (Griffin, 2018). However, US calls for a boycott of Huawei technology within the Five Eyes intelligence-sharing alliance (Tobin, 2019). UK has indicated its willingness to grant permission for the use of Huawei technology in "non-core" parts of the country's new 5G infrastructure (Keane, 2021). However, the chair of the foreign affairs select committee expressing his concerns has said that any involvement with Huawei in the UK 5G telecoms network would erode the trust between the UK and Five Eyes (Sabbagh, D. 2019).

Despite the US stand on Huawei, the UK decision to use Huawei equipment in 5G network comes as a surprise. That raises the question whether the implications of Brexit has played role UK reaching their decision. A member of the UK defence think tank Rusi has stated that if Huawei was banned, we would not know to what extent China might refuse to do business with us in other fields, and the timing for that would not be great as the more attention would be placed on the potential economic impacts of Brexit (BBC, 2018, Huawei: Why has UK not blocked Chinese firm's 5G kit?).

The Five Eyes relationship is built on trust. But the decision to allow Huawei involvement in the 5G network in the UK appeared to have resulted in disagreements between Five Eye partners. Also US administration is expected to exert further pressure on Britain to reconsider the decision (Sabbagh and Boffey, 2019). However, Five Eyes cybersecurity chiefs have played down suggestions of a split in the alliance, at the same time UK has been warned against compromising regional security (Clarke, 2019). Britain should seriously consider whether it would be wise to jeopardise its partnership with Five Eyes and compromise national security if the UK- Huawei deal was to go through.

Britain maintains a long standing partnership with Five Eyes and share a substantial amount of intelligence, including highly sensitive signals intelligence (SIGINT) (Corera, N.D). That makes US jittery about UK's decision to use Huawei equipment in their 5G network. US also believes that Huawei would use its infrastructure to spy on users (Pancevski, 2020) and as a result there is likely to be limited sharing of intelligence within the group. If Five Eyes were no longer seen as relevant, the group members may seek bilateral arrangements which would lead to break up of Five Eyes long-standing intelligence sharing partnership. However, one needs to be satisfied that the US concerns genuinely are in the interest of global security, and are not mere speculations to back up their propaganda on the ongoing trade war between US and China.

Western aligned countries, bonded by security and commercial ties have ensured secure flow of information across the globe, and it is important to sustain that relationship to meet the challenges of cyber threats. If the Five Eyes partnership were to become strained as a result of UK using Huawei equipment, it would undermine the unity of the members and sharing of intelligence information.

References

BBC, (2018) *Huawei: Why has UK not blocked Chinese firm's 5G kit?* [Online]. Available at: https://www.bbc.co.uk/news/technology-46370014 (Accessed: 20 May 2019)

BBC, (2019) *Huawei: Which countries are blocking its 5G technology?* [Online]. Available at: https://www.bbc.co.uk/news/world-48309132 (23 May 2019)

Clarke, H. (2019) *Five Eyes spies play down split as 'Huawei leak' roils UK government* [Online]. Available at: https://www.scmp.com/news/world/europe/article/3007586/five-eyes-spies-play-down-split-huawei-leak-roils-uk-government (Accessed: 3 May 2019)

Corera, G. (N.D) *Diary reveals birth of secret UK-US spy pact that grew into Five Eyes* [Online]. Available at: https://www.bbc.co.uk/news/uk-56284453 (Accessed: 2 May 2019)

Griffin, A. (2018) *Huawei phone equipment in UK to be dismantled amid fears they could be used by China to spy on people* [Online]. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/huawei-5g-phone-masts-equipment-bt-ee-internet-data-chinese-government-a8669076.html (20 December 2018)

International the news (2018) *Huawei rejects Western security fears* [Online]. Available at: https://www.thenews.com.pk/print/407691-huawei-rejects-western-security-fears (Accessed: 14 January 2019)

Karl, S. (N.D) *No, Huawei isn't built on Chinese state funding* [Online]. Available at: https://www.huawei.com/en/facts/voices-of-huawei/no-huawei-isnt-built-on-chinese-state-funding (Accessed: 24 March 2019)

Keane, S. (2021) *Huawei ban timeline: Chinese company settles patent lawsuits with Verizon* [Online]. Available at: https://www.cnet.com/tech/services-and-software/huawei-ban-timeline-chinese-company-settles-patent-lawsuits-verizon/ (Accessed: 23 July 2021)

Kharpal, A. (2019) *Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice* [Online]. Available at: https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html (Accessed: 5 April 2019)

Lecher, C. and Brandom. R. (2019) *Is Huawei a security threat? Seven experts weigh in* [Online]. Available at: https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g (Accessed: 14 April 2019)

Leskin, P. (2018) *Here's everything you need to know about Huawei, the Chinese tech giant whose founder's daughter was arrested and could spark an all-out trade war* [Online]. Available at: https://www.businessinsider.com/huawei-meng-wanzhou-trump-china-trade-war-2018-12?r=US&IR=T (Accessed: 12 January 2019)

Pancevski, B. (2020) *U.S. Officials Say Huawei Can Covertly Access Telecom Networks* [Online]. Available at: https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256 (Accessed: 25 February 2020)

Sabbagh, D. and Boffey, D. (2019) *US to put pressure on UK government after leaked Huawei decision* [Online]. Available at: https://www.theguardian.com/politics/2019/apr/26/huawei-leak-inquiry-philip-hammond-national-security-council (Accessed: 28 April 2019)

Sabbagh, D. (2019) *Tory MPs seek to overturn May's Huawei supply decision* [Online]. Available at: https://www.theguardian.com/technology/2019/apr/24/tory-mps-seek-to-overturn-mays-huawei-supply-decision (2 May 2019)

Tobin, M. (2019) *Huawei ban: Australia becomes increasingly isolated among Five Eyes partners if UK includes Chinese firm in 5G network* [Online]. Available at: https://www.scmp.com/week-asia/geopolitics/article/3007810/huawei-ban-australia-becomes-increasingly-isolated-among-five (Accessed: 3 May 2019)

ANNEXURE C.2

WhatsApp chaos: Only way forward is a comprehensive data security and privacy law

This was published in the info-security magazine as an opinion paper and it takes into account the new security policy introduced by WhatsApp.

Bentotahewa, V. Hewage, C. and Williams, J. (2021) *WhatsApp Chaos: Time for a Comprehensive Data Security and Privacy Law?* [Online]. (Available on https://www.infosecurity-magazine.com/next-gen-infosec/whatsapp-chaos-privacy-law/)

WhatsApp hit the headlines with the launch of its new terms and conditions, a policy agreement that the users are obliged to accept, if they wished to continue using the app after 8 February 2021 deadline (Cuthbertson, 2021). The instant user reaction has been one of dismay within days of the initial message appeared on their accounts asking them to review existing privacy choices and agree to the changes outlined in the new policy. The proposed changes specified by WhatsApp which is now under Facebook ownership, have come under scrutiny by media and app experts. The most concerning issue is that Facebook, under its own privacy policy would be having access to millions of user information (metadata) from WhatsApp, making it one of the biggest media organisations to collect, process and store 'big data' by design. If agreed to the proposed changes, personal information will be shared with Facebook, and if rejected the user accounts on WhatsApp will become void by the set deadline. This is a dilemma the users are having to grapple with, and millions of users have instantly ditched WhatsApp in preference to alternative apps that are readily available free, with hassle-free download facility via app stores. This backlash has prompted Facebook to put on hold proposed policy changes until May (Statt. 2021), but it is still not clear whether Facebook will shift its position.

This is growing concern and is arguably is not in the public interest, and not in line with privacy policies of many nations, specially GDPR applicable ones, the UK and EU member states. However, it must be said there is nothing new about what had been going on and what is envisaged from the new privacy policy. Ever since WhatsApp was acquired by Facebook (in 2014), it had access to variety of user information already available on WhatsApp. These include, active phone number, preferential choices, interests, and in addition user mobile device information, user IP address (Newman, 2021).

There is also another side to all this, as has been explained by WhatsApp that the updates only refer to business communications and does not impact on private end-to-end encrypted conversation between friends or family, and the existing encryptions will remain unchanged (Newman, 2021). It also claims that sharing information with Facebook is a part of the company policy to introduce a payment capability facility for the user when making purchases from sponsored trading outlets and organisations (WhatsApp, N.D). However, the completion of the process is mainly conditional on the user agreeing to company privacy policy terms and conditions, but it is hard to believe that every user was aware of pages of ‘small print’ used in its privacy policy statement about how, why and with whom and how long for, it shares metadata.

Facebook in its own defence claims that revenue from advertising on Facebook is essential for the company to function without imposing subscription charges from the user of its apps, and insists that information they hold will help operate, provide, improve, understand, customise, support, and market their services and offers. May be so, but the longstanding customer preference for WhatsApp will be tested in time when the subscribers turn to other competitive apps with similar features provided completely free to the user, in many cases without conditional agreements and privacy implications.

WhatsApp has end to end encryption (Newman, 2021) and it is free. Therefore, it attracted subscribers billions in number. However, as WhatsApp proposed privacy policy story began to unfold in the public domain, the user concerns began to rise and their reaction that followed was not good news for the company. The users wasted no time in downloading similar apps, mainly Signal and Telegram from other sources, and the numbers abandoning WhatsApp rang alarm bells in Facebook HQ. The worst to come was the rise in popularity of ‘Signal’ in the regions of the world, and it took the top spot for the most downloaded app from the play store (Kharpal, 2021).

WhatsApp is also facing legal challenges as WhatsApp's updated privacy policy on the grounds that it interferes in user surveillance and threatens India's security. India has filed a petition against WhatsApp saying it is jeopardizing national security by sharing, transmitting, and storing user data in another country with the information thus governed by foreign laws (Jain and Moynihan 2021). Pakistan- Federal Minister for Science and

Technology has said that the government was making efforts to introduce a strong data protection law to protect citizens' privacy with WhatsApp chaos (The Express Tribune, 2021).

WhatsApp users within the European region, which includes the UK, are receiving a separate privacy policy to those elsewhere in the world (Sky News, 2021), and there is a clear difference in the policy note. It is also worth noting that data sharing with Facebook is extremely limited for European users due to stronger user privacy protections in the EU. That is because the EU's General Data Protection Regulation (GDPR) is one of the strictest in the world and ensures that consumers have the full rights on their data and how that data is processed and have the right to even demand erasure of information. Companies bound by the European Union's privacy laws are liable for fines as much as 4% of global annual revenue if found in breach of the EU block laws (Wolford, N.D). Also, the GDPR highlights the service providers to collect only essential information that is necessary to provide the services.

The regulatory vacuum is a real concern in terms of data protection as most of the countries are in the process of developing their legal mechanisms. But for most of the other countries even though they are in the process of developing data protection laws until the Personal Data Protection Bill becomes law, it is hard to police technology companies on how user data should be processed. It is clear the users have limited options, and the countries should take protection of privacy rights seriously and come up with a personal data protection law. However, the users who are not conversant with data privacy implications might overlook the risks in downloading and using these popular messaging apps free of charge. Therefore, it is not too late to act, and introduce sound privacy legislation now to ensure that app providers have meaningful clear terms and conditions that will allay doubts and suspicions in the minds of the user. This is also one way to promote competition in the market and allow wider use choice.

References

Cuthbertson, A. (2021) *Whatsapp forces users to agree to share private data including phone number with Facebook* [Online]. Available at https://www.independent.co.uk/life-style/gadgets-and-tech/whatsapp-update-new-privacy-policy-b1783880.html (Accessed: 15 January 2021)

Statt, N. (2021) *WhatsApp to delay new privacy policy amid mass confusion about Facebook data sharing* [Online]. Available at: https://www.theverge.com/2021/1/15/22233257/whatsapp-privacy-policy-update-delayed-three-months (Accessed: 26 January 2021)

Newman, L. H. (2021) *WhatsApp Has Shared Your Data With Facebook for Years, Actually* [Online]. Available at: https://www.wired.com/story/whatsapp-facebook-data-share-notification/ (Accessed: 17 January 2021).

WhatsApp. (N.D) *Shopping, Payments, and Customer Service on WhatsApp* [Online]. Available at: https://blog.whatsapp.com/shopping-payments-and-customer-service-on-whatsapp (Accessed: 2 February 2021)

Kharpal. A. (2021) *Signal and Telegram downloads surge after WhatsApp says it will share data with Facebook* [Online]. Available at: https://www.cnbc.com/2021/01/12/signal-telegram-downloads-surge-after-update-to-whatsapp-data-policy.html (Accessed: 23 January 2021)

Jain, R. and Moynihan, Q. (2021) *WhatsApp's changes to personal data violate users' privacy and pose a threat to national security, according to a court filing in India, the app's biggest market* [Online]. Available at: https://www.businessinsider.com/whatsapp-threatens-user-privacy-india-court-filing-2021-1?r=US&IR=T (Accessed: 4 February 2021).

The Express Tribune. (2021) *Data protection law on the cards in Pakistan after WhatsApp policy shift* [Online]. Available at: https://tribune.com.pk/story/2279417/data-protection-law-on-the-cards-in-pakistan-after-whatsapp-policy-shift (Accessed: 16 January 2021).

Sky News. (2021) *WhatsApp is updating its privacy rules - here's what you need to know* [Online]. Available at: https://news.sky.com/story/whatsapp-is-updating-its-privacy-rules-heres-what-you-need-to-know-12185162 (Accessed: 13 January 2021)

Wolford, B. (N.D) *What are the GDPR Fines?* [Online]. Available at https://gdpr.eu/fines/ (Accessed: 15 August 2020)

ANNEXURE C.3

BREXIT FOR EXIT; Is there an effect on cyber security?

This document was submitted to the Cardiff Met symposium-2020 as an opinion paper.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) BREXIT FOR EXIT; Is there an effect on cyber security?, *CardiffMet Symposium*, Cardiff Metropolitan University, Cardiff, 2019.

After intense negotiations over two years, Brexit has reached a point of no return. UK Prime Minister Theresa May suffered a setback when the Brexit proposal agreed with the EU was overwhelmingly defeated in a parliamentary vote putting the entire Brexit process into an impasse. It is very likely that the Brexit process will to go down to the wire.

Reversing the clock back, the main focus of Brexit negotiations had been on the key issues of the Brexit vision and the popular agenda heading the list whilst other equally important issues had been overlooked. One area is security, particularly cyber threats, a global phenomenon. This lack of focus has drawn the attention of senior members of the security services and other experts, raising concerns about the impact of Brexit on national security, particularly Cyber activities, and their views cannot be ignored. As suggested by the experts, the post Brexit skill shortages are likely to impact on all sectors of life in the UK, and Cyber expertise is one such area where skilled labour , information sharing and regulatory compliance play a crucial part (Winder, 2018), yet there are no known indications as to how future collaborations would be maintained.

The Minister for the Digital Economy has described UK as a world-leading digital economy, and cyber security has been made a top priority by the government (Government of UK, 2016, Two thirds of large UK businesses hit by cyber breach or attack in past year). UK has also been working closely with EU partners to develop Cyber security strategy (King, 2020). This suggests that UK is committed to strengthen European cyber-security but would that last after Brexit, and could there be any significant changes.

1.0 Will there be an immediate effect on skilled labour?

It is hard to predict the effect on skilled labour and expertise, specially the EU migrants, after Brexit. In November 2015, cyber-security was added to the UK skills shortage register, allowing people outside UK to apply for a working visa, provided they had met the skill criteria (Sharf, 2014)

A senior cyber intelligence analyst at Barclays has pointed out that cyber-security already faces a skills shortage, and difficulties in finding qualified candidates (Palmer, 2018, Cybersecurity and Brexit: What does it mean for the fight against hackers?). This suggests that skilled staff shortages had been there even before the start of Brexit campaign. In anticipation of further shortages of skilled professionals after Brexit, as a precautionary measure, last year GCHQ had hired 800 people and BT had 900 for entry-level cyber-security jobs (Sharf, 2014).

2.0 Would there be any changes to data sharing?

The pattern of cyber-attacks makes it clear that that those responsible are well organised and always one step ahead, and their origins and identification are hard to trace, therefore the need to have an effective mechanism to tackle this menace cannot be underestimated. To achieve that, data sharing between nations and security agencies becomes crucially important as no country can address these issues on their own. A research fellow attached to Imperial College Business School has said that in her view co-operation in cyber security will continue after Brexit, also that many international communications cables to Europe land bypass UK, and it would not be possible to replace those without additional cost irrespective of the final deal (Winder, 2018).

UK collaborates with EU organisations such as Europol and the European Cybercrime Centre (EC3) in sharing data and shaping EU cyber-security policy and regulation (Black et al., 2017, P.124). In all probabilities, UK would end up with limited options, to retain its full membership of Europol and get access to European security databases, to reapply for a second-tier membership or to seek a supplementary agreement with Europol (Black et al., 2017, P.124). If however UK were to be left out without closer links after Brexit, the countries could become exposed to cyber threats as the hackers are always on the lookout for vulnerable targets. There is of course the option to use other routes, NATO, United Nations Security Council and the Five eyes. In addition, UK has already looked for partners outside the EU for data sharing, for instance TAC security, an Indian company who has announced that they have a special service in place to fight UK Cyber War (Sahoo, 2016). In addition, TAC-CERT (Cyber Emergency Response Team) the newest service is about to be launched in the UK (Sahoo, 2016).

3.0 Is data protection in question?

In January 2012, the European Commission set out plans for data protection reform across the European Union in order to make Europe fit for the digital age (Palmer, 2019, Everything you need to know about the new general data protection regulations) Britain as a member followed suit in line with the General Data Protection Regulation (GDPR). Any organisation who have clients or market in any part of the EU are under obligations to comply with EU regulations, therefore UK organisations continuing or willing to trade with any EU country after Brexit will be bound by GDPR terms and conditions (Sharf, 2014). UK government has said that GDPR will still work for the benefit of UK despite being outside the EU (Sharf, 2014). Recently UK reformed its Data Protection Act 1998 in line with the GDPR. This has been underpinned by the UK Information Commissioner's Office and has given a pledge not to abandon previous commitments and that British data protection will stay aligned to GDPR (Black et al., 2017. P.132). This could be taken as an indication of the government intention to make people feel confident about security after Brexit. It is highly unlikely that there would be any changes to the applicability of GDPR, changes if any would not be forthcoming immediately.

The most likely scenario is UK will leave EU on 29 of March with uncertainties hanging over Brexit. According to the head of technology at the National Crime Agency's National Cyber Crime Unit, there is no visible impact on their operations and it is too early to make predictions at this stage (Palmer, 2018). The cyber-attacks in reality will continue to be a phenomenon despite the final outcome of Brexit.

It is highly unlikely there would be an immediate impact on cyber security, however there could be possible implication, in the long terms. With the aim of becoming a world leader in cyber security, UK government plans to invest £1.9 billion over the next five years (Black et al., 2017. P.129) tapping into the savings from the EU budget. In addition the government has established a new National Cyber Security Centre (NCSC) along with a new five-year National Cyber Security Programme (Black et al., 2017. P.129). It is reported that even though the new strategy does not directly address the issue of Brexit, it does outline the UK's intent to continue to work closely with international partners, including the EU and other organisations such as the UN, NATO, G20, Commonwealth and Organization for Security and Co-operation in Europe (OSCE) (Black et al., 2017. P.129). Therefore it is evidently clear that regardless of the Brexit outcome UK would not compromise her security under any circumstances.

References

Black et al (2017). *Defence and security after Brexit* [Online] Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1786/RAND_RR1786.pdf (Accessed: 25 January 2020)

Government of UK, (2016) *Two thirds of large UK businesses hit by cyber breach or attack in past year* [Online]. Available at https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year (Accessed: 05 February 2020)

Palmer, D. (2018). *Cybersecurity and Brexit: What does it mean for the fight against hackers?* [Online] Available at: https://www.zdnet.com/article/cybersecurity-and-brexit-what-does-it-mean-for-the-fight-against-hackers/ (Accessed: 28 January 2020)

Palmer, Danny. (2018). *What is GDPR? Everything you need to know about the new general data protection regulations* [Online] Available at: https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/ (Accessed: 2 February 2020)

Sharf, E. (2014) 'Information exchanges: regulatory changes to the cyber-security industry after Brexit: Making security awareness training work', *Science Direct*, Volume 2016 (Issue 7) [Online]. Available at: https://www.sciencedirect.com/science/article/pii/S1361372316300525 (Accessed: 10 February 2020)

TAC Security to provide solution to fight against cyber attacks in UK post Brexit [Online] Available at: http://ezproxy.cardiffmet.ac.uk/login?url=https://search-proquest-com.ezproxy.cardiffmet.ac.uk/docview/1826492608?accountid=15588 (Accessed: 10 February 2020)

King, J. (2020) Cyber security after Brexit [Online]. Available at: https://ukandeu.ac.uk/cybersecurity-after-brexit/ (Accessed: 15 December 2020)

Winder, D. (2018). *Post-Brexit Britain Could Be A Cybersecurity Nightmare With Or Without A Deal* [Online] Available at: https://www.forbes.com/sites/daveywinder/2018/10/16/post-brexit-britain-could-be-a-cybersecurity-nightmare-with-or-without-a-deal/#1dd90b292a34 (Accessed: 03 February 2020)

ANNEXURE C.4

BREXIT ON CYBER THREATS: Would it make UK less safe?

This document in the form of an opinion paper was presented at CRESTCon-2019.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) BREXIT ON CYBER
THREATS: Would it make UK less safe?, *CRESTCon-2019*, London, 2020.

The framework proposals for UK exit have been agreed in principle, but the process is at an impasse due to serious concerns raised by a majority of UK Government. Cyber security is one of the issues amongst other constitutional issues that has drawn the attention of the public because of potential security implications. What all this adds up to is a lack of direction in meeting cyber threats.

The concerns refer mostly to shortage of skilled labour (Winder, 2018), likely difficulties in attracting talented people from EU, potential reduced level of intelligence sharing (Sharf, 2014) leading to less cooperation between the UK security agencies and Europol. Also the impact on the data and privacy sharing leading to redefining Data Protection Regulations. The Data Protection Act (DPA) 2018 is a national law which complements the European Union's General Data Protection Regulation (GDPR) (ICO., N.D., About the DPA 2018). After Brexit, UK will have to either use both GDPR and DPA in parallel or follow their own path. In addition, the loss of access to European technical expertise is considered high on the list.

Cyber security matters to everyone because it protects and promotes national interests. Therefore, continuation of the UK-EU cyber security partnerships is likely to remain high. However, despite the uncertainties and concerns, UK intelligence agencies might continue to maintain their partnerships with Five Eyes and NATO to reap mutual benefits.

Reference

Winder, D. (2018). *Post-Brexit Britain Could Be A Cybersecurity Nightmare With Or Without A Deal* [Online] Available at: https://www.forbes.com/sites/daveywinder/2018/10/16/post-brexit-britain-could-be-a-cybersecurity-nightmare-with-or-without-a-deal/#1dd90b292a34 (Accessed: 03 March 2019)

Sharf, E. (2014) ‘Information exchanges: regulatory changes to the cyber-security industry after Brexit: Making security awareness training work’, *Science Direct*, Volume 2016 (Issue 7) [Online]. Available at: https://www.sciencedirect.com/science/article/pii/S1361372316300525 (Accessed: 1 March 2019)

ICO. (N.D) About the DPA 2018 [Online]. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/ (Accessed: 14 March February 2019)

ANNEXURE C.5

5.4 Is SL becoming a potential target for cyber-attacks launch by terrorist groups?

This article was published in the Daily Mirror, a leading newspaper in Sri Lanka, as an opinion paper.

Bentotahewa, V. Hewage, C. (2019) *Is SL becoming a potential target for cyber-attacks launch by terrorist groups* [Online]. Available at https://www.pressreader.com/sri-lanka/daily-mirror-sri-lanka/20190716/281857235114846

The repression of insurgency and terrorism are hard to achieve, yet what is even more difficult is the containment and sustainability of the victories. In Sri Lankan context, in 2009 Sri Lankan government claimed an emphatic victory by defeating the LTTE who was engaged in a 30 year conflict with the Government of Sri Lanka. That victory had been sustained over the ten years that passed. The deadly multiple terrorist attack on Easter Sunday (21/4), believed to have been carried out by ISIS affiliated local group, and tranquillity of the country has once again been disrupted. It is clear that there were lapses in security despite early intelligence warnings provided by various sources, and such warnings had not been heeded. The questions are being asked about the complacency of the government and soul searching has begun seeking answers to crucial failures in the provision of security.

The use of hard power, the military option, in the first instance of a dispute has shifted from battle field to the cyber space. That has made the use of Cyber space by individual state actors and groups an effective means to engage in espionage and a wide range of criminal activities. The terrorists are one particular group that has taken advantage of the cyber space. And the world has been put on alert from potential cyber threats, not only to powerful nations but also to vulnerable smaller nations alike. The use of sophisticated Information and Communication Technology (ICT) is playing a part in combatting these security threats, but the terrorists have been too smart in using weaknesses in technology to remain a step ahead.

Following the 21/4 attack there were series of cyber-attacks believed to have been launched by the LTTE. These types of attacks are not a new phenomenon to SL. The LTTE had used cyber-attacks during the Sri Lankan conflict, and has carried out cyber-attacks on Sri Lankan government websites. In doing so, the group has proven their capability in the use of new Information Technology for the purpose of creating threat perceptions in the minds of the target users. That has compelled the Sri Lankan government to be more concerned and focus on informational security.

The pro-LTTE diaspora groups made use of their own websites to spread disinformation on the Sri Lankan conflict, in doing so overtly promoted Tamil culture. The LTTE also conducted propaganda campaigns to raise funds from the Tamil diaspora and international sources using social media platforms. That was not all, criminal activities such as cloning of credit cards and credit card fraud had been carried out using ICT. In an examination of the LTTE's military operations against the Sri Lankan state it became apparent that the LTTE had launched cyber-attacks on the government of Sri Lanka's websites and Sri Lankan missions abroad.

In order to counter the LTTE's cyber activities at that time, the Sri Lankan Government had adopted an online cyber strategy which included coercive and preventive methods of countering the cyberspace of the LTTE. The Government of Sri Lanka had imposed a local ban on the www.tamilnet.com during the start of the Eelam War IV signalling that government was offensive against the LTTE's media space on the Internet.

Against that background, Sri Lankan government and the military sought technological support from experts to prevent LTTE attacks on Government websites. In addition, at the organisational level the Ministry of Defence Sri Lanka (MODSL) took measures to revive its Army, Navy, Air force and Police Websites and provided twenty-four hour news updates. By taking coercive and preventive measures, Sri Lankan government had been successful in averting potential cyber threats. These measures enabled GOSL counter the LTTE propaganda news reports internationally, and whilst at the same time attracting Sinhalese diaspora as well.

Soon after Easter Sunday terrorist attacks, Sri Lanka computer emergency response team reported that few local websites with .lk or.com domains including that of the Kuwait Embassy in Sri Lanka had been subjected to a cyber-attacks. Among the websites affected were private companies as well as the Rajarata University and Sri Lanka Tea Research institute in Talawakelle. This attack occurred as Sri Lanka marked the tenth anniversary since the war against the LTTE ended, and the report further suggested that perpetrators were group identified as the Tamil Eelam Cyber Force. This pattern of attacks raise serious questions whether the attacks could have been avoided had the security services been aware of the capabilities and capacities of LTTE and remained vigilant on post conflict threats from the LTTE. However, the TechCERT suggests that LTTE has intentionally picked vulnerable websites equipped with minimum cyber security measures. If that was the case, general public and security services should work together to tackle cyber-attacks by raising public awareness on preventive measures to safeguard against future threats.

The Easter Sunday attack has created another dimension to cyber threats. SL is facing a new threat from IS, and Islamic fundamentalist affiliated to them. The IS blow back from Iraq and Syria is similar to Afghanistan when al Qaeda was dismantled. Despite the battlefield losses and losing ground in Iraq and Syria, the multiple suicide bombings in Sri Lanka demonstrated that the so-called Islamic State (IS) is entering a new phase of global expansion. Reviewing the capabilities of IS, it becomes apparent that there were instances when IS has used their cyber capacities to disrupt stability of countries. Number of questions that needs to be asked are, whether SL is ready to face any potential cyber threat in the aftermath of recent incidents, and the challenges that it would have to face in the future. Furthermore, does Sri Lanka possess sufficient capacities and the right capabilities? In a global dimension, no country can sit back and be complacent about the threats from cyber-criminals because of unimaginable consequences that may even bring the entire country to a standstill. Therefore, taking preventive measures either individually or collectively must be a priority for all.

The IS used social media platforms to spread propaganda mostly through social media radicalising a minority of Sri Lankans. Furthermore, social media sites, mainly face-book, were used to spread hate speeches online to provok anti-Muslim violence. In the aftermath of Easter Sunday attack, GOSL took action to block social media sites, including Facebook, WhatsApp, YouTube, and Snapchat. The over-riding intention of this action was to prevent further inflammatory disinformation being posted, reduce tensions, avoid escalation of sporadic incidents and incitements for violent retaliations in potential flash points. Prior to this, social media platforms in the country came under government scrutiny last year and a ban was imposed then. Recent banning orders appear to be temporary measures to quell public fears and anxiety, and to bring the current situation under control.

Sri Lanka CERT|CC (Computer Emergency Readiness Team | Co-ordination Center) which directly comes under the Ministry of Digital Infrastructure and Information Technology acts as the focal point for cyber security. Its responsibility is to provide advice on potential risks, latest threats, vulnerabilities of computer systems, and to assist the nation in responding to, and recovering from cyberattacks. The next are the Computer Emergency Response Teams (CERTs) and the Finance Sector Computer Security Incident Response Team (FINCSIRT). These are specialised service unit responsible for receiving, reviewing, processing and responding to computer security alerts, and incidents affecting the banks and other licensed financial institutions in the country.

These three outfits currently work largely within their own client domains apparently with little coordination. However, faced with a national security threat ahead, they would have been expected to work together pooling all their technical resources. Failure to do so would make the country prone to cyber-attacks, and it would not be easy to prevent cyber-attacks as the source of the attacks would be hard to trace. In addition, a review of cyber-security aspects and a new Cyber Security Bill are necessary for setting up a National Cyber Security Agency (NCSA) with delegated responsibility for all cyber security activities. On the other hand, Sri Lankan security forces should possess cyber security capabilities and develop further to effectively engage in prevention of cyber threats against the state, whilst sharing information with other relevant authorities.

Cyber threats have gone beyond boundaries and therefore, international cooperation plays a vital role in countering cyber threats. Cyber threats often come as both internal and external threats, and those against the states could affect the financial sector, industrial sector, and tourism sector; or, the military and assets. Therefore, the states need to have well collaborated and coordinated mechanisms comprised with both military and civilian organizations. In support of that, Sri Lanka has already demonstrated its desire to engage by signing the Commonwealth Cyber Declaration, agreed in 2018. In doing so it is reported that members of the Commonwealth agreed to support a cyberspace that supports economic and social development and rights online, to build an effective national cyber security response, and to promote stability in cyberspace through international cooperation.

Furthermore, The European Union (EU) and its member countries are at the forefront of this international effort to deal with global cyber security issues. According to the reports, the EU is committed to helping countries like Sri Lanka to address the challenges of cybersecurity and pave the way for a more robust, resilient and reliable cyber infrastructure. Initiating this collaboration between the European Union and the Ministry of Digital Infrastructure and Information Technology, the Cyber Resilience for Development (CYBER 4DEV) Project has been launched. The British, Dutch and Estonian governments are the partners for the implementation of the project. These EU funded project aims to increase the security and resilience of information infrastructure and networks supporting public and private enterprises, infrastructure and utility services. Through these initiatives, it would be possible for Sri Lanka to obtain technical and financial support in implementing projects and increase awareness of decision makers on cyber security issues to increase organizational capacities to prevent cybersecurity incidence.

ANNEXURE C.6

Gender Balance in ICT: Sri Lankan Perspective in Data Protection

The document on this topic was compiled using the outcome of the researcher's questionnaire and was presented at IEEE International Women in Engineering Symposium.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) Gender Balance in ICT: Sri Lankan Perspective in Data Protection, *IEEE International Women in Engineering Symposium*, Sri Lanka, 2020

Sri Lanka has made impressive strides in the field of evolving technology and its increasing reliance on modern computers and Information Technology feature prominently right across the government and the private sector alike. The use of ICT has inherent risk factors too, in so far as data security and privacy, and they pose significant threats to national security and privacy of the citizens. That has made it necessary to put in place measures to protect critical national infrastructure and, more widely against unauthorised access to computer systems by cyber criminals (Government of Sri Lanka, 2010). To be response ready, Sri Lanka introduced the Computer Crimes Act 2007 and, the draft of the National Cyber Security Bill, 2019 was presented to the Parliament for consideration (Manjula Sirimane, 2020). However, the policies and regulations alone falls short of what is needed to counteract cyber threats, therefore, cyber security awareness must also be looked at as a necessary component in the package.

In this work, authors seek to evaluate the actions the government should initiate to support women to become sufficiently aware of cyber security, and encourage them to take advantage of employment opportunities in the ICT sector. The results indicate to a higher level of cyber security awareness amongst men than amongst women, despite the satisfactory level of cyber security awareness training the women have received from their organisations. The key indicator is that training alone will not be sufficient and, it is important to facilitate awareness programs, ideally from the school level by making information security a part of the school curriculum. And organisations like the national CERT, the SLCERT (Sri Lanka Computer Emergency Readiness Team) can make a

difference by working together alongside the academics and organisations to deliver awareness programs. SLCERT also should seek to establish collaborations with commercial entities and academic institutions outside the country to bring in new knowledge and technical training where deemed beneficial.

Keywords: ICT, Women, Cyber security awareness

1.0 Introduction

The increasing reliance on ICT and other technologies make organizations more vulnerable and prone to cyber-attacks. According to the Information Department, Sri Lanka Army's official news wing, had been hacked on 1st of May 2009 by suspected LTTE hackers or their proxies with insertion of some horrible and gruesome images (UK Border Agency, 2009). The government news portal www.Lankapuvath.lk had also come under a cyber-attack and suspected LTTE hackers were found to have been behind the attack (UK Border Agency, 2009). Furthermore, the Cyber Security Centre of Sri Lanka Air Force stated that the websites of two government entities were attacked on the War Hero commemoration day in May 2020, and five websites containing the domain name .lk and .com had come under a cyber-attack also about the same time (No author, 2020). The lesson learned from those incidents is the need to raise cyber awareness amongst the workforce and to avoid human errors that would result in heavy losses to the organisations.

Women involvement in ICT industry has a history from WWII. Few women who worked at Bletchley park with their male peers were formally recognised as cryptanalysts (Bletchley park research, N.D). However, in Sri Lankan context, it is apparent that social and cultural factors play a defining role in determining the inclusion of women especially in the labour market (International Labour Organisation, 2016). According to the reported statistics, women in Sri Lanka form approximately 51% of a total estimated population of 21 million (Coutrymeters, 2020), and only 36.6% women are in the labour market (Economynext, 2020). However, the active participation of women appeared to be under-represented in the field of cyber security. The researcher quote from the reported statistics that, in 2018, women accounted for 10% of the cybersecurity workforce in the Asia-Pacific region, 9% in Africa, 8% in Latin America, 7% in Europe and 5% in the Middle East (Kshetri, 2020). In a survey of women pursuing careers outside IT fields has indicated that the main reason for not pursuing opportunities in IT was the lack of awareness (Kshetri, 2020).

2.0 Aims and objectives

The aim of this research is to ascertain how the government can support women become sufficiently aware of cyber security and encourage them to make use of the employment opportunities in the ICT sector in Sri Lanka. The objectives are to identify the level of cyber security awareness amongst woman, to explore the level of support they receive from the organisations, and to analyse what actions the government could take to educate women by looking at the examples set by other countries.

3.0 Methodology

This research is qualitative and quantitative in nature. The researcher conducted an extensive literature survey of previous research papers, journal articles, previous survey reports and government publications on the above context. The researcher then developed a questionnaire to evaluate and critically analyse the important parameters identified in the literature review. The outcomes of the questionnaire will be used to formulate ideas, validate the hypothesis.

4.0 Results

The aim of this research was to get an understanding of the level of cyber security awareness and, whether the organisations were providing cyber security awareness training to their staff members. The inference drawn from the responses received for the questionnaire was a clear indication that cyber security awareness amongst men (See table 1) (See figure 1) were higher than that of women (See table 2) (See figure 2). However, the satisfaction rate for the cyber security awareness training they received from their organisations was higher amongst the women (see table 2) (See figure 2) than that of men (See table 1) (See figure 1). This shows that despite the understanding of cyber-attacks is comparatively lower amongst the females than that of the males, the organisations do support women by providing the training to enhance their performance and, minimise the end user errors.

Table 1: Male

QUESTION	SRONGLY AGREE	AGREE	NEUTRAL	DISAGREE	STRONGLY DISAGREE
Q1: I have a good understanding of cyber-attacks affecting me, public and organisations across the globe	6	12	3	1	0
Q2: I regularly do receive cyber security awareness training	4	9	3	5	1

Table 2: Female

QUESTION	STRONGLY AGREE	AGREE	NEUTRAL	DISAGREE	STRONGLY DISAGREE
Q1: I have a good understanding of cyber-attacks affecting me, general public and organisations across the globe	5	8	4	4	2
Q2: I regularly do receive cyber security awareness training	3	4	11	1	3

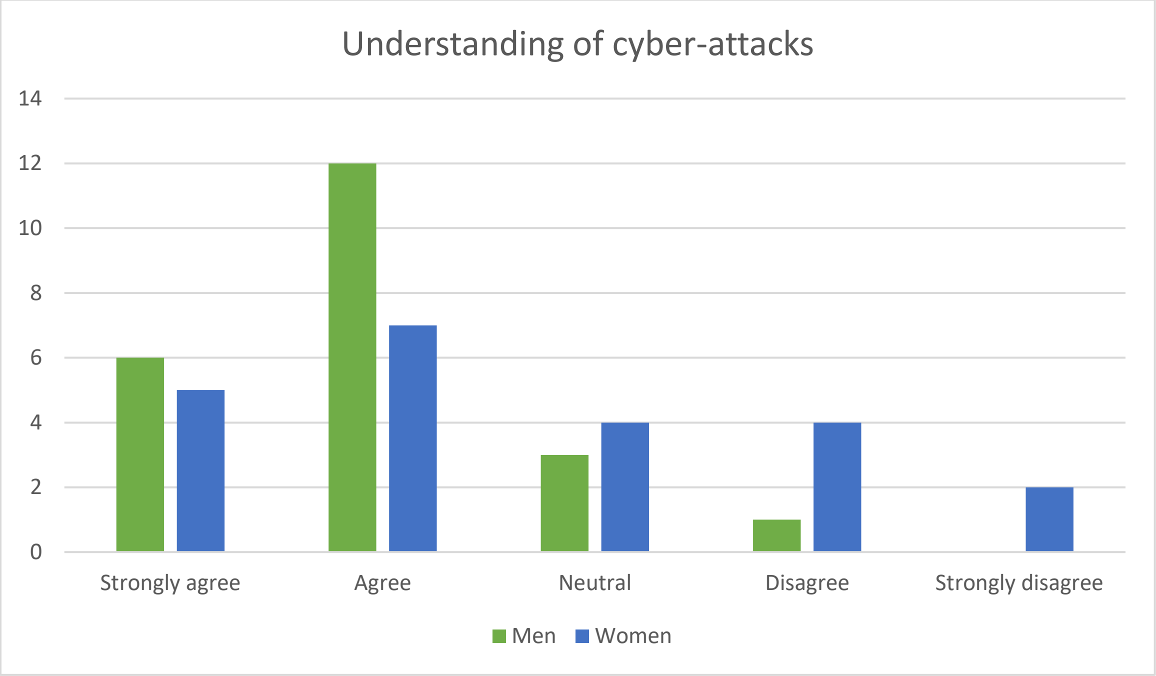


Figure 1: Understanding of cyber-attacks

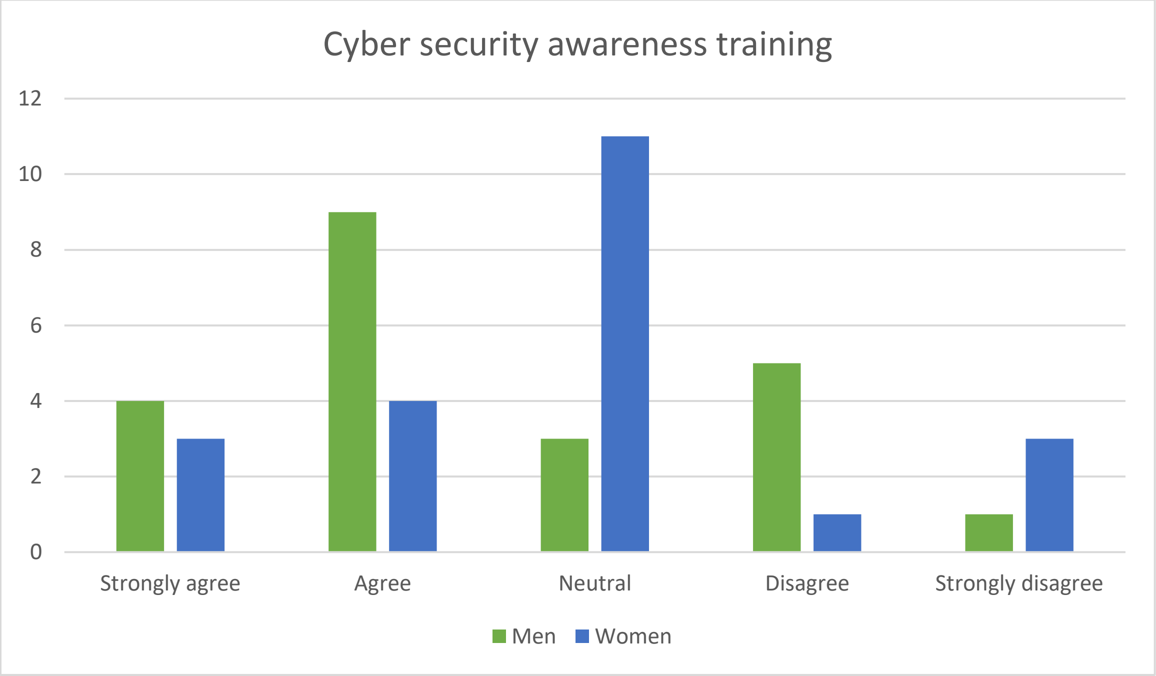


Figure 2: Cyber security awareness training

5.0 Discussion

There are examples of the steps taken at the national level round the world, to improve cyber security awareness mainly amongst women and the reports suggest that professional associations can foster interest in cybersecurity and help women develop applicable knowledge. For example, women engaged in cybersecurity of Spain has initiated a mentoring program that supports female cybersecurity professionals early in their careers (Kshetri, 2020). The government of the United Kingdom also announced the offer of lessons in cybersecurity to the school children in a bid to develop their skills needed to fill the shortages that are currently undermining confidence in the cyber defences in the country (Armstrong-Smith, 2018).

The Information and Cyber Security Strategy of Sri Lanka (2019-2020) emphasises that one of its vision is to increase awareness and empower citizens (Karunasena, N.D). IT related education program is one area that will play a key role to achieve that, and to meet that objective, the government can introduce information security as a subject to the school curriculum to make future generations aware of cyber threats. On a wider scale, the government and private sector employees should also benefit from appropriate awareness programs as they rely on networking technology that is often prone to attacks. Any slack in response preparedness of the users of technology would leave them open to their private information being accessed by the criminals using unethical practices.

Some industry-based groups have collaborated with big companies to address the issue of gender gap in the field of ICT. A good example is the Microsoft of India and the Data Security Council of India launched the Cyber Shikshaa program in 2018, to create a pool of skilled female cybersecurity professionals (Kshetri, 2020). In Sri Lanka, the national CERT, the SLCERT (Sri Lanka Computer Emergency Readiness Team) acts as the national hub for cyber security of the nation (Sri Lanka CERT| CC, N.D). Using these organisations as a resource, the government can bring in experts from the academia and the industry to provide appropriate training to educate females to narrow the gender gap both amongst the general population and those in employment. SLCERT should also seek to establish partnerships with big companies and universities from other countries to bring in new knowledge and technical training where deemed beneficial.

6.0 Conclusion

Cyber criminals are becoming increasingly creative in putting know how to carry out cyber-attacks. Therefore, there is a pressing need to develop a robust response by engaging a diverse and inclusive cybersecurity team equipped with the resources that they need to do their job effectively. This means bringing in together knowledge and expertise from all sections of the community in the ICT discipline, particularly women to produce the desired outcome. To achieve that strategic outcome, it is important to provide women with knowledge and skills and absorb them into the workforce. In this way, the industry will be able to reap the benefits of a diverse talented workforce that will play a crucial role in the organization

References

Armstrong-Smith, S. (2018) *Diversity in Security: A Collaborative Effort* [Online]. 2018 Available at https://www.cbronline.com/opinion/women-cybersecurity (Accessed: 28 July 2020)

Bletchley park research, (N.D) *Women Codebreakers* [Online]. Available at https://www.bletchleyparkresearch.co.uk/research-notes/women-codebreakers/ (Accessed: 3 August 2020)

Coutrymeters, (2020) *Sri Lanka population* [Online]. Available at https://countrymeters.info/en/Sri_Lanka (Accessed: 15 July 2020)

Economynext, (2020) *Without female engagement, Sri Lanka's Growth will sputter* [Online]. Available at https://economynext.com/without-female-engagement-sri-lankas-growth-will-sputter-56554/ (Accessed: 27 July 2020)

Government of Sri Lanka, (2010) *Mahinda Chintana Vision for the Future* [Online]. Available at https://www.adb.org/sites/default/files/linked-documents/cps-sri-2012-2016-oth-01.pdf (Accessed: 15 July 2020)

International Labour Organisation, (2016) *Factors affecting women's in labour force participation in Sri Lanka* [Online] Available at https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms_551675.pdf (Accessed: 12 July 2020)

Karunasena, K. (N.D) *Digital Government & Cyber Security Strategy of Sri Lanka*[Online]. Available http://www.cicc.or.jp/japanese/kouenkai/pdf_ppt/pastfile/r01/191119-12lk.pdf (Accessed date 20 July 2020)

Kshetri, N. (2020) *The lack of women in cybersecurity leaves the online world at greater risk* [Online]. Available at https://theconversation.com/the-lack-of-women-in-cybersecurity-leaves-the-online-world-at-greater-risk-136654 (Accessed: 2 August 2020)

Manjula Sirimane, (2020) *Sri Lanka: Proposed Bill on Personal Data Protection* [Online]. Available at https://www.dataguidance.com/opinion/sri-lanka-proposed-bill-personal-data-protection (Accessed: 20 July 2020)

No author. (2020) *Cyber-attack on two govt. websites* [Online]. Available at http://www.sundayobserver.lk/2020/05/30/news/cyber-attack-two-govt-websites (Accessed: 8 July 2020)

Sri Lanka CERT| CC, (N.D) *About us* [Online]. Available at https://www.cert.gov.lk/aboutUs.php (Accessed: 20 July 2020)

UK Border Agency. (2009) *Country of origin information report- Sri Lanka* [Online]. Available https://www.refworld.org/pdfid/4a4a02f52.pdf (Accessed: 18 July 2020)

ANNEXURE C.7

Infodemic: Have the countries done enough to tackle fake news to protect the people?

This document was presented at UK government Global Security Event 2021.
Bentotahewa, V. Hewage, C. and Williams, J. (2021) Infodemic: Have the countries done enough to tackle fake news to protect the people? UK government Global Security Event 2021.

1.0 Introduction

The COVID-19 pandemic has induced an unprecedented environment for spreading online misinformation, manipulation, and abuse that will have dramatic real-world consequences. Contrary to the positive use of social media, it has become the driving force for spreading fake news and disinformation, to the extent that it has become difficult for people to what is correct and what is not. This is not the first instance and conspiracy theories are not new to a pandemic. Many conspiracy theories were also spread relating Zika virus, Ebola, or even AIDS (Barua et al., 2020).

Governments are obliged to provide adequate access to accurate information as prescribed by international human rights law (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.6). Such access includes the right to seek, and receive information, including information concerning health (law (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P. 6). In the same token, during this ongoing pandemic, education and access to information concerning the health of the community, lie at the core of the human right to health law (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P. 6). To this end, the urgency of governments to promote and protect access to and free flow of information is crucial**.**

In the early stages of the outbreak, the World Health Organization warned the international community about a growing 'infodemic' in social media (WHO, (2020) Novel Coronavirus (2019-nCoV) Situation Report – 13. P.2). The emergence of ‘infodemic’ is characterized by the undisciplined spread of information, including a multitude of low-credibility, fake, misleading, and unverified information (Ferrara, Cresci, and Luceri, 2020) . According WHO, this ‘infodemic’ is causing a psychological panic, misleading medical advises, and economic disruption (Mourad, et al., 2020, P.1). One good example is, this has fuelled fear and irresponsible behaviour, such as the panic buying of toilet roll and other essentials (Coe, 2020).

2.0 Aims and objectives

The aim of this research is to investigate the impact of an emerging infodemic in the pandemic environment

Objectives

- Identify the fake news spread during the pandemic
- Explore potential impact on human life
- Recommend technical and policy mechanisms to tackle ‘fake news spread syndrome’

3.0 Potential impact of this work

Large amount of disinformation can intensify racism, stigmatisation, phobia, apprehension, and even threatening behaviour, characterised by unusual trends in purchasing personal protective equipment, the use of toxic substances, and buying and using drugs without authorised medical prescriptions. These behaviour changes in the midst of a pandemic can potentially be harmful and even lead to life self-harm incidents.

Few reported incidents are:

- A resident USA, having heard (on the news) that the chloroquine could be a cure for COVID-19, had consumed it and died (Waldrop, Alsup, and McLaughlin, 2020).
- Iranian Government revealed that people had died from alcohol poisoning, believing drinking bootleg liquor could save them by the virus (Trew, 2020).

4.0 Findings

According to available literature,

- Over 70% of adults use the internet services to search for healthcare information (Li et al., 2020, P. 1)
- 93.5% of the general public in China used the internet to collect primary health care information during the initial stage of COVID-19 pandemic (Wang et al, 2020, P21).
- According to the Pew Research Centre, Most Americans do pick up news updates from social media platforms but they remain suspicious about the accuracy of media reports (Mourad, at el., 2020, P1).
- Half of the adult population in UK now use social media to keep up with the latest news (Mourad, at el., 2020, P1).
- Facebook's own notifications did indicate that during the period between March and April of 2020, it posted warning labels on approximately 90 million pieces of content that were believed to be misinformation like false cures, anti-vaccination propaganda and conspiracy theories linked to COVID-19 (BBC, 2020, Social media firms fail to act on Covid-19 fake news)

4.1 Sample fake news

- Coronavirus is not heat-resistant and will be killed in a temperature of 26-27 degrees or the virus does not settle in the air but on the ground, so it is not transmitted through the air (WHO–Nepal, 2019)
- The virus being a biological weapon, created by China (Pennycook, et al., 2020, P.770)
- Eating Centella asiatica will prevent coronavirus infection (Islam, 2020, P. 1626)
- Nurse died after taking the coronavirus vaccine (Reuters, 2020)
- Hospital beds are empty (Giles, Goodman, and Robinson, N.D)
- Anti-malaria drug chloroquine phosphate is a cure for COVID-19 (BoomLive, 2020)
- Virus does not infect children (BBC, 2020, Coronavirus: Elon Musk 'child immunity' tweet will stay online)

Literature based evidence describe how violent non-state actors (i.e. terrorist, extremists and organized criminal groups) take advantage of the pandemic, to jeopardize the efficacy of the response measures taken by the government (UNICRI, 2020). Available literature highlights three particular groups of violent non-state actors, the right-wing extremist groups, and organized crime groups, who are actively using the social media during the pandemic for malicious purposes (The Hindu, 2020, Groups associated with al-Qaeda, ISIS spread conspiracy theories about COVID-19: UN report).

These groups attribute the origin of the virus to governments, religious or ethnic groups, secret networks, companies or businessmen. ie. Islamophobic online 'Cyber Hubs' were being formed linking Muslims to the spread of COVID-19, and shared fake news stories (Birmingham City University, N.D) Right wing extremist groups circulated conspiracy theories blaming immigrants and foreigners as the ones who should be responsible for spreading the virus, and ISIL spread conspiracy theories stating that the virus is a "soldier of Allah" and that this is a punishment to all the unbelievers and the enemies that have damaged Muslims over the last years (The Hindu, 2020, Groups associated with al-Qaeda, ISIS spread conspiracy theories about COVID-19: UN report).

4.2 Reported incidents

The United Nation High Commissioner for Human Rights has warned that the pandemic may instigate more discrimination, and has urged nations to combat all forms of prejudices, drawing attention to the emergence of 'tsunami of hate' (Vidgen, et al., 2020).

Italy- Since the start of the pandemic, a wave of xenophobia and hate speech (Sinophobia) against the Chinese community across the country have reportedly intensified (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.18)

United States- Over 1,100 instances of anti-Asian harassment, online and offline, have been recorded by the Stop AAPI HATE reporting forum since it was set up in late March 2020 (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.18)

5.0 Discussion

The emergence of disinformation is unique to the COVID-19 pandemic, and the state actors have been battling both phenomena for a long time. The violent non-state actors have taken advantage of the weaknesses/loopholes inherent in social media and messaging apps, and the contents in them can be uploaded anonymously, instantly, with ease. In the context of an unprecedented health crisis, however, misinformation and disinformation about the pandemic pose a serious risk to public health as well as public action. This has been endorsed by world Health Organisation stating that the consequences of misinformation about Covid-19 are real and serious: fake treatments and mistrust of public health advice can cost lives (Griffin, 2020).

The Resolution WHA73.1 on COVID-19 response was passed by WHO Member States, at the World Health Assembly held in May 2020 (WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, 2020). It recognizes that managing the 'infodemic' is a critical part of controlling the COVID-19 pandemic, and further highlights the importance of Member States providing reliable COVID-19 content taking measures to counter, develop and implement action plans to manage mis- and disinformation (WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, 2020).

5.1 Actions taken by the countries to counter heightened digital security risks

5.1.0 LATIN AMERICAN REGION

Bolivia: A decree issued by the President of Bolivia, provides provisions for prosecution of those who incite disobedience of government measures to fight COVID-19, 'misinform,' or 'create uncertainty' in the population, for crimes against public health (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.12)

Paraguay: The proposed laws allow imposition of fines for people spreading misinformation during the COVID-19 emergency, even if it was done without intent (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.13)

5.1.1 EUROPEAN REGION

In a statement released by the European Commission, ENISA, CERT-EU and Europol, it has highlighted their cooperation to track COVID-19 related malicious activities (OECD, 2020, OECD Policy Responses to Coronavirus (COVID-19)- Dealing with digital security risk during the Coronavirus (COVID-19) crisis).

UK- Announced that it would create a specialist unit to identify and respond to inaccurate or misleading posts about coronavirus (Coe, 2020). The unit will continue to have regular and robust engagement with social media companies. Funding for the Humanitarian-to-

Humanitarian Network was agreed by the UK government, for the purpose of 'tackling the global spread of coronavirus fake news (Coe, 2020).

Hungary- Initially, due to the sensitive nature of the information, the authorities withheld information about the geographical spread of COVID-19 infections; adopted laws enabling imposition of jail terms of up to five years on those found guilty of obstructing virus spread preventive measures, for spreading of disinformation that would make people anxious, or likely to jeopardise the fight against the virus Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.13)

5.1.2 AFRICAN REGION

South Africa- Published regulations under the Disaster Management Act 2002, make fake news an offence, punishable by a fine or up to six months imprisonment, or both (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.13) . To publish a statement through any medium with the intention to deceive the public about COVID-19, reveal anyone's COVID-19 infection status or government measures to address the pandemic (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.13)

Kenya- President encouraged law enforcement agencies to arrest purveyors of fake news. Computer Misuse and Cyber Crimes Act of 2018, includes clauses criminalizing false information and publication of false information, and it is reportedly being used to make arrests and charge persons (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.13)

Tunisia- In 2020, members of the Tunisian Parliament proposed a bill to combat disinformation during the COVID-19 crisis, based on the notion of having to take effective measure to counter fake news and, control the flow of information on social media platforms, and likely impact on national security and stability (Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.14)

5.1.3 ASIAN REGION

China: Citizen Lab reported that from the very beginning of the pandemic, Chinese authorities have blocked COVID-19-related content on social media and the messaging service WeChat Accessnow, 2020, Fighting misinformation and defending Free expression during covid-19: Recommendations for states, P.7)

Bangladesh- The Digital Security Act, thought of to be a controversial law, is the main law used by the government to deal with fake news via the web and social media (Ahmad, 2020, India, P.9). Also, a circular issued by Bangladesh Ministry of Information has notified the establishment of the unit to monitor spreading of rumours about COVID-19 cases by social media and private television channels (Ahmad, 2020, India, P.10).

India- Indian law does not make provisions specifically to deal with fake news. However, existing laws covers certain criminal offenses, and can be used to criminalize forms of speech that may constitute fake news, and sections of the Penal Code and the Disaster Management Act, 2005 have been applied to cases involving the spread of false news regarding COVID-19 (Ahmad, 2020, India, P.15).

Nepal- The spread of false rumours is mainly dealt through the National Penal Code Act 2017(Ahmad, 2020, Nepal, P.25).

Pakistan- The National Command and Operation Centre (NCOC), formed a committee led by the Minister of Interior to prevent the spread of disinformation and fake news about the COVID-19 pandemic on social media (Ahmad, 2020, Pakistan, P.36). It dose not appear that Pakistan has a fake news specific criminal code or one that specifically applicable to COVID-19.

Sri Lanka- Sri Lanka has general provisions in its Penal Code that deal with certain forms of false statements and rumours (Ahmad, 2020, Sri Lanka, P.56). . In early June 2019, the Sri Lankan Cabinet approved an amended Penal Code and Criminal Procedure Code. They are intended to allow action against people spreading fake news on social media, including statements likely to impact national security and incite communal violence (Ahmad, 2020, Sri Lanka, P.57).

It is important all the stakeholders including the media and social media platforms, researchers and technologists, civil society leaders and influencers to come together, to strengthen actions to prevent the spread of disinformation.

Setting up an example, WHO, associating with the Government of the United Kingdom, has started a campaign to counter misinformation about COVID-19 (WHO, 2020, Countering misinformation about COVID-19). The 'Stop The Spread'. WHO is seeking ways to raise awareness of COVID-19 misinformation, and calling a for a joined up campaign to encourage the public to evaluate the credibility of the information, by double-checking with trusted sources, such as WHO and regional and national health agencies (WHO, 2020, Countering misinformation about COVID-19).

The UNICEF has also come forward to play an urgent role in Bangladesh in association with the Islamic Foundation Bangladesh (IFB) (UNICEF, 2020, Religious leaders play key role in battle against COVID-19). UNICEF in Bangladesh noted that the Imams agreed to spread the health-related news before or after the praying time on their megaphone and will help to debunk the misinformation about diagnostic and treatment of the disease (UNICEF, 2020, Religious leaders play key role in battle against COVID-19). In the same manner, both local and international bodies in different regions around the globe can act in unison, and as has been reported by many countries that faith leaders already do take a proactive role in influencing the public.

6.0 Conclusion

It is a mandatory requirement to curtail the flood of fake news and viral disinformation to ensure that people living through the lockdown receive accurately sourced information; and in doing so encourage them to act responsibly to control the pandemic, mitigate the risk, and its impact. There has been an ongoing discussion on the key issue of fake news for a considerable time and plans for mitigating risks and banning harmful content had been in place. However, it appears they had not been forthcoming in making emergency plans to prevent misleading the public with fake news and disinformation in the prevailing emergency. It is also the case that the management of some social media companies have taken steps to restrict COVID-19 related fake news by removing false and potentially harmful information, but stopping it completely has been found to be difficult. Therefore, it is important for the countries to collectively and consensually reach an agreement with the social media platforms to monitor, detect and remove harmful content. Also, it is crucially imported to have a legal mechanism in place to prosecute those found culpable of spreading fake news.

6.1 Recommendations and preventatives

- The respective authority should encourage social media users to evaluate the credibility of information before they take any decision on a matter related to health issues, based on the information they received through social media. Public has the sources like WHO, UN, and other national and local organizations to evaluate the disinformation about COVID-19.

- It is required to get social media platforms to sign up to a Code of Practice on disinformation with an undertaking that action will be taken to remove fake information with immediate effect.
- Develop strong legal mechanisms at national and international level to bring individuals to account for spreading fake news regardless of the medium.
- Educate citizens about the harm and the damage the fake news could do to them, others and the society.
- Encourage individuals to critically evaluate each source of information, and help them understand the nature of information posted online.
- Artificial Intelligence techniques can also be used to detect fake news and to remove them.
- Data analysis and interpretation allow experts to extract information from social media platforms to visualize the spreading of false information and make timely decisions to flag and remove content.

References

Ahmad, T. (2020) 'India' in International Research & Exchanges Board. Freedom of Expression during COVID-19. Available at https://www.irex.org/sites/default/files/pdf/freedom-of-expression-during-covid-19.pdf (Accessed: 3 January 2021)

Ahmad, T. (2020) 'Bangladesh' in International Research & Exchanges Board. Freedom of Expression during COVID-19. Available at https://www.irex.org/sites/default/files/pdf/freedom-of-expression-during-covid-19.pdf (Accessed: 3 January 2021)

Ahmad, T. (2020) 'Nepal' in International Research & Exchanges Board. Freedom of Expression during COVID-19. Available at https://www.irex.org/sites/default/files/pdf/freedom-of-expression-during-covid-19.pdf (Accessed: 3 January 2021)

Ahmad, T. (2020) ‘Pakistan’ in International Research & Exchanges Board. Freedom of Expression during COVID-19. Available at https://www.irex.org/sites/default/files/pdf/freedom-of-expression-during-covid-19.pdf (Accessed: 3 January 2021)

Ahmad, T. (2020) ‘Sri Lanka’ in International Research & Exchanges Board. Freedom of Expression during COVID-19. Available at https://www.irex.org/sites/default/files/pdf/freedom-of-expression-during-covid-19.pdf (Accessed: 3 January 2021)

Accessnow. (2020) *Fighting misinformation and defending Free expression during covid-19: Recommendations for states* [Online]. Available at: https://www.accessnow.org/cms/assets/uploads/2020/04/Fighting-misinformation-and-defending-free-expression-during-COVID-19-recommendations-for-states-1.pdf (Accessed: 5 January 2021)

Barua, Z. et al., (2020) ‘Effects of misinformation on COVID-19 individual responses and recommendations for resilience of disastrous consequences of misinformation’, *Progress in Disaster Science*. Available at: doi: 10.1016/j.pdisas.2020.100119

BBC, (2020) *Social media firms fail to act on Covid-19 fake news* [Online]. Available at: https://www.bbc.co.uk/news/technology-52903680 (Accessed: 20 November 2020)

BBC, (2020) *Coronavirus: Elon Musk 'child immunity' tweet will stay online* [Online] Available at: https://www.bbc.co.uk/news/technology-51975377 (Accessed: 2 January 2021)

Birmingham City University, (N.D) *COVID-19 sparks online Islamophobia as fake news and racist memes are shared online, new research finds* [Online] Available at: https://www.bcu.ac.uk/about-us/coronavirus-information/news/covid-19-sparks-online-islamophobia-as-fake-news-and-racist-memes-are-shared-online-new-research-finds (Accessed: 28 December 2020)

BoomLive (2020) *Misleading Message Claims Anti-Malaria Drug Cures Coronavirus* [Online]. Available at: https://www.boomlive.in/world/coronavirus/misleading-message-claims-anti-malaria-drug-cures-coronavirus-7228?infinitescroll=1 (Accessed: 28 November 2020)

Coe, P. (2020) *The Good, The Bad and The Ugly of Social Media during the Coronavirus pandemic – Peter Coe* [Online] Available at: https://infolawcentre.blogs.sas.ac.uk/2020/04/30/the-good-the-bad-and-the-ugly-of-social-media-during-the-coronavirus-pandemic-dr-peter-coe/ (Accessed: 29 December 2020)

Ferrara, E., Cresci, S. and Luceri, L. (2020) 'Misinformation, manipulation, and abuse on social media in the era of COVID-19', *Journal of Computational Social Science* volume 3, Available at: https://doi.org/10.1007/s42001-020-00094-5

Giles, C. Goodman, J. and Robinson, O (N.D) *Covid: The truth behind videos of 'empty' hospitals* (Online). Available at: https://www.bbc.co.uk/news/55560714 (Accessed: 20 November 2020)

Griffin, R. (2020) *Social media and content moderation in times of COVID-19* [Online]. Available at: https://www.sciencespo.fr/public/chaire-numerique/en/2020/07/09/social-media-and-content-moderation-in-times-of-covid-19/ (Accessed: 6 January 2021)

Islam, M S. et al., (2020) 'COVID-19–Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis', *The American Journal of Tropical Medicine and Hygiene* Volume/Issue: Volume 103: Issue 4. Available at: DOI: https://doi.org/10.4269/ajtmh.20-0812

Li, H O., et al., (2020) 'YouTube as a source of information on COVID-19: a pandemic of misinformation?', *BMJ Global Health* Volume 5. Available at: doi:10.1136/bmjgh-2020-002604

Mourad, A. at el., (2020) *Critical Impact of Social Networks Infodemic on Defeating Coronavirus COVID-19 Pandemic: Twitter-Based Study and Research Directions* [Online]. Available at: https://arxiv.org/pdf/2005.08820.pdf (Accessed: 23 December 2020)

OECD (2020) *OECD Policy Responses to Coronavirus (COVID-19)- Dealing with digital security risk during the Coronavirus (COVID-19) crisis* [Online]. Available at: https://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/ (Accessed: 10 January 2021)

Pennycook, G. et al., (2020) ‘Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy-Nudge Intervention’, *Psychological Science 2020*, Vol. 31(7). Available at: DOI: 10.1177/0956797620939054

Reuters, (2020) *Fact check: Nurse who fainted after COVID-19 vaccine did not die* (Online). Available at: https://www.reuters.com/article/uk-factcheck-nurse-covid-vaccine-dead-idUSKBN29629G (Accessed: 12 January 2021)

The Hindu, (2020) *Groups associated with al-Qaeda, ISIS spread conspiracy theories about COVID-19: UN report* [Online]. Available at: https://www.thehindu.com/news/international/groups-associated-with-al-qaeda-isis-spread-conspiracy-theories-about-covid-19-un-report/article33130686.ece (Accessed: 15 December 2020)

Trew, B. (2020) *Coronavirus: Hundreds dead in Iran from drinking methanol amid fake reports it cures disease* [Online] Available at: https://www.independent.co.uk/news/world/middle-east/iran-coronavirus-methanol-drink-cure-deaths-fake-a9429956.html (Accessed: 13 December 2020)

UNICEF, (2020) *Religious leaders play key role in battle against COVID-19* [Online]. Available at: https://www.unicef.org/bangladesh/en/stories/religious-leaders-play-key-role-battle-against-covid-19 (Accessed: 9 January 2021)

UNICRI, (2020) *Stop the virus of disinformation: the malicious use of social media by terrorist, violent extremist and criminal groups during the COVID-19 pandemic - November 2020* [Online]. Available at: http://unicri.it/node/3279 (Accessed: 5 January 2021)

Vidgen, B. et al., (2020) ‘Detecting East Asian Prejudice on Social Media’, arXiv.org. Available at: https://arxiv.org/abs/2005.03909

Waldrop, T. Alsup, D and McLaughlin, E C. (2020) *Fearing coronavirus, Arizona man dies after taking a form of chloroquine used to treat aquariums* [Online]. Available at: https://edition.cnn.com/2020/03/23/health/arizona-coronavirus-chloroquine-death/index.html (Accessed: 10 January 2021)

Wang, C. et al (2020) ‘Immediate Psychological Responses and Associated Factors during the Initial Stage of the 2019 Coronavirus Disease (COVID-19) Epidemic among the General Population in China', *International Journal of Environmental Research and Public Health* Volume 17 (1729). Available at: doi:10.3390/ijerph17051729

WHO, (2020) *Novel Coronavirus(2019-nCoV) Situation Report – 13* [Online]. Available at: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf (Accessed: 13 January 2021)

WHO –Nepal (2019) *Rumours and Facts on COVID-19* [Online] Available at: https://www.who.int/docs/default-source/nepal-documents/novel-coronavirus/un-rumour-tracking-english-issue-2.pdf?sfvrsn=bd68b830_2 (Accessed: 25 December 2020)

WHO, (2020) *Countering misinformation about COVID-19* [Online]. Available at: https://www.who.int/news-room/feature-stories/detail/countering-misinformation-about-covid-19 (Accessed: 23 October 2020)

WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU. (2020) Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation [Online]. Available at: https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation (Accessed 3 November 2020)

ANNEXURE C.8

Are cyber criminals exploiting Corona pandemic for malicious purposes?

This article was published in the ministry of defence website (defense.lk) in Sri Lanka, Official website for Sri Lanka's response to COVID-19, also in 'The Island newspaper' which is a leading newspapers in Sri Lanka, as an opinion paper.

Bentotahewa, V. Hewage, C. and Williams, J. (2020) *Are cyber criminals exploiting Corona pandemic for malicious purposes?* [Online]. Available at: https://www.defence.lk/Article/view_article/1353

COVID-19 outbreak has become an unprecedented global pandemic that is threatening every aspect of human life, our security and most of all our livelihoods. There are also other unconventional threats in the form of cybercriminal activities. This article focuses on what we know as hacking by criminals, looking to exploit and take advantage of Corona factor.

1.0 What is the risk?

At this moment in time, every nation is implementing preventive measures, including a curfew and social isolation that restrict the normal lifestyles of the people, and the use of the internet is at the highest level. Mostly, people are having to work from home and keep in touch with the outside world. That exposes everyone online to cybercrimes while the world is busy trying to counteract the effects of the Corona virus. It makes us all vulnerable and presents the hackers with an ideal opportunity to exploit the Corona pandemic for malicious purposes. Using their skills and knowhow, the hackers follow everything we do online now, as much as they have done before.

The World Health Organization (WHO) recently issued warnings about suspicious email messages designed to take advantage of the Covid-19 emergency (WHO, N.D, Beware of criminals pretending to be WHO). The message including an attachment claimed to have details about how recipients could prevent spreading of the virus, but the attachment did not contain any useful advice, instead the email was meant to infect computers with malicious software called AgentTesla Keylogger (Tidy, 2020). In addition, there were several fake "diagnosis" scams as well. Therefore, any tools that promise to test you for Corona virus online should not be trusted. Instagram has already banned rogue Coronavirus filters that claim to "diagnose" your condition (Pettit, 2020). Security experts have labelled the new trend as "Fearware", warning that victims may be more susceptible to be tricked or scammed during times of global uncertainty (Cuthbertson, 2020).

Airborne virus scam (Tidy, 2020) was another to instigate fear into people by claiming the rates of transmission of Coronavirus will increase and make them insecure. The scam appears to resemble an email from the Centres for Disease Control and Prevention (CDC) which is faked with their correct email address to make it look genuine and, sent via a spoofing tool (Tidy, 2020). The cyber criminals had redirected the email recipients who had clicked on the link to a fake login page where the user was asked to enter their email and password (Tidy, 2020). ‘Donate here to help the fight’ is another scam asking for donations to develop a vaccine with a request to make payments in cryptocurrency Bitcoin (Tidy, 2020).

Interesting to note that Covid-19 scams are not being used by criminals just for monetary gains, but hackers have also created fake Coronavirus maps to spread malware. According to another interesting report, a malicious Android application has appeared as a Covid-19 tracking map from Johns Hopkins University, with a hidden password-stealing malware AZORult (Doffman, 2020). However, according to the National Fraud Intelligence Bureau (NFIB) majority of reports, scams related to online shopping where people had ordered protective face masks, hand sanitiser, and other products that were never delivered (Avon and Somerset Police, N.D). To avoid being conned, NFIB has advised people not to panic when doing online shopping, be alert, take time to read reviews of the site before proceeding with an order (Avon and Somerset Police, N.D).

2.0 Corona is a visible threat; cyber-criminal is an invisible threat

The Corona virus has the characteristics of a silent killer and a threat just like a hacker, but unlike a hacker the location of the Corona virus is traceable. They both have the capacity to inflict unimaginable damage to humans beyond boundaries without causing structural damage. That makes the Corona virus and the malware spread by the hackers the biggest threat to global wellbeing, and its impact on the global economy, livelihoods and lifestyles is difficult to assess. That makes us all vulnerable and risk being easy prey to hackers, scammers, and spammers who will not waste any time in catching us off guard.

Every one of us as individuals and organisations, state institutions need to be alert to this threat and be over vigilant to protect ourselves from unauthorised access to protected data including health records, bank accounts and credit/debit cards, mobile numbers and other sensitive information held by the relevant organisations. It is incumbent on them to put in place additional measures to deny access to any personal data that they hold. The hackers offer stolen data to third parties, advertising agencies, marketing and sales promotions agencies in rerun for large sums of money. They also use stolen data to blackmail and persecute individuals, and organisations, demanding ransom payments. Widespread fraud is common practice in the hacker’s world.

According to the Identify Theft Resource Centre, one of the top three reasons for major data breaches is employee error and negligence, unauthorised access to protected data, and unrestricted access to remote communications technology to employees without proper vetting procedures in place prior to recruiting (Schoettle, 2020). The demand for prompt action in the working environment and the busy daily lifestyles attract the attention of malicious actors knowing that people will unwittingly open spam emails that look convincing, and that allows malware or ransomware implant in the user’s computers, or even mobile devices.

The sudden increase in remotely working environment makes the organisations more vulnerable to the new set of cyber security risks, and given that communication and data transmission happens entirely online, the hackers find it easier to trick the vulnerable groups to gain access to digital systems. Even the extra precautions that the employees might take, their vulnerability to unauthorised intrusions via malicious emails will be greater because of verbal verification of emails received from colleagues is affected by remote working. Also, access to the internet via home broadband or the network systems has inbuilt risks unless the system itself is protected by reliable firewall software (or VPN) giving added protection as it is the case in organisations.

Phishing is a type of invisible cyberattack usually delivered by email by the scammers to send malicious messages that appear to be from a trusted source with the intention to confuse the recipient in an effort to either obtain login details or infect the user interface with malware, or both (National Cyber security Centre, 2018). In the prevailing Corona affected circumstances and the imposition of curfew, the public is having to depend on shopping using online services rather than conventional methods than ever before. This requires the buyers to become alert to potential cyber intrusions, and the buyer should carry out online checks for authenticity of the products and credibility of the vendor, especially the person or the company name, contact details, not just the address but also the phone number and email address before placing the order.

Another online fraud is to obtain money through donations to fake charities online (Tidy, 2020). The Corona pandemic is an ideal opportunity for the fraudster to trick the public by appealing for donations to a good cause. Therefore, anyone wishing to make donations could be in for a surprise when the generous contribution made had fallen directly or indirectly into scammer's accounts. One of the methods the scammers use is cloning the title of registered charities, and it is for that reason checks should be carried out before making online donations to ensure the funds go to the genuine beneficiary.

The country is in total lockdown and people are confined to their own homes in order to avoid further spread of the virus. The educational institutions are closed and those continuing academic work are having to rely on virtual platforms to progress academic work including the exchange of emails. This will inevitably lead to a higher frequency of use and a larger volume of data transmitted using mobile phones, laptops, desktop computers, portable tabs and mobile broadband equipment, and the use of the telephone networks and the internet place the user in a high risk situation. It is not difficult to be deceived by rogue emails resembling a genuine email originating from a known sender, and to steal credentials of the recipient by linking to a faked log in page. Although mostly emails could be filtered and removed as spam by standard firewall software (National Cyber security Centre, 2018), those carrying aggressive malware will get through to cause serious damage to the system and compromise personal information held in the system in use. Therefore, it is important to maintain constant vigilance and increased awareness of the threats of phishing attacks.

3.0 What should be done to prevent cyberattacks and remain secure online?

The task force including the ministry of health set up by the government, issue health advice and guidance on the ways to avert the spread of Corona epidemic. One of the important preventive measures is to cleanse and sanities hands to avoid contamination from the virus (WHO, 2020, Interim Recommendation). This advice is also repeated by the cyber security experts stressing that the computer users must be aware of the risks when downloading email attachments from unknown sources (McAfee, N.D). The 'must do' rule is to validate the authenticity of the email and the sender and, 'must not do' rule is open the email. The best way to avoid inadvertently opening the email is to hover your mouse cursor over the email and see whether it has come from a genuine organisation or a person, if in doubt do not open it.

Here are a few tips you need to follow when you work from home. Cybercriminals use emergencies such as COVID-19 to get people to make decisions quickly. Therefore, do not make hasty decisions because if you did, it would be too late to undo it. Always take your time and think twice about a request for your personal information. However, if you believe that your credentials such as your username or passwords were compromised by the cybercriminals, immediately change your credentials on each site you had used.

Ensure all the devices used including the internet routers are up to date with anti-virus software, run regular updates to ensure the laptops and PCs have the latest firewall protection against emerging malware. Always use secure and known internet connections and, any special software needed, download or install them only from trusted sources. Hackers often set up Uniform Resource Locators (URL) that resemble real websites, to harvest passwords. Therefore, verify the URL of any website before you proceed. It has been revealed that there are number of Corona virus related domain name registrations recently. To protect yourself from phishing attacks online, users need to be extra vigilant. If you have any questions about the validity of an internal company email, do not hesitate to contact the sender before making any transactions or changed payment instructions.

Confidential means exactly that. Therefore, the employees should always remember that the same care should be taken when working remotely as you would do if you were in the office. A Personal email should not be used for any company business.

Companies also have a role to play. They should put in place a communication mechanism to stay in touch outside company hours, in case of an emergency arising from a cyberattack (malware, ransom, DDoS or other types). Furthermore, they can also set up controls that mitigate risks, such as restricting access to employees working off site. It is also a good practice to encourage employees to report anything that looks suspicious to the company in order to increase awareness amongst the staff.

References

Avon and Somerset Police, (N.D) *COVID-19 Fraud* [Online]. Available at: https://www.avonandsomerset.police.uk/media/32957917/covid-19-fraud-guide.pdf (Accessed: 20 August 2020)

Cuthbertson, A. (2020) *Coronavirus 'fearware' sees hackers exploit covid-19 panic to target victims* [Online]. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/coronavirus-hackers-covid-19-china-fearware-malware-a9400141.html (Accessed: 28 September 2020)

Doffman, Z (2020) *Warning: You Must Not Download This Dangerous Coronavirus Map* [Online]. Available at: https://www.forbes.com/sites/zakdoffman/2020/03/11/warning-you-must-not-download-this-dangerous-coronavirus-map/?sh=2567dda73253 (Accessed 14 August 2020)

McAfee, (N.D) *McAfee Security Tips: 13 Ways to Protect Your System* [Online]. Available at: https://www.mcafee.com/enterprise/en-gb/threat-center/protect-system.html (Available at: 18 August 2020)

National Cyber security Centre, (2018) Phishing attacks: defending your organisation [Online]. Available at: https://www.ncsc.gov.uk/guidance/phishing (Accessed: 23 August 2020)

Pettit, H. (2020) SQUASH THE BUG Instagram bans coronavirus filters – including dangerous one that 'diagnoses' killer virus [Online]. Available at: https://www.thesun.co.uk/tech/11180756/instagram-ban-coronavirus-filter-diagnose/ (Accessed: 12 September 2020)

Schoettle, A. (2020) *Hackers pounce as coronavirus spread triggers work-at-home movement* [Online]. Available at: https://www.ibj.com/articles/hackers-pounce-as-coronavirus-spread-triggers-work-at-home-movement?__cf_chl_jschl_tk__=pmd_7pJoYFJfdqgBBViuML_8R0qXczOEjb.ZCwaJnIn2z60-1630934509-0-gqNtZGzNAjujcnBszQhR (Accessed: 12 August 2020)

Tidy, J. (2020) *Coronavirus: How hackers are preying on fears of Covid-19* (Online). Available at: https://www.bbc.co.uk/news/technology-51838468 (Accessed: 4 November 2020)

WHO, (N.D) *Beware of criminals pretending to be WHO* [Online]. Available at: https://www.who.int/about/cyber-security (Accessed: 12 October 2020)

WHO, (2020) *Interim Recommendation* [Online]. Available at: https://www.who.int/docs/default-source/inaugural-who-partners-forum/who-interim-recommendation-on-obligatory-hand-hygiene-against-transmission-of-covid-19.pdf (Accessed: 19 July 2020)

ANNEXURE C.9

Do we need to revisit GDPR in the wake of Big Data during COVID-19?
This document was submitted to the Breaking Boundaries Conference- 2021.

Bentotahewa, V. Hewage, C. and Williams, J. (2021) Do we need to revisit GDPR in the wake of Big Data during COVID-19?, *Breaking Boundaries Conference*, Cardiff, 2021, Available at: https://miro.com/app/board/o9J_lHO0lqA=/)

Abstract

This poster focuses on challenges that associated with generation of large volume of data (Big data) during COVID -19 and, whether there is a necessity to revisit GDPR in the wake of emerging challenges. The GDPR is a mutually agreed framework established for the purpose of harmonising data privacy laws across Europe as well as providing greater protection and rights to the individuals, and to ensure that sharing of information will not infringe on personal data privacy.

In modern digital age, data is collected using multiple sensors as well as by way of various applications that are designed to monitor and record user movements, communications, interactions, and transactions. The generation of big data in this way by countries and organisations to control the pandemic has become common practice especially during the current pandemic. Therefore, it is important to ensure that the information is securely collected, processed, transmitted, stored, accessed, and retrieved. The data protection laws are designed to do just that, to provide a citizens personal data protection safety screen.

Key words: COVID-19, Big Data, GDPR, Data privacy

1.0 Introduction

The urgency of the need to manage and find cures for the COVID-19 has also made it necessary to collect data in volumes. Number of countries had developed contact tracing apps as a digital tool to diagnose the presence of the virus, and to prevent transmission and mitigate the risk of worsening of the pandemic (Bentotahewa, et al. 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?) *(*Bentotahewa, et al. 2020, Big Data in the wake of Data Protection Laws – Asian Perspective). The contact-tracing apps do generate large amount of big data, and the impact of contact tracing apps cannot be taken in isolation, the focus should also be on the impact of using wearable bands and police surveillance drones (Bentotahewa, et al. 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?) *(*Bentotahewa, et al. 2020, Big Data in the wake of Data Protection Laws – Asian Perspective).

The growing dependency on digital technology is becoming a way of life and, the increased use of video technology (CCTV) for surveillance operations to collect data of personal identities raises concerns. This method has become a common practice in gathering information about people, their movements at workplace as well as in public places (Bentotahewa, and Hewage, 2020, Challenges and Obstacles to Application of GDPR to Big Data) (Bentotahewa, et al., 2020, Big Data in the wake of Data Protection Laws – Asian Perspective), particularly during the pandemic. The concerning implication is whatever and whoever using such mechanisms will be infringing on public privacy in one way or another. In this context, the application of data protection law faces many challenges in the digital age, and the emergence of Big Data is perhaps considered to be the greatest. Although many organisations insist that once information has been processed anonymously, the identifiers will be hidden, but the protection of privacy cannot effectively be achieved through anonymous protection only (Bentotahewa, et al., 2020, Big Data in the wake of Data Protection Laws – Asian Perspective).

2.0 Aims and objectives

This poster intends to focus on the conflict between Big Data and GDPR. The objectives of this research is to highlight the sources of Big Data, Principles of GDPR that contradicts Big Data concept and to present a roadmap that would encapsulate the interests of Big Data and GDPR.

3.0 Methodology

The researcher conducted an extensive literature survey of previous research papers, journal articles, previous survey reports and government publications on the above topic/s.

4.0 Discussion

Regardless of technology used in processing Big Data and storing in an IT system, the GDPR provides protection to personal data (European Commission, N.D, What is personal data?). In all cases, unless personal data can be truly anonymised, personal data is subjected to protection requirements set out in the GDPR (European Commission, N.D, What is personal data?).

The Section 5(1)(b) of the GDPR article sets out the fundamental notion that personal data must be collected for a specific, explicit, and legitimate purpose (Information Commissioner's Office, 2018, Guide to the General Data Protection Regulation (GDPR)) but in the case of Big Data, the purpose is not clearly defined. Big Data is generated using different devices and it is impossible to give a legitimate reason for collecting data. In addition, the GDPR specifies that it is important to obtain consent before collecting any personal information (Information Commissioner's Office, 2018, Guide to the General Data Protection Regulation (GDPR)) but in practice it is difficult to do so.

Data Minimization and Proportionality is another key principle in GDPR (Information Commissioner's Office, 2018, Guide to the General Data Protection Regulation (GDPR)). Only the minimum data necessary should be collected, and processing activities should be proportionate to the legitimate interests of the company in responding to COVID-19. There is a clearly visible mismatch between the principle of GDPR and the practices of Big Data analysis. Under the Big Data concept, firms do provide a clear incentive to collect and retain as much data as they can for as long as possible (Bentotahewa, et al., 2020, Big Data in the wake of Data Protection Laws – Asian Perspective). In theory, more data will provide greater knowledge and greater benefit to the organisations and the society in general (Bentotahewa, et al., 2020, Big Data in the wake of Data Protection Laws – Asian Perspective). However, it does not necessarily guarantee personal privacy of the people in all means.

5.0 Conclusion

The biggest challenge for big data from a security point of view is the protection of individual privacy. Big data often contains huge amounts of personal identifiable information (PII) that makes privacy of users a huge concern. Given the large amount of data stored, breaches affecting big data would have devastating consequences that would in effect be more serious than the data that has already been exposed due to the security breach.

Against that background, it is crucially important to strike a balance between privacy of individuals and security of the state and the organisations. In researcher's view, that makes the case for understanding the importance of Big Data generated, and the need to develop a 'Big Data friendly' data protection measures that would serve the interests of organisations as well as the individuals. Not doing so, organisations will not reap the benefits of Big Data on one hand, and on the other, it will also affect privacy of individuals in the long term.

References

Bentotahewa, V and Hewage, C. (2020) *Challenges and Obstacles to Application of GDPR to Big Data* [Online] Available at: https://www.infosecurity-magazine.com/next-gen-infosec/challenges-gdpr-big-data/ (Accessed: 23 February 2021)

Bentotahewa, V. et al. (2020) *Do Privacy Rights Override #COVID19 Surveillance Measures?* [Online] Available at: https://www.infosecurity-magazine.com/next-gen-infosec/privacy-rights-covid19/ (Accessed: 22 February 2021)

Bentotahewa, V. et al. (2020) *Big Data in the wake of Data Protection Laws – Asian Perspective* [Online]. Available at: http://southasiajournal.net/big-data-in-the-wake-of-data-protection-laws-asian-perspective/ (Accessed: 13 March 2021)

European Commission. (N. D) *What is personal data?* [Online]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (Accessed: 2 March 2021)

Information Commissioner's Office. (2018) *Guide to the General Data Protection Regulation (GDPR)* [Online]. Available at: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (Accessed: 3 March 2021)

ANNEXURE C.10

Security and privacy issues associated with Coronavirus diagnosis and prognosis

This document was presented at the EAI conference and the paper was published in the SpringerLink

Bentotahewa, V., Hewage, C., and Williams, J. (2021) Security and Privacy Issues Associated with Coronavirus Diagnosis and Prognosis. In: Paiva S., Lopes S.I., Zitouni R., Gupta N., Lopes S.F., Yonezawa T. (eds) Science and Technologies for Smart Cities. SmartCity360° 2020. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol 372. Springer, Cham. Available at: https://doi.org/10.1007/978-3-030-76063-2_8

Abstract

The urgency of the need to manage and find a cure for the COVID-19 has made it necessary to share information. However, sharing information involves potential risks that are inevitably likely to infringe individual privacy. Therefore, whether permissible under extenuation circumstances or not, sharing and handling of information for medical diagnosis and prognosis need consideration without ignoring the need to protect privacy. This makes it important to strike a balance between protecting individual privacy and collecting information to combat the virus, the responsibility for doing so rests with the state. However, circumstances in which the COVID-19 pandemic appears to be accelerating, the medical professionals and the government seem to be focusing more on collecting information that could be used to limit the extent of the outbreak and mitigate the risks. Such a strategy overrides perception of the need to protect personal privacy. This paper investigates the security and privacy challenges associated with SARS-CoV-2 diagnosis and prognosis using case studies from different countries.

Keywords: Security, Privacy, Data Protection, General Data Protection Regulation, Coronavirus diagnosis, COVID-19

1.0 Introduction

In general, there is a wide public appreciation of their health privacy. The GPs (General Practitioners) and health clinicians take necessary measures to keep vast majority of sensitive information confidential. However, in unprecedented circumstances like COVID-19 pandemic, the privacy protection measures in the health sector may outweigh the risks to the public when measured against the privacy risk to the individual (Wetsman, 2020). In such instances, the need to share patient information with research institutes and third parties can become necessary and can be justified, given that the overriding aim is to monitor and control the spread of the virus, and to provide guidance on preventive measure to keep the communities safe.

Over time, the General Data Protection Regulation (GDPR) has been reviewing the necessity for data processing in the interest of public health and, in recognition of the public interest, has accepted the need for lawful processing activities for the purpose of monitoring the spread of the epidemic. This provision has been endorsed in the article 9(2) (i) in the GDPR with an exemption to processing health related data that is otherwise considered sensitive and prohibited from processing (Information Commissioner's office, N.D, Guide to the General Data Protection Regulation (GDPR)). However, concerns have already been raised about the measures taken by the government and the tech industry, and their response to the coronavirus outbreak, and the implications of the use of contact tracing apps and digital immunity passports on privacy, during and after COVID-19 pandemic. The use of technological solutions to combat COVID-19 is perceived with scepticism by the public and should remain vigilant of those using them.

2.0 Research Background (The use of personal information during COVID-19)

European Data Protection Board issued a statement in March 2020, confirming that the GDPR contained a provision for legal grounds for enabling employers to process data in the context of epidemics such as COVID-19 without consent of the employees but obtaining consent in unforeseen circumstances will become necessary to comply with national legislations (European Data Protection Board, 2020, Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak). However, commercial organisations based in Italy or France do not conduct autonomous systematic collections of health data from employees (PrivSec Report, 2020). That includes requesting information relevant to potential symptoms, temperature-taking requirements, or details of medical reports. As stated in the guidelines issued by the Italian data protection authority, the collection of COVID-19 associated health data must be left to the public health authorities (PrivSec Report, 2020). Also, the French data protection authority has set out examples of unlawful processing of data, specifically for collecting daily temperature readings of the employees and the visitors, and for collecting medical files from all employees (PrivSec Report, 2020). On the flipside, the employees in Italy and France are obliged to inform employers of any suspected symptoms of the coronavirus as a measure to protect health and safety of their work environment (PrivSec Report, 2020).

In general, countries such as Belgium, Luxemburg, Estonia, Netherlands, France and Peru prohibit collection of data in the form of temperature readings and medical questionnaires, and the disclosure of the identity of individuals who are suspected of carrying coronavirus or confirmed infected by it (Tuttle, and McKenzie, 2020). Philippines, China, Russia, European Union, Singapore, Hong Kong, South Africa, Ireland, Israel, Switzerland, Italy, United Kingdom, Japan, United States are less restrictive (Tuttle, and McKenzie, 2020). They acknowledge the need to process and disclose data without consent for the purpose of contact tracing, response measures. Also, according to the reports, the recorded data could be processed and exchanged among data controllers and law enforcement institutions (Tuttle, and McKenzie, 2020). The guidelines for data collection are more specific in Argentina, Australia, Iceland, Austria, Canada, Mexico, New Zealand, Norway, Czech Republic, Portugal, Finland, Germany, Greece, Sweden, Turkey (Tuttle, and McKenzie, 2020). Personal information collected for COVID-19 prevention should be used for collected purpose only and should be deleted after the pandemic. The disclosure of the identity of the patient requires consent and processing is permissible only on a need basis to protect the vital interests of the individuals and the public (Tuttle, and McKenzie, 2020). Clearly different countries have different rules and regulations in place to combat the common enemy in coronavirus, therefore, over focusing on personal privacy should not divert attention away from the key objective to combat the virus, for the sake of personal privacy.

To mitigate the risks of spreading and worsening of the pandemic, scanning methods are being used to diagnose the presence of the virus whilst some countries are developing contact tracing apps. The google/apple apps provide a decentralised software architecture and save a log of the user contacts within the app without uploading to a government server (Kelion, 2020, NHS rejects Apple-Google coronavirus app plan) (Bentotahewa, Hewage, Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?). In contrast, the initially proposed NHS contact tracing app in the UK logged information of users in a centralised database of government servers (Kelion, 2020, NHS rejects Apple-Google coronavirus app plan) (Bentotahewa, Hewage, Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?). According to experts, centralised contact tracing system allows better management of the pandemic as data collected from all part of UK can be used for macro managements of the pandemic (e.g. enforcing local lockdowns). However, understandably, this method of holding personal data in a centralised database with access to government departments and law enforcement agencies makes the public jittery about how and when the said authorities would use personal information, they have access to. Therefore, public concerns about the use of surveillance operations on a scale never seen before stand to reason.

France is one of the few European countries to have opted for a centralized model for coronavirus contacts tracing. The French government has chosen to have user information fed into a central server. However, downloading and installation of the app is voluntary (Osborne, 2020) (Bentotahewa, Hewage, Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?). UK also adopted a centralized approach to track and trace (Kelion, 2020, NHS rejects Apple-Google coronavirus app plan) (Bentotahewa, Hewage, Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?), and to allay any public concerns about the contact-tracing app, those who developed the NHS app, gave assurances that collected data would not be shared with other government departments or private companies (Sabbagh, Hern, and Proctor, 2020) (Bentotahewa, Hewage, Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?). However, UK discontinued the contact tracing app in use at the time and shifted to a model provided by Apple and Google (Kelion, 2020, UK virus-tracing app switches to Apple-Google model).

The World Health Organisation (WHO) meanwhile has listed two diagnostic tests for emergency use during the COVID-19 pandemic. One is genesis Real-Time PCR and the second is cobras SARS-CoV-2 (World Health Organisation, 2020, WHO lists two COVID-19 tests for emergency use). Aligning with WHO recommendations, two different types of tests are used in the UK. These tests include staff-administered regional test sites, mobile test units and self-administered home tests (Department of Health and Social Care, 2020). The testing process involves the collection of personal information of the targeted individual, such as the first and the last names, and even vehicle registration numbers. In the case of an individual taking the test at a regional test site, the information of other household members are also collected, and retained for further testing, if the person tested happened to be diagnosed positive (Department of Health and Social Care, 2020). That in effect is an infringement not only on individual privacy but also on everyone associated with the COVID-19 diagnosed person.

However, regardless of questionable infringement on personal privacy, the GDPR and the Data Protection Act 2018 provide a legal basis to justify collecting and withholding personal data. Article 6(1)(e) in GDPR states that processing is necessary to assess the performance of its official tasks that are carried out in the public interest, and to provide and manage a sustainable health service (Information Commissioner's office, N.D, Guide to the General Data Protection Regulation (GDPR) (Department of Health and Social Care, 2020). Also, the Article 9(2) (i) in GDPR states that processing is necessary to serve in the interest of public health (Information Commissioner's office, N.D, Guide to the General Data Protection Regulation (GDPR) (Department of Health and Social Care, 2020). The Data Protection Act 2018, Schedule 1, Part 1, (2) (2) (f) also states that the authorities can collect and process data for health or social care purposes (Department of Health and Social Care, 2020).

3.0 Discussion and recommendations

The world has been affected by the COVID-19 and is facing an unprecedented pandemic. With the rising demand for essential items and testing equipment, the health services call for urgent response to save lives. The biggest challenge the authorities faced was to prevent the spread of the virus going out of control. Given the urgency of the situation, number of states resorted to digital surveillance technologies for tracking and monitoring purposes.

The use of surveillance equipment infringes privacy of individuals even in the middle of a worldwide public health crisis, and the application of human rights laws stands regardless, and the states cannot simply turn a blind eye to privacy and freedom of expression. The human rights and civil society organisations around the world reacted with one voice calling all governments to adhere to human rights laws when employing digital surveillance technologies. In practice, the contact tracing app entails data gathering on an unprecedented level and that makes it open to unauthorised disclosure. Adding to the concerns, the Amnesty International UK director suggested that the Government should be looking at decentralised app models that do not store contact-tracing data on state run data bases (Robinson, 2020) (Bentotahewa, Hewage, Williams, 2020, Do Privacy Rights Override #COVID19 Surveillance Measures?). In response, the UK government released the current version of the app based on decentralised architecture, and Amnesty International UK welcomed this change of heart by the government (Amnesty International UK, 2020, Amnesty gives cautious welcome to UK government U-turn on contact tracing app). Therefore, it is recommended to pursue privacy preserving contact tracing efforts to tackle privacy and security infringements during the global pandemic.

Healthcare professionals also do have a vital role to play in protecting privacy of individuals during this pandemic. U.S. Department of Health and Human Services posted a bulletin to remind health-care workers that information about 'an identifiable patient' may not be disclosed to the media or the public without 'written authorization of the patient' except in special circumstances (Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information, 2009), and issued a briefing page specifying how Health Insurance Portability and Accountability Act (HIPAA) relates to the COVID-19 outbreak. The health care providers including the doctors receive professional advice on restrictions barring the release of specific information about personal identity of the patients tested Coronavirus positive or negative without written authorization from the patient (Tompkins, 2020). However, if it is deemed necessary to have patient information for monitoring or prevention purposes, the authorities can get 'de-identified' data (e.g., the use of anonymized and pseudonymized data). The Personal Information Protection and Electronic Documents Act (PIPEDA) is the national privacy law of Canada, and it regulates personal information disclosure. Under PIPEDA and, under provincial patient privacy legislation where it exists, consent is required to collect, use, or disclose an individual's personal health information (Zhang, 2020) Increased awareness about handling sensitive data focusing health professionals would reduce the impact of privacy and security risks.

In the prevailing pandemic environment, companies, employers, and public institutions face with unique privacy, data security, and cybersecurity implications are grappling with finding response solutions to the Coronavirus, and how to handle the legal implications of collecting and sharing health information of their employees and customers. Also, they are obliged to consider the circumstances under which the information about the employee health conditions and diagnosis could be disclosed to the workforce, and to the public health authorities. Given the exemption in Article 9 of GDPR for processing of health data, companies should track and follow the guidance provided by the data protection authorities in the applicable jurisdictions (Information Commissioner's office, N.D Guide to the General Data Protection Regulation (GDPR). However, it has been reported, the overarching theme amongst the EU member states puts emphasis on the employers to focus on facilitating measures and encouraging voluntary self-reporting by the employees, instead of obligatory gathering of private medical information from them (PrivSec Report, 2020).

Data Minimization and Proportionality is one of the key principles in GDPR. Only the minimum data necessary should be collected, and processing activities should be proportionate to the legitimate interests of the company in responding to COVID-19. For instance, to maintain a safe and healthy workplace in the interests of the company, it may not be a requirement to share with other employees, the identity of an employee or identities of his family members with reported symptoms of COVID-19. Theoretically however, more data will provide greater knowledge beneficial to the organisations and the society but enforcing data minimisation will limit the success of the desired purpose. According to the GDPR, data minimization could be achieved by pseudonymization (Bentotahewa and Hewage, 2020, Challenges and Obstacles to Application of GDPR to Big Data) (Zarsky, 2017, P.995-1020). However, one can argue that removing identifiers to achieve pseudonymization could potentially undermine the quality of the results derived as the data would be purposefully altered (Bentotahewa and Hewage, 2020, Challenges and Obstacles to Application of GDPR to Big Data).

A report released by the General Medical Council in the UK states that passing information about notifiable diseases to the relevant authorities for communicable disease control and surveillance is of vital importance (General Medical Council, 2017, P. 1-4), and in the same context, it is important to gather patient information mostly for educational and training purposes. According to one of the key principles of the GDPR, the processed data should only be used for the purpose for which it is collected and should not be kept for longer than it is necessary (Goddard, 2017, P.1-4). However, the UK Government has informed that they would be using information about people for different purposes that are not directly relevant to healthcare (Department of Health and Social Care, 2020). These include research into COVID-19, planning of services or actions in response to COVID-19, monitoring progress and development of COVID-19 (Department of Health and Social Care, 2020). However, it has been emphasised that the information self-collected and provided by the public for COVID-19 testing will not be used for any other purpose that is not linked to COVID-19 (Department of Health and Social Care, 2020). The use of anonymised information by the authorities would be the better option to avoid any privacy implications. However, if it deemed necessary to use patient identifiable information, or it became practically not feasible to anonymise information, the relevant authorities have the option to inform the patient and obtain explicit consent from the patient before disclosing information to anyone not involved in the provision of direct care to the patient. That will reassure the public that their privacy would remain confidential, and authorities and governments could expect public support with the knowledge that their privacy would not be compromised even for a good cause.

Apart from the medical professionals and governments, media also should play a responsible role when reporting on COVID-19 diagnosed individuals. The media has a responsibility to report facts and expose the truth to the public. They should also be aware of any distress that may be caused to the individuals when reporting on privacy issues. In South Korea, fears of a homophobic backlash are reported to be growing after a man infected with coronavirus had been spotted in clubs around Seoul's gay district (Kim, 2020). Homosexuality is not legal in South Korea and many Korean gay people manage to maintain anonymity and keep their sexuality discrete from family members and colleagues (Kim, 2020). According to media reports, a 37-year-old IT engineer had been spotted in three clubs after staying away for months, and since had been in fear of losing his job, and even had been reluctant to come forward to take the test (Kim, 2020). The privacy concerns arise from fear of being stigmatised, discriminated, and socially isolated. These prejudices have caused stress to gay community members and they have been in fear of identity exposure and retribution, also the social attitudes run so deep they would even lose their jobs. Irresponsible reporting by the media has led to this situation. It is unfortunate that lack of concerns for the gay community and open media reporting of their rights to individual to privacy has caused immense damage to a selected group of people for being different.

Also, similar cases of social stigmatisation of COVID-19 affected people, and infringements on their privacy have been reported in many parts of India. The names and addresses of 46 people (in Ajmer) suspected of having contacted the virus have been published in some local Hindi newspapers (Jaiswal, 2020), and a report containing personal details of 300 people who were home-quarantined or confined to self-isolation (Jaiswal, 2020), posted on a social media has gone viral. In Delhi and Chandigarh, posters carrying the names, quarantine period and the number of people in the family who had been asked to remain in isolation have been glued outside the homes of those suspected to carry the virus (Jaiswal, 2020), (Bhandari,2020). The Mohali district administration has gone as far as publishing on its website, the names, phone numbers and residential addresses of not only those presumed to have been coronavirus positive but also the details of their family members (Jaiswal, 2020).

The repercussions of privacy violations through reporting could be long lasting and could leave people mentally affected for being stigmatised. This will also impact on those living in close knit communities. The unauthorised disclosure of privacy data compromises personal security and confidentiality of people, also it has a negative impact on medical ethics. Therefore, it is vitally important to implement necessary mechanisms to contain the pandemic and it is also equally important the government or the media organisations do not arbitrarily share data of COVID-19 positive case in the public domain. Some U.S. states (Ohio, Florida) took the same stand making patient privacy a priority (Zhang, 2020).

There is also another security and privacy debate surrounding SARS-CoV-2 antibody tests and immunity passports. Those with low or no antibodies against SARS-CoV-2 are prohibited from returning to work until they were either immunised or hard evidence of immunity established (Loike and Fischbach, 2020). Those with certified immunity to COVID-19 are provided with an immunity passport, and those without will be denied access to a workplace, school, or restaurant until scanned security clearance as applicable. Whether the disclosure of antibody protection information violates personal privacy issues or not is a big question. If governments were to use SARS-CoV-2 antibody tests to control access to the workplace, people will have to compromise their privacy, at least to some extent than before. It is a choice between protecting privacy and protecting the masses and, practically, it is difficult to maintain self-respect, dignity and protect privacy to a high standard whilst fighting the pandemic. The reality is the protection of one person's confidentiality endangers another's welfare or public health.

A recent report by artificial intelligence research group, Ada Lovelace Institute warned that the immunity passports would be of high risks in terms of social cohesion, discrimination, exclusion, and vulnerability (Ada-Lovelace-Institute, 2020, P. 5-19) However, China has been using the Alipay Health Code for a while, but this version is not explicitly called an immunity certificate, instead functions same as the immunity passport (Ada-Lovelace-Institute, 2020, P. 5-19) Chile also has launched its own COVID-19 Immunity Card program (Thomson, 2020). Immunity certificates are still in their infancy, but as antibody testing becomes more widely available, more countries are likely to join in. U.S., UK, Italy, Chile, Germany have expressed interest in 'immunity passports' (Hancock, and Gullo, 2020), a system of requiring people to present proof of immunity to COVID-19 to gain access to public spaces, work sites, airports, schools, and other venues.

It is envisaged that the digital form of immunity passport system could easily be expanded to check not just a person's immunity status, but also to check other personal information, such as age, gender, pregnancy, health records (e.g., HIV status), or criminal history if relevant (Hancock, and Gullo, 2020). In such circumstances, the chance of people being exposed to the danger of data breaches could be high. It is worth noting that even before the COVID-19 the world experienced data breaches when medical data was compromised by the hackers. One such incident is in 2019, an HIV database in Singapore leaked personal information of more than 14,000 individuals living with HIV (Leyl, 2019).

It is crucially important to keep medical records securely stored in either paper or in electronic format (Harman, and Bond, 2012 , P.712). As a solution to the question of security and privacy implications, the idea of blockchain has been suggested by some, particularly regarding the immunity passport (Seifert, 2020). The blockchain technology (e.g., verifiable claims and Self Sovereign Identities (SSI)) could be the core innovation of digital immunity passport development. It will not only leave complete control of managing health data in the hands of the end user, but also give the employers and other stakeholders' peace of mind knowing that the data will not be unduly tampered with (Seifert, 2020). Looking ahead the same technology could be used for contact tracing, gathering and collating patient data, monitoring patients' movements and adherence to social distancing rules, whilst protecting their identity in doing so. Also, emerging technologies like Blockchain could device a platform that would directly or indirectly help future recurrences of an epidemic and manage it without compromising privacy and security of individuals.

4.0 Conclusion

The COVID-19 outbreak is an unwelcome unprecedented global pandemic threatening every aspect of human life across each continent of the world. The death toll continues to rise to an unimaginable level in some countries, whilst few have managed to contain it and minimise the impact. On top of that the economic costs are causing hardships and affecting livelihoods in every nation including the rich ones.

There are also other important issues emanating from the use of information of those tested positive and its impact on their privacy. Testing and tracing are considered necessary and essential to respond to the pandemic, and to prevent it spreading in the community. That requires personal data to be retained by the government and other authorities, inevitably raising a conflict between person's right to privacy and the need to log and share collected test results. Although technology has the capacity to contribute to pandemic combating strategy, it does also infringe privacy rights in circumstances where tracking and surveillance are used to monitor coronavirus affected individuals. The difficulty is to visualise the degree of surveillance and unexpected outcomes that will arise.

To start with, some countries have resorted to surveillance cameras and contact tracing apps to track the spread of COVID-19. That did raise public concerns about the use of such technology, but despite the concerns, the authorities continue with testing to identify those having the symptoms. The spectrum of data collected includes personal details of associates and those living with them. The latest development in the COVID-19 containment process will be the immunity passports that will make way for phased easing of restrictions towards normalising wider social interaction. Although the immunity passports look likely to compromise privacy, it fits the purpose. However, the researcher believes that the use of blockchain ledger will provide a compromised balance between health security and privacy of individual, as suggested by the experts.

Moving away from technology, people are becoming more concerned about the behaviour of media in reporting incidents related to COVID-19 and the media in many nations has come under scrutiny for failing to respect privacy of coronavirus affected individuals. The unethical insensitive reporting has caused distress to people and harmed them mentally, in some cases has treated disrespectfully and made them feel indignant. This supports the general belief that privacy is a sensitive issue and should not be open to violations. Therefore, the onus is on all parties, the government, healthcare professional and media to act in the public interest and protect their privacy. That said, it is also important to respond positively to extraneous circumstances which COVID-19 is one. Therefore, the use of technology and the measures taken to contain the pandemic can be justified given the risks of the incident developing into a crisis of unimaginable proportion in terms to loss to human life and the economic impact that will follow. It is equally important (for medical practitioners) to share patients' information for research purposes and to support the government in its effort to avoid a crisis. That underscores the importance of the need to strike a balance between privacy of individuals and the need to act positively in response to an unprecedented pandemic.

References

Ada-Lovelace-Institute. (2020) *Exit through the App store. Ada-Lovelace-Institute* [Online]. Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf (Accessed:10 June 2020)

Amnesty International (2020) *Amnesty gives cautious welcome to UK government U-turn on contact tracing app* [Online]. Available at: https://www.amnesty.org.uk/press-releases/amnesty-gives-cautious-welcome-uk-government-u-turn-contact-tracing-app (Accessed: 3 July 2020)

Bentotahewa, V., Hewage, C. and Williams, J. (2020) *Do Privacy Rights Override #COVID19 Surveillance Measures?* [Online] Available at: https://www.infosecurity-magazine.com/next-gen-infosec/privacy-rights-covid19/ (Accessed: 22 February 2021)

Bentotahewa, V. and Hewage, C. (2020) *Challenges and Obstacles to Application of GDPR to Big Data* [Online] Available at: https://www.infosecurity-magazine.com/next-gen-infosec/challenges-gdpr-big-data/ (Accessed: 23 February 2021)

Bhandari, H. (2020) *COVID-19 poster outside west Delhi house keeping people away* [Online]. Available at: https://www.thehindu.com/news/cities/Delhi/covid-19-poster-outside-west-delhi-house-keeping-people-away/article31176892.ece (Accessed 5 June 2020)

Department of Health and Social Care. (2020) *Coronavirus (COVID-19) testing: privacy information* [Online]. Available at: https://www.gov.uk/government/publications/coronavirus-covid-19-testing-privacy-information/testing-for-coronavirus-privacy-information (Accessed 15 June 2020)

Department of Health and Social care. (2020) *Guidance- Testing for coronavirus: privacy information* [Online]. Available at: https://www.gov.uk/government/publications/coronavirus-covid-19-testing-privacy-information/testing-for-coronavirus-privacy-information--2 (Accessed: 15 August 2020)

European Data Protection Board. (2020) *Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak* [Online]. Available at: https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en (Accessed 5 June 2020)

General Medical Council. (2017) *Confidentiality: disclosing information about serious communicable diseases*. *General Medical Council* [Online] Available at: https://www.gmc-uk.org/-/media/documents/gmc-guidance-for-doctors---confidentiality---disclosing-information-about-serious-communica-70061396.pdf?la=en&hash=354295801490DDF76262B585A680B52DCEB37D8B (Accessed: 23 September 2020)

Goddard, M. (2017) 'The EU General Data Protection Regulation (GDPR): European regulation that has a global impact'. *Sage Journals* Vol. 59 Issue 6. Available at: https://journals.sagepub.com/doi/abs/10.2501/IJMR-2017-050 (Accessed: 23 April 2020)

Hancock, A and Gullo, K. (2020) *Immunity Passports Are a Threat to Our Privacy and Information Security* [Online]. Available at: https://www.eff.org/deeplinks/2020/05/immunity-passports-are-threat-our-privacy-and-information-security (Accessed: 4 June 2020)

Harman, L B. and Bond, K. (2012) 'Electronic Health Records: Privacy, Confidentiality, and Security', *AMA journal of ethics*. Volume 14-9. Available at: https://journalofethics.ama-assn.org/sites/journalofethics.ama-assn.org/files/2018-05/stas1-1209.pdf (Accessed: 14 June 2021)

Information Commissioner's office. (N.D) *Guide to the General Data Protection Regulation (GDPR)* [Online]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (Accessed: 25 July 2020)

Institute of Medicine (US) *Committee on Health Research and the Privacy of Health Information. (2009) Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* [Online]. Available at https://pubmed.ncbi.nlm.nih.gov/20662116/ (Accessed: 13 June 2020)

Jaiswal, P B. (2020) *Privacy of COVID-19 suspects violated; names, addresses made public* [Online]. Available at: https://www.theweek.in/news/india/2020/03/22/privacy-of-covid-19-suspects-violated-names-addresses-made-public.html, (Accessed 12 June 2020)

Kelion L. (2020) *NHS rejects Apple-Google coronavirus app plan* [Online]. Available at:https://www.bbc.co.uk/news/technology-52441428 (Accessed 2 May 2020)

Kim, N. (2020) *Anti-gay backlash feared in South Korea after coronavirus media reports* [Online]. Available at: https://www.theguardian.com/world/2020/may/08/anti-gay-backlash-feared-in-south-korea-after-coronavirus-media-reports, (Accessed: 14 June 2020)

Leyl, S. (2019) *Singapore HIV data leak shakes a vulnerable community* [Online]. Available at: https://www.bbc.co.uk/news/world-asia-47288219 (Accessed: 11 June 2020)

Loike, J D and Fischbach, R L. (2020) *Opinion: Public Health Trumps Privacy in a Pandemic* [Online]. Available at: https://www.the-scientist.com/news-opinion/opinion-public-health-trumps-privacy-in-a-pandemic-67429 (Accessed: 5 June 2020)

Osborne, C. (2020) *France asks Apple to relax iPhone security for coronavirus tracking app development* [Online]. Available at: https://www.zdnet.com/article/france-asks-apple-to-relax-iphone-security-for-coronavirus-tracking-app-development/ (Accessed: 27 May 2020)

PrivSec Report, (2020) *CCPA & COVID-19: A Practical Guide to Addressing Privacy and Data Security Implications of the Coronavirus* [Online]. Available at:

https://gdpr.report/news/2020/03/23/ccpa-covid-19-a-practical-guide-to-addressing-privacy-and-data-security-implications-of-the-coronavirus/, (Accessed 3 June 2020)

Robinson, M. (2020). *How does the NHS COVID-19 contact tracing app work? Will it track my every move? Will it drain your battery? And why has the government shunned Apple and Google's system?* [Online]. Available at: https://www.dailymail.co.uk/news/article-8288211/How-does-NHSCOVID-19-contact-tracing-app-work.html (Accessed: 25 May 2020)

Sabbagh, D., Hern, A and Proctor, K. (2020) *UK racing to improve contact-tracing app's privacy safeguards* [Online]. Available at: https://www.theguardian.com/technology/2020/may/05/uk-racing-to-improve-contact-tracing-apps-privacy-safeguards (Accessed: 13 April 2020)

Seifert, R. (2020) *Blockchain can answer immunity passport security concerns, but any roll-out must be dictated by the science* [Online]. Available at: https://www.itproportal.com/features/blockchain-can-answer-immunity-passport-security-concerns-but-any-roll-out-must-be-dictated-by-the-science/ (Accessed: 13 June 2020)

Thomson, E. (2020) *World's first immunity cards are coming to Chile* [Online]. Available at: https://www.bloomberg.com/news/articles/2020-04-16/chile-to-start-controversial-coronavirus-immunity-card-system (Accessed 12 June 2020)

Tompkins, A. (2020) *What is HIPAA and how does it affect our understanding of the coronavirus?* [Online]. Available at: https://www.poynter.org/reporting-editing/2020/hipaa-and-coronavirus/ (Accessed: 3 June 2020)

Tuttle, B. and McKenzie, J. (2020) *Global Regulatory Guidance for COVID-19 Privacy and Security Issues* [Online]. Available at https://www.jdsupra.com/legalnews/global-regulatory-guidance-for-covid-19-43117/, (Accessed: 25 May 2020)

Wetsman, N. (2020) *Personal privacy matters during a pandemic — but less than it might at other times* [Online]. Available at: https://www.theverge.com/2020/3/12/21177129/personal-privacy-pandemic-ethics-public-health-coronavirus (Accessed: 28 May 2020)

World Health Organisation. (2020) *WHO lists two COVID-19 tests for emergency use* [Online]. Available at https://www.who.int/news-room/detail/07-04-2020-who-lists-two-covid-19-tests-for-emergency-use (Accessed 14 May 2020)

Zarsky, T. (2017) ‘Incompatible: The GDPR in the Age of Big Data’, Seton Hall Law Review Vol. 47 Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646 (Accessed: 23 May 2020)

Zhang, H. (2020). *With coronavirus containment efforts, what are the privacy rights of patients?* [Online]. Available at: https://theconversation.com/with-coronavirus-containment-efforts-what-are-the-privacy-rights-of-patients-131752 (23 April 2020)

ANNEXURE C.11

Privacy and security challenges and opportunities for IoT Technologies during and beyond COVID-19

This article was submitted to the IoTSCPSF-2021 in the form of a book chapter.

Abstract

The prevailing COVID-19 pandemic has put IoT based technologies to the test. It has given rise to diverse predictions for the future, and the expectations are that IoT inspired technologies will play a significant role in the new normal. However, one of the key challenges for the success of IoT is its privacy and security issues. This chapter presents a comprehensive review of privacy and security challenges and opportunities for IoT inspired solutions. Also, it provides an in-depth analysis of IoT inspired Big Data issues, data protection, and security concerns around IoT. The contributions of this chapter cover a comprehensive review of the IoT privacy issues and data protection policies, regulations, and laws, IoT security challenges and opportunities that need to be addressed in the next normal.

Keywords: Internet of Things, Privacy, Security, Big Data, Data protection, GDPR, COVID-19

1.0 Introduction

The Internet of Things (IoT) technology sees extensive growth with the increased number of smart devices connected via the Internet. The global market for IoT solutions is expected to grow to around 1.6 trillion USD by 2025 (Vailshery, 2021). These predicted trends will give rise to the expansion of opportunities created by the COVID-19 pandemic. The IoT solutions such as remote health monitoring, and contact tracing enabled authorities to successfully manage the spread of the Coronavirus. However, wider deployment of IoT inspired technologies face challenging obstacles such as privacy and security concerns. This chapter uptakes a comprehensive review of these challenges and an in-depth analysis of the issue.

1.1 IoT role during COVID-19 pandemic

Coronavirus disease 2019 (COVID-19) is an infectious illness caused by a novel and newly discovered Coronavirus (WHO, N.D). Some symptoms of the disease are shortness of breath, chest pain, and fever. On the 11th of March 2020, the World Health Organization (WHO) declared a global pandemic due to the COVID-19 outbreak. To reduce social contact during the pandemic, "some businesses must remain closed or follow restrictions on how they provide goods and services." (Government of UK-Cabinet office, 2021).

HARVARD Medical school has highlighted that in certain COVID-19 related heart injury patients, the initial symptoms might have occurred in several forms (Pesheva, 2020). Those without previous underlying cardiac problems might remain healthy, whilst in others, Oxygen supply failure to heart muscles might cause heart damage. In the context of COVID-19, the contributory factor would be the imbalance between 'supply and demand' for Oxygen to the heart. In the process of stabilizing Oxygen levels in the body, IoT played a key role in efficiently managing the Pulse Oximeter, Nebulizers and Oxygen tanks.

IoT technology has been used extensively for many purposes across diverse sectors during the pandemic as was referred to earlier, and their applications and frameworks have enabled successful management of the pandemic. Prior to the onset of the COVID-19 pandemic, IoT had been linked to certain key areas or catch phrases such as SMART homes, self-driving cars, smart metering, etc. However, in the aftermath of the pandemic, IoT was put into effective use across a wide range of sectors for purposes such as contact tracing, retail, and hospitality. The key IoT sectors affected by the pandemic, the economic/social impact, Technology Readiness Levels (TRL) are discussed in (Yousif, Hewage and Nawaf, 2021). An elaboration of the industries affected and the IoT solutions used during the pandemic is set out in the following subsections.

1.1.1 Affected industries

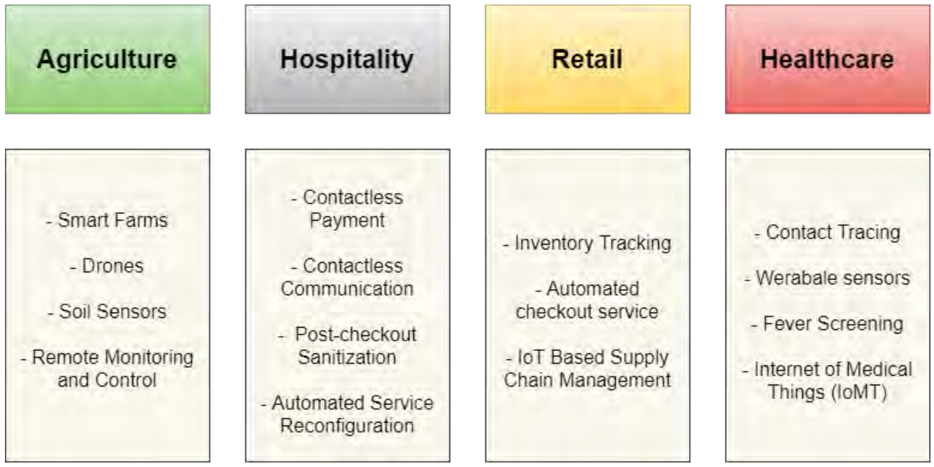
Different industries, such as the Hospitality sector and the Restaurant industry were affected by the COVID-19 pandemic. The knock-on effect was felt in small and medium enterprise sectors, and consequently, they were badly hit. For instance, 3% of restaurants remained permanently closed (Song, Yeon, and Lee, 2021); Tourism sector (Altuntas and Gok, 2021) 'because of travel restrictions and freedom of movement due to social distancing rules; Airline industry because of operational changes in air travel and airports, and the Travel agencies for the same reasons; Agricultural sector (Dutta, and Mitra, 2021), on which other sectors, mentioned above, depended on; the Retail industry on which the consumers relied on to sustain their livelihood (OECD, 2020, COVID-19 and the retail sector: impact and policy responses); Education delivery system switching to virtual distance learning (Ilieva, and Yankova, 2000); Healthcare services overwhelmed by the virus and COVID-19 cases. These are some of the examples of the affected industries, and the IoT solutions applied are highlighted in each case. The selected industries were chosen based on the background knowledge of the authors and the reviewed articles [16- 22].

1.1.2 IoT solutions

In the agriculture industry and with the use of sensors IoT based smart farms could survive. IoT smart farms allow data collection, tracking re- mote monitoring, and remote control. The use of IoT in agriculture makes factories more efficient, optimize treatment and input required, efficient water use, and will make the environment better (Dutta, and Mitra, 2021). By implementing IoT technologies such as drones and sensors we can monitor crop health, seed inspection, seed harvesting, and soil examination. The author in (Rowan, and Galanakis, 2020) proposes the use of immersive technologies and Information and Communications Technology (ICT) for remote end-user applications, also, to inform disruptive innovations.

The author in (Pillai et al., 2021) describes how IoT devices can lead to a hassle-free post-checkout sanitization that eliminates human to human interaction and enabled service reconfiguration, based on customer preferences survey of consumer behaviour and predictions in the hospitality industry. In addition, improvements to workplace safety can be made by installing real-time alarms to alert emergencies. IoT can also be used to ensure maintenance of hygiene standards in the sales outlets (cleanliness of restaurant tables, sanitiser solution concentration, contactless payment and communication) and adherence to social distancing rules (Suleman, 2021) (Embree, 2021) to minimize the need for manual interventions. The use of IoT retail self-checkouts such as kiosks, IoT automated systems such as Amazon warehouse, and RFID inventory tracking can help limit interaction between humans, thereby avoiding, human error, excess staff numbers, and enhance supply chain management with inventory, delivery, and storage (Panchal, 2019) (Dilmegani, 2021). There are diverse types of IoT wearables and devices for contact tracing, temperature screening used in the healthcare industry to ensure social distancing, accurate diagnosis, tracking, and health monitoring and provide exposure notification Triax Technologies, (N.D) (Metro Security, N.D).

The figure 6.1 below provides a summary of IoT solutions that are used in different industries.



Agriculture	Hospitality	Retail	Healthcare
- Smart Farms - Drones - Soil Sensors - Remote Monitoring and Control	- Contactless Payment - Contactless Communication - Post-checkout Sanitization - Automated Service Reconfiguration	- Inventory Tracking - Automated checkout service - IoT Based Supply Chain Management	- Contact Tracing - Werabale sensors - Fever Screening - Internet of Medical Things (IoMT)

Figure 6.1: Key IoT Solutions during COVID-19 Pandemic

This review provides an in-depth understanding of the main IoT sectors that played a vital role in managing the global pandemic and their potential applications in the post-COVID-19 future. Authors expect the usage of IoT based technologies, and applications to increase significantly during the next normal, matching lifestyle patterns such as working from home, distance learning, telemedicine, that have emerged during the pandemic.

The potential for this technology is immense, but the challenges are likely to be equally immense. Amongst other concerning issues, energy requirements of these IoT devices, and privacy and security are key priorities for consideration (Obaidat et al., 2020, P.1) (Waheed, et al., 2020) (Celik, et al., 2019). However, there is a lack of COVID-19 pandemic relevant literature published on the issues touched upon earlier. Therefore, in the absence of informative literature, the primary focus of this chapter will be on privacy and security issues associated with IoT data collection (Big Data) and security challenges. Subsec tion 1.2 summarises the privacy and security challenges of IoT.

1.2 Privacy and security concerns of IoT

Since the Internet of Things (IoT) came to being, its applications and the range of connected devices has multiplied, and in parallel, the expanding usage of IoT also induces many technical challenges potentially threatening the security and privacy of IoT end-users. Therefore, there is an imperative requirement to put in place risk mitigating solutions, sooner than later.

In the IoT environment, whilst safeguarding online security remains a major concern and a challenge, preserving privacy will also remain a significant challenge needing added attention. As an example, the privacy of the IoT end-users could be at risk if personal data happens to be leaked to unauthorized persons, or even through a security breach in the IoT (devices). Such incidents would potentially allow the attacker access to IoT end-user data without being tracked or traced by (face recognition) security cameras located in smart homes. Given the heterogeneity of IoT connected devices and in-built vulnerabilities of hardware and software in some of them, safeguarding end-user privacy might face many security challenges (Bertino, 2016, P. 1-3)

There are reported studies focussing on the privacy and security challenges of IoT (Obaidat et al., 2020) (Waheed, et al., 2020) (Celik, et al., 2019). However, this chapter provides an in-depth analysis of these important challenges especially in the aftermath of COVID-19. The discussion in Section 2 of this chapter focuses on the large volume of information generated through IoT devices, the analysis of security and privacy challenges associated with Big Data, and the provision of legal and policy solutions to protect privacy for maintaining trust between the data subject and data controller. IoT threats, security challenges, and proposed solutions are discussed in Section 3 of this Chapter. In addition, the impact of COVID-19 and the role of IoT in different industries is highlighted at the end of Section 3.

1.3 Study Methodology

The aim of this study is to review the privacy and security challenges of IoT technologies for the next normal. The research objectives of this study are listed below:

a. Identification and in-depth analysis of privacy and data protection challenges associated with Big Data generated via IoT Technologies

b. Analysis and discussion of security challenges for IoT technologies for next normal, and finally the identification and analysis of best practices and code of practices for IoT technologies

The review was carried out by using publicly available secondary data sources that explore and discuss different aspects of IoT technologies in diverse sectors. The main data sources used in this review are the SCOPUS library, Web of Science citation database, ACM library, IEEE Xplorer, Google Scholar and Researchgate. A number of keyword searches were used to find relevant studies and reviews necessary to answer the research questions of this study. An exclusion criterion was not used to provide a wider overview of the issue. In addition to the initial research by the authors, recommendations by previously published research, tutorials, surveys, and reviews were used to select the prominent privacy and security challenges to focus on in this study.

1.4 Structure of the chapter

This chapter is organized as follows: Section 2 discusses IoT vs Data protection; Security architectures are discussed in Section 3; Section 4 summarises the future privacy and security landscape for IoT. The conclusion of the study is provided in Section 5.

2.0 Data Protection vs IoT

IoT technology has been used widely during the COVID-19 pandemic for the purpose of mitigating and preventing the spread of the Coronavirus. These internet-connected devices did serve the purpose, but they also gave rise to an up surge of privacy and security risks associated with the collection of a large volume of data. Section 2 is dedicated to investigating IoT generated Big Data and what actions could be taken to protect them. Section 2.1 focuses on literature-based definitions for Big Data generated by IoT, associated threats, and the importance of protecting Big Data. The authors have dedicated section 2.2 to highlight the data protection challenges and existing solutions to overcome potential challenges. In section 2.3, the authors have flagged up relevant Data laws associated with Big Data in parallel with GDPR. Section 2.4 highlights policy mechanisms and their purpose in the context of Big Data.

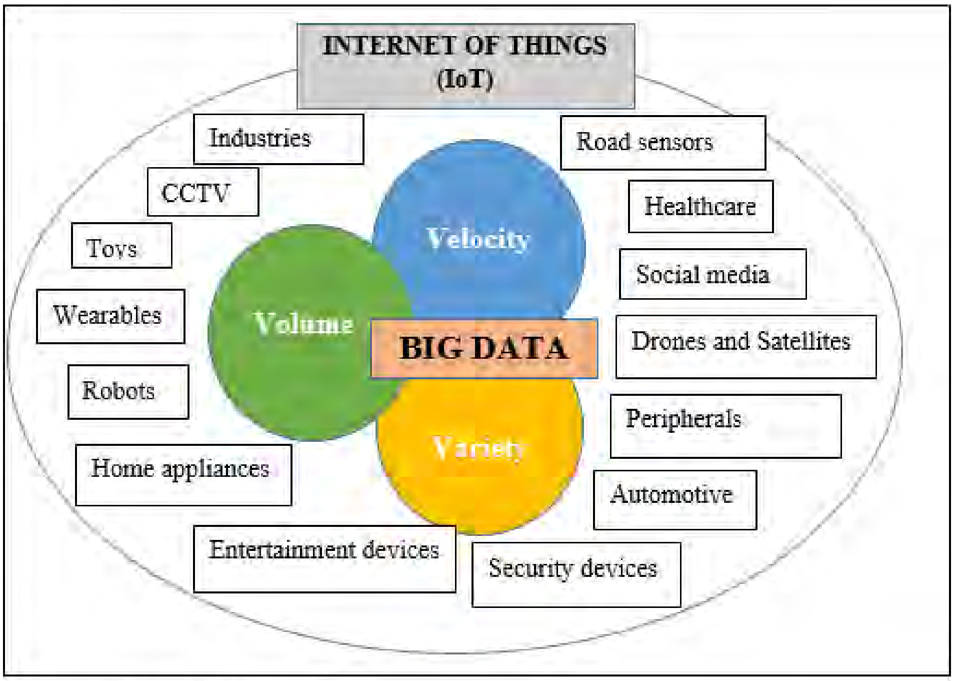
2.1 Usefulness and security of Big Data generated by IoT

The question that is often asked by those who are not familiar with modern tech jargon is ‘what is Big Data’. To explain it in simple terms, it is a vast amount of information collected for understanding and decision-making purposes using innovative forms of information processing (Wu, et al., 2014, PP.97-107). In professional literature, the definition of Big Data refers to, the volume of data collected, the variety of sources, the speed of analysis and interpretation that could be achieved through the analytical process (Erevelles, Fukawa, and Swayne, 2016, PP.897-904). Data collected in this way have the capacity to reveal information about individuals in terms of their habits, location, interests and a host of other personal information, and varying preferences that are stored in the systems for usage with ease. While there is no single definition of Big Data, the Information Commissioner's Office (ICO) believes that it is useful to regard Big Data as data which, due to several varying characteristics, is difficult to analyse using traditional data analysis methods (Richard, N.D].

Big Data comes in various formats (See figure 6.2), such as cell phone location information, CCTV recordings, social media contents from a variety of sources and satellite images (Oussous, et al., 2018, pp.431-448), and handling them is a significant challenge. Primarily, data that relates to an identifiable living individual is considered as Big Data in (Article 4(1), General Data Protection Regulation (GDPR) (Eur-Lex, 2016), but not all the Big Data, for example, climate and weather data is not personal data (Richard, N.D). Reports highlight the significant increase in the frequency of data breaches since 2015; 60% in the USA only (Tawalbeh, et al., 2020, P.4102). In 2016, the world was introduced to the security risks and vulnerabilities associated with smart technology aftermath of the Mirai IoT botnet Denial-of-Service (DoS) attack which caused widespread internet outages throughout the US and Europe (Rosenthal, and Oberly, 2020, P. 155). Another report suggests that according to a survey conducted in Japan, Canada, the UK, Australia, the USA, and France has discovered that 63% of the IoT consumers thought these devices could not be trusted due to inadequate security (Tawalbeh, et al., 2020, P.4102). Also, research findings have highlighted that 90% of consumers did not seem to have confidence in IoT cybersecurity (Tawalbeh, et al., 2020, P.4102).

There is no doubt that connected things in various sectors do bring tangible benefits that make life better, but also, they carry with them serious concerns about data security. There is no single magical solution to solve the identified Big Data security and privacy challenges. There are various challenges connected with data collecting, processing, and storing. Vast volumes of data become irrelevant unless they are pro- cessed to get something useful out of them. Therefore, it is important to ensure that the sensors function properly and the quality of the data coming for analysis is reliable, and not spoiled by factors such as environmental conditions, and sensor malfunction/breakdown.

Security of Big Data and privacy is an essential element that will ensure data trustworthiness in the data collection process and usage. In general, the majority of data breaches and IoT attacks happen due to a lack of user awareness (Jurcut, et al., 2020) (Tawalbeh, et al., 2020, P.4102). Therefore, documented user guidelines should be compulsory to strengthen security awareness. It has been reported that IoT security measures and guidelines had not been usually mentioned when the users purchased these devices (Tawalbeh, et al., 2020, P.4102). To avoid any controversies, the device manufacturers ought to take the lead to bring potential IoT threats to the attention of the user, and the organisations should produce a package of effective training programs to enhance security awareness. In a positive move, in contrast, data protection authorities point out that, like any other form of data processing, Big Data falls within the framework of data protection law and must comply with data protection legislation in accordance with GDPR which was established with technological advancements in mind.



Source: Authors, 2021

Figure 6.2. Generation of Big Data

2.2 Big Data protection challenges

In practice, data protection and security become extremely challenging in an IoT environment, as a communication interface between objects and persons is at the core of the system, without human intervention. Given the pace of change, it is not surprising that there is little evidence to presume that data protection is keeping up with the pace of change. Even though when legislative drafters demonstrate their awareness of specific concerns in processing data on a large scale, their understanding of risk implications may not be sufficient in practice.

Big data applications typically tend to collect data from diverse sources, without careful verification of the relevance or accuracy of the data thus collected (Mortier, Debussche, and César, 2019). Google's unsuccessful attempts at health diagnostic, and most recently, the use of analytics to predict the US election results (McDermott, 2017) can be taken as good examples of the inaccuracy of Big Data. On that basis, the accuracy principle can be challenged as the GDPR underscores the importance of accuracy (Eur-Lex, 2016) in personal data.

The GDPR applies to the processing of personal data, regardless of whether the processing takes place in the EU (Eur-Lex, 2016). The controllers and processors and those acting as controllers of Big Data as well as those acting as processors on their behalf are obliged to comply with GDPR. The application of data protection principles could be challenging when using personal data in the Big Data context, especially where it involves the use of techniques made possible by AI. These implications arise not only from the volume of data but also from the ways in which data is generated, stored, and processed.

The creation of personal data in vast amounts through Big Data techniques allow organisations to combine different data sets, and that is likely to increase the capability of data to identify living individuals in new ways (Brogan, 2019). As a result, the capacity to mine and analyse datasets increases in volumes, variability, and velocity effectively giving rise to an exponentially increased volume of personal data. To overcome the challenges, in the context of Big Data, it is advisable to consider whether personal data can be fully anonymised. The GDPR specifies that the principles of data protection should not apply to anonymous information that does not relate to an identified or identifiable real person, or personal data classified 'anonymous' (GDPR.Eu, N.D, Recital 26 Not Applicable to Anonymous Data) in such a manner data subject's information is not protected under the GDPR. Therefore, organisations who use anonymised data are expected to verify that they had carried out a robust assessment of the risk of re-identification and adopted proportionate solutions (Information Commissioner's Office, N.D, Big data and data protection, P. 12-13). This may involve a range of technical measures, such as data masking, pseudonymisation, aggregation and banding, as well as legal and organisational safeguards (Information Commissioner's Office, N.D, Big data and data protection, P. 12-13).

The UK Anonymisation Network (UKAN) plays a significant role in providing expert advice on anonymisation techniques (UK Anonymization, N.D). It also enables the organisation to reassure people that collected data capable of identifying them will not be used for Big Data analytics (Information Commissioner's Office, N.D, Big data and data protection, P. 12-13). This is an important criterion for building trust and in taking Big Data forward. However, some commentators have made references to examples where it had been possible to identify individuals in anonymised datasets but had concluded that anonymisation was becoming increasingly ineffective (Information Commissioner's Office, N.D, Big data and data protection, P. 12-13) (Information Commissioner's Office, N.D, Big data, artificial intelligence, machine learning and data protection, P. 59,). However, personal data that had been pseudonymised, in other words, identify an individual in conjunction with additional information could still be possible and will remain as classed personal data (Richard, N.D).

In the ICO Big Data Paper 2017, the ICO emphasises the importance of fairness, transparency, and the need for meeting the data subject's reasonable expectations in Big Data processing (Information Commissioner's Office, N.D, Big data, artificial intelligence, machine learning and data protection, P. 59). However, as vast amounts of data are processed through massive networks daily basis, there is limited transparency in how these algorithms work and how data is processed. Furthermore, the ICO Big Data Paper 2017 notes that the complexity of Big Data analytics can lead to mistrust and potentially be a barrier to data sharing, particularly both in the public and the private sector. This can lead to reduced competitiveness as a negative perception of the consumer will impact trustworthiness (Richard, K, N.D). Therefore, in the Big Data context, privacy notices (Information Commissioner's Office, N.D, What privacy information should we provide?) serve as an important means of providing transparency, while also the consent factor (Eur-Lex, 2016) has been the most reliable in ensuring transparency. The ICO Big Data Paper 2017 makes it clear that the complexity of Big

Data should not be taken as an excuse for failing to obtain consent if and when required to do so (Information Commissioner's Office, N.D, Big data, artificial intelligence, machine learning and data protection, P. 59). The GDPR also follows this approach by asserting that data processing is conditional on obtaining prior consent from the data subject (Eur-Lex, 2016). However, the assertion to obtain consent for processing might not turn out to be a workable solution in all circumstances because of the complexity of the analytics. A study in the US suggests that companies overestimate customers' concerns about the use of their personal data. It claims that in reality, people are primarily concerned about what the organisations plan to do with their data (Information Commissioner's Office. N.D, Big data and data protection, P. 12-13). This leads to the point that personal security re mains uppermost in their thinking. Then it is arguably clear that emphasis should be on the data collection process and use rather than focusing on controlling what happens after data is collected. Therefore, where an organisation is relying on consent in the Big Data context, people must have an understanding of how the organisation will use their data, and a clear indication of consent given for the intended purpose only. To determine the intended purpose compatibility of data originally collected and used will increasingly become challenging with Big Data. If an organisation had collected personal data for one purpose and then decided to start analysing for completely different purposes, the users need to be made aware of the changes and, where necessary, further consent needs to be obtained.

Connected things generate terabytes of data, therefore, deciding which data to store and which to drop is a demanding task in data minimisation. The custodians of stored data may need to retain them for use over a long period for use in the future. The challenge is to secure critical data from criminals and unauthorised access. Any breaches will compromise the privacy of the users and have a negative impact on the image of the custodian, affect trustworthiness, and the users will lose faith not only in the organisation but also in the system. According to an assumption that emerged in 2006, there were notable concerns about invasion of privacy amongst the adult population than the younger generation who felt comfortable about revealing their personal information (Maple, 2017, P.155-184). But there had been proposed changes and the Oxford Internet Institute had released a report, in which it had stated that young people were found to be more likely to take action to protect their privacy than the elderly (Maple, 2017, P.155-184).

The principle of data minimisation is set out in Article 5(1)(c) – per personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed (Eur-Lex, 2016). Data minimisation therefore fundamentally collides with the concept of Big Data, which involves collecting as much data as possible. In the context of data minimisation, questions arise whether the data is excessive and relevant. Therefore, it is important for organisations to be able to articulate at the outset the need to collect and process specific datasets.

Furthermore, the GDPR states that personal data shall not be retained for longer than necessary after serving the purpose for which the data had been processed (Eur-Lex, 2016), however, this requirement is likely to face challenges in the context of Big Data. The GDPR does not specify exact timelines for data retention given that they are context-specific (Eur-Lex, 2016) and difficulties that may arise in relation to the storage limitation principle in Big Data analytics. Most importantly storage limitation principle may under mine the predictability of the future as algorithms can potentially compare current data with stored historical data.

The principle of purpose limitation (Eur-Lex, (2016) is seen as a challenge to Big Data and a barrier to the development of Big Data analytics in the absence of clarity of the purpose for which the data will be used. Also, there has been suggested that the purpose limitation principle restricts freedom the organisations need to make discoveries and innovations happen, and the blunt statement that collection of data for big data analytics without a purpose does not stand to reason.

A privacy impact assessment (Eur-Lex, 2016) is also an important method that can help identify and mitigate privacy risks prior to the processing of personal data in any Big Data scenario. The unique features of Big Data can make some aspects of a privacy impact assessment additionally difficult, but these challenges can be overcome. The impact assessment of complex data collection and processing systems should be conducted by a third party under the supervision of national data protection authorities, that define the professional requirements of these third parties to produce unbiased, high standard outcomes (Mantelero and Vaciago, 2015, P.104-109).

Looking at the potential challenges clearly privacy remains is a major in the IoT, therefore, the service providers have a responsibility to respect consumer privacy by maintaining trustworthiness. That is a consumer-friendly essential to allay public fears when adopting new technology. Research suggests there will be 75 billion internet-connected de vices, in homes around the world by the end of 2025 (Department for Digital, Culture, Media & Sport, National Cyber Security Centre, and Warman, 2020). The individuals are likely to be unaware of the processing of their personal data collected using IoT applications. There are only a few IoT-related policies and regulatory frameworks currently in place, therefore, an effective law implementation mechanism is required to protect millions of users who will otherwise fall victims to cyber-related threats and hacks linked to internet-connected household items. The table (See table 6.1) below provides a summary of identified challenges and proposed solutions.

Table 6.1: Identified challenges and proposed solutions

Challenges	**Proposed solutions**
Collection of data from diverse sources, without careful verification of the relevance or accuracy (Mortier, Debussche, and César, 2019)	Use AI technologies to verify the ac-curacy of collected data.
Big Data techniques allow organisations to combine different data sets, and that increases the likelihood of data being capable of identifying living individuals (Brogan, 2019).	Use of a wide range of technical measures, such as data masking, anonymization, pseudonymisation, aggregation, as well as legal and organisational safeguards (Information Commissioner's Office, N.D, Big data and data protection, P. 12-13.).
Limited transparency in howdata is processed (Information Commissioner's Office, N.D, Big data and data protection, P. 12-13.).	Improve transparency by providing privacy notices (Information Commissioner's Office, N.D, What privacy information should we provide?) and obtaining consent (Eur-Lex, 2016) before processing any collected data.
The complexity of Big Data analytics can lead to mistrust (Richard, N.D].	Improve transparency by providing privacy notices (Information Commissioner's Office, N.D, What privacy information should we provide?) and obtaining consent (Eur-Lex, 2016) before processing any

	collected data.
The challenge of determiningwhich purposes are compatiblewith the purpose for which the data was originally collected.	Purpose limitation (Eur-Lex, 2016); If an organisation has collected personal data for one purpose and then decided to start analysing it for completely different purposes, then the users need to be made aware of the changes and, where necessary, further consent needs to be obtained.
The custodians of stored data may need to retain them for useover a long period for use in thefuture.	Use of technical measures, such as anonymization and pseudonymisation (Information Commissioner's Office, N.D, Big data and data protection, P. 12-13).
Any breaches will compromisethe privacy of the users and have a negative impact on the image ofthe custodian, affect trustworthiness, and the users will lose faith not only in the organisation but also in the system.	Use of technical measures, such as anonymization, pseudonymisation, data masking, encryption keys and blockchain technology. Physical security systems such as access control, use of video surveillance and security logs can also be used.
Protection of privacy of individuals.	Conducting privacy risks assessment will provide an early warning system to detect privacy problems (Eur-Lex, 2016)
Lack of IoT-related policies and regulatory frameworks at the national, regional and global level.	It is important to bring, countries, multinational organisations, industrial partners, security and IoT specialists from the industry and academia, to build dialogues on how to protect personal information generated through IoT. That will enable us to get a balanced view to move forward in developing policies and regulations associated with Big Data.
Principles in national and re- regional laws contradict with advancement of technologies.	It is important to review the policiesat least twice a year to make sure there is a balance between upcoming technologies and legal

	mechanisms to protect the privacy of individuals and national security.

2.3 Emerging laws and regulations of data protection in IoT

Legal regulation is of increasing importance for Big Data, particularly for data protection. In this context, the application of established and developing data protection techniques are rapidly evolving. The managing of compliance with the GDPR will play an essential part in the Big Data handling projects involving data harvested from the expanding range of available digital sources. Many organisations do have established data protection governance structures and, policy and compliance frameworks in place, and these act as pathfinders towards Big Data governance.

The GDPR has recognised the rapid technological developments and globalisation with a special reference to Big Data technology (GDPR.Eu, N.D, Recital 6 Ensuring a High Level of Data Protection Despite the Increased Exchange of Data), therefore, has provided further opportunity for regulators and organisations to consider Big Data compliance. In particular, the GDPR has introduced specific tools, like privacy by design (Intersoft Consulting., N.D, GDPR Privacy by Design) and pseudonymisation (GDPR.Eu, N.D, Recital 28 Introduction of Pseudonymisation), to help deal with Big Data. Consequently, the ICO (Information Commissioner's Office, N.D, The UK GDPR) and other data protection authorities have been addressing Big Data for some time by further developing existing tools like notice and consent, anonymisation and privacy impact assessments in line with GDPR (Information Commissioner's Office, N.D, The UK GDPR).

The Government of the United Kingdom recently launched a consultation process for regulating consumer Internet of Things (IoT) security, UK will be one of the first countries to legislate specifically in relation to IoT security, and other countries are likely to follow the UK model (Beverley-Smith, Perowne, and Weiss, 2020). The UK government has proposed designating a regulator to monitor industry compliance. The proposals included civil enforcement powers, such as fines potentially up to 4% of annual worldwide turnover and product forfeiture, suspension, and recall. However, the omission of Wi-Fi security, as has been reported, would have a significant impact on general IoT security (Beverley-Smith, Perowne, and Weiss, 2020).

The EU Cyber Security Act 2019 initiated the development of a comprehensive cybersecurity certification schemes across the EU, but the US has so far failed to pass any federal legislation that will match the UK proposal (Beverley-Smith, Perowne, and Weiss, 2020). The Government of UK is engaged with international partners to ensure that the guidelines drive a consistent, global approach to IoT security. As a step forward, in February 2019, ETSI, a global standards organisation, published the first globally applicable industry stand- ard consumer IoT security, based on the UK Government's Code of Practice (Department for Digital, Culture, Media & Sport, National Cyber Security Centre, and Warman, 2020).

The UK government introduced a self-regulatory Code of Practice in October 2018 (CoP), and proposed to widen IoT devices related requirements, which included a ban on universal default passwords in IoT products, implementation of the vulnerability disclosure policy, and provision of a defined support period in terms of receiving security updates (Beverley-Smith, Perowne, and Weiss, 2020). The proposals covered both producers and distributors, and the intended purpose was for all IoT devices sold in the UK to be compliant with the security requirements, including goods imported from elsewhere (Beverley-Smith, Perowne, and Weiss, 2020). The included obligations were to ensure that all IoT devices met the security requirements, maintain thorough records of compliance, and cooperate fully with the regulator.

In January 2020, the UK government announced it was going to introduce new mandatory requirements for IoT device manufacturers for the purpose of improving consumer data security (Fernandez, 2020). The aim was to ensure these products had strong cybersecurity built-in by design and move responsibility to secure their own devices away from the consumers (Fernandez, 2020). The three main requirements included were, unique passwords compulsory for all connected devices, provision of a point of contact for the public to report vulnerabilities, and a minimum period of security updates specified when sold (Fernandez, 2020).

In places where devices and services process personal data, the custodian should do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR). The emphasis should be for the individuals to remain in control of their personal data that are collected through IoT. In real circumstances, obtaining consent from the users may not be easy. Therefore, the device manufacturers and IoT service providers should make users aware of the way their data is being used, by whom, for what purposes, and clear instructions on how to delete their personal data for each device and service (Eur-Lex, 2016). In cases where the data is being kept for a longer period than needed (Eur-Lex, 2016), all the credentials should be stored securely within services and on devices by using techniques like cryptographic keys, device identifiers and initialisation vectors (Department for Digital, Culture, Media & Sport, 2018, P.9). In addition, significant sanctions for violations of data protection obligations should be introduced and, mandatory personal data breach notifications should be extended to all areas of personal data processing (Eur-Lex 2016).

To ensure the implementation of data protection legislation by professionals, the role of data protection officers should be mandatory (Eur-Lex 2016). In addition to ensuring a high level of compliance, data protection officers themselves can provide data protection education to staff and management of their respective companies. Therefore, they could play an important role in the design of IoT systems by sharing their expert knowledge on data protection with relevant actors.

The proposals seek to protect the privacy of consumers and online security. The emphasis is also on the urgent need to ensure strong cybersecurity built into smart products by design. According to the director of marketing, the concerns over weak IoT security act as a barrier to the delivery of real benefits to individuals and societies (Department for Digital, Culture, Media & Sport, National Cyber Security Centre, and Warman, 2020). Therefore, tech UK has been supporting the government's commitment to legislate for integrating cybersecurity into consumer IoT products at the design stage (Muncaster, 2020).

2.4 Policies and standards landscape for IoT

The data protection aspects of Big Data have been addressed in a number of reports, guidance and policy documents issued at the national and international level over the past few years (see table 6.2). The report sign posted Big Data's direction of travel and articulated a focus on data solutions and Big Data as a key IT driver over the next two decades (Richard, N.D).

UK government 2013 strategy paper: Seizing the data opportunity: a strategy for UK data capability, presented a positive view of the UK's ability to seize the data opportunity (Government of UK, 2013, Seizing the data Opportunity; A strategy for UK data capability). It addressed privacy and data protection issues through a clear and pragmatic policy to ensure public trust in the confidentiality of their data while increasing the availability of data to maximise its economic and social value (Government of UK, 2013, Seizing the data Opportunity; A strategy for UK data capability).

The Executive Office of the US President's May 2014 report: Big Data: Seizing Opportunities, Preserving Value (Government of US, 2015), focused on the way in which Big Data will transform everyday life, and it considered Big Data and privacy both in the public and the private sector and concluded that the existing notice and consent approach to data privacy may have to be reviewed in the light of Big Data (Government of US, 2015).

The European Commission's 2014 Communication publication: Towards A Thriving Data-Driven Economy (European Commission, 2014, Towards a thriving data-driven economy) sets out a number of activities it considered necessary for the EU to be able to seize Big Data opportunities. This report includes a data-friendly legal framework and policies. The report states that policies on issues relevant to Big Data like data protection and security should lead to more regulatory certainty for businesses and create consumer trust in data technologies (European Commission, 2014, Towards a thriving data-driven economy).

The European Data Protection Supervisor's 2014 (European Union, 2015, European Data Protection Supervisor- Resolutions, recommendations and opinions) and European Data Protection Supervisor's 2015 (European Union, 2015, European Data Protection Supervisor; Annual Report 2015) opinion on the challenges of Big Data. The EDPS 2015 emphasised that data protection law must continue to protect existing rights and values even in the context of Big Data (European Union, 2015, European Data Protection Supervisor; Annual Report 2015). In general, the EDPS has called on the EU institutions to use the reform of the EU data protection framework to strengthen the data protection mechanisms to protect personal privacy and secure personal information (Richard, N.D).

In March 2017, the ICO published an updated paper on Big Data, artificial intelligence, machine learning and data protection with GDPR compliance elements (Information Commissioner's Office, N.D, Big data, artificial intelligence, machine learning and data protection, P. 59). This updated paper refers to the GDPR where relevant, but it is not intended to be a guide to the GDPR. In particular, the ICO presents six recommendations to help organisations achieve compliance which includes anonymisation, privacy impact assessments (PIAs), appropriate privacy notices, privacy by design, the development of ethical principles and auditable machine learning algorithms (Information Commissioner's Office, N.D, Big data, artificial intelligence, machine learning and data protection, P. 59).

Big Data cannot be secured by way of policies and legal mechanisms only. The use of encryption keys is one effective way to protect Big Data. The practicality of using public key encryption for encryption of data also enables decryption using the private key by the recipient, without undermining privacy and security (Pandey, Milan, and Shukla, 2018. PP. 74-77). Physical security systems, on the other hand, have built-in the capacity to deny data centre access to strangers or staff members, restricted to their status (Rahfaldt, 2019). Similarly, the use of video surveillance and security logs will serve the same purpose (Rahfaldt, 2019). These methods will contribute to maintaining and preserving confidentiality, integrity, and generated data availability.

Companies should continually monitor and identify, and rectify security vulnerabilities in their own products, and services as a part of the product security lifecycle (Department for Digital, Culture, Media & Sport, 2018, P.7). On identifying any disclosed vulnerabilities, prompt action should be taken on the organisations. The sharing of known or identified vulnerabilities with the industrial entities will enable them to be best prepared for potential vulnerabilities in the future internet.

In the absence of any regulation, it is unlikely that privacy, data pro- protection and information security will be addressed meaningfully and adequately by the market. In developing, accepting, and implementing policies associated with IoT, careful consideration should be given to avoiding violation of human identity, human integrity, human rights, the privacy of the individual and the public. The control of personal data should remain in their hands. To ensure harmonisation of privacy to a high standard, data protection, and information security, the development of a binding global data protection framework for IoT is appropriate and desirable.

Table 6.2: Implemented mechanisms and their purposes

Mechanisms	Purposed
UK government 2013 strategy paper: Seizing the data opportunity: a strategy for UK data capability (Government of UK, 2013, Seizing the data Opportunity; A strategy for UK data capability).	It planned to address privacy and data protection issues through a clear and pragmatic policy that ensures public trust in the confidentiality of their data, while increasing the availability of data to maximise its economic and social value (Government of UK, 2013, Seizing the data Opportunity; A strategy for UK data capability).
The Executive Office of the US President's May 2014 report: BigData: Seizing Opportunities, Preserving Value (Government of US, 2015).	This report considered Big Data and privacy both in the public andthe private sector and concluded that the existing privacy notice and consent approach to data privacy may have to be reviewed in the light of Big Data (Government of US, 2015).
The European Commission's 2014 Communication publication: Towards A Thriving Data-Driven (Economy European Commission, 2014, Towards a thriving data-driven economy).	The report states that policies on issues relevant to Big Data like data protection and security should lead to more regulatory certainty for businesses and create consumer trust in data technologies (Economy European Commission, 2014, Towards a thriving data-driven economy).
The European Data Protection Supervisor's 2015 (European Union, 2015, European Data Protection Supervisor; Annual Report 2015).	The EDPS 2015 emphasised that data protection law must continueto protect existing rights and values even in the context of Big Data (European Union, 2015, European Data Protection Supervisor; Annual Report 2015).
In March 2017, the ICO published an updated paper on Big Data, artificial intelligence, machine learning and data protection with GDPR compliance element (Information Commissioner's Office, N.D, Big data, artificial intelligence,	This updated paper presents six recommendations to help organisations achieve compliance which include anonymisation, privacy impact assessments (PIAs), appropriate privacy notices, privacy by design, the development of ethical principles and auditablemachine learning algorithms (Information Commissioner's

machine learning and data protection, P. 59,).	Office, N.D, Big data, artificial intelligence, machine learning and data protection, P. 59).
Use of encryption keys	The practicality of using public-key encryption (PKE) for encryption of data also enables decryption using a private key by the recipient, without undermining privacy and security (Pandey, Milan, and Shukla, 2018, PP. 74-77).
Implementation of physical security systems	Physical security systems have the capacity to deny data centre access to strangers or staff members, restricted to their status (Rahfaldt, 2019).

3.0 Security Challenges and Opportunities for IoT solutions

The Internet of Everything (IoE) is the next step to IoT as it will connect data, processes, devices, and people via the Internet (Kalyani, and Sharma, 2015, P.20). The frog- leap in these exciting technological advancements come with risks, challenges, and opportunities of their own. Most of these risks are security relevant issues that will have a significant impact on individuals, organizations, and governments in general. This section highlights a multitude of IoT security challenges and the proposed solutions.

3.1 Security challenges

Due to device differences, protocols, and services in IoT, there needs to be a set of standards and well-defined architecture with interfaces, data models, and protocols. There is a concern that many researchers are focused mainly on authentication and access control protocols. When IoT devices are connected for the first time and share identifying information many attacks can happen such as the man in the middle (MITM) attack. To this end, authors in (Yousuf, et al., 2015, P.614) stated that cryptography applied by predefined identity management entities that can monitor the connection of devices is needed to prevent identity theft. IoT requires more devices that will switch the use from IPv4 to IPv6 which will require more bandwidth. The implementation of both IPv6 and

5G the new generation of communication for better speed also open the doors for more threats and challenges that need to be addressed.

Different features of IoT devices can create threats and security challenges (Zhou, et al., 2019). A better understanding of these features can help us mitigate some of these issues and rely on the consequences for a better solution. Features such as mobility, interdependency, diversity, intimacy and many more bring different challenges and threats such as firmware vulnerabilities, storage, computing power, network attacks, policies and standards that require more research. It requires thorough investigations to identify the root causes of IoT threats and also to build pragmatic countermeasures (e.g., “the real risk which may be involved behind these vulnerabilities in the industrial context needs further investigation in the future” (Varga, 2017).

There are methods that use blockchain to ensure privacy and security (Dorri, et al., 2017). Confidentiality, Authorization, Integrity, and Availability are achieved by using symmetric encryption, shared keys, hashing, and limiting acceptable transactions by the device. This method could be manageable for low resource IoT devices however, it produces some delay. The delay and the extra overheads are insignificant compared to its security and privacy gains to some applications but critical in others. Also, there is a blockchain IoT system that manages keys using RSA public key (Huh, Cho, and Kim, 2017) . In this work, private keys are stored in the devices and public keys are stored in Ethereum. The proposed idea was implemented in a small scale IoT system and only a few IoT devices were used. The system showed two weaknesses. The first is the time it requires for data transactions and the latter is the requirement for larger storage for light IoT devices. In terms of threat and security, prevention from DDoS attacks was the only mentioned security measure that the system could provide. Data encryption is used to limit security risks as they increase for both business and consumers in the IoT environment and studies show that using AES in the algorithm is faster than both HAN and RSA algorithms (Yousefi, and Jameii, 2017).

There are major forensic challenges that face the IoT domain as there is no reliable and documented tool to collect residual evidence (Conti, 2018). The autonomous and real-time interactions with different IoT devices and nods make it difficult to collect, identify, and preserve evidence data. Identifying activities of different parties that can access IoT nods is a challenge with the lack of a proper authentication system.

As there are some solutions that can be implemented to mitigate the security concerns, “there is a clear lack of performance evaluation and assessment in real-life scenarios. Furthermore, there is a conflict between protecting user privacy and the granularity of data access needed to provide better services. This raises the challenge of how to support consumer-specific privacy preferences while maintaining the same level of service” (Seliem, Elgazzar, and Khalil, 2018).

3.2 Proposed secure IoT architectures

There is no single architecture or model of IoT. The proposed layer models vary from a 3-layers model to a 6-layers model. Many technologies are involved to create an IoT system such as RFID, WSN, cloud computing, and different network technologies. This may result in different IoT security and privacy challenges such as Unauthorized Access to RFID, Sensor-Nodes Security Breach, and Cloud Computing Abuse.

To mitigate the threats that the IoT technology faces, there should be a better understanding of the technology used, architecture, type of at- tacks and where they all meet.

Different IoT layering systems: the 3-layers approach used by (Yousuf, et al., 2015, P.608-609) (Seliem, Elgazzar, and Khalil, 2018) and (Jia et al., 2012, P.1282) (Application, network, and perception layer). The 4-layers approach used by (Varga, 2017) (Application, data processing, network, and sensor and actuators layer). The 4-layers approach used by (Farooq et al., 2015) and (Leloglu, 2017) (Application, middleware, network, and perception layer). The 6-layers approach used by (Farooq, et al., 2015) (Business, application, middleware, network, perception, and coding layer). 3 layers approach used by (Conti, et al., 2018) and (Yousefi, and Jameii, 2017) (Application, transport, and sensing layer).

Many studies present the threats and challenges that the IoT based on a layering system faces. There are different layering approaches which make it difficult to allocate the same problem from one layering system to another. This increases the complexity and the time needed to find a proper solution. Here, we used the simplest layering system (See figure 6.3) to demonstrate the most essential factors in a simpler way.

.

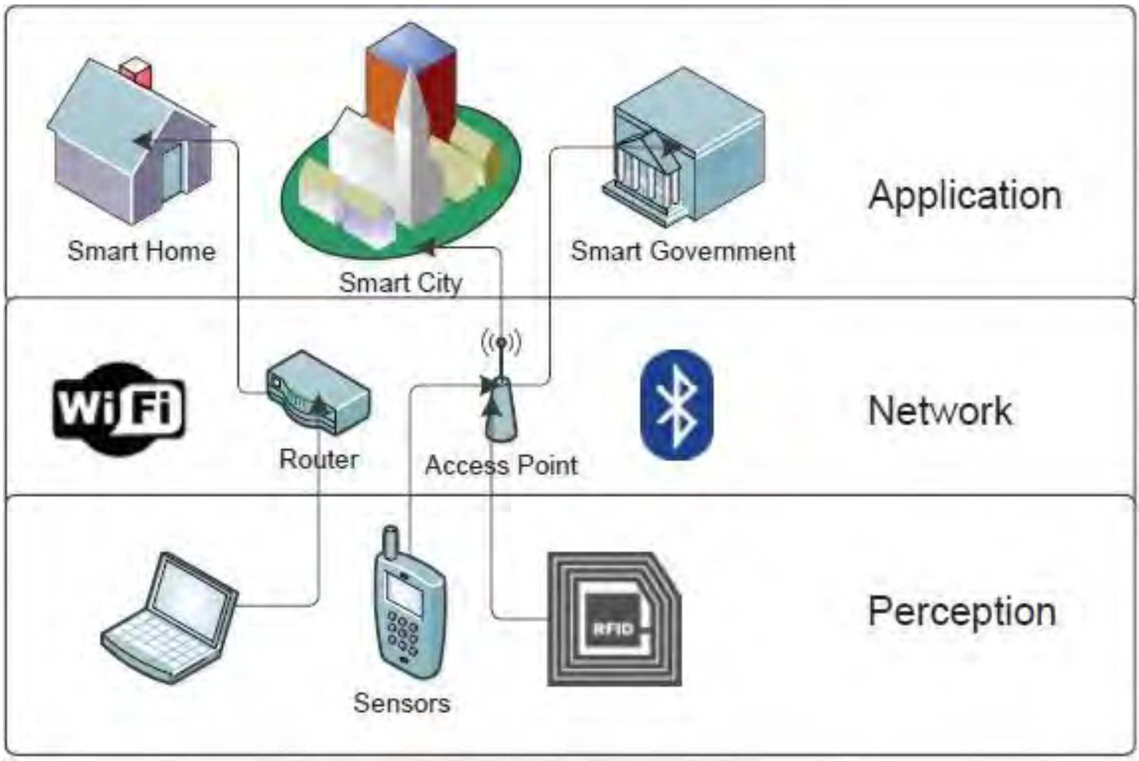


Figure 6.3 IoT layers (Yousuf, et al., 2015, P.609)

First, the authors describe the most important technologies used in each layer bearing in mind that technology can be used in more than one layer. Figure 6.4 below provides a simplified example of some technologies used.

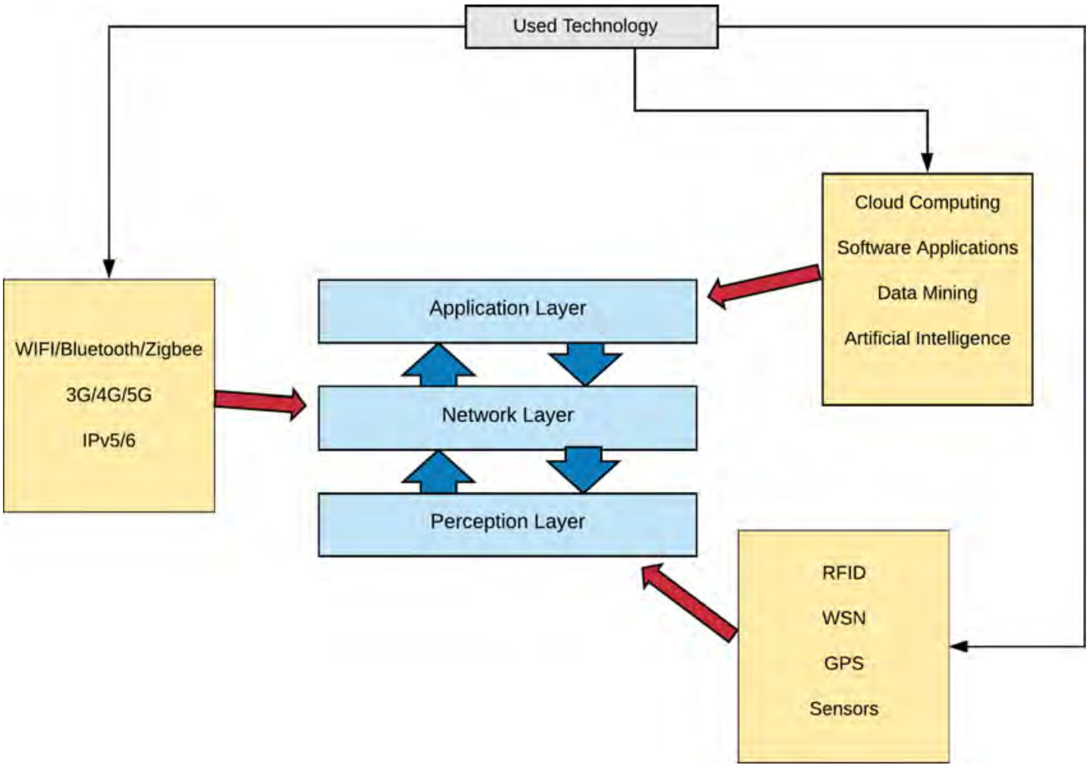


Figure 6.4 Used technologies in IoT layers.

In Figure 6.4, the authors explain different technology used in each layer. Threats can then be divided by the technology used rather than the layers they are in. This enabled authors to focus on the main technology used and how to implement the appropriate method to mitigate threats.

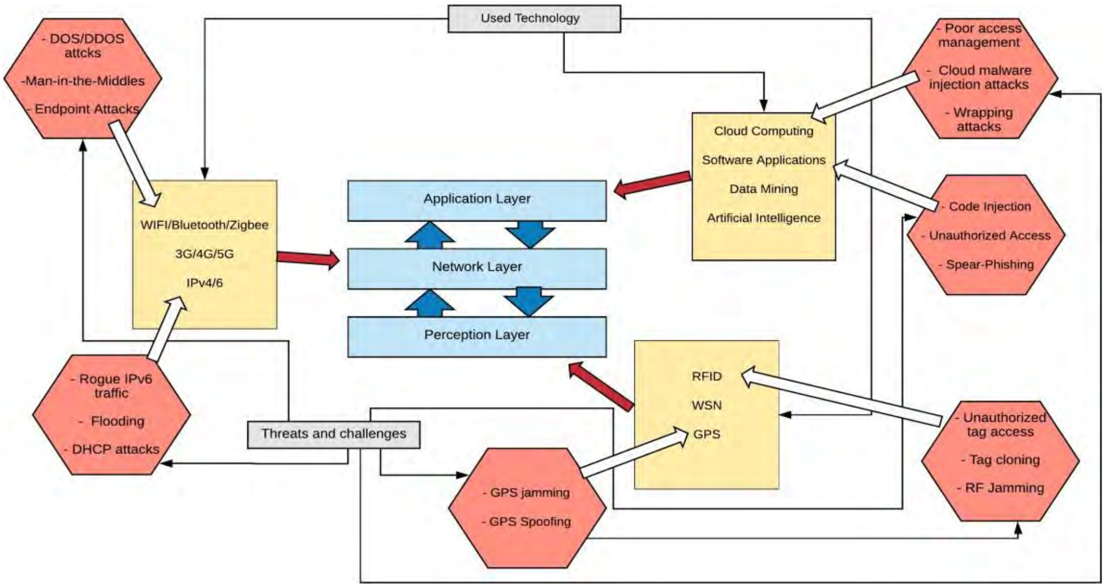


Figure 6.5 Threats on the used technologies

Figure 6.5 demonstrates risks associated with the used technology. This enables threats to be identified with ease. IoT systems do not facilitate all the technologies at once thus not all protection methods should be implemented. Protection and mitigation methods should be implemented based on the technology used. An example of this would be a system that uses either Bluetooth or Zigbee technology. Security implementation can be specific for the technology used rather than for all the options. This is very important for lightweight IoT devices because protection and security mechanisms tend to need more storage resources and computing power (Zhou, et al., 2019, P.2) (Varga, 2017) (Huh, Cho, and Kim, 2017).

Table 6.3: Example of used technologies and their implementations

IoT Technologies	**used/not used**	**Threats**	**Implementation**
GPS	□	- GPS Jamming - GPS spoofing	- Implement blocking antennas. - Obscure antennas
IPv4	□	- DHCP Flooding	- Implement Port security
Cloud computing	□	- Interception of Data	- Advanced web application firewalls - Data Encryption

An example of this would be listing the technologies that would be used in IoT rather than the layers in the model. Creating a manual or a table (such as Table 6.3) that lists all the used technologies, their threats and mitigation methods. In a simplified scenario, a company may need to create a new IoT device/application to serve a specific purpose. Users or researchers could first check all the technologies that will be used to create this tool (for example, not all the devices require cloud computing technology). Therefore, after an initial evaluation of the used technology, the appropriate control measures can be added to mitigate the threats associated with the technology. For instance, if GPS technology is used in the device, the “blocking antennas” method can be implemented as a control measure (See table 6.3).

4.0 Future privacy and security landscape of IoT (post-COVID-19)

COVID-19 has made people work from home, shop online and students learn online. It is envisaged that these new normalcies will remain post COVID-19 as well. There are many privacy and security challenges associated with this new normalcy. Such challenges are not a phenomenon unique to the context of COVID-19. Yet both cyber threats and the enforcement gap were running at unacceptably high levels before the pandemic and have continued to do so throughout the crisis (Hakmeh, et al., 2021).

Even though the long-term impact of the COVID-19 crisis on the evolving threat of cybercrime cannot yet be assessed, there are several pressing questions about how the developments seen during the pandemic will affect the future privacy and security of people. Policymakers, practitioners, and advocates will have to come up with mandatory risk assessment frameworks to make sure the technology development companies will follow a strict risk assessment before they deploy any innovative technologies. This will prevent any security and privacy complications in the near future.

The response of the government and the technology industries to the Coronavirus outbreak became headlines news but at the same time, concerns were raised about the contact tracing apps, mobile location data tracking, and police surveillance drones (Holmes, McCurry, and Safi, 2020). Also, new privacy issues have emerged as the organisations started strengthening surveillance using thermal cameras and face-recognition technology in preparation for the resumption of normal working patterns. At one point during the pandemic, the WHO called the situation an Infodemic due to the increased collection of information (WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, 2020). According to the findings released from a survey conducted in the US, more than two-thirds of respondents believe that their government should be able to bring the virus under control without them having to sacrifice their privacy (Lovejoy, 2020). In this context, the governments, having to comply with the use of surveillance tools in combating the pandemic, should also need to strike a balance without compromising data privacy laws.

In a post COVID-19 world, we cannot expect the world to behave comparatively in the same manner as it did in pre COVID-19. It is extremely necessary to address privacy and security concerns during, and in post COVID-19. In doing so, the private sector can play an effective role in identifying cybercriminals and avoid disruptions to their infrastructure, but only the governments have the legal authority to prosecute and bring them to justice (Daniel et al., N.D). Therefore, it is crucially important for the public and private sectors to work together on cybercrime issues. That having said, the possibility of some disparities in organisational culture and capacity between the institutions cannot be discounted.

As it stands, there is a clear visible gap in the development of IoT devices and regulatory laws do exist. Therefore, it is imperative to revisit national and regional data protection mechanisms to address upcoming potential threats, and it would be beneficial to capture data protection principles highlighted in the GDPR. The specific principles such as anonymisation, pseudonymisation, right to be erasure, obtaining consent before collecting and processing of personal information, deletion of collected data within a specified time scale, informing the data subject how the organisations will use their personal information. The adherence to these principles helps build a trustworthy relationship between data controllers and the data subject. However, some have opined that revisiting data protection laws and regulations such as GDPR will jeopardise the success of Big Data (Zarsky, 2017) (Bentotahewa, and Hewage, 2020, Challenges and Obstacles to Application of GDPR to Big Data).

5.0 Conclusion

This chapter discusses the process of Big Data generated through IoT, the challenges and opportunities that have come to light during the COVID-19 pandemic. The authors have reviewed the conceptual meaning of 'BIG Data', and the process of generating a vast volume of data as the definition suggests. The nations have relied on technological solutions to minimise and contain the spread of the pandemic, and the increase in numbers of IoTs connected through the internet has generated vast volumes of information. As much as the outcomes are tangible and clearly visible, the focus has shifted to concerning security implications on personal privacy and security. In searching for solutions, the authors have identified the importance of accepting and implementing laws, regulations, and policies associated with IoT, with a special focus on GDPR. In this article, the authors have explored legal mechanisms already in place and have highlighted the importance of developing and revisiting national and regional data protection mechanisms. A consensus-based set of legislation in line with data protection principles highlighted in the GDPR is needed to confront future threats against personal privacy and security. Implementation of such policies and technical solutions will provide guidance and binding responsibility on the part of the manufacturers and organisations to protect the privacy of the individual whilst achieving the objectives of IoT deployment.

References

Altuntas, F. and Gok, M. S. (2021) ‘The effect of COVID-19 pandemic on domestic tourism: A DEMATEL method analysis on quarantine decisions’, *International Journal of Hospitality Management*, vol. 92 [Online]. Available at: https://doi.org/10.1016/j.ijhm.2020.102719 (Accessed: 14 March 2020)

Bentotahewa, V. and Hewage, C. (2020) *Challenges and Obstacles to Application of GDPR to Big Data* [Online] Available at: https://www.infosecurity-magazine.com/next-gen-infosec/challenges-gdpr-big-data/ (Accessed: 23 February 2021)

Bertino, E., (2016). ‘Data Security and Privacy in the IoT’, *EDBT*. Available at: DOI:10.5441/002/edbt.2016.02 (Accessed: 3 April 2019)

Beverley-Smith, H., Perowne, C. H.N. and Weiss, J G. (2020) ‘Internet of Things: How the U.K.’s Regulatory Plans Could Raise Compliance Standards’, *The National Law Review*, Volume XI, Number 104. Available at: https://www.natlawreview.com/article/internet-things-how-uk-s-regulatory-plans-could-raise-compliance-standards (15 June 2019).

Brogan, C. (2019) *Anonymising personal data ‘not enough to protect privacy’, shows new study* [Online] Available at: https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/ (Accessed: 15 November 2019)

Celik, Z B. et al., (2019). ‘Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities’, *ACM Computing Surveys*. Volume 52, Issue 4, Article 74. Available at: DOI: https://doi.org/10.1145/3333501 (12 November 2019)

Conti, M. et al., (2018) ‘Internet of Things security and forensics: Challenges and opportunities’, *Future Generation Computer Systems*, vol. 78. Available at: https://doi.org/10.1016/j.future.2017.07.060 (Accessed: 24 March 2019)

Daniel, M. et al., (N.D) *How do we beat COVID-19 cybercrime? By working together* [Online]. Available at: https://www.weforum.org/agenda/2020/07/alliance-tackling-covidclass="•-No-break">-19-cybercrime (Accessed 3 January 2021)

Department for Digital, Culture, Media & Sport, National Cyber Security Centre, and Warman, M. (2020) *Government to strengthen security of internet-connected products* [Online]. Available at: https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products (Accessed: 14 May 2020)

Department for Digital, Culture, Media & Sport. (2018) *Code of Practice for Consumer IoT Security* [Online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf (Assessed: 23 May 2020)

Dilmegani, C. (2021) *Self Checkout Systems in 2021: Comprehensive Guide* [Online]. Available: https://research.aimultiple.com/self-checkout/. [Accessed: 23-Apr-2021].

Dorri, A. et al., (2017) 'Blockchain for IoT security and privacy: The case study of a smart home', *IEEE International Conference on Pervasive Computing and Communications Workshops*, Available at: 10.1109/PERCOMW.2017.7917634 (Accessed: 15 October 2020)

Dutta, P K. and Mitra, S. (2021) *Application of Agricultural Drones and IoT to Understand Food Supply Chain During Post COVID-19* [Online]. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119769231.ch4 (Accessed: 3 May 2020)

Embree, R. (2021) *Four IoT Trends for Hospitality | Hospitality Technology* [Online]. Available: https://hospitalitytech.com/four-iot-trends-hospitality. [Accessed: 22-Apr-2021].

Erevelles, S., Fukawa, N. and Swayne, L., (2016). 'Big Data consumer analytics and the transformation of marketing', Journal of Business Research, Volume 69(2), Available at: DOI: 10.1016/j.jbusres.2015.07.001 (12 April 2019)

European Commission. (2014) *Towards a thriving data-driven economy* [Online]. Available https://ec.europa.eu/transpa-rency/regdoc/rep/1/2014/EN/1-2014-442-EN-F1-1.Pdf (Accessed: 12 July 2020)

European Union. (2015) *European Data Protection Supervisor- Resolutions, recommendations and opinions* [Online]. Available https://ec.europa.eu/dorie/fileDownload.do;jsessionid=UdwG4bm1A8b_m1-1-UyfY02xUZ1JtAlxTYCJelGukIsnFGJyQCuC!-898031139?docId=2199637&cardId=2199636 (Accessed: 10 June 2020)

European Union. (2015) *European Data Protection Supervisor; Annual Report 2015* [Online]. Available https://ec.europa.eu/dorie/fileDownload.do;jsessionid=UdwG4bm1A8b_m1-1-UyfY02xUZ1JtAlxTYCJelGukIsnFGJyQCuC!-898031139?docId=2199637&cardId=2199636 (Accessed: 25 May 2020)

Eur-Lex, (2016) *Regulation (EU) 2016/679 of the European parliament and of the council* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434 (12 January 2019)

Farooq, M U., et al., (2015) 'A Critical Analysis on the Security Concerns of Internet of Things (IoT)', *International Journal of Computer Applications* Volume111(7) Available at: DOI: 10.5120/19547-1280 (23 March 2020)

Farooq, M. et al., (2015) 'A Review on Internet of Things (IoT)', *International Journal of Computer Applications* vol. 113, no. 1 Available at: DOI:10.5120/19787-1571 (5 April 2020)

Fernandez, A. (2020) *New IoT security regulations: what you need to know* [Online]. Available at: https://www.allot.com/blog/new-iot-security-regulations-what-you-need-to-know/ (Accessed: 12 April 2020)

GDPR.EU. (N.D) *Recital 26- Not applicable to anonymous data* [Online] Available at: https://gdpr.eu/recital-26-not-applicable-to-anonymous-data/ (Accessed: 12 August 2020)

GDPR.EU. (N.D) *Recital 6- Ensuring a high level of data protection despite the increased exchange of data* [Online] Available at: https://gdpr.eu/recital-6-ensuring-a-high-level-of-data-protection-despite-the-increased-exchange-of-data/ (Accessed: 20 August 2020)

GDPR.EU. (N.D) *Recital 28 Introduction of Pseudonymisation* [Online] Available at: https://gdpr.eu/recital-28-introduction-of-pseudonymisation/ (Accessed: 8 August 2020)

Government of UK- Cabinet office. (2021) *Coronavirus: how to stay safe and help prevent the spread* [Online]. Available: https://www.gov.uk/guidance/covid-19-coronavirus-restric-tions-what-you-can-and-cannot-do#businesses-and-venues. [Accessed: 22-Apr-2021].

Government of UK. (2013) *Seizing the data Opportunity; A strategy for UK data capability Government of UK* [Online]. Available https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/254136/bis-13-1250-strategy-for-uk-data-capability-v4.pdf (Accessed: 19 May 2020)

Government of US. (2015) *Big Data: seizing opportunities, preserving values* [Online] Available https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf (Accessed: 20 April 2020)

Hakmeh, J. et al., (2021) *The COVID-19 pandemic and trends in technology* [Online] Available: ISBN: 978 1 78413 436 5 (Accessed: 23 April 2021)

Holmes, O., McCurry, J. and Safi, M. (2020) *Coronavirus mass surveillance could be here to stay, experts say* [Online]. Available at: https://www.theguardian.com/world/2020/jun/18/coronavirus-mass-surveillance-could-be-here-to-stay-tracking (Accessed 4 February 2021)

Huh, S. Cho, S. and Kim, S. (2017) 'Managing IoT devices using blockchain platform', *International Conference on Advanced Communication Technology*, Available at: 10.23919/ICACT.2017.7890132 (17 July 2020)

Ilieva, G. and Yankova, T. (2000) 'IoT in Distance Learning during the COVID-19 Pandemic', *TEM Journal*, vol. 9, no. 4, Available at: DOI: 10.18421/TEM94-45 (23 May 2020)

Information Commissioner's Office. (N.D). *Big data and data protection* [Online]. Available: https://rm.coe.int/big-data-and-data-protection-ico-in-formation-commissioner-s-office/1680591220 (Accessed: 23 October 2020).

Information Commissioner's Office. (N.D) *Big data, artificial intelligence, machine learning and data protection* [Online]. Available: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (Accessed: 4 April 2021)

Information Commissioner's Office. (N.D) *What privacy information should we provide?* [Online]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/ (Accessed: 17 March 2020)

Information Commissioner's Office. (N.D) *The UK GDPR* [Online]. Available at: https://ico.org.uk/for-or-ganisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-tran-sition-period-has-ended/the-gdpr (Accessed 24 November 2019)

Intersoft Consulting. (N.D) *GDPR Privacy by Design* [Online]. Available at: https://gdpr-info.eu/issues/privacy-by-design/ (Accessed 2 April 2019)

Jia, X., et al. (2012) 'RFID technology and its applications in Internet of Things (IoT)', *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)* Available at: DOI:10.1109/CECNET.2012.6201508 (10 May 2020)

Jurcut, A. et al., (2020) 'Security Considerations for Internet of Things: A Survey', *SN Computing Science*. Available at: DOI: https://doi.org/10.1007/s42979-020-00201-3

(27 April 2020)

Kalyani, V. L. and Sharma, D. (2015) IoT: Machine to Machine (M2M), Device to Device (D2D) *Internet of Everything (IoE) and Human to Human (H2H): Future of Communication," Journal of Management Engineering and Information Technology (JMEIT)* Volume -2, Issue- 6. Available at:

http://www.jmeit.com/JMEIT_Vol_2_Issue_6_Dec_2015/JMEITDEC0206003.pdf (Accessed: 28 March 2020)

Leloglu, E. (2017) 'A Review of Security Concerns in Internet of Things', *Journal of Computer and Communications* vol. 05, no. 01 Available at: DOI: 10.4236/jcc.2017.51010 (17 June 2020)

Lovejoy, K. (2020) *COVID-19: How future investment in cybersecurity will be impacted* [Online]. Available at: https://www.ey.com/en_uk/consulting/how-the-covid-19-pandemic-is-impacting-future-investment-in-security-and-privacy (Accessed: 25 October 2020)

Mantelero, A. and Vaciago, G. (2015) 'Data protection in a big data society. Ideas for a future regulation,' *Digital Investigation*, Volume 15 Available at: DOI: https://doi.org/10.1016/j.diin.2015.09.006 (12 March 2020)

Maple, C. (2017) 'Security and privacy in the internet of things', *Journal of Cyber Policy*, Volume 2:2 Available at: DOI: 10.1080/23738871.2017.1366536 (26 August 2020)

McDermott, Y. (2017) 'Conceptualising the right to data protection in an era of Big Data', *Big Data & Society*, Volume 4(1). Available at: DOI: 10.1177/2053951716686994

Metro Security (N.D) *Temperature Screening System* [Online]. Available: https://www.metrosecurity.co.uk/services/temperature-screening/. [Accessed: 23-Apr-2021].

Mortier, S. Debussche, J. and César, J. (2019) *Big Data & Issues & Opportunities: Privacy and Data Protection* [Online]. Available at: https://www.twobirds.com/en/news/arti-cles/2019/global/big-data-and-issues-and-opportunities-privacy-and-data-protection (Accessed: 12 January 2021)

Muncaster, P. (2020) *UK's IoT Law Hopes to Drive Security-by-Design* [Online]. Available at: https://www.infosecurity-magazine.com/news/uks-iot-law-hopes-to-drive/ (Accessed: 23 July 2020)

Obaidat, M.A. et al., (2020) 'A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures', *Computers 2020*, 9(2), 44; Available at: https://doi.org/10.3390/computers9020044 (16 March 2020)

OECD. (2020) *COVID-19 and the retail sector: impact and policy responses* [Online]. Available: https://www.oecd.org/coronavirus/policy-responses/covid-19-and-the-retail-sector-impact-and-policy-responses-371d7599/. [Accessed: 23-Apr-2021].

Panchal, J. (2019) *How IoT-enhanced warehouses are changing the supply chain management - Part 1 - IoT Now News - How to run an IoT enabled business* [Online]. Available: https://www.iot-now.com/2019/01/07/91762-iot-en-hanced-warehouses-changing-supply-chain-management/. [Accessed: 03-Mar-2021].

Pandey, K. K. Milan, R and Shukla, D. 2018. *Security and Privacy Challenges in Big Data* [Online]. Available at: https://www.researchgate.net/publication/324482789_Security_and_Privacy_Challenges_in_Big_Data (Accessed: 20 May 2020)

Pesheva, E. (2020) *Coronavirus and the Heart* [Online]. Available: https://hms.harvard.edu/news/coronavirus-heart (Accessed July 21, 2020).

Pillai, S. G. et al. (2021) "COVID-19 and hospitality 5.0: Redefining hospitality operations," *International Journal of Hospitality Management,* vol. 94. Available at: https://doi.org/10.1016/j.ijhm.2021.102869 (16 March 2021)

Oussous, A., et al. (2018). 'Big Data technologies: A survey', *Journal of King Saud University - Computer and Information Sciences*, Volume 30(4) Available: DOI: https://doi.org/10.1016/j.jksuci.2017.06.001

Rahfaldt, K. (2019) *How Leveraging Big Data Changes the Perception of Security* [Online]. Available at: https://www.securitymagazine.com/articles/90766-how-leveraging-big-data-changes-the-perception-of-security (Accessed: 22 February 2020)

Richard, K. [N.D]. *Big data and data protection (UK)* [Online]. Available at: https://uk.practi-callaw.thomsonreuters.com/w-017-1623?transitionType=Default&context-Data=(sc.Default)&firstPage=true (Accessed 14 March 2021)

Rosenthal, J. and Oberly, D. (2020). 'The Rise of Internet of Things Security Laws: Part I', *Pratt's Privacy & Cybersecurity Law Report*, Vol. 6, No. 5. Available at: https://www.jdsupra.com/legalnews/the-rise-of-internet-of-things-security-50035/ (Accessed: 10 May 2020)

Rowan, N J. and Galanakis, C M. (2020) "Unlocking challenges and opportunities presented by COVID-19 pandemic for cross-cutting disruption in agri-food and green deal innovations: Quo Vadis?," *Science of the Total Environment,* vol. 748. Available at: https://doi.org/10.1016/j.scitotenv.2020.141362 (15 May 2020)

Seliem, M., Elgazzar, K. and Khalil, K. (2018) 'Towards Privacy Preserving IoT Environments: A Survey', *Wireless Communications and Mobile Computing* vol. 2:15, Available at: DOI: 10.1155/2018/1032761 (17 October 2019)

Song, H. J., Yeon, J. and Lee, S. (2021) 'Impact of the COVID-19 pandemic: Evidence from the U.S. restaurant industry', *International Journal of Hospitality Management*, vol. 92 Available at: https://doi.org/10.1016/j.ijhm.2020.102702

Suleman, H. (2021) *How to Use the IoT to Keep Your Restaurant Clean and Safe | FoodSafetyTech* [Online]. Available: https://foodsafetytech.com/co-lumn/how-to-use-the-iot-to-keep-your-restaurant-clean-and-safe/ [Accessed: 22-Apr-2021].

Tawalbeh, L., et al. (2020) 'IoT Privacy and Security: Challenges and Solutions', *Applied Sciences*, Volume 10(12) Available at: https://doi.org/10.3390/app10124102 (13 February 2020)

Triax Technologies, (N.D) *Proximity Trace » Triax Technologies* [Online]. Available: https://www.triaxtec.com/resource/fact-sheet/proximity-trace/. [Accessed: 23-Apr-2021].

UK Anonymization Network. (N.D) *Home* [Online]. Available at: https://ukanon.net/ (Accessed 23 March 2021)

Vailshery, L S. (2021*) Forecast end-user spending on IoT solutions worldwide from 2017 to 2025(in billion U.S. dollars)* [Online]. Available at: https://www.statista.com/statis-tics/976313/global-iot-market-size/ (Accessed 14 March 2021).

Varga, P. (2017) 'Security threats and issues in auto-mation IoT', *IEEE International Workshop on Factory Communication Systems - Proceedings,* Available at: DOI:10.1109/WFCS.2017.7991968c (15 August 2020)

Waheed, N. et al., (2020) 'Security and Privacy in IoT Using Ma-chine Learning and Blockchain: Threats and Countermeasures'. ACM Computing. Surveys. Volume 53, Issue 6, Article 122. Available at: DOI: https://doi.org/10.1145/3417987 (22 September 2020)

WHO. (N.D) *Coronavirus* [Online]. Available: https://www.who.int/health-topics/coronavirus#tab=tab_1. (Accessed: 22 April 2021).

WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, (2020) *UN Global Pulse, and IFRC Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation* [Online]. Available at: https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation (Accessed 18 December 2020)

Wu, X., et al. (2014). 'Data mining with big data', *IEEE Transactions on Knowledge and Data Engineering*, Volume 26(1), Available at DOI: 10.1109/TKDE.2013.109 (10 October 2020)

Yousif, M. and Hewage, C. Nawaf, L. (2021) 'IoT Technologies during and beyond COVID-19: A Comprehensive Review', *Future Internet* 13(5):105. Available at: https://doi.org/10.3390/fi13050105 (13 February 2020)

Yousuf, T. et al., (2015) *Internet of things (IoT) security: Current status, challenges and prospective measures* [Online]. Available at: DOI: 10.20533/ijisr.2042.4639.2015.0070 (23 May 2020)

Yousefi. A. and Jameii, S M. (2017) "Improving the security of internet of things using encryption algorithms," *IEEE International Conference on IoT and its Applications*, Available at: DOI:10.1109/ICIOTA.2017.8073627 (18 May 2020)

Zarsky, T. (2017) 'Incompatible: The GDPR in the Age of Big Data', Seton Hall Law Review Vol. 47 Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646 (Accessed: 23 May 2020)

Zhou, W. et al., (2019) 'The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved', IEEE Internet of Things Journal, vol. 6, issue 2 Available at: 10.1109/JIOT.2018.2847733 (Accessed: 2 April 2020)

ANNEXURE C.12

Solutions to Big Data privacy and security challenges associated with COVID-19 surveillance systems

This paper was submitted to the Frontier journal

Bentotahewa, V. Hewage, C. and Williams, J. (2021) ‘Solutions to Big Data privacy and security challenges associated with COVID-19 surveillance systems’, *Frontier*. Available at: doi: 10.3389/fdata.2021.645204

Abstract

The growing dependency on digital technology is becoming a way of life, and at the same time, the collection of data using them for surveillance operations has raised concerns. Notably, some countries use digital surveillance technologies for tracking and monitoring individuals and populations to prevent the transmission of the new coronavirus. The technology has the capacity to contribute towards tackling the pandemic effectively, but the success also comes at the expense of privacy rights. The crucial point to make is regardless of who uses and which mechanism, in one way another will infringe personal privacy. Therefore, when considering the use of technologies to combat the pandemic, the focus should also be on the impact of facial recognition cameras, police surveillance drones and other digital surveillance devices on the privacy rights of those under surveillance. The GDPR was established to ensure that information could be shared without causing any infringement on personal data and businesses, therefore, in generating Big Data, it is important to ensure that the information is securely collected, processed, transmitted, stored, and accessed in accordance with established rules. This paper focuses on Big Data challenges associated with surveillance methods used within the COVID-19 parameters. The aim of this research is to propose practical solutions to Big Data challenges associated with COVID-19 pandemic surveillance approaches. To that end, the researcher will identify the surveillance measures being used by countries in different regions, the sensitivity of generated data, and the issues associated with the collection of large volumes of data, and finally to propose feasible solutions to protect the privacy rights of the people, during the post-COVID-19 era.

Keywords: GDPR, Big Data, Privacy, Surveillance, COVID-19, Contact tracing, data protection

1.0 Introduction

The urgent need to manage and find solutions to overcome the effects of the Coronavirus necessitate collecting data in large volumes. On the one hand, Big Data acquisition and storage apparently poses a significant threat to the privacy of individuals, and on the plus side, it helps make informed decisions that are crucial for the prevention of COVID-19. Data protection law faces many challenges in the digital age, and the emergence of Big Data is the most conspicuous and challenging. In the Big Data era, the public enjoys many benefits that internet technology offers to them, but they also do face potential privacy breaches. The failure to protect user accounts and personal data will directly threaten their privacy and security.

The keynote of this paper seeks to support the notion that a pandemic should not be used as a panacea for the introduction of new general surveillance measures without consent. The response of the government and the technology industries to the Coronavirus outbreak became headline news, and concerns were raised about the contact tracing apps, mobile location data tracking, and police surveillance drones (Matthan, 2020, 100). Also, new privacy issues have emerged as the organisations started levelling up surveillance using thermal cameras and face-recognition technology in preparation for the resumption of normal working patterns. The governments also having to comply with the use of surveillance tools in combating the pandemic, sought to strike a balance without compromising data privacy laws.

Civil rights organisations, data protection authorities, and research scholars also have highlighted the risk of increased digital surveillance after the pandemic (Gasser, 2020, E425-E434). These groups have emphasised the need for having baseline conditions such as lawfulness, necessity, and proportionality in data processing, and the need for social justice and fairness (Gasser, 2020, E425), and these conditions should be considered before implementing digital surveillance technology. However, the UN holds the view that the use of AI and Big Data for tackling COVID-19 could threaten human rights globally and has expressed concerns about the deployment of data surveillance techniques during the current crisis. It has also underscored the risk in the adaptation of technology in the future becoming the justified norm (Whitehead, 2020).

The data protection regulations of the European Union are based on the premise that types of data considered to be sensitive require stricter protection than other types due to the higher security risk factor involved in processing them (Kuskonmaz and Guild, 2020). The European Court of Human Rights (ECtHR) has upheld the view that health data must be subjected to stricter safeguards than non-sensitive data (Kuskonmaz and Guild, 2020). The processing of a special category of data is prohibited unless it is carried out for purposes specified under certain conditions (Kuskonmaz and Guild, 2020). The information that is necessary to fight the virus must be up-to-date and should not be retained for longer than required to and should be deleted after the crisis is over without delay (Accessnow, 2020, P.14).

The lessons learned in responding to health sector crises in the past show that the deployment of invasive surveillance could be misguided and may have potentially harmful consequences for human rights and public health (Accessnow, 2020, P.14). The Big Data tracking systems used during the Ebola outbreak led to the violation of privacy rights of millions of people and had minimal effect on the intended purpose to combat the virus (Accessnow, 2020, P.14). The presumption here was that the urgency to tackle the outbreak overshadowed the importance of safeguarding the privacy rights of the citizens. Therefore, even during a health crisis, the right balance should be struck to protect the privacy rights of the citizens.

2.0 Deployed Surveillance measures

The history of surveillance measures goes back to the 14th-century plague outbreak in Europe (Tognotti, 2013). Isolation of affected groups and movement restrictions on the population were imposed as constraining measures to control and prevent spreading the plague, and surveillance measures have been used on similar occasions (Tognotti, 2013). During the severe acute respiratory syndrome in 2003, Hong Kong identified clusters of diseases using electronic data systems (Leung et al., 2004, P. 662-673.). During the Ebola outbreaks in West Africa in 2014–2016, mobile phone data were used to model travel patterns (Wesolowski et al., 2014), and hand-held sequencing devices enabled effective contact tracing and to understand better the dynamics of the outbreaks (Quick et al., 2016). Similarly, digital technologies are in use during the COVID-19 pandemic.

The types of tools deployed during the current pandemic are specifically for the purpose of mitigating the risk and preventing the pandemic from spreading to a wider community. The purpose-built tracing tools are in use for measuring spatial proximity between users and tracking their interaction (Gasser, 2020, E426). Two closely located smartphones used for proximity tracking help determine whether an infected person and an uninfected person being in closed proximity contributed to the transmission of the virus from one to the other, in which case the health authorities can take necessary measures to deal with anyone identified positive of the virus (Jalabneh et al., 2020, P.14-15). Proximity tracking technology when used with a smartphone app can be an effective way to reduce the rate of transmission. Also, a large population in developed countries as well as in low and middle-income countries will benefit from installing the app in their smartphones (Hussein et al., 2020. Trust Concerns in Health Apps collecting Personally Identifiable Information during COVID-19-like Zoonosis, P.1). For example, the Singaporean application Trace Together uses Bluetooth connections to log other telephones nearby and alerts those who have been close to an individual diagnosed COVID-19 positive (Gasser, 2020, E426). Symptom checkers are tools of syndromic surveillance that collect, analyse, interpret, and disseminate health-related data (Berry, 2018). Spanish Government, using this technology worked in collaboration with the citizens, health professionals and the private sector to monitor the disease, respond quickly, allocate resources, and minimise or control the outbreaks (Gasser, 2020, E426). Quarantine compliance tools enable real-time monitoring to determine whether individuals are symptomatic or non-symptomatic and, are complying with quarantine restrictions (Gasser, 2020, E426). One such example is the use of Taiwan's Electronic Fence application installed mobile phones to track overseas quarantined arrivals. (Gasser, 2020, E426).

However, the launching of such automated contact tracing applications carries inevitable privacy and security challenges (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations, P.1). It has been reported that the apps could be repurposed to target their users, and jamming, storage and power drain attacks, active and passive eavesdroppers are such security challenges (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations, P.4). An adversary, on the other hand, can tag an individual’s mobile phone with the contract tracing app to a carrier, which will broadcast false proximity data to the masses. Such actions will lead to wastage of expensive diagnosis resources and are likely to affect trust in, and the efficiency of government mechanisms (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations, P.3).

The world community seems to have made a concerted effort to ease Coronavirus lockdown restrictions and create a conducive environment for people to return to normal work patterns. In anticipation of less restrictive measures, employers have started setting up tech measures in the workplace to protect their employees from COVID-19 and avoid related incidents. These measures mean the installation of new surveillance systems including tracking software to identify individuals who may have been exposed to the virus, monitor social distancing and locate them using blue-tooth beacons embedded in their security passes (Chesler, 2020). In addition, cameras with body temperature measuring capabilities are in use to identify infected individuals entering the building (Chesler, 2020). The cameras take a reading close to a person's eyes, if fever is detected a warning alert emitted, then the person can be sent home (Chesler, 2020). This technology is being used by Amazon to check employees at the entrances to its European and U.S. warehouses as well as to the food store chain (BussinessFirst, 2020).

The use of technical safety applications enables companies to identify contaminated locations once a positive case is found and, carry out cleansing procedures quickly (Chesler, 2020). This is a time-saving cost-effective way for the organisation. Also, the managers can be alerted in a circumstance where the number of employees in a congregation is found to be excessive, and more than allowed at any one time (Chesler, 2020). Japan has been looking into limiting the number of employees in close proximity to avoid too many warning alerts being sent in closely grouped situations (Chesler, 2020).

Also, many countries use Drone technology to control the pandemic. However, the reports suggest that the use of drone surveillance would lead to violation of privacy, especially if the data in the form of image or video is downloaded by an intruder (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations, P.5). The images or video clips of an individual obtained without consent from a drone during an upload or extracted from the cloud server could be used in malicious ways against the individual (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations, P.4). Also, photo image formats such as JPEG contain details of the location and the time photo was taken in the image header files, and some argue the stolen photos would cause additional damage to personal privacy (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations, P.4).

In the next section, the researcher examines the range of technological solutions that the countries have already taken to tackle the pandemic and the steps taken to respond to the sensitive nature of the data generated. The pre-cursor to developing solutions to alleviate long term privacy concerns is having a good understanding of different mechanisms in place to do so.

3.0 Specific measures taken by countries from a regional perspective.

3.1 Asian region

South Korea refrained from imposing nationwide lockdown or travel restrictions despite the risks from Coronavirus incidents in the country (Fahim, Kim, and Hendrix 2020). But instead, the South Korean authorities have been using different covert tech methods to manage the pandemic. The health authorities resorted initially to track public movement tracking the public and follow up tracing of those diagnosed positive with the use of GPS phone tracking, credit card records, video surveillance and interviews with the patients (Fahim, Kim, and Hendrix 2020) (See table 6.4). As a supplementary measure, South Korean authorities have been sending health advisory texts containing details of infected patients and hyperlinks with details of their movements (Servick, 2020). The reaction to this covert monitoring method aroused strong concerns about the potential breaches of medical confidentiality and the inevitable stigmatisation of virus-carrying individuals due to the exposure of their identities in the public domain. Also, according to the reports, patient travel history, excluding the names, was published by the in-country authorities to make others aware of the risks of coming to contact with a person diagnosed positive (Fahim, Kim, and Hendrix 2020). The authorities also use another smartphone app to monitor thousands of people in self-quarantine and report their movements to the government (Fahim, Kim, and Hendrix 2020).

Singapore also assembled technical measures to contain the epidemic by aggressively tracking chains of infection. The apps for mobile phones were developed to help enforce self-quarantine rules and, support contact-tracing efforts using ‘Bluetooth technology’ (Fahim, Kim, and Hendrix 2020) (See table 1). According to the reports, the government of Singaporean has published personal information belonging to Coronavirus patients as a warning to those who may have been in close proximity (Franceschi-Bicchierai, N.D). Kazakhstani citizens placed in quarantine use a SmartAstana tracking app, and it enables the officials to ensure that those in quarantine remain in isolation (Gussarova, 2020). By contrast, the city of Almaty Ministry of the Interior relies on video surveillance technology called Sergek, produced locally by the telecommunications firm, Korkem Telecom, to detect individuals breaching quarantine rules (Gussarova, 2020). These two are the only known measures of new surveillance technologies the government uses as anti-pandemic tools (See table 6.4)

The use of CCTV footage to identify people wearing masks had become a challenging task to do. Therefore, in Bangladesh, a local company has developed a CCTV camera feed system for surveillance and, to successfully identify COVID-19 infected people, and/or those identified positive (DhakaTribune, 2020) (See table 6.4)

China has been using practically every surveillance system at their disposal (Gershgorn, 2020) (See table 6.4). Face recognition cameras are located in public places by the authorities to carry out facial recognition searches and also, mobile phones are used for location tracking (Gershgorn, 2020). Surveillance cameras have also been installed inside private dwellings as well as outside people's front doors, and the inhabitants are placed under mandatory quarantine. (Gan, 2020). The Chinese government is engaged in tracking individuals through smartphone apps such as Alipay and WeChat that grades their health and assigns them a classification of green, yellow, or red (Pisa, 2020). The app transmits that data to the police, and it works as an entry pass to certain public places (Gershgorn, 2020). China has not stopped there and has gone as far as exerting pressure on private companies in the country to hand over data and to support the pandemic containment effort (Gershgorn, 2020). In Hong Kong, airport arrivals are supplied with electronic tracking bracelets that must be synced to their home location by way of the mobile phone GPS signal (Saiidi, 2020).

Indian authorities have expanded tracking citizens through digital and analogue means (Gershgorn, 2020). Location data and CCTV footage are used to track citizens in the southern Indian state of Kerala (Gershgorn, 2020) (See table 6.4). In addition to personal tracking, Indian authorities are also collecting passenger information from airlines and railroad companies. There has been a case in the state of Madhya Pradesh where the authorities had published the personal information of about 5,400 quarantined people on an online public dashboard but according to reports, it was unintentional. (Gershgorn, 2020).

Taiwan uses active mobile network monitoring means to enforce home quarantine for new arrivals, or at-risk individuals (Accessnow, 2020, P.11) (See table 6.4). Public authorities receive an alert if an individual's mobile device happened to be active outside their home (Accessnow, 2020, P.11). The reports have also noted that to prevent those under home quarantine from circumventing the measures, public authorities call the number twice a day to ensure that those being quarantined have not abandoned their mobile devices and ventured outside (Accessnow, 2020, P.11).

Table 6.4: Summary of measures taken to tackle the pandemic by countries in the Asian region

	GPS tracking	Credit card records	Video surveillance	Contact tracing using Bluetooth technology	Face recognition cameras	Mobile network monitoring	Drones
South Korea	✓	✓	✓				
Singapore				✓			
Kazakhstani	✓		✓				
Bangladesh			✓				
China	✓		✓		✓		✓
Hong Kong	✓						
India			✓				
Taiwan						✓	

3.2 Middle Eastern region

Saudi Arabia has taken steps to update two mobile and web-based applications, known as the Mawid (‘Appointment’) and the Sehhaty (‘My Health’) to respond to the COVID-19 pandemic, by way of a symptom checker enabling people suspected of having COVID-19 to directly book appointments at dedicated COVID-19 clinics and countrywide drive-through mass testing locations. (Hassounah,2020). The Health Electronic Surveillance Network (HESN) serves as a national platform for communicable disease surveillance, which is mainly used as a reliable data source for all COVID-19 laboratory tests in the Kingdom (Hassounah, 2020). Moreover, the Patient Tracing Unit (Taqasi) platform was implemented to enhance contact tracing tasks around the Kingdom using laboratory results generated from the HESN (Hassounah, 2020).

The National Health Emergency Operation Centre had launched a smartphone app, Tetamman, ('Rest Assured') to provide preventative and clinical guidelines for home isolation. (Hassounah, 2020). This app is remotely linked to a smart bracelet that can be used by those individuals returning from abroad, as well as those isolated at home. (Hassounah, 2020). Two smartphone apps implemented by the Saudi Data and Artificial Intelligence Authority (SDAIA) follow the international Google and Apple guidelines on data privacy in contact tracing (Hassounah, 2020) (See table 6.5). The first is the Tawakkalna, a GPS-enabled app for monitoring and restricting movements of individuals during curfew hours, with the capacity to issue exemption permits. The second is the Tabaud, ('Distancing') for transmitting de-identified data for preventing close contact with COVID-19 confirmed cases. (Hassounah, 2020).

The cited report suggests that Iran appears to be using smartphones to track citizens in the fight against COVID-19 (Doffman, 2020) (See table 6.5). Iranian researcher Nariman Gharib has revealed that the citizens are put under pressure to download an app that would, according to the researcher, help diagnose the coronavirus vector (Doffman, 2020). However, further, the report cited that Google has removed the app from the Play Store, but the Iranian Ministry of Health has assured that no privacy lines were being crossed (Doffman, 2020).

The Israeli government's domestic security agency, the Shin Bet, is using data from telecom providers to track the locations of millions of citizens to find people diagnosed with the Coronavirus and alert those with whom the infected person might have interacted (Scheer and Cohen, 2020) (See table 6.5). This has raised security concerns amongst many civil liberties groups (Altshuler and Hershkowitz, 2020).

Qatar has made it mandatory for every citizen to download the Ehteraz app and keep it installed indefinitely if they intend to leave their home (Gershgorn, 2020) (See table 6.5). It requires permission to share data, including location, access to all files, and access to call information (Gershgorn, 2020).

Table 6.5: Summary of measures taken to tackle the pandemic by countries in the Middle Eastern region

	GPS tracking	Credit card records	Video surveillance	Contact tracing using Bluetooth technology	Mobile network monitoring	Drones
Saudi Arabia	✓					
Iran				✓		
Israel					✓	
Qatar	✓			✓		

3.3 European region

The project OASIS (UK) collects data from third-party app providers who collect information on COVID-19 related symptoms and demographic data to assist the NHS in its pandemic response work (Ministry of Defence, Strategic Command, and jHub Defence Innovation, 2020) (NHSX, 2020) (See table 6.6). The UK government says Project OASIS will strictly comply with data protection legislation when sharing personal data, and the Ministry of Defence Strategic Command's technology innovation hub, JHub, has been given the remit to oversee the secure transfer of relevant symptom and epidemiology data from the third-party apps to NHSx (Ministry of Defence, Strategic Command, and jHub Defence Innovation, 2020). A specific role of JHub is to remove any identified information, erase incorrect or duplicate data, and check for security issues (NHSX, 2020).

The United Kingdom is reportedly in discussions with telecom companies to engage in tracking its citizens' location data (Gershgorn, 2020). Also, in the meantime, the National Health Service (NHS) has partnered with Palantir to track the spread of the virus and its impact on the health system (Gershgorn, 2020). The mobile industry continues to supply location data of individuals to local, state, and federal government organizations to enhance movement tracking (Gershgorn, 2020). The quality of data enables accurate detection of people movement and whether they comply with the requirement to stay-at-home or not by hanging around open public places.

The Turkish government tracks the locations of Coronavirus patients using their cellular data, automatically sends warning messages to those detected violating quarantine rules, and the cellular companies operating in Turkey are cooperating with the government in its effort to gathering essential data (BIA News Desk, 2020). However, as has been reported, people have become worried about downloading (government provided) surveillance apps (See table 6.6) and entering requested information on them (Fahim, Kim, and Hendrix 2020).

The surveillance tool supplier Cy4Gate in Italy is setting up surveillance tools to track every citizen and their contacts to multiple governments around the world, including their own (Franceschi-Bicchierai, N.D) (See table 6.6). Governments using a system which Cy4Gate calls Human Interaction Tracking System (HITS), has shown the movements of an individual patient. People, by downloading the app and enabling it to track their location as a part of the system, will give voluntary consent (Franceschi-Bicchierai, N.D). According to the reports, Cy4Gate will anonymize the data and only the governmental agency will be able to de-anonymize it (Franceschi-Bicchierai, N.D). Immuni is an app used in Italy to control the spread of the pandemic. It is an open-source COVID-19 contact tracing app (Guerrini, 2020). After a testing phase in four Italian regions, the app started being active in the whole country (Reuters Staff, 2020). Immuni has been designed and developed while taking great care to safeguard user privacy (Presidenza del Consiglio dei Ministri, 2020). To this end, the app does not collect any information such as first name, last name, or date of birth, telephone number, email address, the identity of the people you meet, location or your movements (Presidenza del Consiglio dei Ministri, 2020).

In Germany, privacy laws allow the government to compel a technology company to share an individual's location data in the interests of national security (Servick, 2020). The "GeoHealth" app in development relies partly on the location of Google account holder’s data anonymised and stored in a central server, and data analytics would compare users' movements to those of infected people and send colour coded alerts based on how recently they may have acquired the virus (Servick, 2020) (See table 6.6). One issue associated with Geohealth is the collected data will be stored on a central server and the government can get access to the peoples’ information (Servick, 2020). According to the human rights organisation, such as Amnesty international, developing apps based on centralised architecture has an impact on peoples’ privacy, and for that reason, these human rights organisations do encourage to develop apps based on the decentralised architecture (Bentotahewa, Hewage and Williams, 2020. Do Privacy Rights Override #COVID19 Surveillance Measures?)(Robinson, 2020).

In Belgium, authorities use drones used to make announcements and to capture surveillance footage (Limam, 2020) (See table 6.6). Also, telecoms in Belgium provide data to Dalberg Data Insights (private company) the analyse obtained information to detect widespread trends of movement in the country (Gershgorn, 2020).

France has grave concerns about the potential risk of privacy violations. It is not an obligatory requirement to use the French government's 'Stop Covid' App (Gershgorn, 2020) (See table 6.6). The security cameras on Paris metro-based systems have the capability to identify those wearing masks and those not, and reports point out that these systems are not meant for tracking individuals, but for gathering information on compliance by the commuters (Handler and Liu, 2020 (See table 6.6).

Poland introduced its own app called 'Home Quarantine' with which the quarantined (Polish) citizens were required to check in periodically and send pictures of themselves in their homes, within a 20-minute time-lapse, and those who failed to do so would incur a fine, effective from 19 March (Gershgorn, 2020) (Nicolas, 2020) (Amnesty International, 2020) (See table 6.6). This is to ensure that the person is complying with quarantine orders. According to the reports similar apps are deployed in other countries, including one in India capable of geo-tagging selfies (Amnesty International, 2020). Polish authorities have insisted that this information would remain in government custody for six years (Nicolas, 2020). However, there seems to be no explanation of the purpose for retaining the images in government servers for six years if it were meant to be a temporary measure.

In Bulgaria, the police authorities at their request have been able to obtain information from telephone and internet operators to monitor the conversations between the citizens (See table 6.6). That has allowed them to trace the accurate location of the citizen, monitor those under quarantine, and track the websites visited by the target groups (Vou, 2020). There is a question mark on whether it is necessary for intrusion into the private conversation for the purpose of mitigating the risk of transmission of the virus

Table 6.6: Summary of measures taken to tackle the pandemic by countries in the European region

	GPS tracking	Credit card records	Video surveillance	Contact tracing using Bluetooth technology	Mobile network monitoring	Drones
United Kingdom				✓		
Turkey				✓		
Italy	✓			✓		
Germany	✓			✓		
Belgium						✓
France			✓	✓		
Poland				✓		
Bulgaria					✓	

3.4 African region

In Kenya, mSafari app is being rolled out to help contact tracing (Accessnow, 2020, P.10) (Otieno, 2020) (See table 6.7). As reported, the app would be used to track passengers in public service vehicles including buses, taxis, and other transportation services (Accessnow, 2020, P.10). The drivers are expected to download this app and register all passengers (Accessnow, 2020, P.10). In addition, the government uses electronic surveillance to track individuals subjected to 14-day self-isolation based on their latest travel history, mainly by monitoring their mobile phone usage activities including geo-locations (Ombat, 2020). Also, those in government-imposed self-isolation are instructed to leave their mobile phones switched on, and to carry the devices with them (Ombat, 2020).

GH COVID-19 Tracker App was developed by Ghana (See table 6.7). This app has the capacity to trace those coming into contact with infected person/s (Hussein et al., 2020). In South Africa, telecom service providers, have agreed to share customers' location data with the government, but it is not yet clear whether it is applicable to location data of confirmed cases only, or to the entire population whose information is shared with the government (Business Insider South Africa, 2020) (See table 6.7).

Table 6.7: Summary of measures taken to tackle the pandemic by countries in the African region

	GPS tracking	Credit card records	Video surveillance	Contact tracing using Bluetooth technology	Mobile network monitoring	Drones
Kenya	✓			✓		
Ghana	✓					
South Africa					✓	

3.5 American region

Canadian police has access to a government database, and records of people who tested positive with Coronavirus, and their personal information is held with them (Gershgorn, 2020) (See table 6.8). To allow direct access to personal information for community health purposes on a priority basis is understandable but to provide direct access to law enforcement agencies in this way does amount to an invasion of privacy unless permission had been granted for justifiable reasons.

In the United States, researchers are using Facebook data to measure social distancing. Data collected from Facebook users with their location history enabled and is used to develop maps with aggregated, de-identified location data (Servick, 2020) (Lapowsky, 2020) (See table 6.8). This project presents significant privacy and data protection risks as the users have not given consent to use their location history in the fight against Coronavirus and to share their data with researchers.

In Colombia, the CoronApp, is used to provide information on the virus (Accessnow, 2020, P.16) (See table 6.8). The application requests a large amount of personal information such as data on ethnicity to function, without transparency as to who would be acquiring the data, and how it would be used (Accessnow, 2020, P.16).

The government Guatemala has launched an official application named Alerta Guate with the intent to inform people about COVID-19. To download the app, the users are obliged to allow access to location data, phone microphone, and to provide an email address or phone number (Juarez, 2020).

The Mexican government uses drones for surveillance operations (See table 6.8) of public gatherings, and to issue warnings to people. Also, other measures like hand sanitiser gel and face masks are distributed along the public roadsides, in popular neighbourhoods, and on public transport (Tonantzin, 2020).

Table 6.8: Summary of measures taken to tackle the pandemic by countries in the American region

	GPS tracking	Credit card records	Video surveillance	Contact tracing using Bluetooth technology	Mobile network monitoring	Drones
Canada				✓		
United States	✓					
Colombia	✓					
Mexico						✓

3.6 Oceania region

New Zealand uses NZ Covid Tracer App based user interactions to control and manage the COVID- 19 pandemic when the user is diagnosed positive of COVID-19 during sharing his/her credential with the application, and the user not given the option to raise objections to sharing of personal information. However, it has two-factor authentication and data encryption prior to sending. (Hussein et al., 2020. Trust Concerns in Health Apps collecting Personally Identifiable Information during COVID-19-like Zoonosis, P.5). Apparently, the process has a high standard of privacy protection but comparatively, it is not as effective as other contact tracing applications (Hussein et al., 2020. Trust Concerns in Health Apps collecting Personally Identifiable Information during COVID-19-like Zoonosis, P.5).

Table 6.9: Summary of the approaches adopted by countries and the reasons

Region	Approaches to surveillance	Most adopted approaches and reasons
Asian Region	Smartphone app, CCTV, Electronic tracking bracelets and mobile network providers.	It appears that most of the countries in the Asian region are relying on smartphone apps to tackle the pandemic, and the need for expert knowledge to use Smartphone-based apps is not a factor due to their popularity in the region. Also, technologically advanced countries like China and India are seemingly resorting to CCTV technology as well.
Middle Eastern Region	Smartphone apps and telecom providers	Easy access to mobile phones makes the smartphone-based apps commonly used technology.
European Region	Smartphone apps, drones, telecom and internet providers	In comparison to other regions, most of the European countries use well-advanced technologies alongside basic technologies such as mobile phone apps.
African Region	Smartphone apps and telecom service providers	The reliance on smartphone apps to tackle the pandemic is common in many countries.
American region	Government databases, Facebook, smartphone apps and drones	Leaving basic technologies such as smartphone applications aside, some countries in America's region rely on government databases and data collected from Facebook to manage the pandemic.
Ocean region	Smartphone app.	Despite the high reliance on smartphone apps, there is no sufficient literature about the mechanisms taken by countries in this region.

These overall measures (See table 6.9) may prove effective in helping contain the outbreak, but at the same token, the governments should ensure these tools are implemented with full transparency, accountability, and with a commitment to cease collection or to reserve exceptional use of data once the crisis had been overcome. The data controllers must still have a lawful and fair basis to collect and use personal data. But privacy experts have raised concerns about how governments were using the data, how it was being stored, and the potential for authorities to maintain heightened levels of surveillance after the Coronavirus pandemic is over (Kharpal, 2020). During an extraordinary crisis, many governments appear prepared to overlook privacy implications in preference to saving lives as a priority for them.

4.0 Sensitivity of data generated and associated issues in collecting a large volume of data

Governments have an obligation to guarantee the right to health and to prevent, treat and control epidemics but it is unlawful to use increased surveillance measures unless strict criteria for doing so can be met. The implemented measures must be necessary, proportionate, time-bound, and are implemented with transparency and adequate oversight to comply with any legal obligations. In the wake of the attacks of 11 September 2001 (9/11), the use of apparatus expanded significantly, and the lessons learned from recent history tell us that there is a real danger of surveillance measures becoming permanent fixtures (Amnesty International, 2020).

The governments in several countries have started to use geolocation data gathered from local telecommunications providers and, from social media organisations, Google, and Facebook to monitor the movements of groups of people within a selected certain region (Pisa, 2020). However, name, address, and other identifying information can be generally removed from these types of datasets, but reidentifying individuals have been proven to be considerably easy unless protected by additional privacy protection (Narayanan and Shmatikov, 2019, P.2).

Also, in addition to the risk of reidentification and infringement on personal privacy, digital public health technologies also carry an inherent risk of discrimination (Gasser, 2020, E428), and such technologies can be used to collect large amounts of data from the entire population. These data can include race, ethnic group, gender, political affiliation, and socioeconomic status, and in turn can be used to demographically classify the population (Gasser, 2020, E428). Many of these demographics are sensitive and not necessarily related to a person's health and might lead to stigmatisation of ethnic or socioeconomic groups. Further, information such as racial demographics might lead to a surge in discrimination, as seen by a rise in attacks on people of Southeast Asian descent in the COVID-19 crisis (Gasser, 2020, E428).

The GDPR provides an exception clause to the processing of personal data by employers and public health authorities, in epidemic circumstances without having to obtain consent from the data subject (CIPESA staff, 2020). However, obtaining consent validates the legal basis for data processing in compliance with the GDPR. Also, consent must be obtained from the data subject in an unambiguous statement. Does this mean that for example, proximity-based contact tracing applications might rely on obtaining consent? Some experts do argue that obtaining consent would be meaningless unless the data subject is given a choice to object to the processing of his data. This suggests that voluntary participation for contact tracing applications might not necessarily rely on consent as the legal basis to process the data. However, mishandling or abusing the data surveillance work will lead to loss of citizens' trust in data-based initiatives, and jeopardise the government's effort to control the spreading of the Coronavirus.
The Health Insurance Portability and Accountability Act (HIPAA) was set up to protect sensitive health information about patients, and to prevent them from disclosure without consent or knowledge of the patients (U.S, Department of Health &amp; Human Service, N.D). One specific area to which privacy regulations were applicable was the health care providers who collect and store health information in electronic form (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations'). However, HIPAA does not stress the importance of the consent factor and the right to be forgotten as prescribed in the GDPR, and in such instances, stored private data can be misused after the pandemic (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID- 19: Privacy and Security Challenges with Recommendations, P.4). There is a policy incompatibility between HIPPA and GDPR, which will lead to likely privacy violations in the future.

There are valid questions that need clear answers; on the assumption that the purpose of collection is justified, what is the time scale for data collection and the retention period, following up from that when will collected data be deleted. These are the questions arising from the collection of a massive amount of personal data of the citizens. Also, another crucial question is what options are available to the public to contest any unethical purposes.

In a matter of months, millions of people in countries around the world have been placed under surveillance. Governments, private enterprises, and researchers monitor the health, behaviour, and movements of the citizens, often without their consent (Fahim, Kim, and Hendrix, 2020). This enormous effort serves as a necessity to enforce quarantine rules and for tracing the spread of the Coronavirus. Epidemiologists and government health officials have been deeply involved in designing Coronavirus tracking programs (Fahim, Kim, and Hendrix, 2020).

The groups with interests in privacy issues have been far more concerned about the leading roles taken by the intelligence agencies in gathering personal information (it has been the case in Pakistan and Israel), and when tracing is outsourced to private companies (Fahim, Kim, and Hendrix, 2020). For instance, an Israeli company, NSO which is an infection-tracking software developer, is well known for designing surveillance tools used by authoritarian governments (CIPESA staff, 2020) for spying on dissidents, journalists, and others, and for that reason, has come under criticism (Franceschi-Bicchierai, N.D).

The collection of data raises privacy concerns about the implications of using technology once the people are back at work, and the likely possibility of them coming under more surveillance. The data generated from these technologies can now be used to target these employees, and as such, some privacy advocates already believe that technical solutions already have put people under over surveillance and feel concerned about their job security (Chesler, 2020).

Another concerning issue is the face recognition technology using advanced surveillance cameras capturing people movements without obtaining consent. As far as monitoring individuals under suspicion of posing a threat to people security and national security is understandable but inevitably the identity of those going about their daily business are also recorded.

The experts have highlighted the potential for heightened surveillance to continue even after the Coronavirus outbreak has been brought under control (Kharpal, 2020). The surveillance technologies once introduced have a habit of becoming permanently embedded in the systems (Amnesty International, 2020) (Zhong, 2020) and their use becomes the accepted consequence of living in a world threatened by real threats, mainly cyber and conflict. But we have seen recently that a pandemic such as Coronavirus can be even more devastating and combating it has stretched resources to the limit, and the introduction and the use of technology systems have become the only effective weapon to combat the prevailing COVID-19 pandemic. That has demanded increased deployment of all technology-based systems to mitigate the potential health risks to the communities and manage the virus before it got out of control. The overarching priority is to protect the people and the nation and taking measures to counter such threats will inevitably infringe on civil liberties.

The aftermath of the 9/11 terrorist attack in New York in 2001 was a game-changer for security services all over the world, and the use of advanced technology became the norm for surveillance purposes (Amnesty International, 2020). Soon after the attack, the US promulgated the Patriot Act and it had a direct impact on democratic liberties, such as the right to protection against unwarranted surveillance (Larsen, 2020) (Gasser, 2020, E429). This is a good example of how the protection of the citizens overrides the privacy of individuals in extenuating circumstances. But, whilst recognising the need to take prompt action in critical circumstances, the public should be given a clear indication of the purpose of surveillance operations, the proposed types of data to be collected, time scale and retention period, and the consequence of not doing so would place those individuals engaged in covert operations in danger. However, collected data should remain in the custody of authorised agencies who should be held accountable for any breaches of confidentiality, and as required by law, they should inform those affected by the breaches. These are GDPR specified requirements that many countries have signed up to.

Table 6.10: Issues associated with the collection of large volumes of data during COVID-19

Issue ID	Issue
4.0.1	Geolocation data gathered from local telecommunications providers, social media organisations, Google, and Facebook to monitor movements of groups of people within a selected region (Pisa, 2020) generated Big data, and additional privacy protection measures should be put in place to protect their privacy (Narayanan and Shmatikov, 2019, P.2).
4.0.2	Digital public health technologies can be used to collect large amounts of data from the entire population, but it also has an inherent risk of causing discrimination (Gasser, 2020, E428).

4.0.3	The GDPR sets out legal grounds for enabling employers and competent public health authorities to process personal data in epidemic circumstances without the need to obtain consent from the data subject (CIPESA staff, 2020).
4.0.4	The Health Insurance Portability and Accountability Act (HIPAA) was set up to protect sensitive health information about patients, and to prevent them from disclosure without consent or knowledge of the patients (U.S. Department of Health &amp; Human Service, N.D). However, HIPAA does not stress the importance of the consent factor and the right to be forgotten as prescribed in the GDPR (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID- 19: Privacy and Security Challenges with Recommendations, P.4). Collection, processing and sharing of personal data without consent have been happening for years. The implementation of the GDPR gives the data subject the right to request deletion of gathered data and the data controller is obliged to obtain consent from the data subject in the collection of data. Both have come to light in the aftermath of the pandemic which necessitated the mass collection of information.
4.0.5	The questions arising from the collection of a massive amount of personal data of the citizens are specific; on the assumption that the purpose of collection is justified, what is the time scale for data collection and the retention period, following up from that when will collected data be deleted, and what options are available to the public to contest any unethical purposes.
4.0.6	The collection of data using technology raises privacy concerns and the implications on people becoming under increased surveillance.
4.0.7	Face recognition technology used in advanced surveillance cameras to track people movements without obtaining consent raises privacy and security concerning issues.

4.0.8	There is a real danger of surveillance measures becoming permanent fixtures (Amnesty International, 2020).

5.0 The Proposed Roadmap Framework

Since the emergence of COVID-19 in Asia in 2020, it evolved into a global pandemic that spread across every continent beyond borders (UNDP, N.D.). To meet the mammoth challenges the world community faced, every nation resorted to implementing a variety of technical solutions to arrest and mitigate the catastrophic impact of the pandemic. However, the collection of the mass amount of data using implemented devices contravenes GDPR principles on privacy security, and Big Data generated in this way could potentially undermine the privacy of people in the long term. Therefore, it is strategically important to develop a post-pandemic privacy protection 'solution framework', and global level mechanisms set up to manage pandemics, like the COVID-19, in the future.

The purpose of the tables below (See table 6.11, table 6.12, table 6.13, table 6.14, table 6.15, table 6.16, table 6.17, table 6.18 and table 6.19) is to illustrate the methodology used to identify the available mechanisms and to identify privacy risks associated with those mechanisms. The objective is to develop appropriate immediate, medium, and long-term solutions to underpin privacy protection, and to help management preparedness of a pandemic like COVID-19 in the future. Referring to our observations and investigations made in each section of the tabulated data, the authors provide a summary of different surveillance systems, their objectives, type of data collected, privacy risks and implications with the aim of developing consistent solutions for the immediate, medium, and long term.

Table 6.11: Community surveillance: Immediate and long-term solutions proposed by the researcher

Surveillance systems	**Community Surveillance**
Mechanisms used	Contact tracing

Mechanism objective/purpose	• Break the pandemic transmission chain. Contact tracing identifies and tracks individuals suspected positive of COVID-19. This allows quarantining individuals in the high-risk category and prone to infection /or ill, to prevent transmission to others (WHO, 2020. Contact tracing in the context of COVID-19- Interim guidance, P.1).
Data types collected	• Name, contact number, locations, and movement of the person (ICO, N.D. Maintaining records of staff, customers, and visitors for contact tracing purposes) (Jalabneh et al., 2020, P.8).
Privacy risks and implications	• Difficult or impossible to anonymize user movements and associations (Zang and Bolot, 2011). • It is not deemed necessary to collect location data for effective contact tracing (European Data Protection Board, 2020, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, P.15). • Issues associated with architecture. Centralised architecture could compromise all user data (Bentotahewa, Hewage and Williams 2020. Do Privacy Rights Override #COVID19 Surveillance Measures?) (Robinson, 2020). • Authoritarian entities such government, employer or university may have exceptional control over the individual (Howell and Talbert, 2020). • Not all the countries have specified the storage policy (Jalabneh et al., 2020, P.6-7).
Preventive mechanisms applied	• Apple-Google's joint solution uses Bluetooth technology (Howell, and Talbert, 2020). • Bluetooth signal strength between two user devices tracks the distance between them whether they have been in close contact (Howell and Talbert, 2020).

	• Track potential contact between users without having to track their locations (Howell and Talbert, 2020). • Reliance on decentralised architecture for storing data collected from user devices (Criddle and Leo, 2020) (European Commission, 2020).
The researcher proposed/immediate solutions	• Transparency (ICO. N.D. Right to be informed) is crucial. Governments should make the users aware of the methods of collecting, processing, and storing data. • Data minimisation is a key principle in GDPR (ICO. N.D. Principle (c): Data minimisation): Users should be made aware of the type of data, and collection restrictions, only what is required. • Help build trust and reduce the risk of an entity contravening privacy regulation. • Countries using a centralised version should be aware of the backlash. • The apps should be used on a voluntary basis, not be compulsory (European Data Protection Board, 2020, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, P.4). • Proper learning should be arranged to overcome any potential cyber-attacks (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations, P.5). • App manual should cover the topic of how to be secured from hackers (Hussein et al., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations, P.5).
The researcher proposed long term solutions	• Crucially important to develop a national-level privacy mechanism guaranteeing the protection of privacy of users especially in a pandemic situation

	- Should anonymise data to retain data longer than necessary (ICO. N.D. Principle (e): Storage limitation). If difficult to do so, consent must be obtained from users. - Important to have an international level agreement on the retention period for information collected during the pandemic. - National level decisions will not suffice as pandemic has gone beyond national borders.

Table 6.12: At the primary care level surveillance: Immediate and long-term solutions proposed by the researcher

Surveillance systems	**At the primary care level Surveillance**
Mechanisms used	Community testing facilities: (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3) - Drive-through sites - Fixed sites in community buildings
Mechanism objective /purpose	- To detect individual cases and clusters in the community. (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3)
Data types collected	- Generic data: age, sex, location of residence, illness detected date, samples taken and test results (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3) Additional information collected by some countries (i.e., UK): - Ethnicity, vehicle registration number, National Insurance number, NHS number, employer details, and of other members of the household (Department of Health and Social care. 2020)

Privacy risks and implications	• In the testing process, a large amount of data is collected (by different countries) and exposed to undue risks of breaches (BBC. 2020) by the hackers thereby allowing them easy access to personal data records. • The samples analysed and results supplied to NPEx by the laboratories are forwarding to the NHS. Given the length of the process chain, chances of human error in transmitting test results in this way potentially impact the individuals (NPEx, N.D)
Preventive mechanisms applied	
The researcher proposed immediate solutions	To keep in line with GDPR guidelines. • Important to collect a minimum amount of information (ICO. N.D. Principle (c): Data minimisation). A better option is to collect optimum data needed at the symptom diagnosis stage, including any other symptomatic health conditions, and voluntary self-declaration of other information such as the vehicle number, ethnicity, and other useful information. • Crucially important to provide training to those who assist in sending final test results (General Medical Council, N.D).
The researcher proposed long term solutions	• Need a global level mechanism/policy in place setting out the maximum allowable time duration for store collected data during the pandemic. • If required to retain data for research purposes, only anonymised data should be used (ICO. N.D. Principle (e): Storage limitation).

Table 6.13: Hospital-based surveillance: Immediate and long-term solutions proposed by the researcher

Surveillance systems	**Hospital-based surveillance**
Mechanisms used	• Data records taken and reported daily. (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3) (Goethem, et al. 2020).
Mechanism objective/purpose	• To identify the spread of the virus and the affected communities (Goethem, et al. 2020)
Data types collected	• Age, gender, and place of residence (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3). • Illness onset date, sample collection date, admission data (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3). • Type of laboratory test and laboratory test results (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3). • Whether a health care worker or not (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3). • Condition of the patient, severe or not, at the time of reporting, post-admission medication ventilation or in intensive care unit (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3). • Either the discharge date or cause of death, as applicable (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, P.3).

Privacy risks and implications	• Breaches of sensitive health information will reveal clinical information of the patients, their inherent health conditions, and the entire medical records (Beltran-Aroca, et al., 2016).
Preventive mechanisms applied	• Blockchain technology has been suggested for use in the health care sector (Seiferty,. 2020).
The researcher proposed immediate solutions	• Limit access to the patient medical record. • Back up medical records at least twice a week. • Should not share the identifiable information with the media groups without the patient's consent (Zhang, 2020). • It seemed important to share information with other organisations, to be aware of the severity of the virus, always choose anonymised data, limited data as much as possible (ICO. N.D. Principle (e): Storage limitation).
The researcher proposed long term solutions	• Need a global level mechanism/policy limiting maximum time duration the authorities are allowed for storing information. • If the authorities are interested in retaining collected data for research purposes, only the anonymised data should be used (ICO. N.D. Principle (e): Storage limitation).

The table 6.14: Healthcare-associated surveillance: Immediate and long-term solutions proposed by the researcher

Surveillance systems	**Healthcare-associated surveillance**
Mechanisms used	• Take daily figures and report them (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 3-4).

Mechanism objective /purpose	• To allow rapid control: All cases and clusters in health care settings should be investigated and documented for their source and transmission patterns (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4).
Data types collected	• The number of COVID-19 cases and deaths amongst health workers (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4).
Privacy risks and implications	• Health information is sensitive information (European Data Protection Supervisor, N.D). • A data breach will reveal medical information, conditions as well as medical history pertaining to any other conditions (Beltran-Aroca, et al., 2016).
Preventive mechanisms applied	
The researcher proposed immediate solutions	• Limit access to the patient medical record. • Back up records at least twice a week. • Should not share identifiable information with the media organisation, or departments in the hospital without the patient's consent (Zhang, 2020).
The researcher proposed long term solutions	• Important to use only anonymised data if retaining for research purposes, anonymised data should be used (ICO. N.D. Principle (e): Storage limitation). • Need a global level mechanism/policy to obtain consent from the patients before deciding to use personal information by the authorities for research purposes

Table 6.15: Laboratory testing data surveillance: Immediate and long-term solutions proposed by the researcher

Surveillance systems	**Laboratory testing data surveillance**
Mechanisms used	• Take daily figures and report them (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4).
Mechanism objective/purpose	• To identify the total number of individuals tested for SARS-CoV-2 virus. (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4) • To monitor the trends (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4).
Data types collected	• The number of tests conducted, and the cases confirmed by each diagnostic method used should be logged and reported (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4).
Privacy risks and implications	• Should not reveal identifiable information of COVID-19 positive patients without consent (Zhang, 2020).
Preventive mechanisms applied	
The researcher proposed immediate solutions	• Anonymise the identity of the patient. • Access control.
The researcher proposed Long term solutions	• Need a global level mechanism/policy setting out a maximum time duration allowed for storing of information. • Important to use only anonymised data if retaining for research purposes (ICO. N.D. Principle (e): Storage limitation).

Table 6.16: Mortality Surveillance: Immediate and long-term solutions proposed by the researcher

Surveillance systems	**Mortality Surveillance**
Mechanisms used	• Take daily figures and report them. (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4)
Mechanism objective/purpose	• To identify the death rates (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4).
Data types collected	• The number of COVID-19 deaths occurring in the community, including in long-term-care facilities. Details collected are age, sex, and location of death (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance).
Privacy risks and implications	• The GDPR only applies to information that relates to an identifiable living individual (ICO. N.D. What is personal data?).
Preventive mechanisms applied	• The GDPR only applies to information that relates to an identifiable living individual (ICO. N.D. What is personal data?).
The researcher proposed immediate solutions	• The GDPR only applies to information that relates to an identifiable living individual (ICO. N.D. What is personal data?).
The researcher proposed long term solutions	• The GDPR only applies to information that relates to an identifiable living individual (ICO. N.D. What is personal data?).

Table 6.17: Participatory surveillance: Immediate and long-term solutions proposed by the researcher

Surveillance systems	**Participatory Surveillance**
Mechanisms used	• Voluntary reporting (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4-5).
Mechanism objective/purpose	• For self-reporting signs/symptoms to the government, medical staff to remain informed of the extent of the spread (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4-5).
Data types collected	
Privacy Risks & Implications	• Even people are coming forward, their privacy should not be compromised.
Preventive mechanisms applied	
The researcher proposed immediate solutions	• It is ideal to design questionnaire/voluntary reporting portals to collect data anonymously.
The researcher proposed long term solutions	• The data which are not important can be deleted after the analysis process. • Important to anonymise data if retaining for research purposes (ICO. N.D. Principle (e): Storage limitation).

Table 6.18: Event-based surveillance: Immediate and long-term solutions proposed by the researcher

Surveillance systems	**Event-based surveillance**
Mechanisms used	• Formal and informal channels such as online content, radio broadcasts & print media. WHO-led Epidemic Intelligence from Open Sources (EIOS) uses to filter data (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4).
Mechanism objective/purpose	• To detect any changes in the overall COVID-19 situation (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 4).
Data types collected	
Privacy risks and implications	• Revealing the identity and the movement of people would cause critical mental distress to the patients (Bentotahewa, Hewage and Williams. 2020. Security and privacy issues associated with Coronavirus diagnosis and prognosis).
Preventive mechanisms applied	• Anonymise the identity.
The researcher proposed immediate solutions	• Sensible reporting by not highlighting any group of people based on their gender orientation, ethnicity, or any sensitive nature (Bentotahewa, Hewage and Williams. 2020. Security and privacy issues associated with Coronavirus diagnosis and prognosis).
The researcher proposed long term solutions	• There should be a global level media ethics policy in related to pandemic situations.

Table 6.19: Closed settings: Immediate and long-term solutions proposed by the researcher

Surveillance systems	**Closed settings**
Mechanisms used	- Daily screening (i.e., daily temperature monitoring) for signs and symptoms for COVID-19 (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 3-4).
Mechanism objective/purpose	- To identify the carriers of the virus before it spreads amongst the extended communities (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 3).
Data types collected	- Body temperature of the person (WHO. 2020. Surveillance strategies for COVID-19 human infection-Interim guidance, 3-4).
Privacy risks and implications	- Some organizations can use or disclose sensitive information, such as health data or temperature monitoring results, to prevent or manage COVID-19.
Preventive mechanisms applied	- Use of automated thermal cameras (Practical Law Data Privacy Advisor, 2020). - Organisations in some countries do not record the temperature readings (Tuttle and McKenzie. 2020). - In some countries, organisations do record temperature readings but not personal information. (Practical Law Data Privacy Advisor, 2020).
The researcher proposed immediate solutions	- Every workplace should have a guidance document to ensure personal privacy when recording temperature readings. - Depending on the country if a workplace is disclosing any sensitive information, the information should be anonymised.

The researcher proposed long term solutions	• Need a global level mechanism/ policy in place stating the maximum time duration the authorities can store information. • If the authorities would like to keep data for research purposes it is important to use only the anonymised data (ICO. N.D. Principle (e): Storage limitation).

6.0 Discussion and Author recommendations

6.1 Need to revisit developed guidance documents for global surveillance during an influenza pandemic.

In May 2020, WHO released an interim guidance document addressing the risks elements associated with the use of digital proximity tracking technologies that were enacted by the nations in response to COVID-19 (WHO, 2020). A most notable inclusion is the need to undo extraordinary surveillance activities after a crisis has passed, and for that reason, the WHO should urge governments to enact sunset clauses that would automatically deactivate emergency surveillance measures within a set timeline, unless further legislative action is deemed necessary in response to a specific event.

Global research collaboration for infectious disease preparedness (GLoPID- R) on the other hand has published a protocol on data sharing, and under key principles of data sharing it noted the importance of ethical requirement and transparency (GLoPID-R, 2017). It is also important to consider the following points when GloPID-R and WHO are revisiting their guidance document on global surveillance during an influenza pandemic.

6.1.1 The proposed techniques

- Roles and responsibilities of WHO and member states, based on national and regional level data protection mechanisms.
- Reference to new techniques used by different nations and the tendency of implications that would occur if the mechanisms do not align with data protection and privacy.
- Compulsory reporting on privacy and security risk assessment before releasing a new technique.

- Obligatory policy requirement on disclosure of collected information to media, health authorities or any other party.

- Specification on time limits for holding collected data by member states. This step is crucial in addressing issue 4.0.5 (See table 6.10). This will give individuals the confidence they need for sharing personal information with the relevant authorities and help the government approach tackling the pandemic.

- Recommendations to media and healthcare professionals when releasing identifiable information on a case-by-case basis reporting.

- Encourage countries to provide a report on the effectiveness of the deployed devices in instances where the number of reported cases is low, and to assess whether there would be added value in future deployment of technical devices to tackle pandemic situations.

- A national focal point for the purpose of reporting privacy violations to WHO will help to address the issue 4.0.3 (See table 6.10). It is also important to establish a department under the WHO umbrella to monitor the use of technical measures, behavioural effects on individual privacy, track any privacy violation, potential threats to individual privacy, and take urgent impartial actions to prevent escalation of the situations.

6.1.2 Lessons learned

- Outline the roles and obligations of WHO and the Member States in connection with the protection of privacy when using surveillance during a pandemic.

- Clarity on the type of data being collected at different stages of the pandemic; quantity of data collected should be to a minimum level, where possible. This will also contribute to addressing issue 4.0.3 (See table 6.10).

- A global level mechanism in line with GDPR requirements, to enforce deletion of data within a set time scale; also, a global level agreement that makes the government obliged to justify the purpose for retaining personal data collected during the pandemic, and which organisations would be entitled to access information, and what actions could be taken to prevent disclosure of personal identities of individuals.

- There should be a binding international legal agreement with collective involvement of all nations across the globe, with a pledge to develop a global level ethics report that applies to healthcare professionals, media and any other organisations participating in data handling processes, collection, and storage of personal information of individuals.
- Clear guidance made available on timing to de-escalate or cease surveillance activities will help to address the issue of 4.0.6 and 4.0.8 (See table 6.10).
- A defined limit to what extent technology can intervene in people's privacy will help to address the issue 4.0.6 (See table 6.10).
- The norms and obligations on violations of personal privacy must be underwritten by legal procedures.

6.2 Proposed feasible solutions to overcome potential security concerns to protect citizens' right to privacy during post-COVID-19

An influenza pandemic will affect every country. Therefore, it is essential to have a standardized coordinated information-sharing mechanism at the global and national levels to effectively manage a serious incident (such as COVID-19). At the national level, authorities need to have informed knowledge of the momentum of the pandemic and awareness of the potential risks not only in their own country but also that of neighbouring countries, and in the regions. That approach requires having in place appropriate surveillance systems for gathering personal data, and to avoid contravening laws in member states, there should be laws on surveillance, data collection, storage and reporting, and confidentiality of the patients must be followed. The patients must be informed of the reasons for sampling and processing of the specimens, and they must be made aware of the benefits that would bring with recommended good practice, also, they should be reassured of their safety and confidentiality in the process itself.

The question is whether there is a strong case for inducing technology into surveillance operations in extenuating circumstances where public safety and security matters, regardless of the nature of the risks. The answer must be a clear 'Yes' and can be justified because surveillance plays an important role in times of a pandemic situation or incidents threatening the security of the state. Having all that said, in the context of the COVID-19 pandemic, the enforcement of new digital surveillance powers can also threaten privacy, freedom of expression, freedom of association, and can also lead to scepticism and loss of public trust in the system itself, further undermining the effectiveness of intended public health response. To avoid such misconceptions, it is essential to clearly set before the public the purpose for the imposition of such measures and why they are needed, and arbitrary measures are contested by the activists, as has been seen during the recent health crisis.

There should also be a plan to address post-COVID-19 privacy implication issues associated with the technical solutions, and how the public can be reassured of their confidentiality in the long term, and the pandemic is not used as an excuse to retain surveillance measures indefinitely. That must be embedded in the decision-making process in accordance with the accepted ethical norms to 'obtain consent' before retaining and disclosing personal data collected during the pandemic. One option available to countries for data collection is to have strict data privacy laws when requesting telecommunications and other tech companies to share anonymous, aggregated information in their possession.

The United States and the European Union have specific laws to regulate data collection from the app and device users (Servick, 2020). In the first instance, the collection of data is conditional on consent being obtained from the user of the apps and devices by the collecting organisation (collector) (Servick, 2020). However, the requirement for obtaining consent will not apply to face recognition technologies. Beyond that, the collector specifying the purpose, process, usage, storage, and disclosure procedures, particularly sharing of personal data will at least address the issue of 4.0.7 (See table 6.10) up to some extent. The mobile carriers in Germany and Italy have started to share cell phone location data with health officials in an aggregated, anonymized format (Servick, 2020). Even though individual users are not identified, the data could reveal their general trends, and track and trace their gathering locations, and take action to prevent the infection from spreading. The ministry of health of Germany, according to reports, has drafted changes to their Infection Protection Act to enable, tracking of people suspected of having in contact with Coronavirus infected individuals (Rimpiläinen, Thomson, and Morrison, 2020, P.23).

The introduction and adoption of the contact tracing apps and the use of drones and CCTV were considered essential tools to control the virus and prevent transmission within the communities, and reduce the additional burden on the already overstretched healthcare sector. But the low level of focus on privacy and security implication on the citizens and the lack of foresight on legal aspects masked the importance of surveillance measures. It is right to point out that compliance with legal obligations to protect confidentiality and personal privacy is also important in managing the pandemic, and the responsibility for that rests with the government. Therefore, the emphasis should be to strike a balance to successfully manage the pandemic without infringing individual privacy.

Privacy-by-design can help address the risks. Privacy-by-design seeks to deliver the maximum degree of privacy by ensuring that personal data protection is built into the system, by default. For example, privacy-by-design may involve the use of aggregated, anonymised, or pseudonymous data to provide added privacy protection, or deletion of data once its purpose is served. For example, the COVID-19 app developed by the Norwegian Institute of Public Health is designed to store location data for 30 days only (OECD, 2020. Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics). Simultaneously, data minimisation principles specify that organisations should collect required information only (ICO, N.D), and it provides a solution to issue 4.0.2 (See table 6.10). For instance, when the identities of the employees suspected of having Coronavirus symptoms is needed, and to know whether they had been exposed to risk whilst visiting any high-risk country. However, collecting information about their household members, as far as the workplace is concerned is contestable. The organisations should exercise caution and ensure appropriate data safety security measures are in place when collecting other health data.

RAND Corporation researchers also have developed a concise, standardised, and transparent privacy scorecard that would help health officials understand and evaluate the privacy implications of mobile surveillance programs (Boudreaux, et al., 2020). Also, with the availability of a wide range of mobile surveillance programs capable of monitoring COVID-19, it had been their intention to have a standardised approach. The RAND wanted public health agencies to be able to compare the efficacy and usability of such programs as well as the inclusion of privacy protection means in different programs that will help make decisions appropriate to intervention selection (Boudreaux, et al., 2020). For example, Australia’s COVIDSafe contact tracing program fulfilled 16 of the 20 scorecard criteria and partially did two others; but in contrast, South Korea’s contact tracing program fully or partially met only six, and failed in nine, the remaining five were either unclear or not applicable (Boudreaux, et al., 2020).

Privacy and security researchers are engaged in producing a package of protection mechanisms that would provide the basis for developing a consistent and meaningful privacy protection policy. For example, Harvard University's Centre for Ethics, in a recent publication, has identified tracing protocols with the capacity to mitigate privacy risks and, promote the use of critical security and privacy controls that would enable acceleration of medical responses while maintaining people's rights (Sharma and Bashir, 2020. 1166). Another team of researchers has come up with a system that has the ability to secure privacy-preserving proximity tracing at a large scale (Sharma, and Bashir, 2020. 1166). It is aimed to help the application of anonymous identifiers and functional requirements of fundamental security and privacy, such as data minimization and retention (Sharma, and Bashir, 2020. 1166). Also, emerged in other publications are suggestions for anonymization and encryption to generalize peoples' data while at the same time protecting user privacy (Sharma, and Bashir, 2020.1165). However, recent research suggests that despite the anonymisation of personal data, people could still be identified by a limited set of data points. (OECD, 2020. Ensuring data privacy as we battle COVID-19) (Almeida, et al., 2020).

Also, risking privacy violations will reflect badly on accountability and public trust in the government. The possibility of violating one's privacy by state officials or technology companies might make citizens reluctant to come forward for COVID-19 testing, downloading public health-oriented mobile phone apps, or sharing symptom or location data. More broadly, actual, or perceived privacy violations might discourage citizens from believing government messaging or complying with government warnings and enforceable regulations concerning COVID-19. Therefore, it imperative to have a privacy governance mechanism in place if the citizen were to have faith in the government, and confidence in the actions being taken to mitigate the risk of the pandemic from spreading.

Also, ignoring privacy will have a negative impact on accountability and public trust in the government. The possibility of violating one's privacy by state officials or technology companies might make citizens reluctant to come forward for COVID-19 testing, downloading public health-oriented mobile phone apps, or sharing symptom or location data. Therefore, it imperative to have a privacy governance mechanism in place if the citizen were to have faith in the government, and confidence in the actions being taken to mitigate the risk of transmission.

Privacy enforcement authorities (PEAs) also have a leading role to play. By proactively advising governments on proposed new legislation, they can ensure clarity in the application of the existing privacy and data protection framework (OECD, 2020. Ensuring data privacy as we battle COVID-19). PEAs in Argentina, Australia, Canada, Finland, France, Germany, Ireland, New Zealand, Poland, Slovakia, Switzerland, and the United Kingdom have issued general guidance to the data controllers and processors, about the application of privacy and data protection laws during the pandemic (OECD, 2020. Ensuring data privacy as we battle COVID-19).

As a result, many countries have recently passed or are about to pass laws incorporating guidance specific to data collection restrictions, time limits, and the purpose for the collection. For example, The Italian government published a decree to create a special legal framework for collecting and sharing health-related personal data by the health authorities and their associated partners in the private sector, with set guidelines on time limits during the state of emergency (OECD, 2020. Ensuring data privacy as we battle COVID-19). The German government has proposed amendments to the Infection Protection Law thereby allowing the Federal Ministry for Health to request persons at 'risk' to self-identify and provide their travel history and contact details (OECD, 2020. Ensuring data privacy as we battle COVID-19).

The announcement made by the Information Commissioner's Office (United Kingdom) noted the public interest in the application of its data protection law, and the urgent need to enable data controllers to balance their obligations to respond to public requests (OECD, 2020. Ensuring data privacy as we battle COVID-19). The introduction of additional privacy protection measures will protect personal privacy during the pandemic and will provide a solution to issue 4.0.1 (See table 6.10). However, there are other governments that have collected and processed COVID-19 related geolocation data without the need to adopt new legislation. The Republic of Korea, for instance, the authorities do have existing extraordinary powers to collect personal data, when it is necessary to prevent infectious diseases and prevent the infection from spreading (OECD, 2020. Ensuring data privacy as we battle COVID-19). In Singapore, personal data can be collected, used, and disclosed without consent to enable contact tracing and other measures in response to an outbreak such as it has been in the case during the pandemic (OECD, 2020. Ensuring data privacy as we battle COVID-19).

7.0 Conclusion

There is much interest in privacy as nations are engaged in collecting massive amounts of personal data of their citizens in response to the COVID-19 pandemic. The positive steps taken by individual states or collectively by groups of states, the European Union being one, demonstrate the importance of regulating data collection and the impact on the privacy rights of the citizens. There may be a justification for gathering, storing, processing, and sharing personal data, however, COVID-19 must not be a panacea for collecting personal data in this way. The most concerning is the risk of unauthorised disclosure of personal data for unethical purposes, and that makes the case for having unambiguous laws to prevent infringements on the privacy of individuals. The failure to do so will affect the credibility of the Big Data collection process, and the public will become even more sceptical and lose faith. The lack of clarity in the purpose for collecting a large amount of data in the first place, and what happens to the collected data once the pandemic is over has become an issue for public scrutiny. Therefore, to allay any concerns and fears in the minds of the public, the onus is on the collectors, governments, and organisations to reassure the public that their personal information will remain confidential and secure from unauthorised access.

There are initiatives that the world as a whole or as individual states can take to institutionalise data protection and privacy laws. That requires consensus amongst the states and a commitment to developing a legal framework containing a set of data protection and privacy principles, purpose limitation and data minimisation, and personal data handling that governments and companies should follow. Personal data access limitation, data security, data retention, and research purposes should be the determining factors for collecting data, and the use of personal data should be conditional on public-interest purposes only. Also, personal health data should not be sold or transferred to third parties unless their involvement specifically serves the public interest. An organisation collecting new categories of personal data from individuals and use such data for new purposes should update privacy notices to reflect the new changes in the collection of data. The data handling organisations should keep under constant review existing privacy notices and ensure that they provide up to date information of data collected and, the purposes for processing. It is the sharing of covertly gathered personal data by organisations without any reference to the data subject that is the most concerning to the public and should be addressed in earnest.

The reality is the prevailing Coronavirus crisis is here to stay for some time yet, and the concerns about surveillance methods the governments and companies are putting in place will not go away either. It is important to have the right laws to cover a range of issues concerning the data collection process and handling of collected data in the long term. However, given the trends and uncertainties associated with COVID-19, it remains to be seen whether after this pandemic the world will be more tolerant than before, to the surveillance approach of governments and other organisations. However, to be prepared for any privacy concerns likely to arise in the long term, and to be response ready to face future health crises similar to that of COVID-19, it is crucially important to develop a global-level framework that will be readily available to protect individual privacy during a pandemic.

The national-level privacy mechanism should provide safeguards and guarantee the protection of privacy of its citizens. On a wider scale of a global pandemic, it is important to have an international level framework or mechanism that clearly defines time limits for the retention period of information collected during the pandemic, requirements for anonymization of data when transferring to, or sharing with a third party, or when retaining for research purpose. It is also important to include healthcare-related norms and media ethics in pandemic situations.

The researcher has highlighted the privacy and security issues related to evolving technologies and emphasised the importance of protecting personal privacy by developing a unified global level data protection mechanism.

References

Accessnow. (2020) *Recommendations on privacy and data protection in the fight against COVID-19. Accessnow.org* [Online]. Available at: https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf (Accessed: 14 May 2019)

Almeida, B. D. A. (2020). 'Personal data usage and privacy considerations in the COVID-19 global pandemic' [Online], *SciELO* volume 25, supl.1. DOI: https://doi.org/10.1590/1413-81232020256.1.11792020.

Altshuler, T. S. and Hershkowitz, R. A. (2020) *How Israel's COVID-19 mass surveillance operation works* [Online]. Available at: https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/ (Accessed: 18 June 2019)

Amnesty International. (2020). *COVID-19, surveillance, and the threat to your rights* [Online]. Available at: https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/ (28 January 2021)

BBC. (2020). *Coronavirus: 18,000 test results published by mistake*. BBC. https://www.bbc.co.uk/news/uk-wales-54146755 9Accessed: 10 December 2020)

Beltran-Aroca, C. M. et al. (2016) 'Confidentiality breaches in clinical practice: what happens in hospitals?'. *BMC Med Ethics*. 2016; 17(1): 52. DOI: 10.1186/s12910-016-0136-y (Accessed: 12 April 2020)

Bentotahewa V., Hewage C., Williams J. (2021) Security and Privacy Issues Associated with Coronavirus Diagnosis and Prognosis. In: Paiva S., Lopes S.I., Zitouni R., Gupta N., Lopes S.F., Yonezawa T. (eds) Science and Technologies for Smart Cities. SmartCity360° 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 372. Springer, Cham. https://doi.org/10.1007/978-3-030-76063-2_8 (22 January 2021)

Bentotahewa, V., Hewage, C. and Williams, J. (2020) *Do Privacy Rights Override #COVID19 Surveillance Measures?* [Online] Available at: https://www.infosecurity-magazine.com/next-gen-infosec/privacy-rights-covid19/ (Accessed: 22 February 2021)

Berry, A. C. (2018) "Online Symptom Checker Applications: Syndromic Surveillance for International Health." *Ochsner Journal* volume 18, issue 4(Winter): 298–299. DOI: 10.31486/toj.18.0068 (Accessed: 17 May 2020)

BIA News Desk. (2020) *Turkey Launches 'China-Style' Coronavirus Tracker* [Online]. Available at: https://bianet.org/english/health/222695-turkey-launches-china-style-coronavirus-tracker (14 September 2020)

Boudreaux, B., et al. (2020). *Strengthening Privacy Protections in COVID-19 Mobile Phone–Enhanced Surveillance Programs* [Online]. https://www.rand.org/pubs/research_briefs/RBA365-1.html (23 August 2020)

Business Insider South Africa. (2020) *South Africa will be tracking cellphones to fight the Covid-19 virus* [Online]. Available at:

https://www.businessinsider.co.za/south-africa-will-be-tracking-cellphones-to-fight-covid-19-2020-3 (3 May 2020)

BussinessFirst. (2020) *Scrap everything you know: company survival in the 'new normal'* [Online]. Available at https://www.businessfirstonline.co.uk/editors-choice/scrap-everything-you-know-company-survival-in-the-new-normal/ (Accessed: 4 June 2020)

Chesler, C. (2020) *Coronavirus will turn your office into a surveillance state* [Online]. Available at: https://www.wired.co.uk/article/coronavirus-work-office-surveillance (Accessed: 2 July 2020)

CIPESA staff. (2020) *Covid-19 in Africa: When is Surveillance Necessary and Proportionate? [Online].* Available at: https://cipesa.org/2020/03/covid-19-in-africa-when-is-surveillance-necessary-and-proportionate/ (23 July 2020)

Criddle, C. and Kelion, L. (2020) *Coronavirus contact-tracing: World split between two types of app* [Online]. Available at: https://www.bbc.co.uk/news/technology-52355028 (Accessed: 12 October 2020)

Department of Health and Social care. (2020) *Guidance- Testing for coronavirus: privacy information* [Online]. Available at: https://www.gov.uk/government/publications/coronavirus-covid-19-testing-privacy-information/testing-for-coronavirus-privacy-information--2 (Accessed: 15 August 2020)

DhakaTribune. (2020) *Bangladeshi developers devise a surveillance system to identify people with masks* [Online]. Available at: https://www.dhakatribune.com/bangladesh/2020/04/07/bangladeshi-developers-devise-a-surveillance-system-to-identify-people-with-masks (Accessed: 2 June 2020)

Rimpiläinen, S., Thomson, J., and Morrison, C. (2020) *Global examples of Covid 19 surveillance technologies Flash Report. Digital Health and Care Institute.* [Online]. *Available at:* https://strathprints.strath.ac.uk/72028/1/Rimpilainen_etal_DHI_2020_Global_examples_of_Covid_19_surveillance_technologies.pdf (10 September 2020)

Doffman, Z. (2020) *Coronavirus Spy Apps: Israel Joins Iran And China Tracking Citizens' Smartphones To Fight COVID-19* [Online]. Available at:

https://www.forbes.com/sites/zakdoffman/2020/03/14/coronavirus-spy-apps-israel-joins-iran-and-china-tracking-citizens-smartphones-to-fight-covid-19/?sh=711877ce781b (Accessed: 20 June 2020)

European Data Protection Board. (2020) *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. European Data Protection Board.* [Online]. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (Accessed: 3 May 2020)

European Data Protection Supervisor, (N.D) *Personal Data Breach* [Online]. Available at: https://edps.europa.eu/data-protection/our-role-supervisor/personal-data-breach_en (Accessed: 22 February 2021)

Fahim, K., Kim, M.J., and Hendrix, S. (2020) *Cellphone monitoring is spreading with the coronavirus. So is an uneasy tolerance of surveillance* [Online]. Available at: https://www.washingtonpost.com/world/cellphone-monitoring-is-spreading-with-the-coronavirus-so-is-an-uneasy-tolerance-of-surveillance/2020/05/02/56f14466-7b55-11ea-a311-adb1344719a9_story.html (17 July 2020)

Franceschi-Bicchierai, L. (N.D) *We Saw NSO's Covid-19 Software in Action, and Privacy Experts Are Worried* [Online]. Available at: https://www.vice.com/en_us/article/epg9jm/nso-covid-19-surveillance-tech-software-tracking-infected-privacy-experts-worried (Accessed: 24 September 2020)

Gan, N. (2020) *China is installing surveillance cameras outside people's front doors ... and sometimes inside their homes* [Online]. *Available at:* https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html (Accessed: 3 November 2020)

Gasser, U., et al., (2020) ‘Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid’, The Lancet journal volume 2, Issue 8(August): Available at: DOI:https://doi.org/10.1016/S2589-7500(20)30137-0 (Accessed: 23 November 2020)

General Medical Council. (N.D) *Managing and protecting personal information* [Online]. Available at: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/managing-and-protecting-personal-information (Accessed: 22 August 2020)

Gershgorn, Dave. (2020) *We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World* [Online]. Available at: https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9 (Accessed: 2 June 2020)

GLOPID-R. (2017) 'Principles for Data Sharing in Public Health Emergencies', *Wellcome Trust Journal contribution*. Available at: https://doi.org/10.6084/m9.figshare.4733590.v2 (Accessed: 23 May 2020)

Goethem, N. V. et al., (2020) Rapid establishment of a national surveillance of COVID-19 hospitalizations in Belgium. *Arch Public Health* 78, 121 (2020). Available at: DOI: https://doi.org/10.1186/s13690-020-00505-z (Accessed: 13 October 2020)

Guerrini, F. (2020) *Contact tracing: Italy's open-source app finally lands, taking the Google-Apple model* [Online]. https://www.zdnet.com/article/contact-tracing-italys-open-source-app-finally-lands-taking-the-google-apple-model/ (3 February 2021)

Gussarova, A. (2020) *Kazakhstan uses electronic surveillance to enforce quarantine. Eurasia Daily Monitor* [Online]. Available at: https://privacyinternational.org/examples/3661/kazakhstan-uses-electronic-surveillance-enforce-quarantine (Accessed: 23 January 2021)

Handler, S., and Liu. L. (2020) *Fighting COVID-19 with surveillance: Perspectives from across the globe* [Online]. https://www.atlanticcouncil.org/blogs/new-atlanticist/fighting-covid-19-with-surveillance-perspectives-from-across-the-globe/ (Accessed: 13 September 2020)

Hassounah, Marwah., Raheel, H. and Alhefzi. M (2020) 'Digital Response During the COVID-19 Pandemic in Saudi Arabia'. *Journal of Medical Internet Research*. 22(9). DOI: 10.2196/19338.

Howell, C. T., and Talbert. C. (2020) *Privacy Risks and Implications of Contact Tracing Apps and Related Technologies* [Online]. https://www.natlawreview.com/article/privacy-risks-and-implications-contact-tracing-apps-and-related-technologies (Accessed: 17 August 2020)

Hussein, M. R. et al. (2020) ‘Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations’, *2nd International Conference on Advanced Information and Communication Technology.* 30 June 2020. Cornell University. DOI: arXiv:2007.13182. (14 July 2020)

Hussein, R.M. el al. 2020. ‘Trust Concerns in Health Apps collecting Personally Identifiable Information during COVID-19-like Zoonosis’, *23rd International Conference on Computer and Information Technology*. Cornell University. DOI: arXiv:2009.07403v1. (16 November 2020)

ICO. (N.D) *Maintaining records of staff, customers, and visitors for contact tracing purposes* [Online]. Available at: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/maintaining-records-of-staff-customers-and-visitors-for-contact-tracing-purposes/#consent. (Accessed: 14 May 2020)

ICO.(N.D) *Principle (c): Data minimisation*. [Online]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ (3 June 2020)

ICO. (N.D) *What is personal data?*. [Online]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/#:~:text=The%20GDPR%20only%20applies%20to,not%20subject%20to%20the%20GDPR. (Accessed: 23 May 2020)

ICO. (N.D) *Right to be informed*. [Online]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/ (Accessed: 14 July 2020)

ICO. (N.D) *Principle (e): Storage limitation*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ (Accessed: 5 July 2020)

Jalabneh, R. et al. (2020) ‘Use of Mobile Phone Apps for Contact Tracing to Control the COVID-19 Pandemic: A Literature Review’, *SSRN*. DOI: http://dx.doi.org/10.2139/ssrn.3641961 (Accessed: 15 December 2020)

Juarez, E. (2020) *Sandoval on Guatemalan Alert: "Whoever wants to download it can do so* [Online]. Available at: https://lahora.gt/sandoval-sobre-alerta-guate-quien-la-quiera-descargar-lo-puede-hacer/ (Accessed: 14 July 2020)

Kharpal, A. (2020) *Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends* [Online]. Available at: https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html (Accessed: 14 13 January 2021)

Kuskonmaz, Elif Mendos, and Elspeth Guild. 2020. 'Covid-19: A New Struggle over Privacy, Data Protection and Human Rights?.' *European Law Blog*, Available at: https://europeanlawblog.eu/2020/05/04/covid-19-a-new-struggle-over-privacy-data-protection-and-human-rights/ (Accessed: 27 June 2020)

Lapowsky, I. (2020) *Facebook data can help measure social distancing in California* [Online]. Available at: https://www.protocol.com/facebook-data-help-california-coronavirus (Accessed: 23 July 2021)

Larsen, L. (2020) *Impact of the 9/11 attack on US Citizens' Privacy* [Online]. Available at: https://storymaps.arcgis.com/stories/1882937c0c1742ae90d96f69def2e5e8 (Accessed: 17 July 2019)

Leung, Gabriel M. et al. 2004. "The Epidemiology of Severe Acute Respiratory Syndrome in the 2003 Hong Kong Epidemic: An Analysis of All 1755 Patients." *Annals of Internal Medicine* volume 141, Issue 9(November): DOI: https://doi.org/10.7326/0003-4819-141-9-200411020-00006.

Limam, A. (2020). *Should I worry about mass surveillance due to COVID-19? [Online]. Available at:* https://newseu.cgtn.com/news/2020-07-03/Should-I-worry-about-mass-surveillance-due-to-COVID-19--RNQLZgoHWE/index.html (Accessed: 19 August 2020)

Matthan, R. (2020) 'The Privacy Implications of Using Data Technologies in a Pandemic', *Journal of the Indian Institute of Science* 611–621: Available at: https://doi.org/10.1007/s41745-020-00198-x (Accesses: 14 February 2021)

Ministry of Defence, Strategic Command, and jHub Defence Innovation. (2020). *jHub support NHSX to securely share COVID-19 symptom data* [Online]. Available at: https://www.gov.uk/government/news/jhub-support-nhsx-to-securely-share-covid-19-symptom-data (Accessed: 21 January 2021)

Narayanan, A. and Shmatikov. V. (2019) *Robust de-anonymization of large sparse datasets: a decade later* [Online]. Available at: https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf (Accessed: 13 October 2020)

NHSX. (2020) *Project OASIS*. [Online]. Available at: https://www.nhsx.nhs.uk/covid-19-response/data-and-covid-19/project-oasis/ (Accessed: 23 October 2020)

Nicolas, E. S. (2020). *Coronavirus: Are we trading privacy for security?*. [Online]. Available at: https://euobserver.com/coronavirus/148041 (Accessed: 7 July 2020)

OECD. (2020) *Ensuring data privacy as we battle COVID-19* [Online]. Available at: http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/ (17 September 2020)

OECD. (2020) *Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics* [Online]. Available at: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/ (10 June 2020)

Ombat, C. (2020). *State taps phones of isolated cases* [Online]. Available at: https://www.standardmedia.co.ke/nairobi/article/2001365401/state-taps-phones-of-isolated-cases (17 August 2020)

Otieno, B. (2020) *App uses passenger data to trace virus path* [Online]. Available at: https://www.standardmedia.co.ke/health/article/2001365263/app-uses-passenger-data-to-trace-virus-path (3 June 2020)

Pisa, M. (2020) *COVID-19, Information Problems, and Digital Surveillance* [Online]. Available at: https://www.cgdev.org/blog/covid-19-information-problems-and-digital-surveillance (Accessed: 13 May 2020)

Practical Law Data Privacy Advisor. (2020) *COVID-19: Workplace Temperature Monitoring Privacy Guidance Chart (Global)* [Online]. Available at: https://uk.practicallaw.thomsonreuters.com/w-025-

4732?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true (Accessed: 18 June 2020)

Presidenza del Consiglio dei Ministri. (2020) *Immune* [Online] Available at: https://www.immuni.italia.it/ (Accessed: 17 July 2020)

Quick, J. et al. 2016. 'Real-time, portable genome sequencing for Ebola surveillance', *Europe PubMed Central- Nature* volume 530(7589)(February): 228–232. DOI: 10.1038/nature16996 (Accessed: 22 April 2020)

Reuters Staff. (2020) *Italy launches COVID-19 contact-tracing app amid privacy concerns* [Online]. Available at: https://www.reuters.com/article/us-health-coronavirus-italy-app-idUSKBN2383EW (7 July 2020)

Saiidi, U. (2020). *Hong Kong is putting electronic wristbands on arriving passengers to enforce coronavirus quarantine* [Online]. Available at: https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html (28 June 2020)

Scheer, S., and Cohen. T. 2020. *Parliament grants Israeli government three more weeks of mobile phone surveillance* [Online]. Available at: https://privacyinternational.org/examples/3833/parliament-grants-israeli-government-three-more-weeks-mobile-phone-surveillance (22 July 2020)

Seifert, R. (2020) *Blockchain can answer immunity passport security concerns, but any roll-out must be dictated by the science* [Online]. Available at: https://www.itproportal.com/features/blockchain-can-answer-immunity-passport-security-concerns-but-any-roll-out-must-be-dictated-by-the-science/ (Accessed: 13 June 2020)

Servick, K. (2020). *Cellphone tracking could help stem the spread of coronavirus. Is privacy the price?* [Online]. Available at: https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price 13 August 2020)

Sharma, T., and Bashir. M. (2020) "Use of apps in the COVID-19 response and the loss of privacy protection." *Nature Medicine* volume 26. Available at: DOI: https://doi.org/10.1038/s41591-020-0928-y (Accessed: 19 September 2020)

Tognotti, E. (2013) 'Lessons from the History of Quarantine, from Plague to Influenza A', *Emerging Infectious Diseases* volume 19, Issue 2 (February), Available at: DOI: 10.3201/eid1902.120312

Tonantzin, P. (2020). *Jojutla uses drones to avoid concentrations in parks and squares* [Online]. Available at: https://www.excelsior.com.mx/nacional/jojutla-usa-drones-para-evitar-concentraciones-en-parques-y-plazas/1371886 (Accessed: 16 August 2020)

Tuttle, B. and McKenzie, J. (2020) *Global Regulatory Guidance for COVID-19 Privacy and Security Issues* [Online]. Available at https://www.jdsupra.com/legalnews/global-regulatory-guidance-for-covid-19-43117/, (Accessed: 25 May 2020)

UNDP. (N.D) *COVID-19 pandemic: Humanity needs leadership and solidarity to defeat the coronavirus* [Online]. Available at: https://www.undp.org/content/undp/en/home/coronavirus.html (Accessed: 12 June 2020)

US. Department of Health & Human Service. (N.D) *HIPAA for Individuals*. [Online]. Available at: https://www.hhs.gov/hipaa/for-individuals/index.html (Accessed: 20 July 2020)

Vou, A. (2020) *COVID-19 has served as the pretext for widespread surveillance* [Online]. Available at: https://www.europeandatajournalism.eu/eng/News/Data-news/COVID-19-has-served-as-the-pretext-for-widespread-surveillance (Accessed: 13 June 2020)

Wesolowski, A. et al. (2014). 'Commentary: Containing the Ebola Outbreak - the Potential and Challenge of Mobile Network Data', *PLoS Currents* version 1, Issue 6(September). Available at: DOI: 10.1371/currents.outbreaks.0177e7fcf52217b8b634376e2f3efc5e (17 May 2020)

Whitehead, M. (2020) *Surveillance Capitalism in the Time of Covid-19*. United Kingdom: Independent [Online]. Available at: https://www.isrf.org/2020/05/11/surveillance-capitalism-in-the-time-of-covid-19-the-possible-costs-of-technological-liberation-from-lockdown/ (Accessed: 23 20 May 2020)

WHO. (2020) *Contact tracing in the context of COVID-19- Interim guidance* [Online]. Available at: file:///C:/Users/sm77809/Downloads/WHO-2019-nCoV-Contact_Tracing-2020.1-eng.pdf (Accessed: 14 May 2020)

WHO. 2020. *Surveillance strategies for COVID-19 human infection-Interim guidance* [Online]. Available at: file:///C:/Users/sm77809/Downloads/WHO-2019-nCoV-National_Surveillance-2020.1-eng.pdf (28 May 2020)

Zang, H. and Bolot. J. (2011) *Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study* [Online]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.651.44&rep=rep1&type=pdf (25 May 2020)

Zhang, H. (2020). *With coronavirus containment efforts, what are the privacy rights of patients?* [Online]. Available at: https://theconversation.com/with-coronavirus-containment-efforts-what-are-the-privacy-rights-of-patients-131752 (23 April 2020)

Zhong, R. (2020) *China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears* [Online]. Available at: https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html%20Writer:%20Raymond%20Zhong (Accessed: 14 July 2020)

ANNEXURE D

Sri Lanka: Male

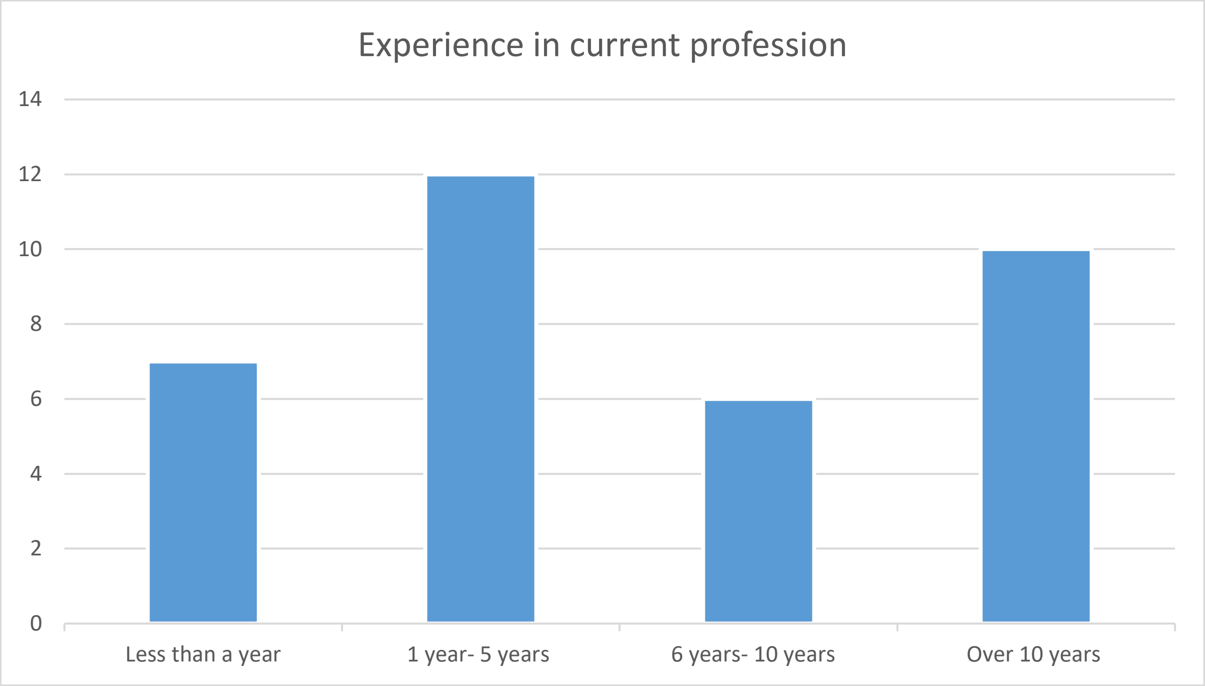


Figure D.1: Experience in current profession (Male)

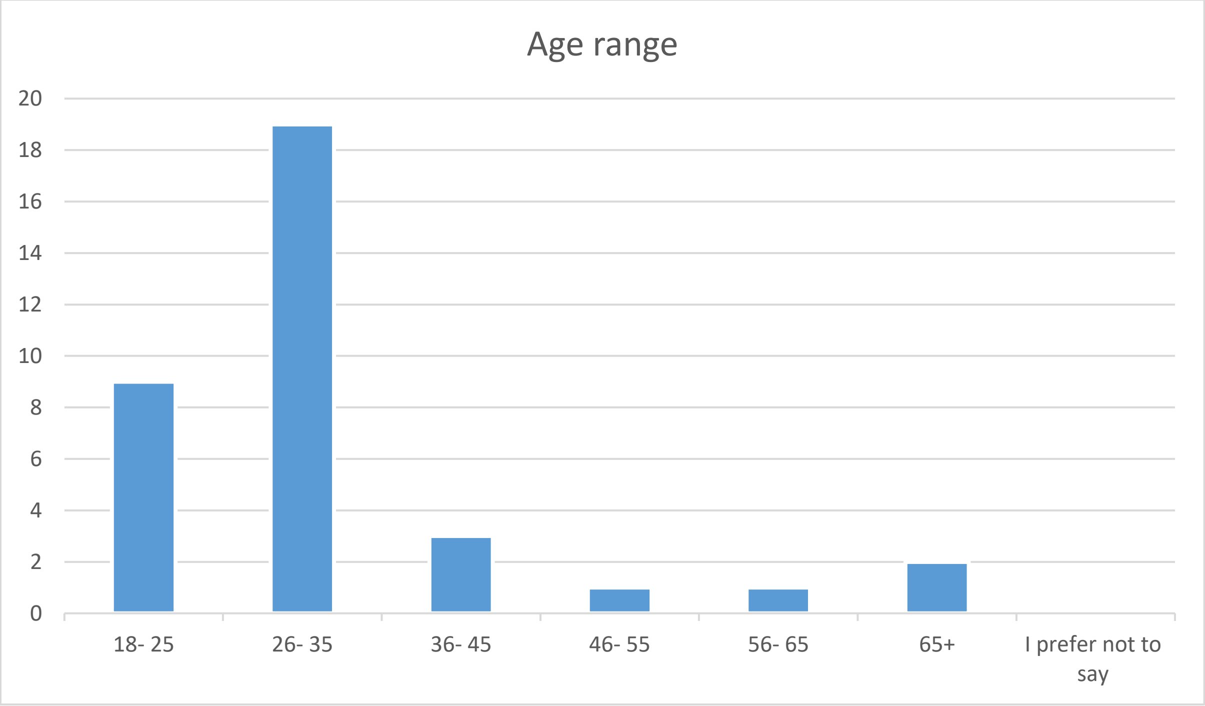


Figure D.2: Age range (Male)

This analysis is based on the responses received from 35 Sri Lankan male participants, aged between 18-65 plus, and 54 percent of them in the 26-35 age range (See figure D.2). They have been working industry for less than a year to over 10 years durations (See figure D.1).

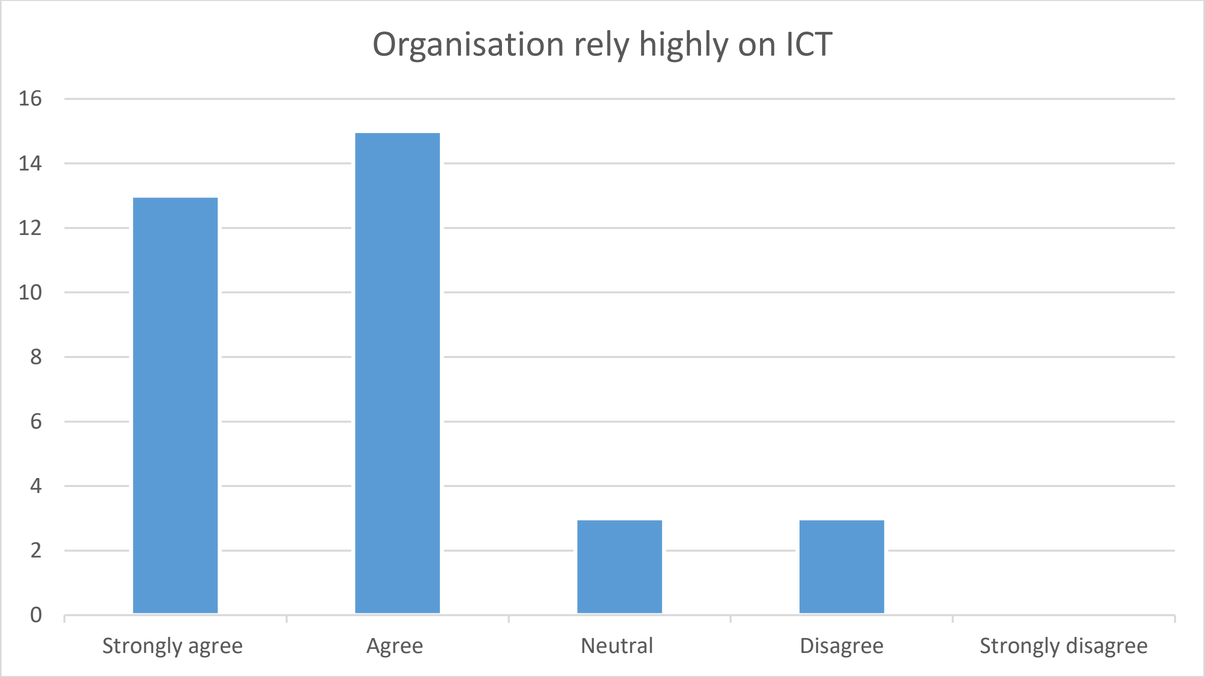


Figure D.3: Organisation rely highly on ICT (Male)

Of the 35 respondents, 28 have worked in a technology reliance working environment; 3 not aware because of the nature of the work assigned to them; 3 'disagreed' on ICT (See figure D.3). This makes it clear that the majority of males employed in the organisation have high reliance on ICT.

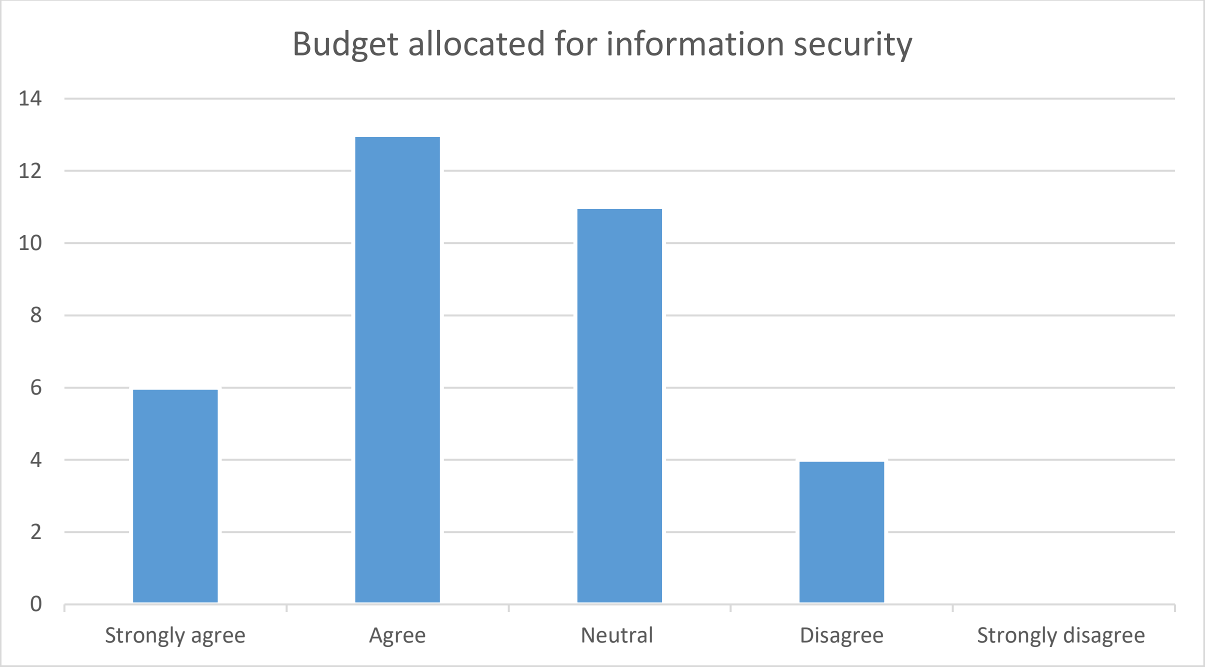


Figure D.4: Budget allocated for information security (Male)

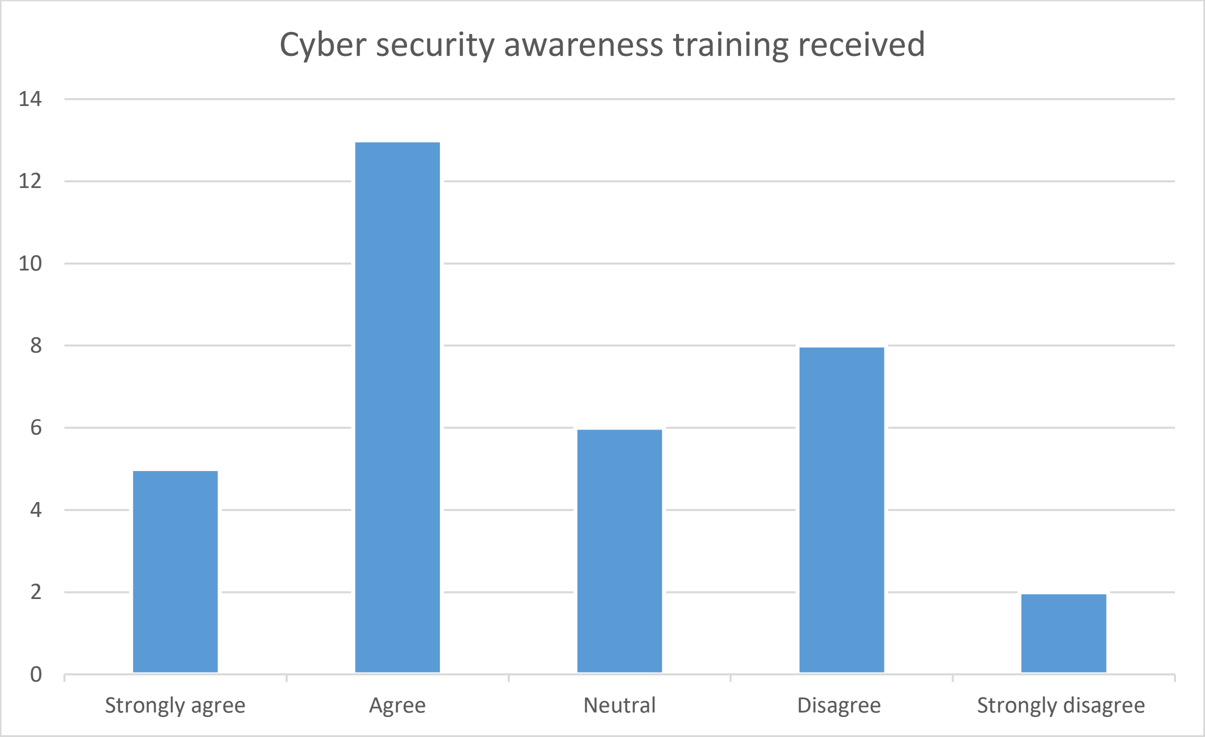


Figure D.5: Cyber security awareness training received (Male)

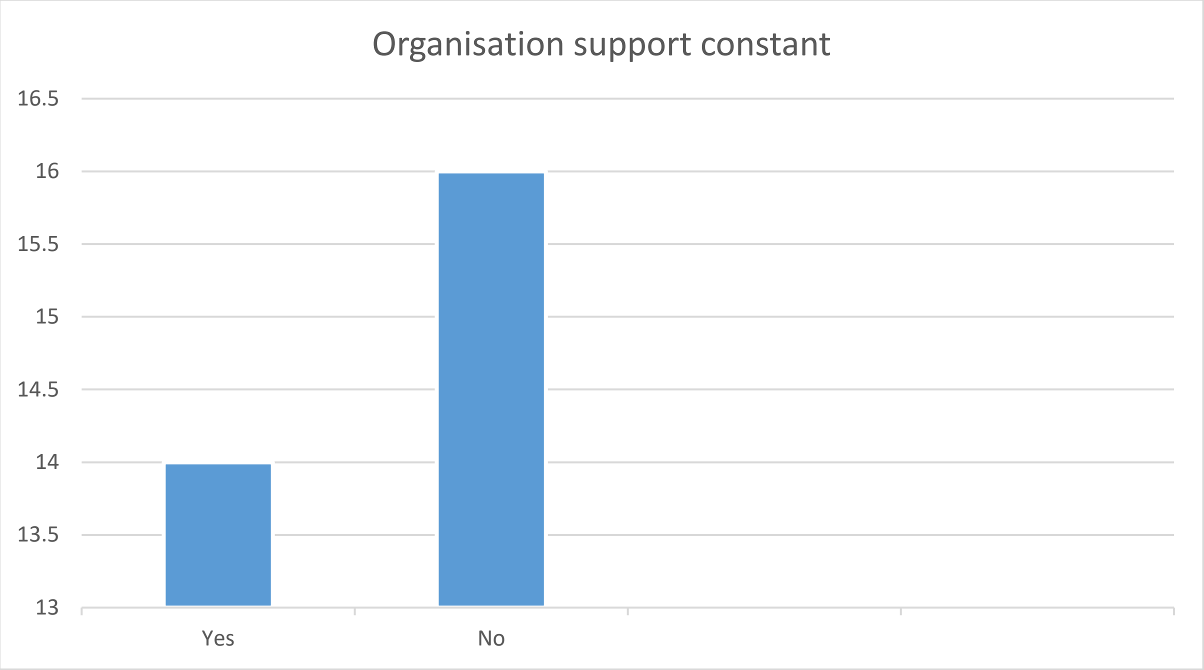


Figure D.6: Organisation support constant (Male)

19 out of the 35 shows that their organisations had a budget allocation for information security; 11 did not express an opinion either way; according to the 4 who disagreed, their organisations had no budget allocation for information security (See figure D.4). According to some of the participants, their organisations have a separate budget, and they received security awareness training regularly. 18 participants received regular cybersecurity awareness training, and 6 neither did nor did not; 10 participants did not receive security awareness training (See figure D.5). Only 14 received support from the organisation to protect personal information, and 16 did not (See figure D.6). This indicates lack of organisational support to protect personal information despite the budget allocated for information security and high reliance on technology.

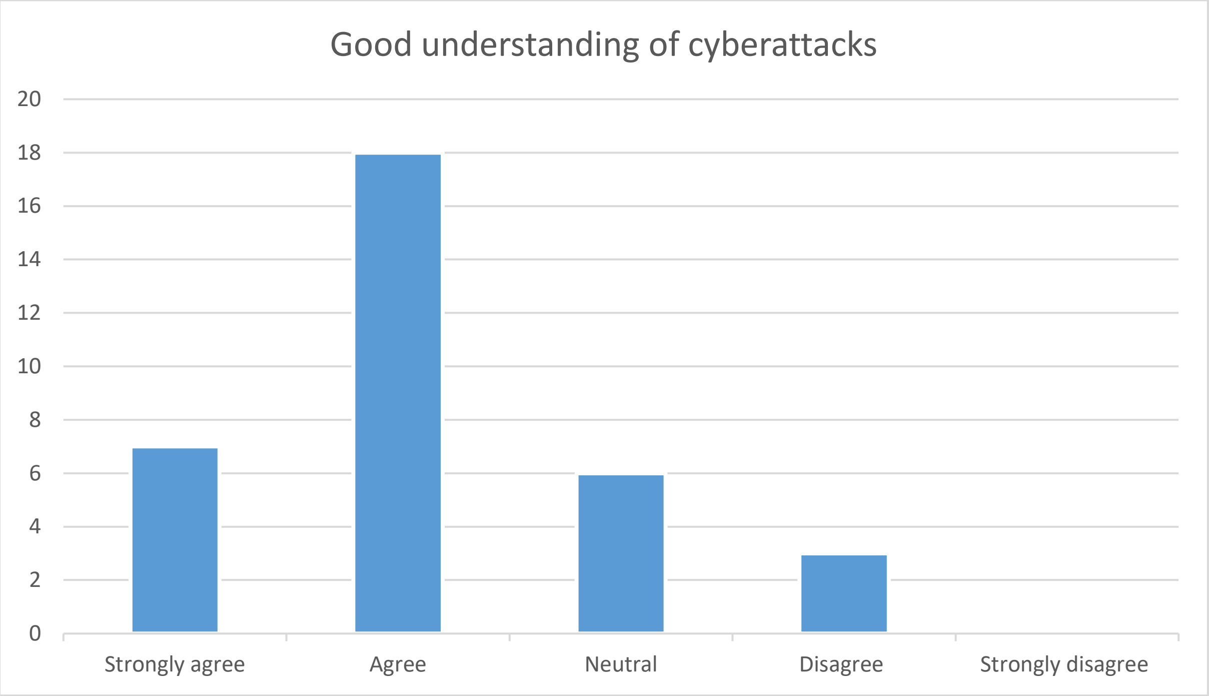


Figure D.7: Good understanding of cyberattacks (Male)

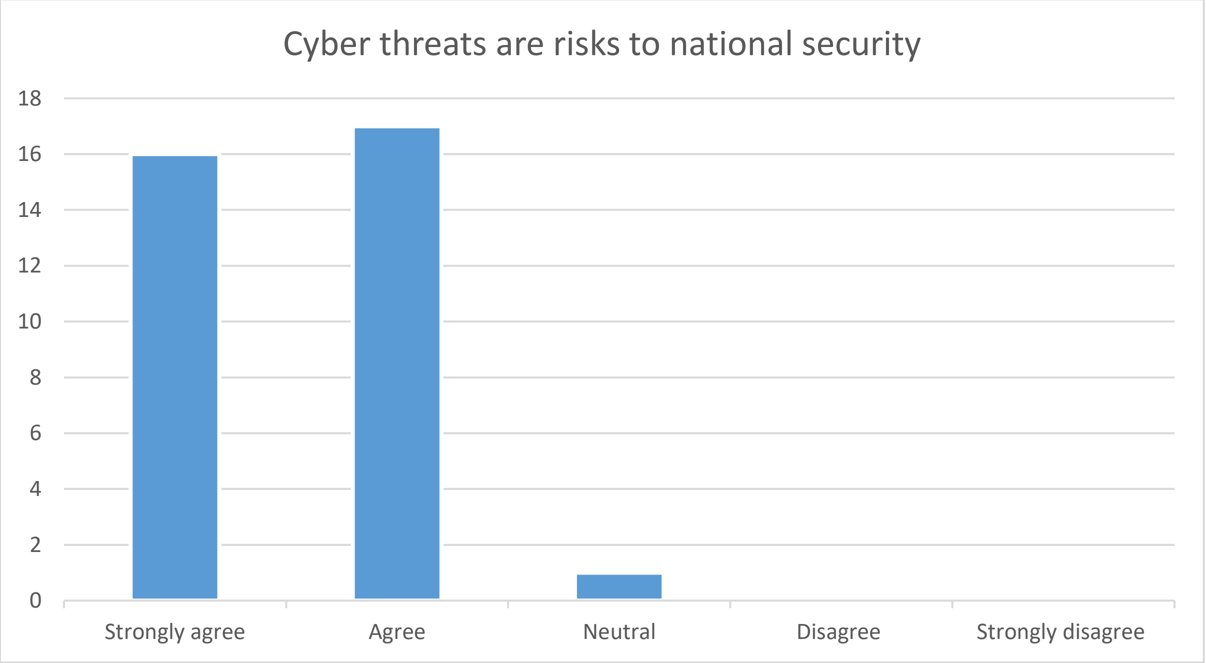


Figure D.8: Cyber threats are risks to national security (Male)

25 participants have a high understanding of the impact of cyberattacks on the public and the organisation, despite the satisfactory level of security awareness training they received; 6 did not specify either way; 3 did not have an understanding (See figure D.7). Furthermore, 94 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure D.8). In general, understanding cyber threats and their impact on national security make people act responsibly to minimise end-user errors, and in time, they would play an influencing role in accepting and implementing a national, regional, and global level mechanism.

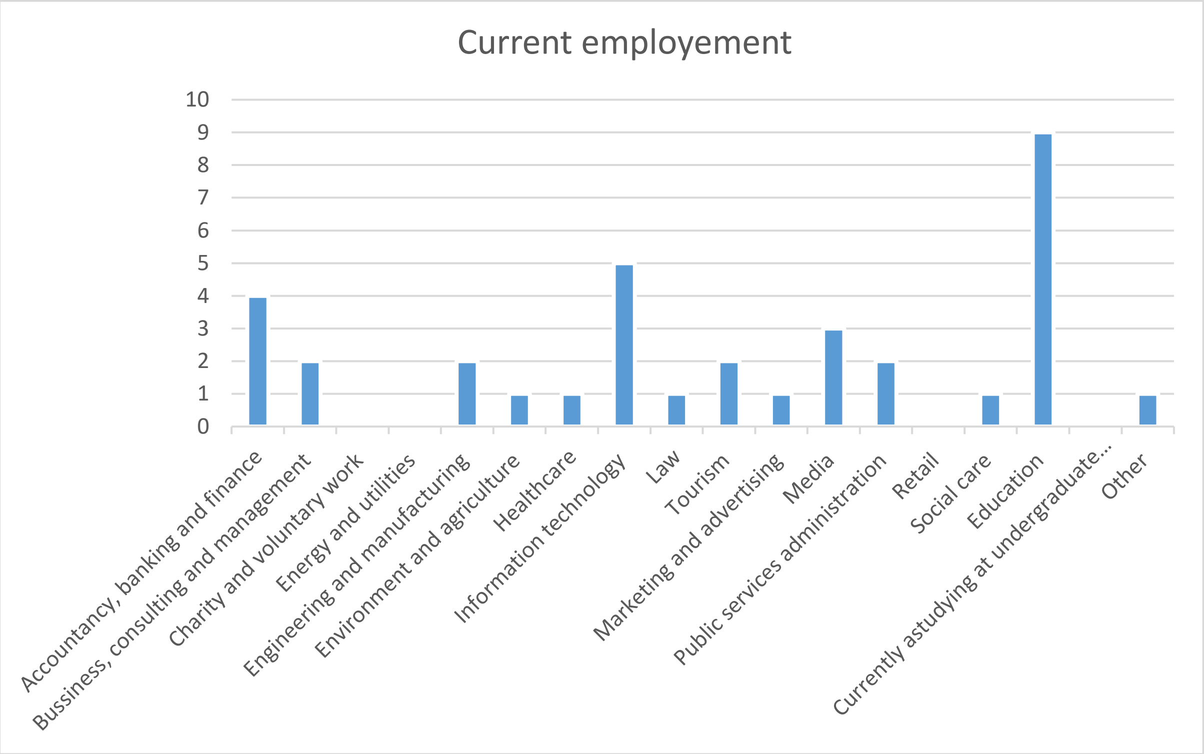


Figure D.9: Current employment (Male)

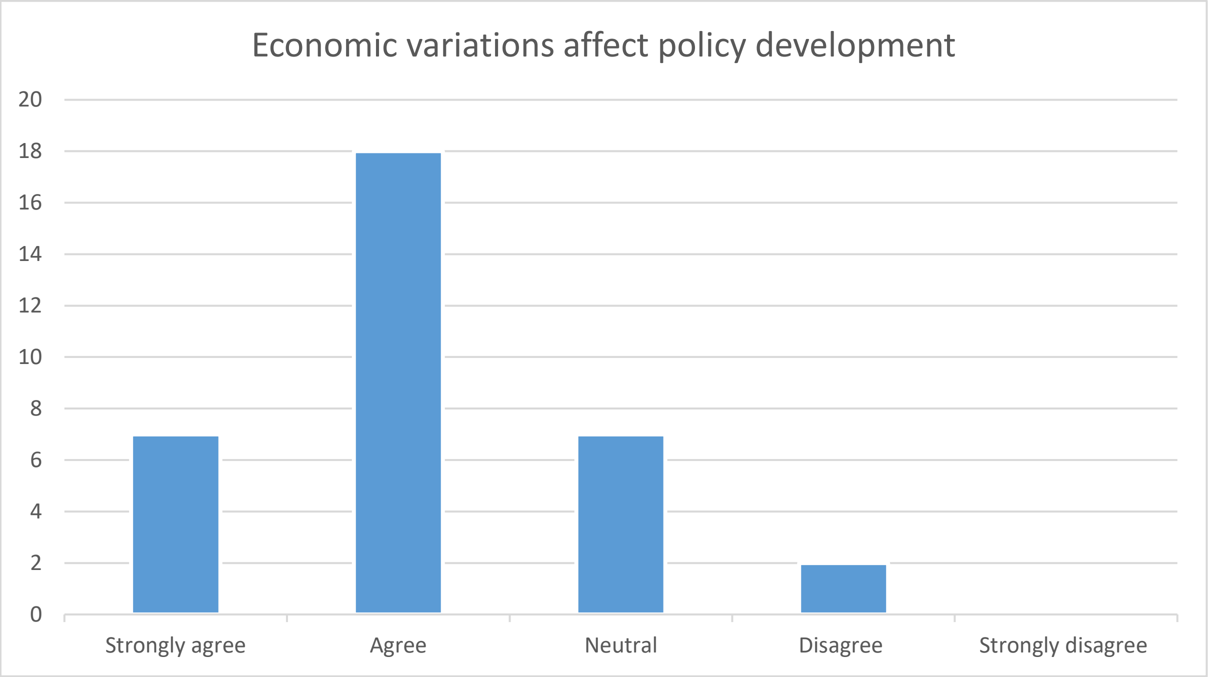


Figure D.10: Economic variations affect policy development (Male)

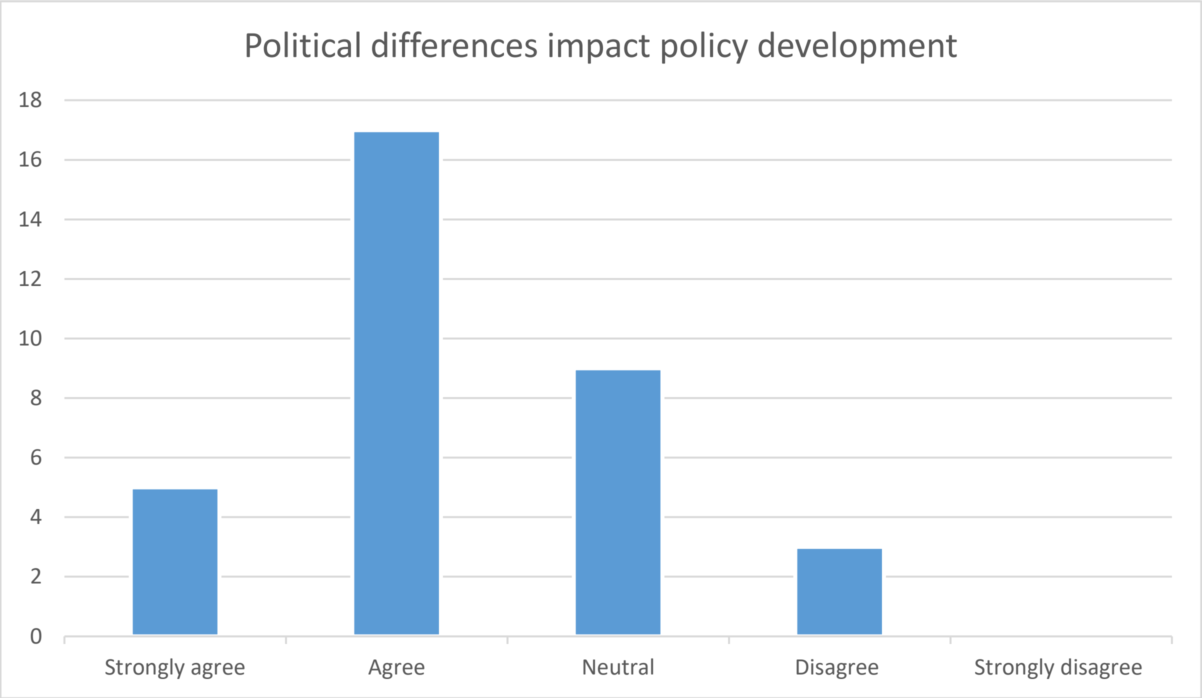


Figure D.11: Political differences impact policy development (Male)

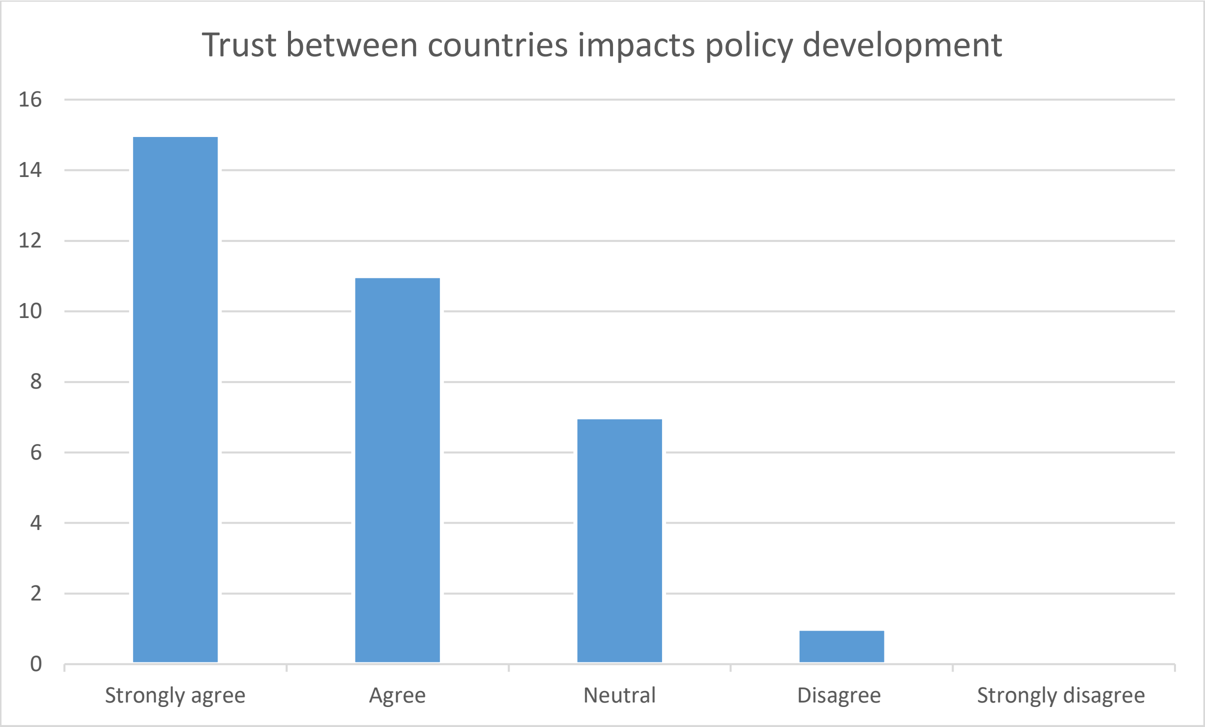


Figure D.12: Trust between countries impact policy development (Male)

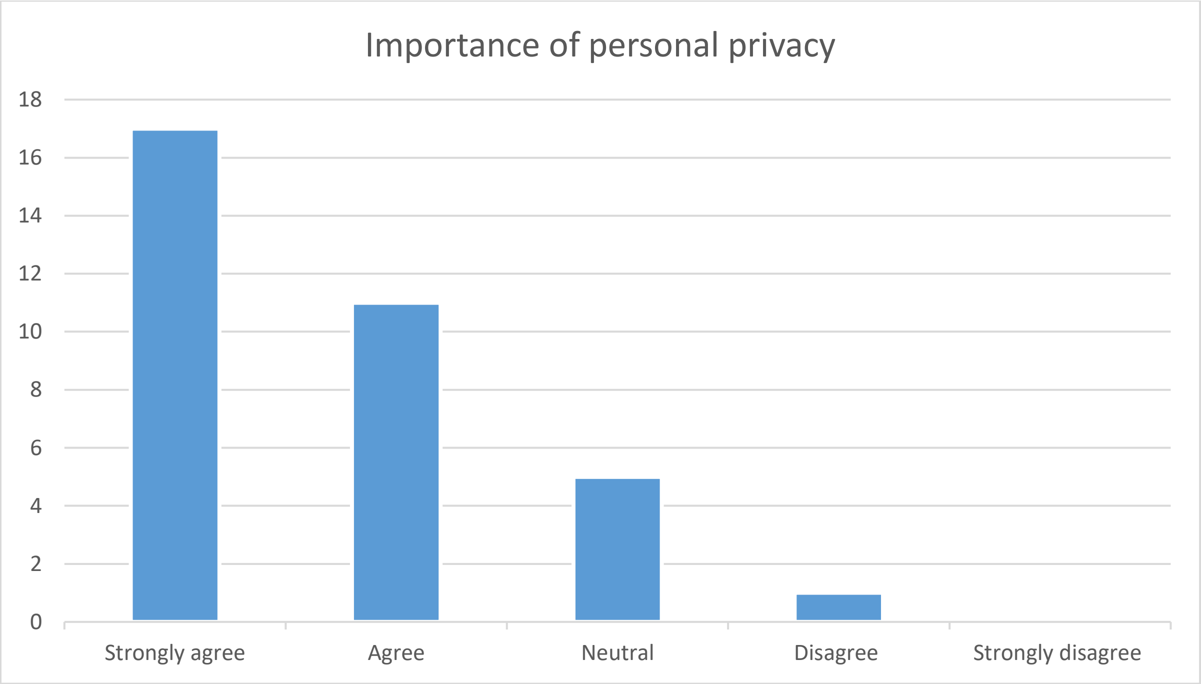


Figure D.13: Importance of personal privacy (Male)

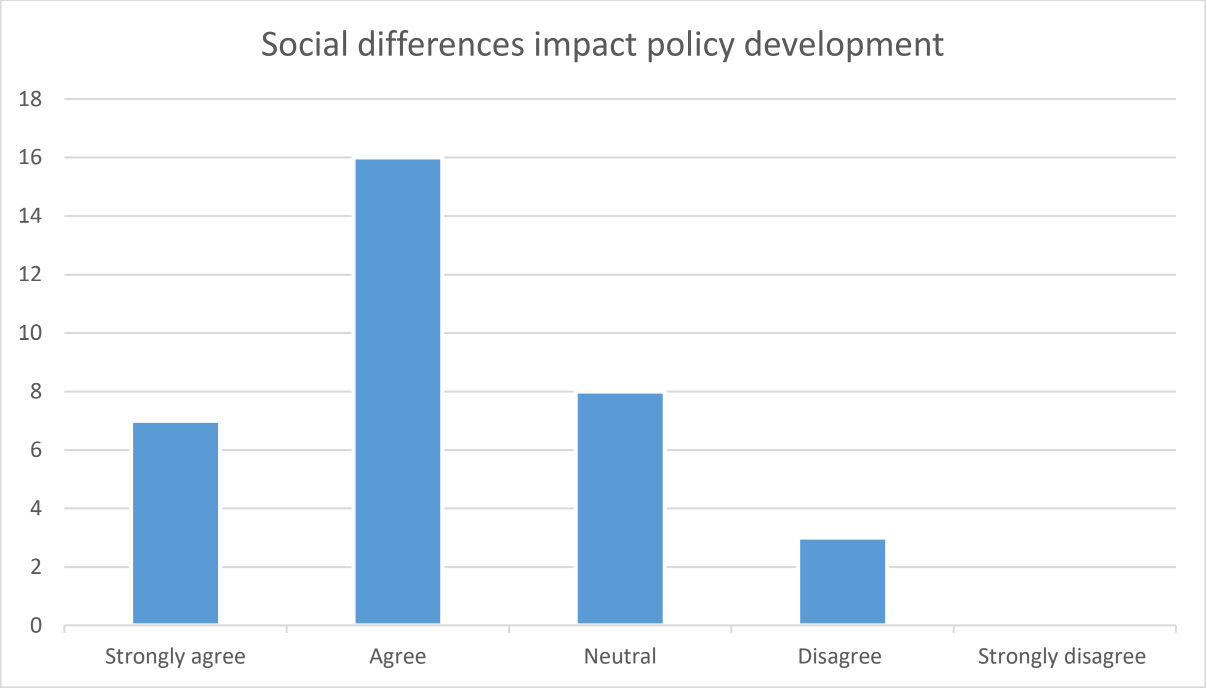


Figure D.14: Social differences impact policy development (Male)

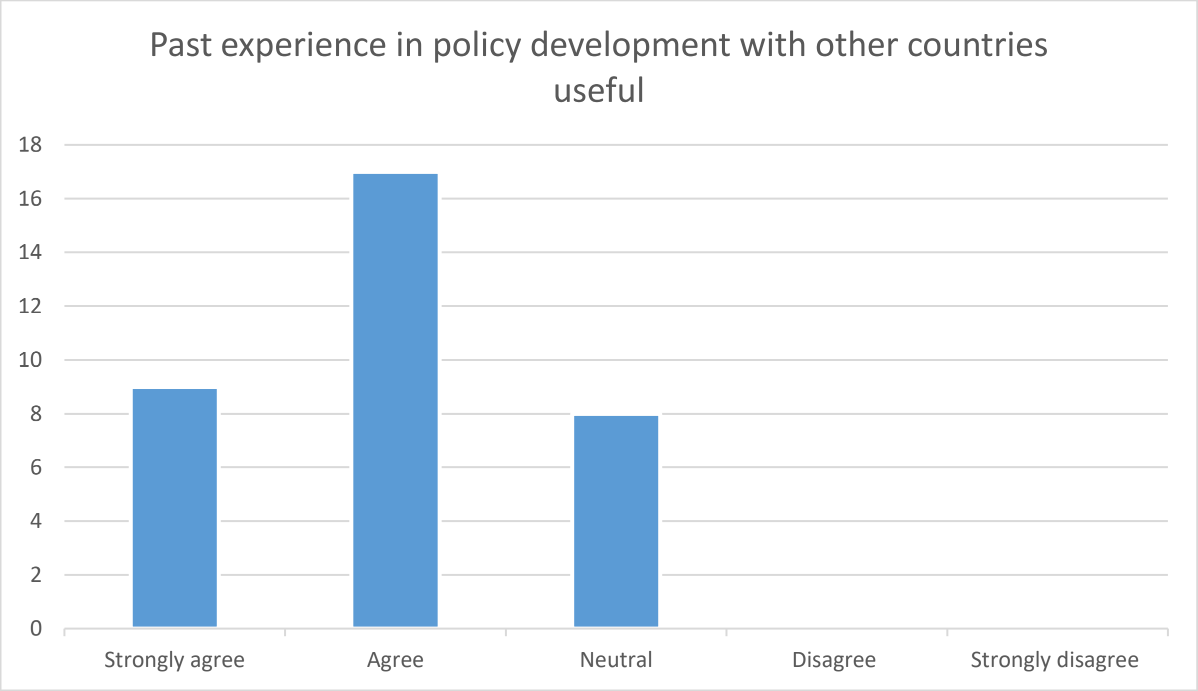


Figure D.15: Past experience in policy development with other countries useful (Male)

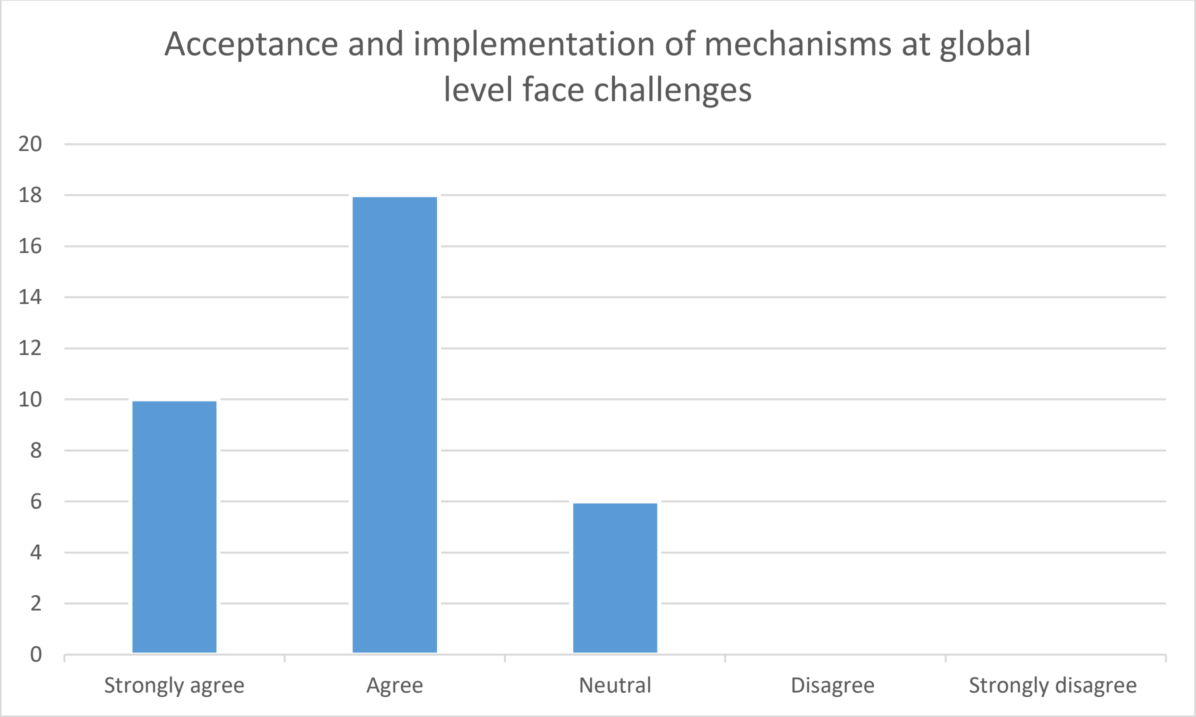


Figure D.16: Acceptance and implementation of mechanisms at global level face challenges (Male)

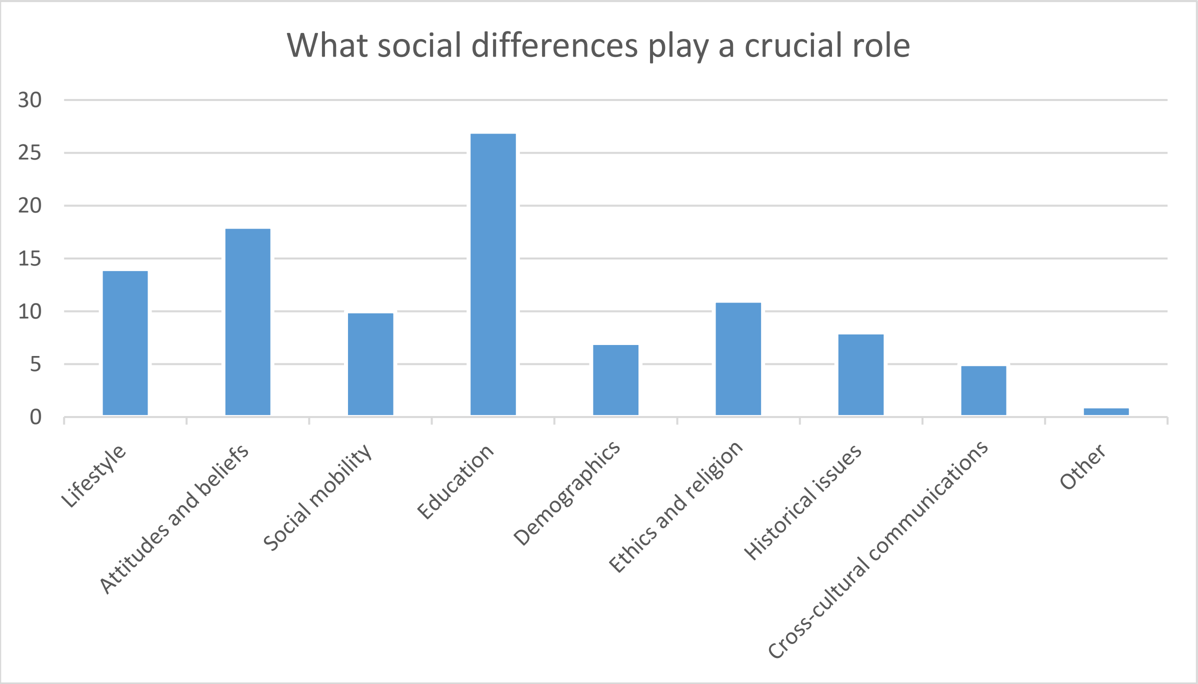


Figure D.17: What social differences play a crucial role (Male)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure D.17). There is consensus on knowledge and awareness of potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to deliver cybersecurity awareness training at the school and organisational level. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

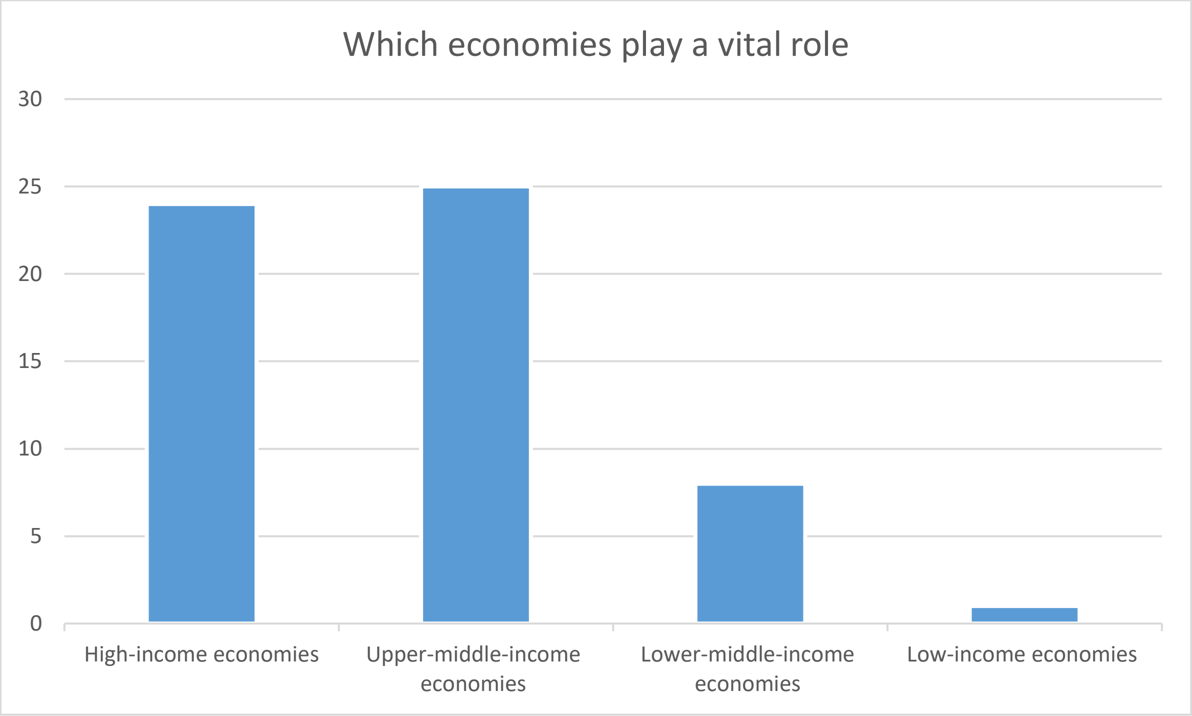


Figure D.18: Which economies play a vital role (Male)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure D.18). The key stages in the policymaking process aim to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the resources necessary, implement, and finally evaluate the policy. These stages are time-consuming and require sufficient funding and resources. Therefore, achieving success to a large extent depends on the economic stability of the country, which counts as a crucial factor in policymaking.

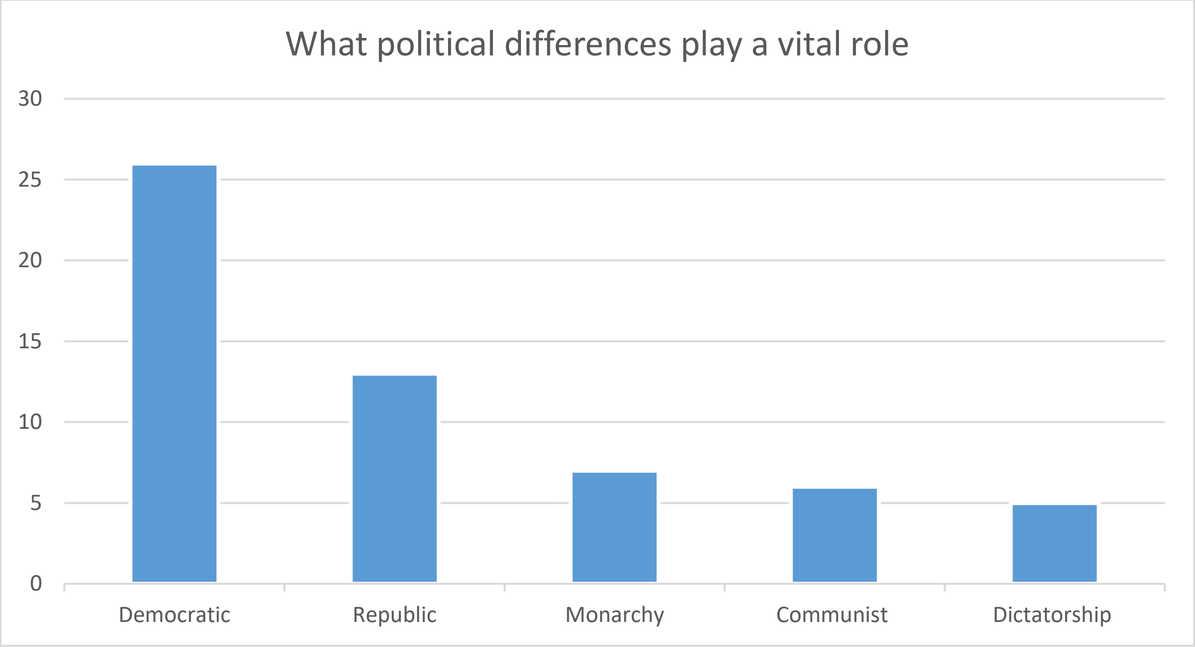


Figure D.19: What political differences play a vital role (Male)

The majority has have chosen democratic political system (See figure D.19), in preference to others because it allows the public an influential voice in policy development and encourages consensus and collective responsibility for their actions. These contribute to developing public trust between them and the organisations and ensure coherence and transparency in the policy development process.

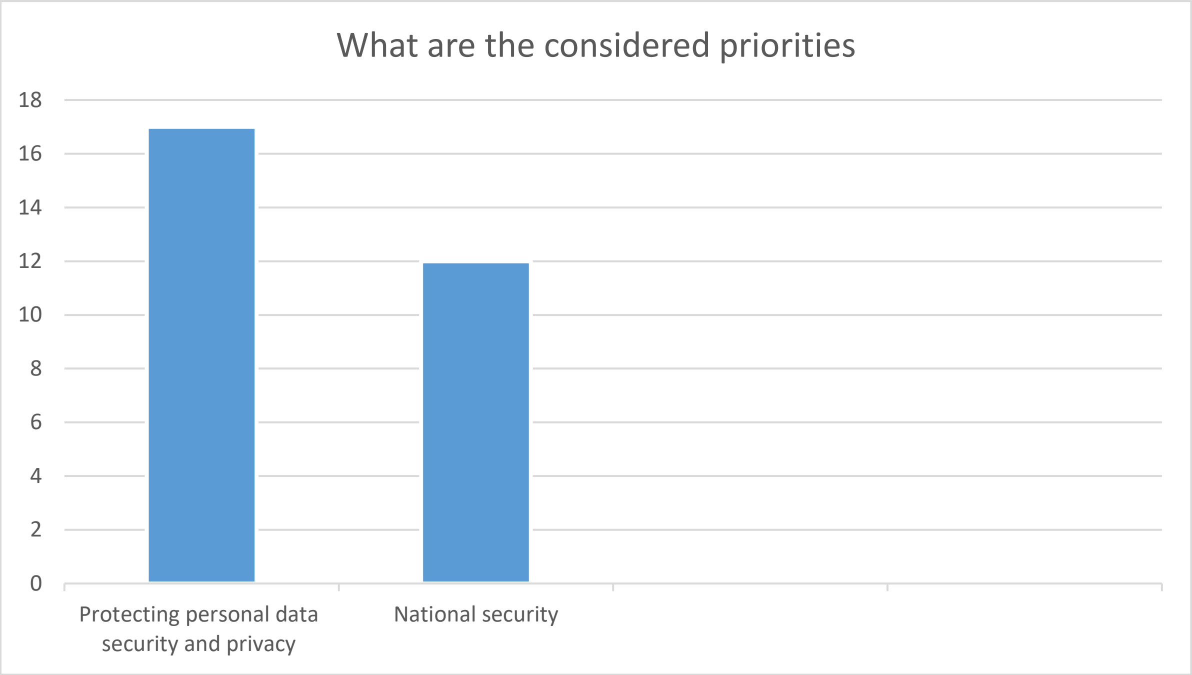


Figure D.20: What are the considered priorities (Male)

The majority mentions neither the importance of protection of personal data security and privacy nor protection of national security in accepting and implementing global data privacy and security policies (See figure D.20). This is a distinct change of opinion. The implications of a personal data breach incident will have a knock-on effect on personal data security and privacy, and national security, and it will also be felt right across the groups as well as the community alike.

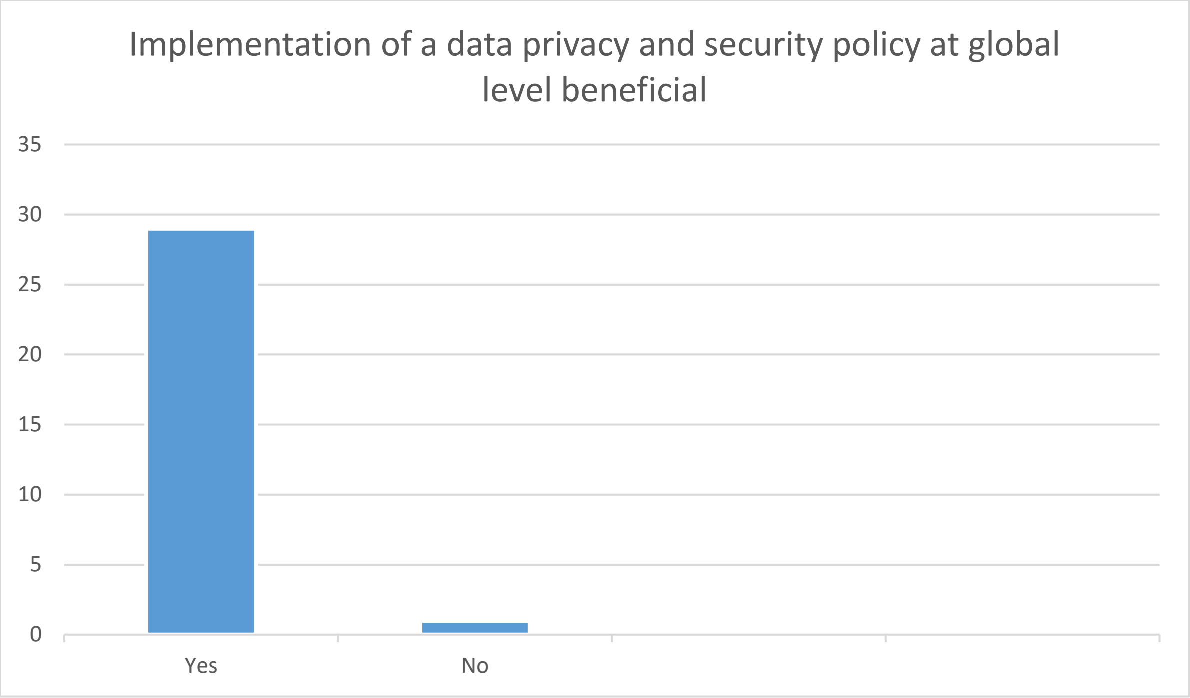


Figure D.21: Implementation of a data privacy and security policy at global level beneficial (Male)

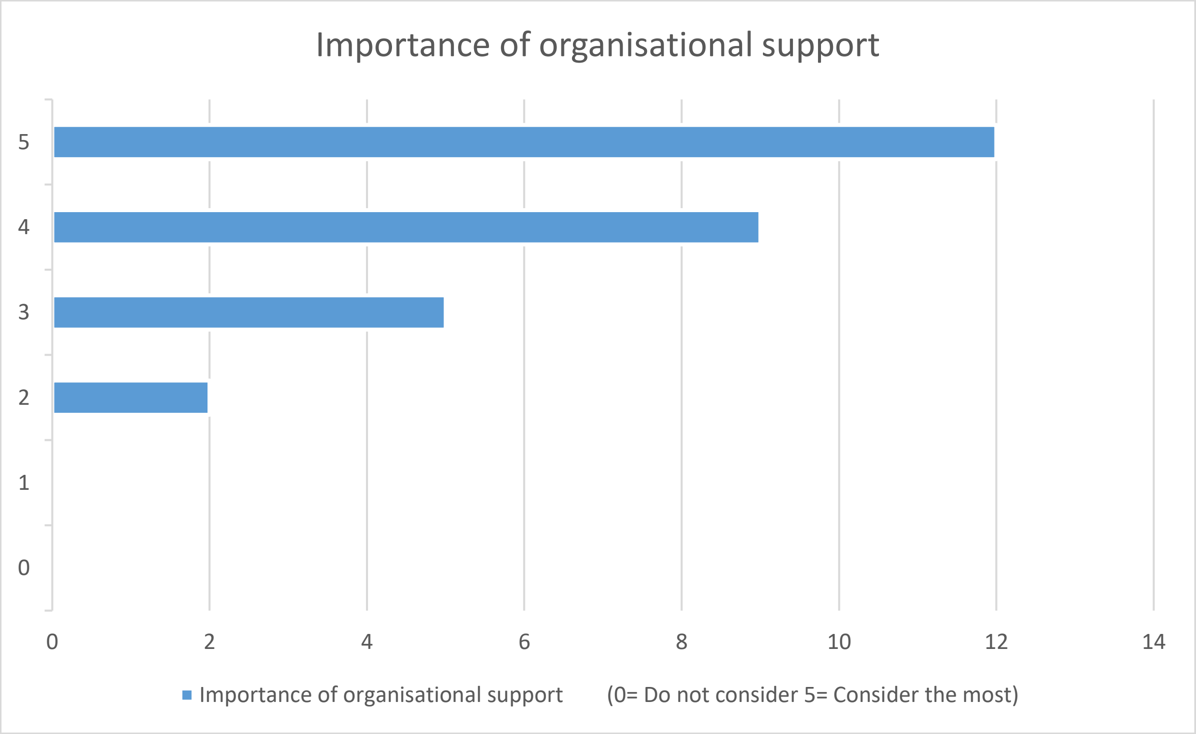


Figure D.22: Importance of organisational support (Male)

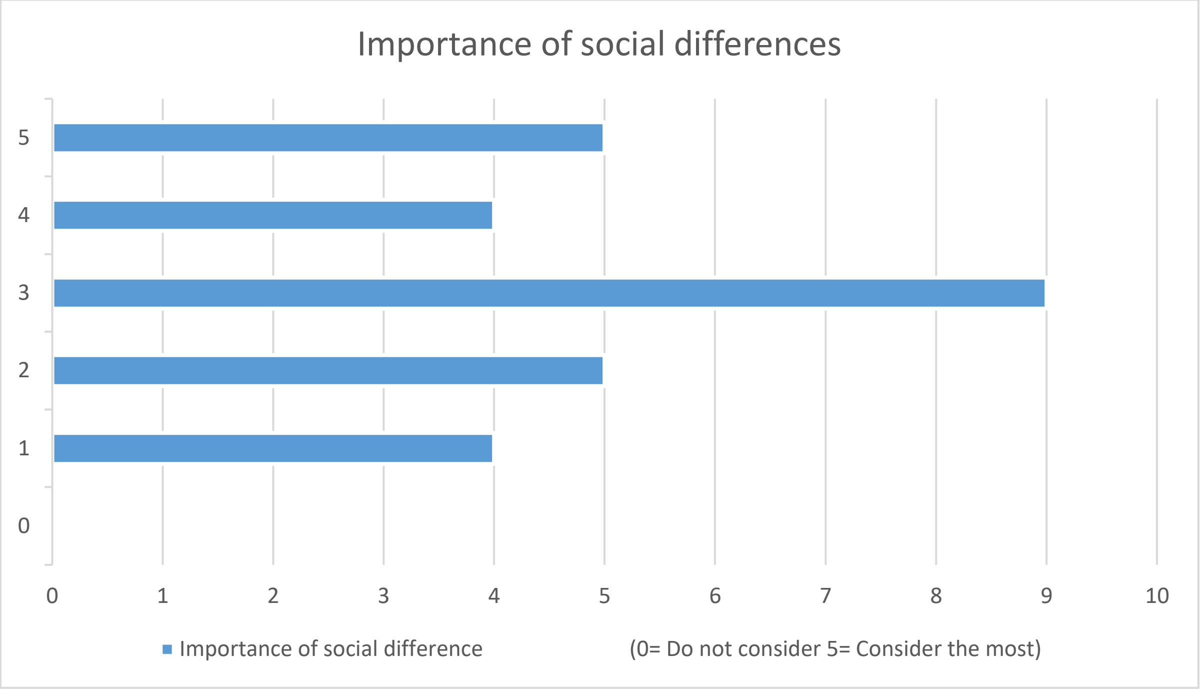


Figure D.23: Importance of social differences (Male)

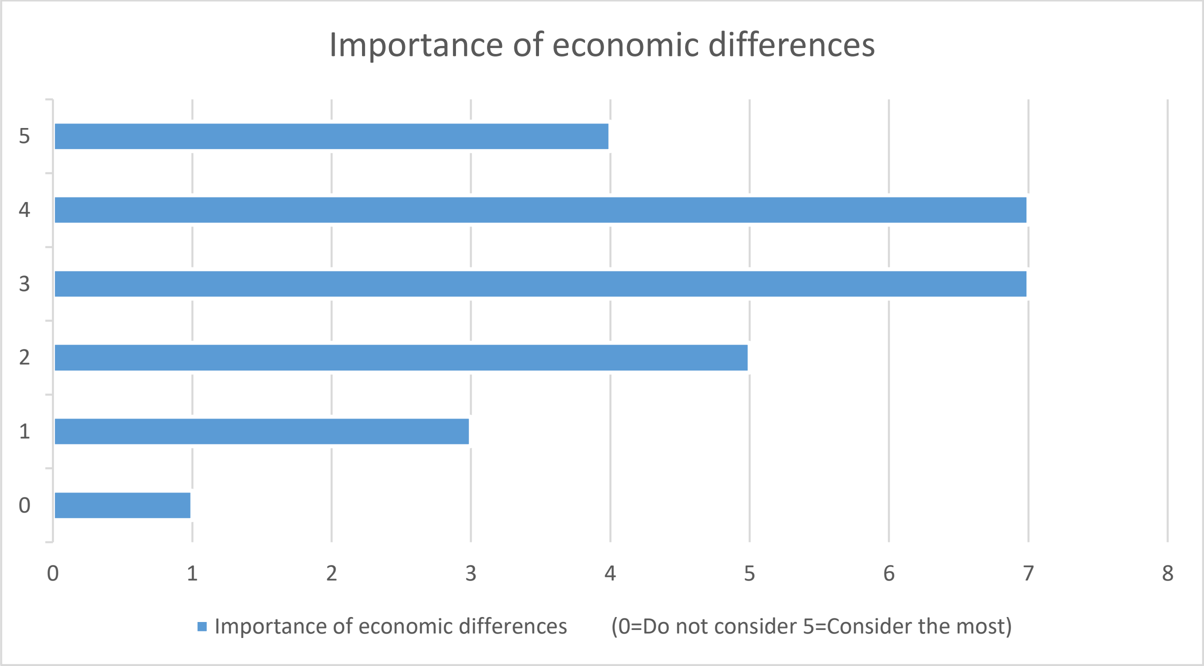


Figure D.24: Importance of economic differences (Male)

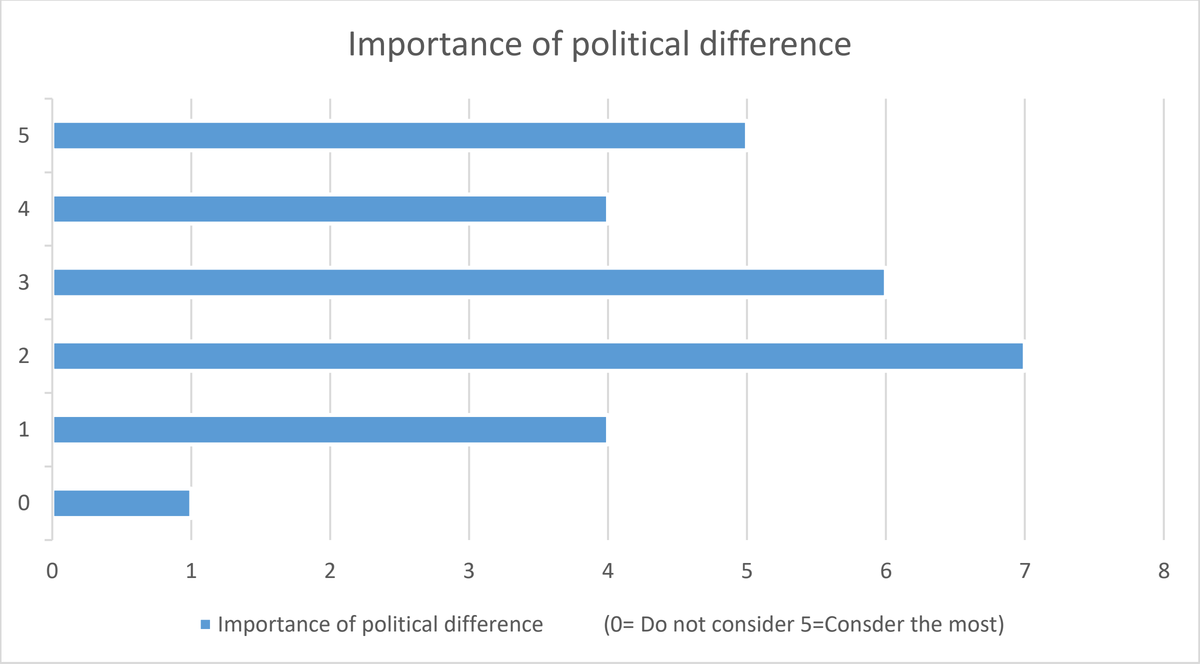


Figure D.25: Importance of political difference (Male)

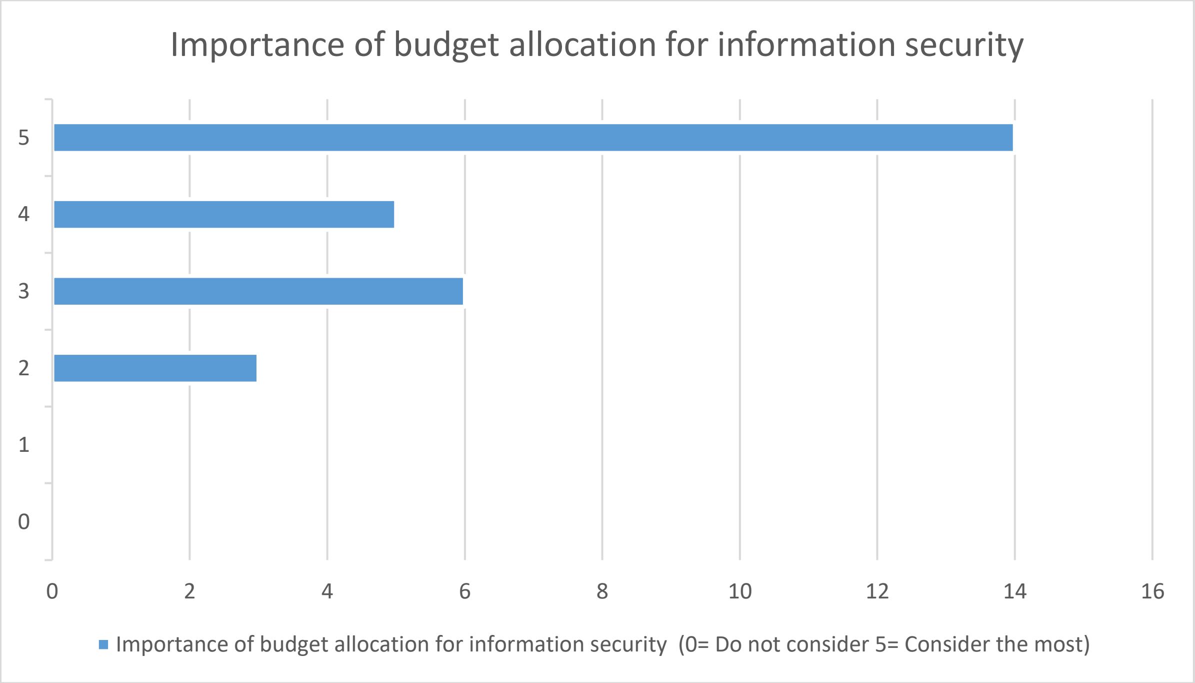


Figure D.26: Importance of budget allocation for information security (Male)

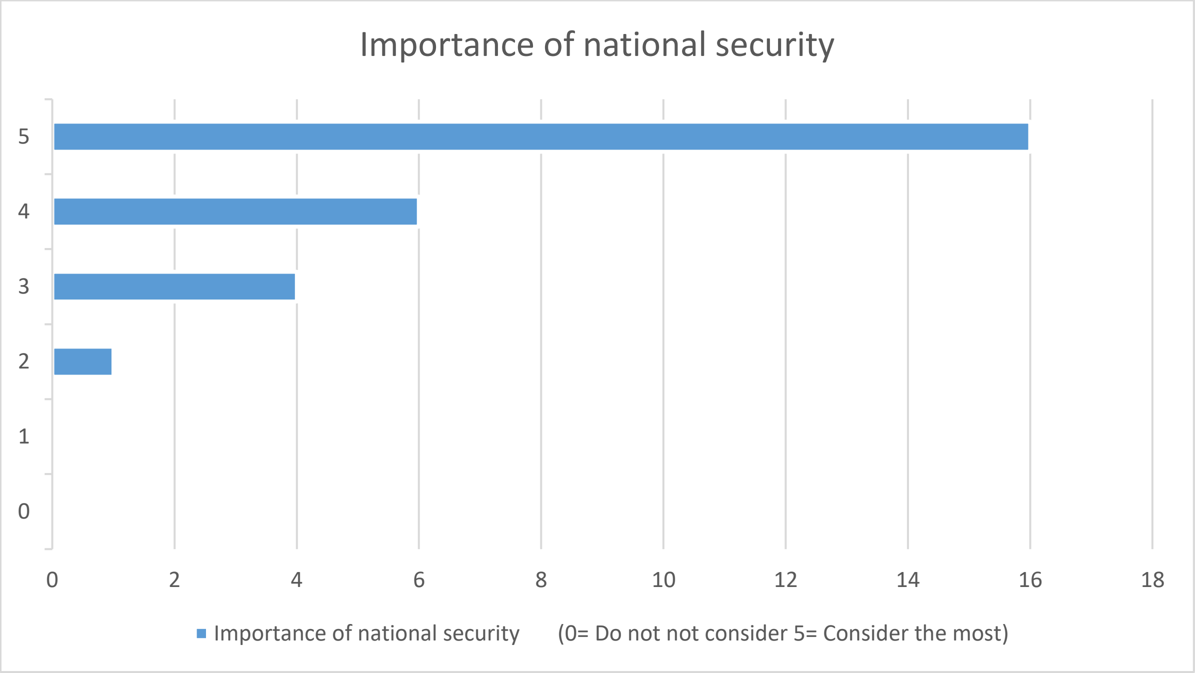


Figure D.27: Importance of national security (Male)

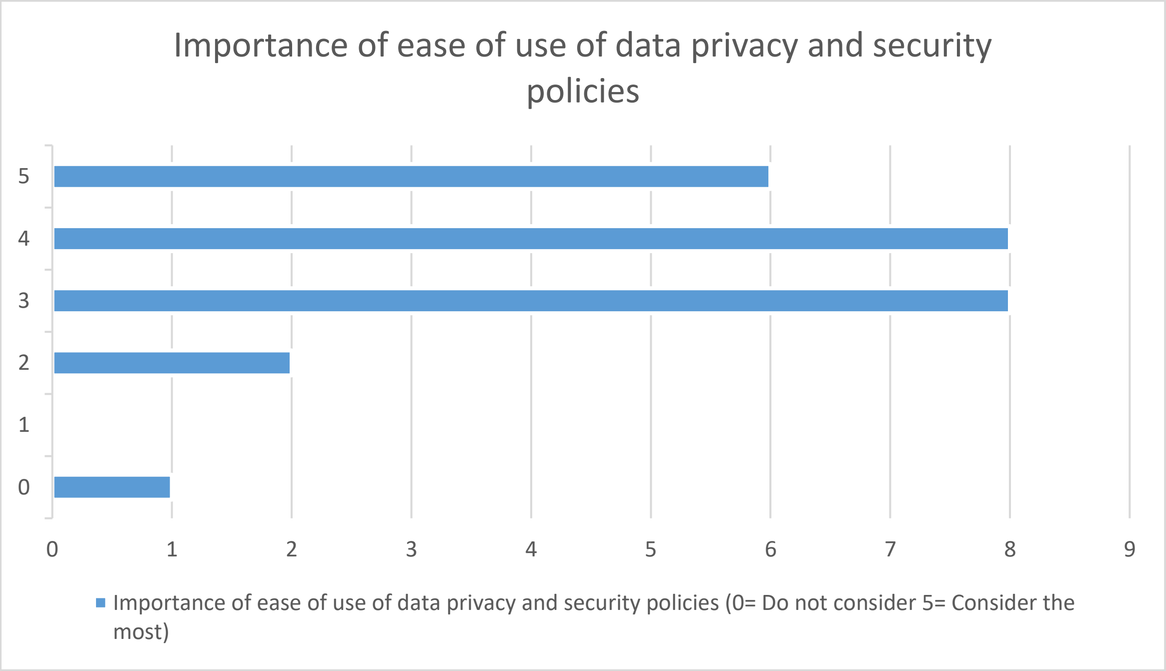


Figure D.28: Importance of ease of use of data privacy and security policies (Male)

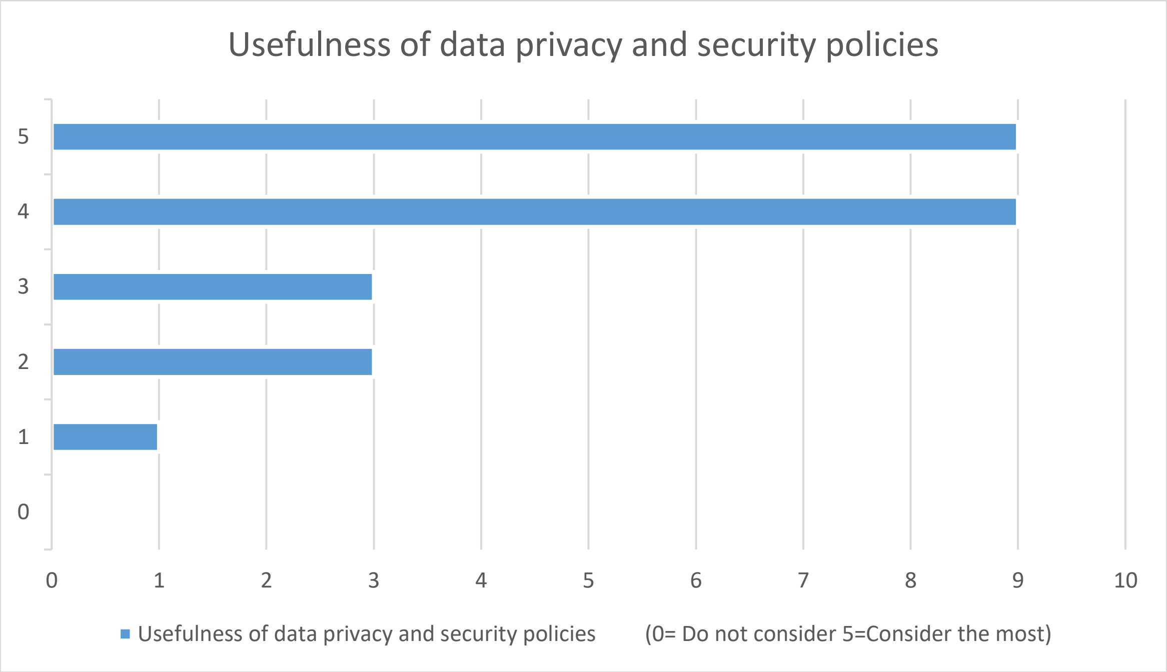


Figure D.29: Usefulness of data privacy and security policies (Male)

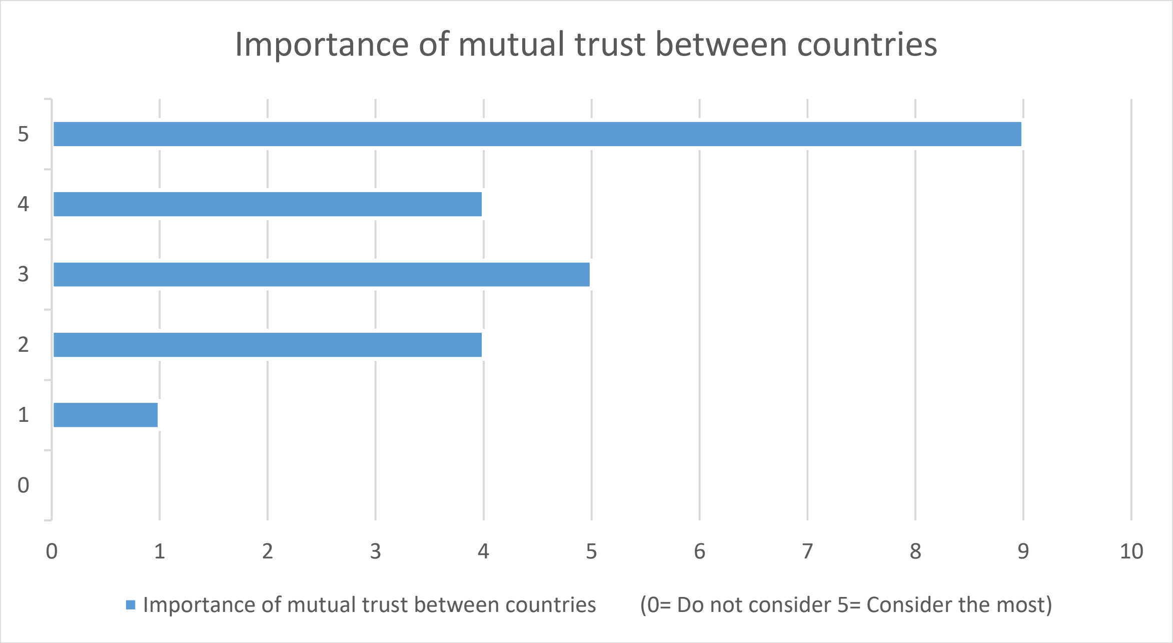


Figure D.30 Importance of mutual trust between countries (Male)

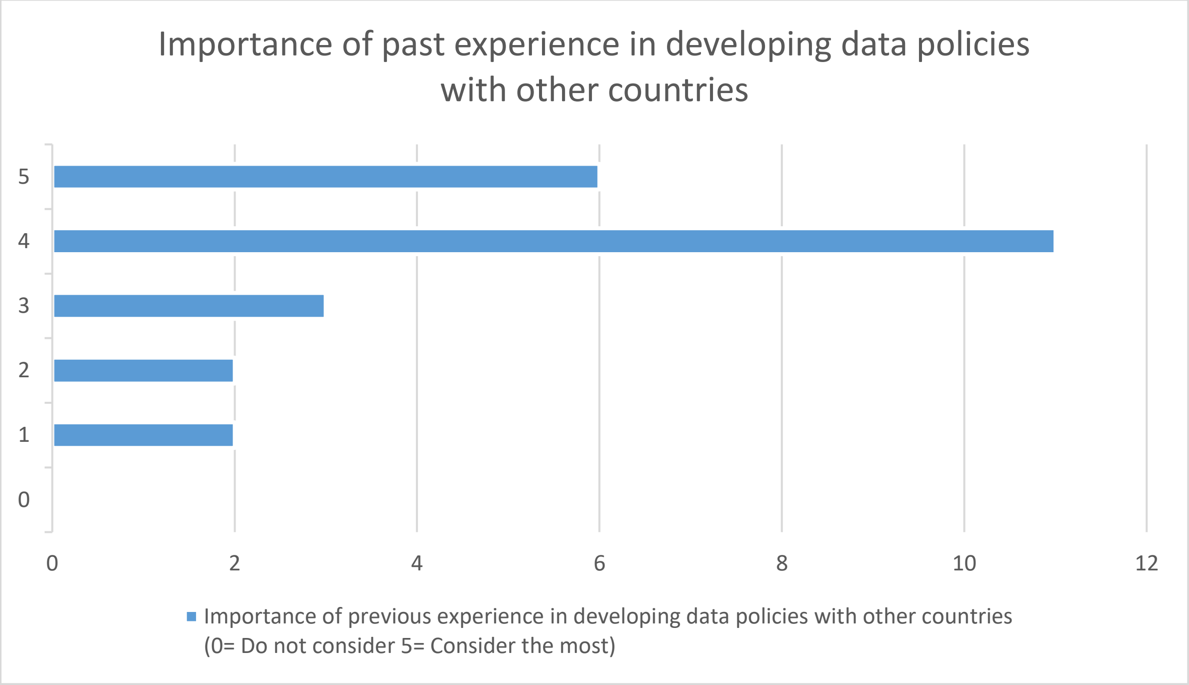


Figure D.31: Importance of past experience in developing data policies with other counties (Male)

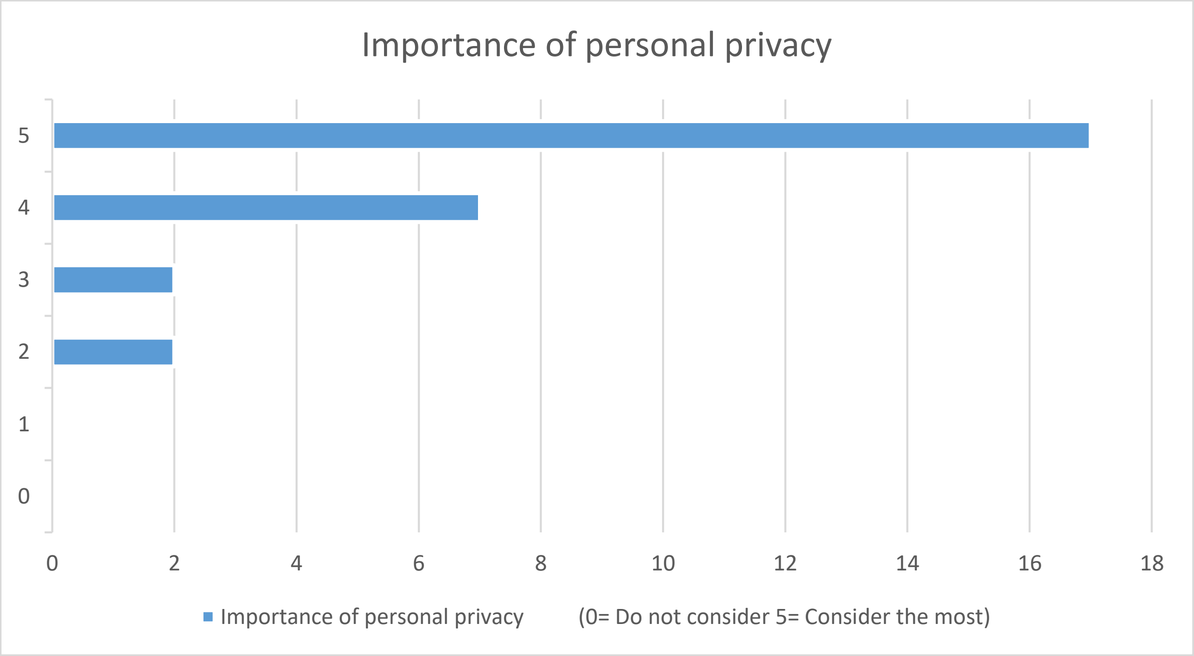


Figure D.32: Importance of personal privacy (Male)

The clear message coming out from the respondents is consensus amongst the 86 percent of the males the need to have a global level data protection mechanism (See figure D.21). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between the countries, and previous experience in developing policies with other countries (See figure D.10-20) (See figure D.22-32).

Sri Lanka: Female

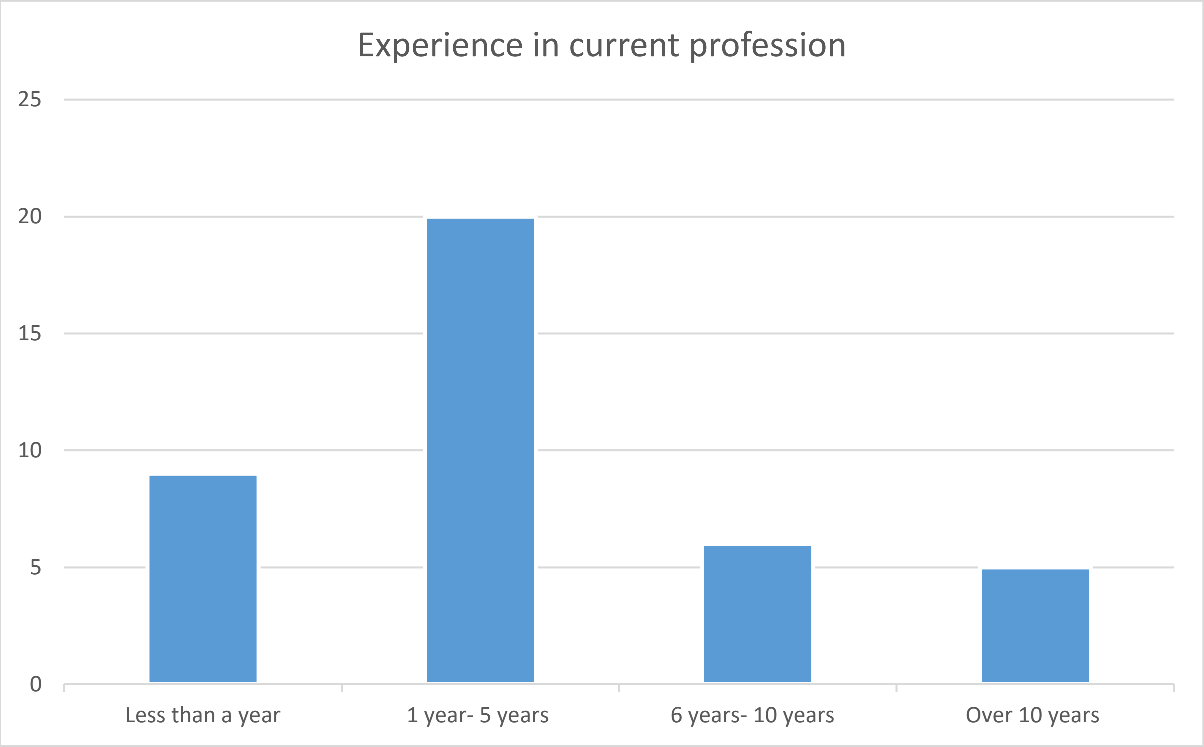


Figure D.33: Experience in current profession (Female)

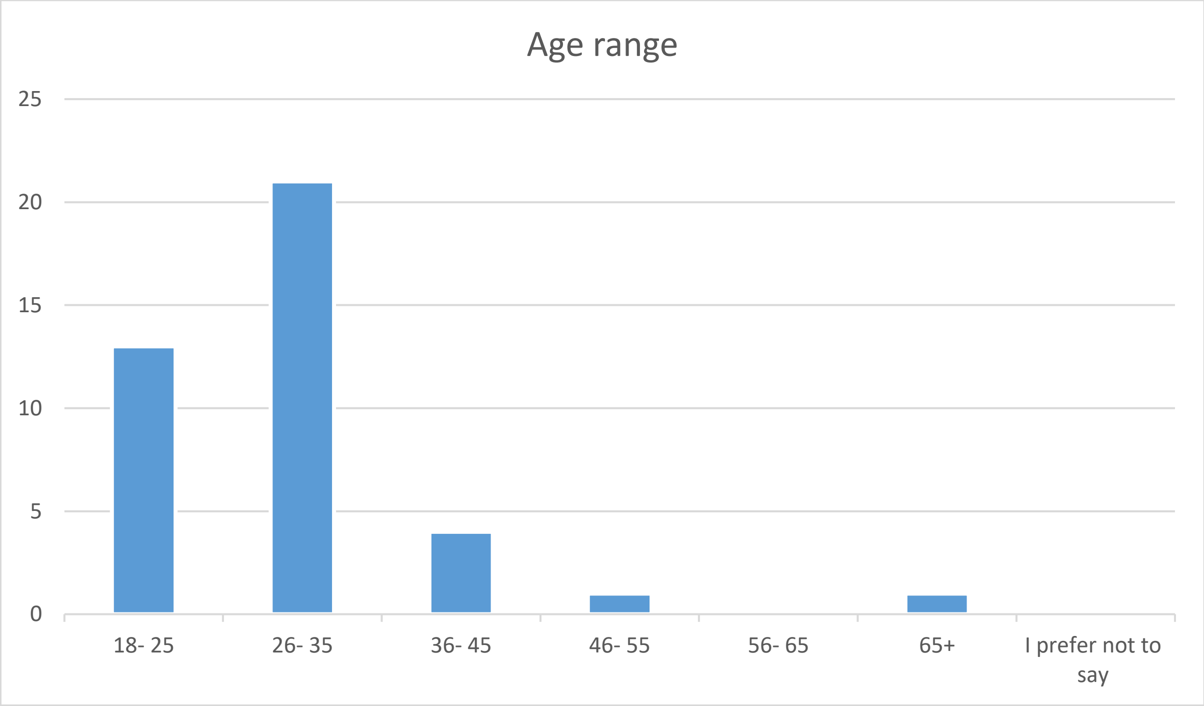


Figure D.34: Age range (Female)

This analysis is based on the responses received from Sri Lankan females out of the 40 participants, representing the 18-65 plus age range, and 53 percent of them are in the 26-35 age range (See figure D.34). They have been in work for less than a year to over 10 years in various industries, and 50 percent of the females have been in work for 1-5 years (See figure D.33).

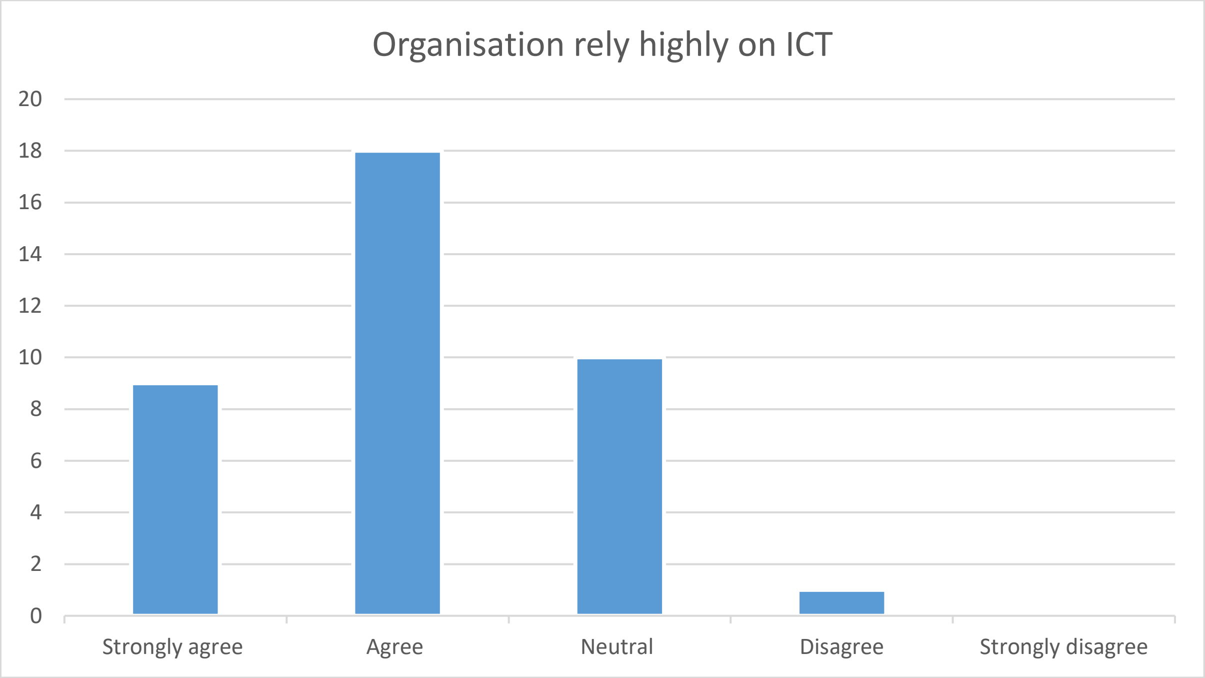


Figure D.35: Organisation rely highly on ICT (Female)

27 out of the 40 respondents work in a technology reliance working environment, 10 unaware because of the nature of the work assigned to them, 1 scored 'disagree' on ICT (See figure D.35). This shows the majority of females work in organisations with a high reliance on ICT.

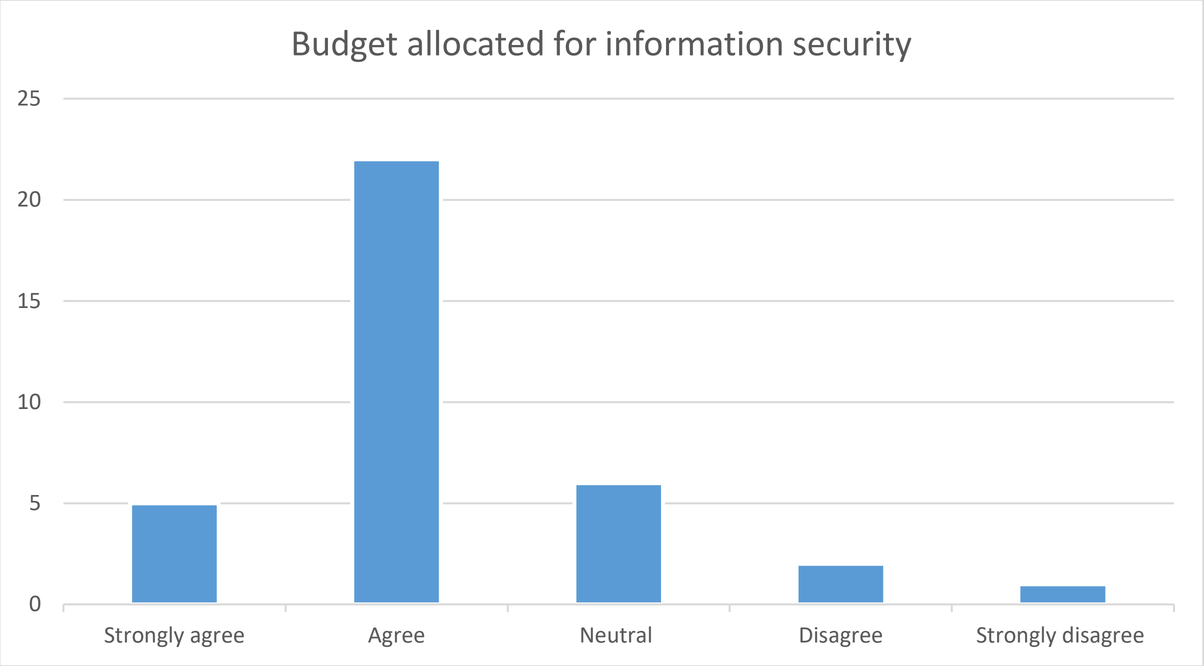


Figure D.36: Budget allocated for information security (Female)

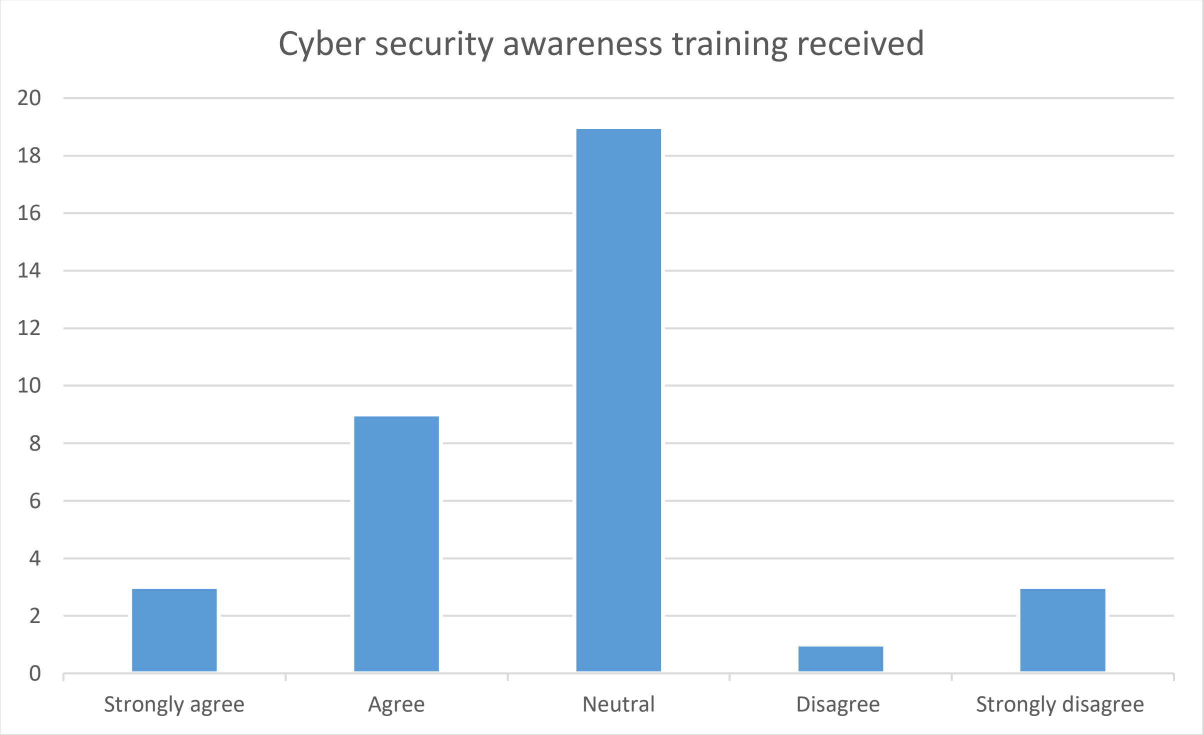


Figure D.37: Cyber security awareness training received (Female)

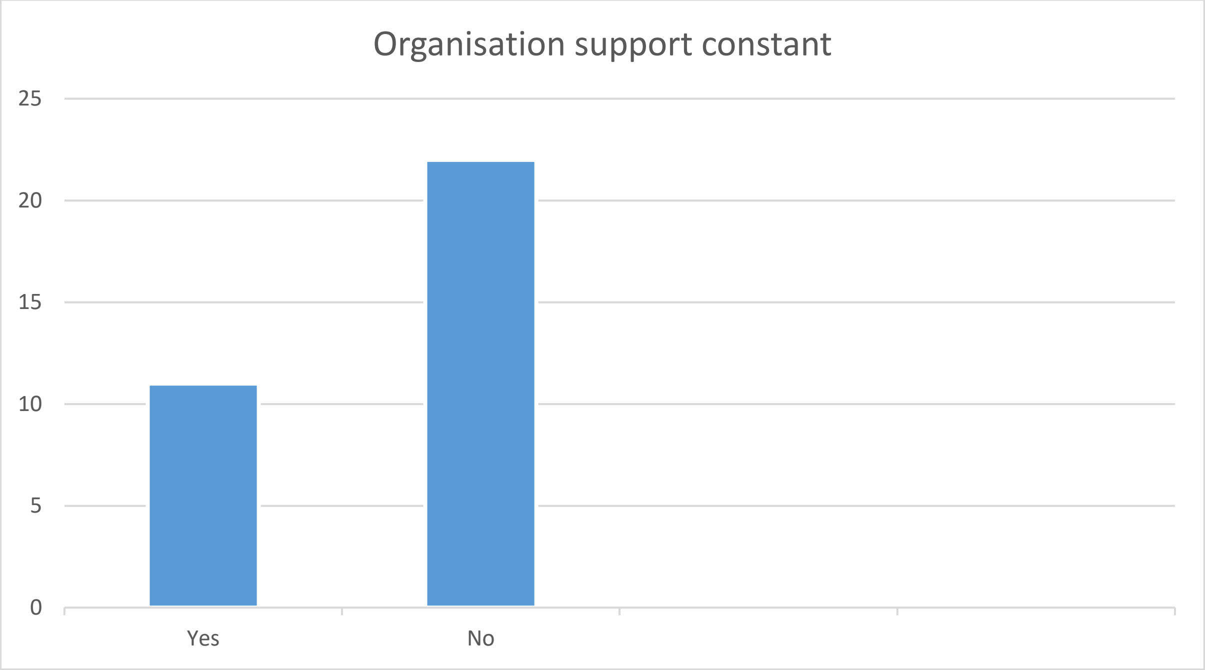


Figure D.38: Organisation support constant (Female)

According to 27 of the 40, their organisations had an allocated budget for information security; 6 had not expressed an opinion either way; notably according to the 3 who disagreed, their organisations had no allocated budget for information security (See figure D.36). According to some of the participants, a satisfactory level of funding allocated for information security, however, an adequate level of regular security awareness training not received . Only 12 participants received regular cybersecurity awareness training; 19 neither agreed nor disagreed; 4 not received training (See figure D.37). In terms of protecting personal information, 22 did not get support from the organisation, only 11 did (See figure D.38).That indicates the lack of organisational support to protect personal information despite the allocation of funds for information security and high reliance on technology.

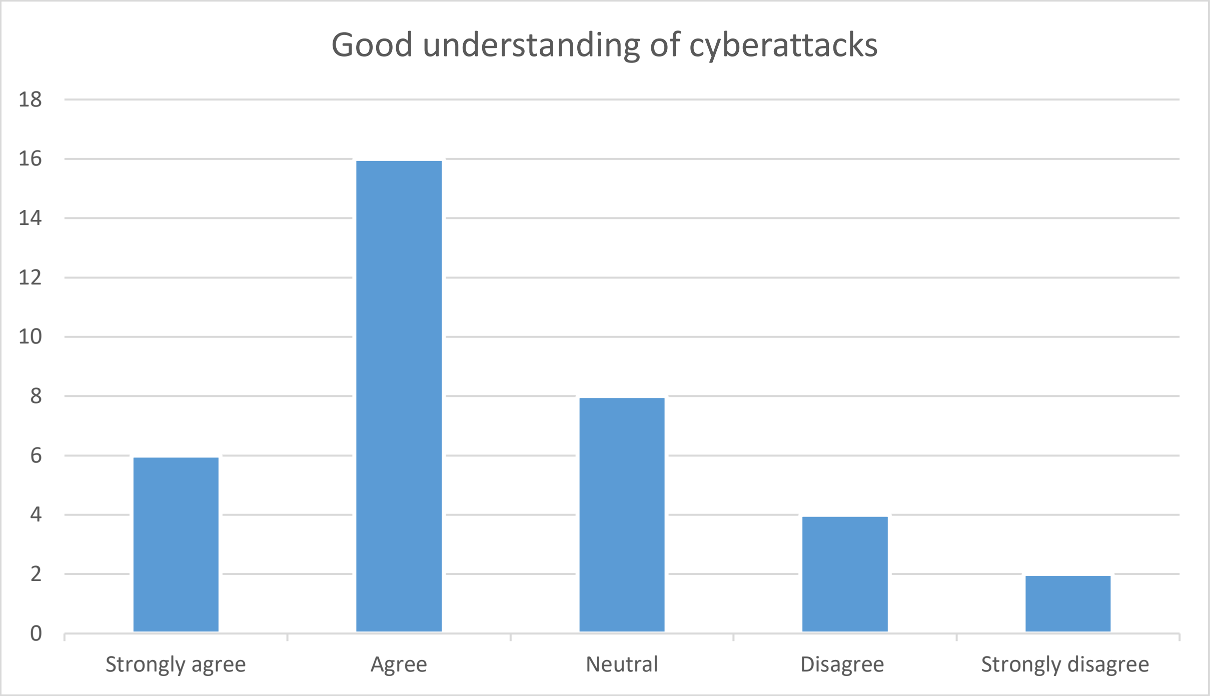


Figure D.39: Good understanding of cyberattacks (Female)

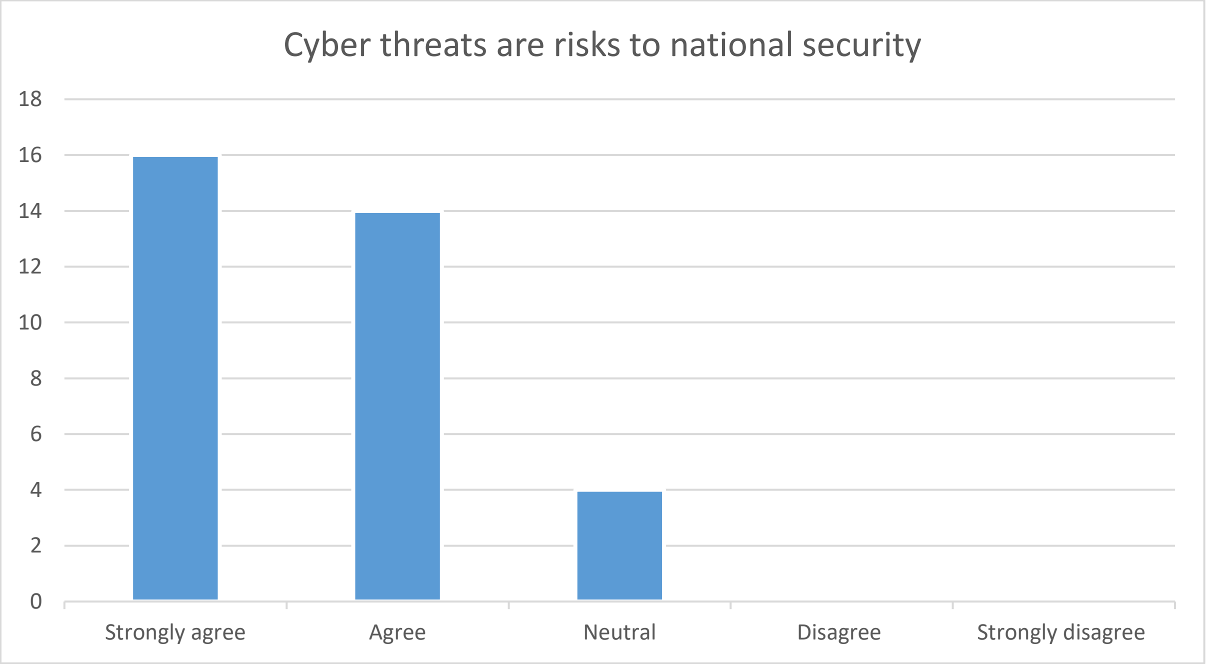


Figure D.40: Cyber threats are risks to national security (Female)

Despite the lack of security awareness training, the responses show that 22 participants have a good understanding of the impact of cyber-attacks on the public and the organisation; 6 participants did not; 8 did not express an opinion either way (See figure D.39). Furthermore, 75 percent of the participants realise the potential threats to national security from cyber-attacks (See figure D.40). In general, understanding cyber threats and their impact on national security should encourage people to act responsibly to minimise end-user errors, and in time, they will be in a strong position to influence the process in accepting and implementing a national, regional, and global level mechanism.

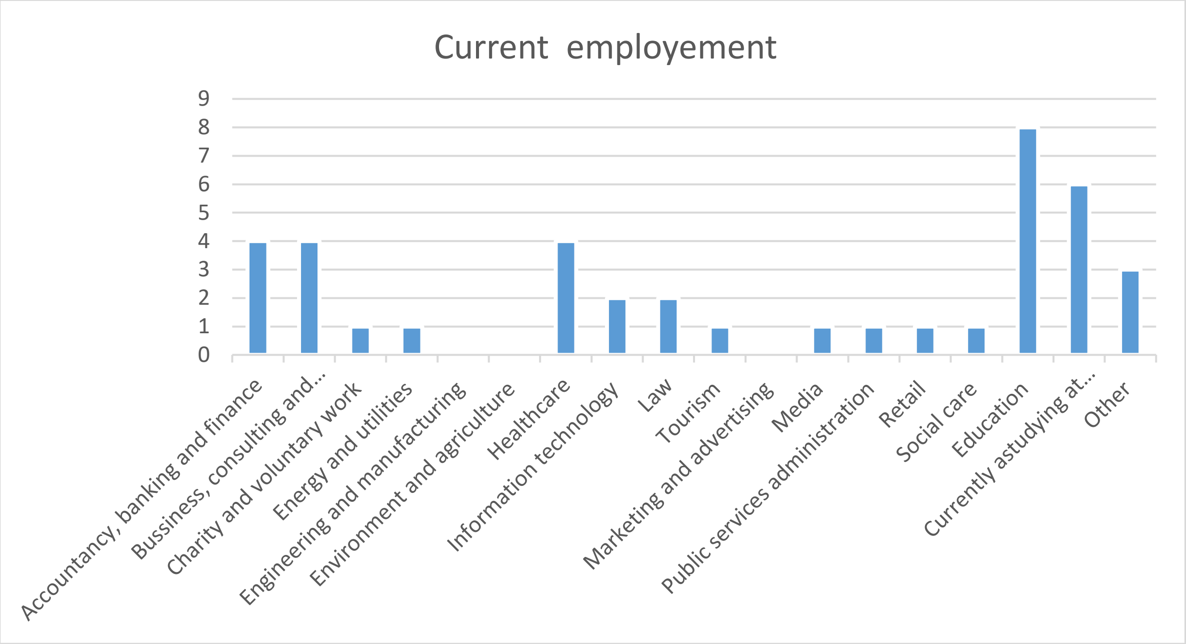


Figure D.41: Current employment (Female)

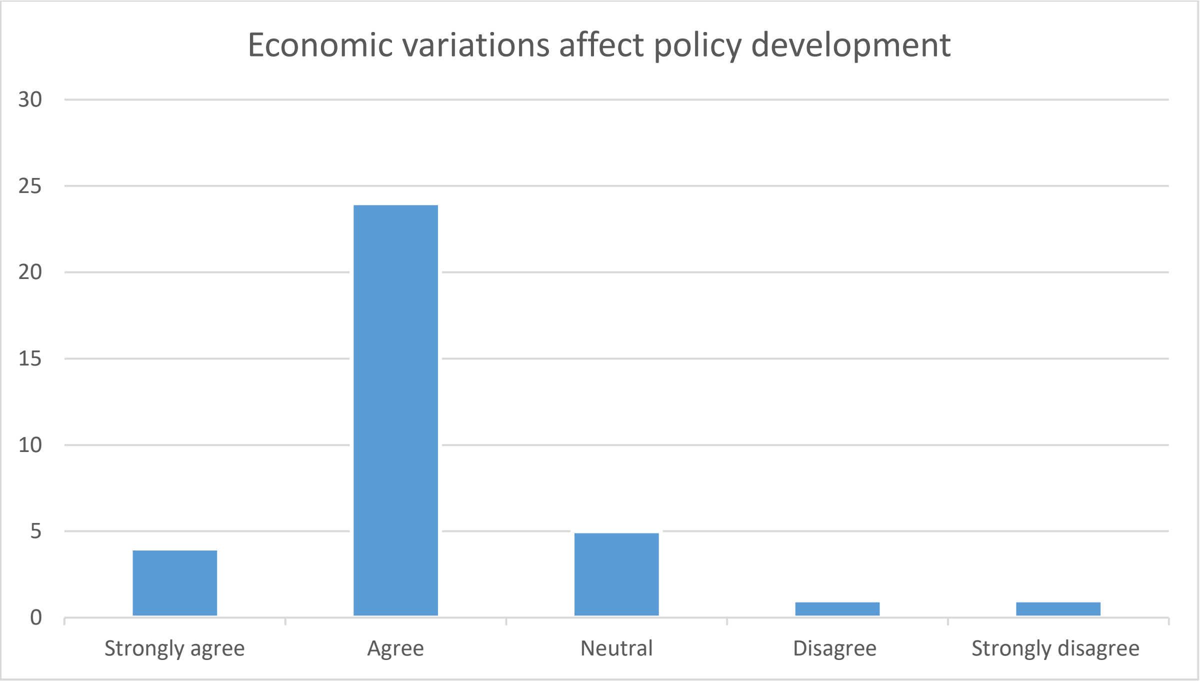


Figure D.42: Economic variations affect policy development (Female)

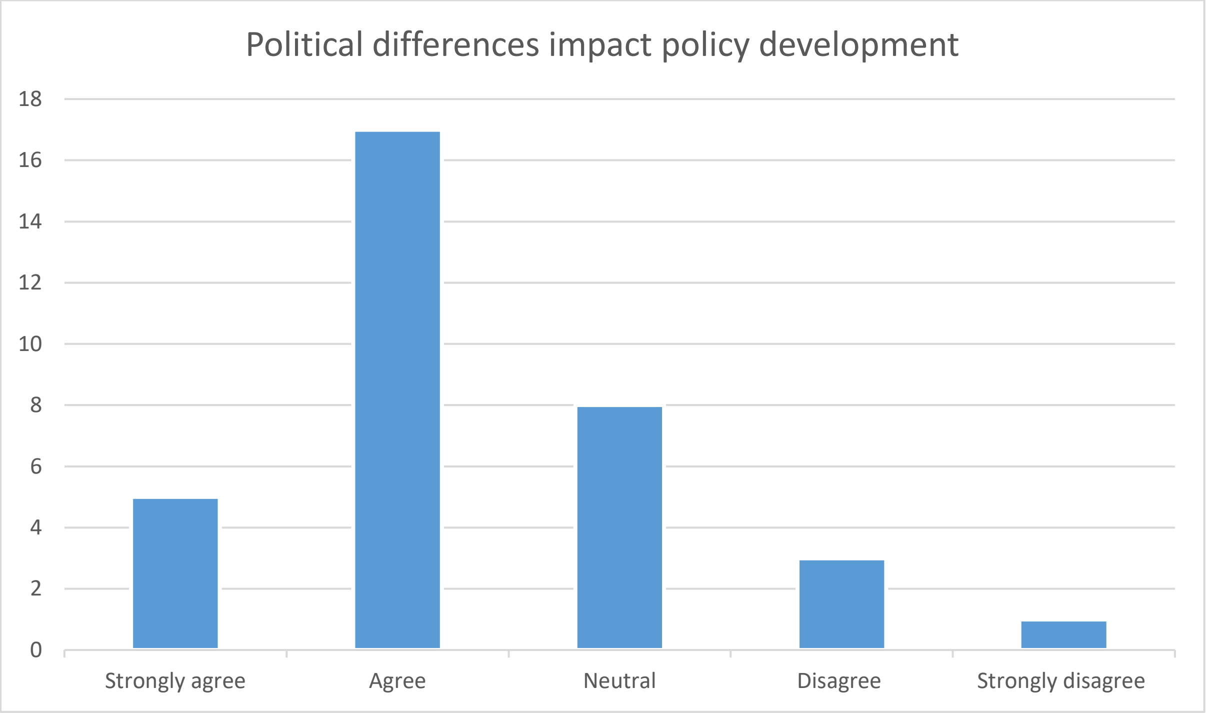


Figure D.43: Political differences impact policy development (Female)

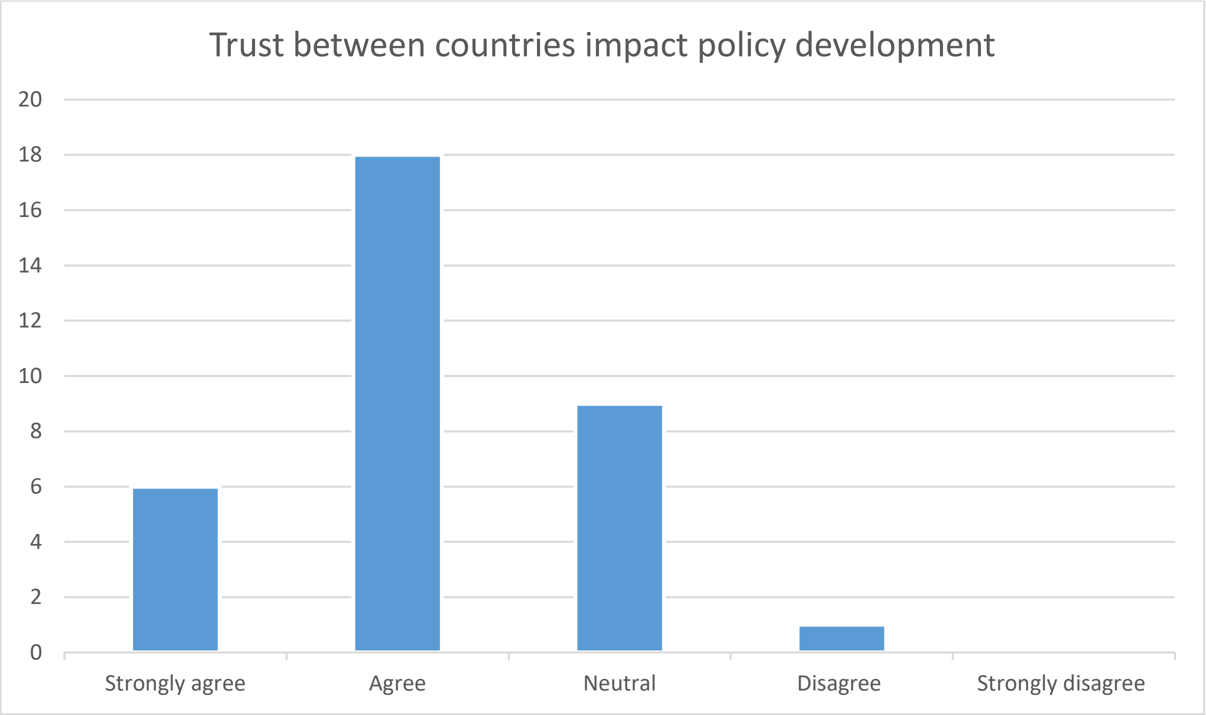


Figure D.44: Trust between countries impact policy development (Female)

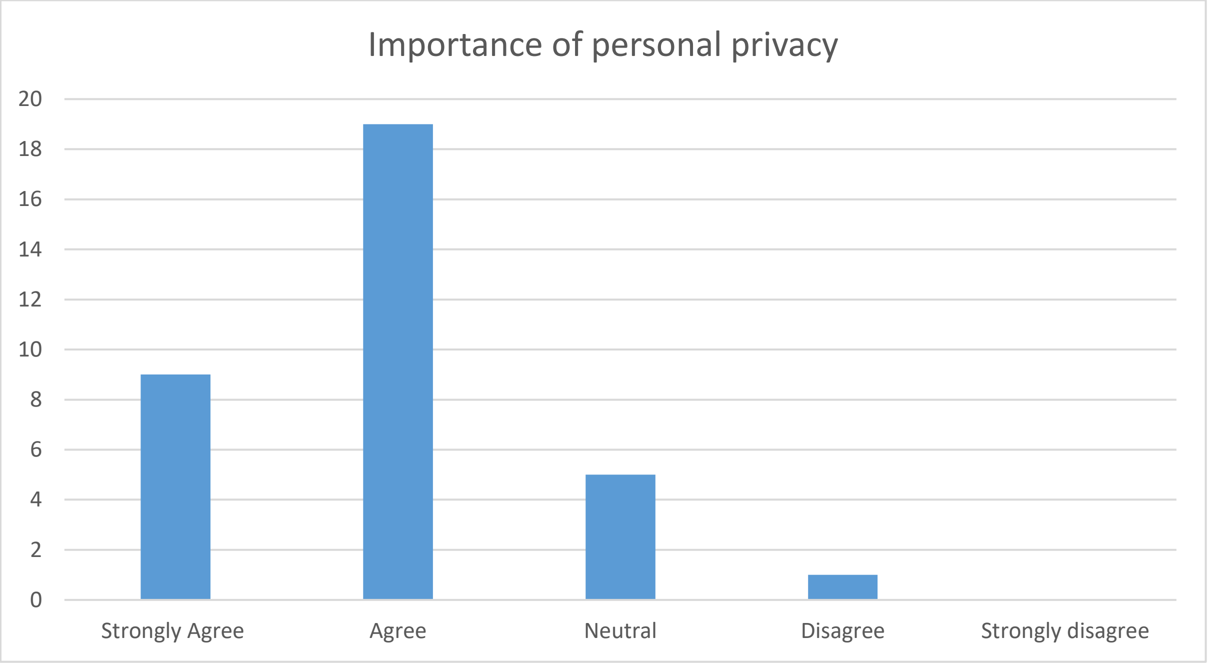


Figure D.45: Importance of personal privacy (Female)

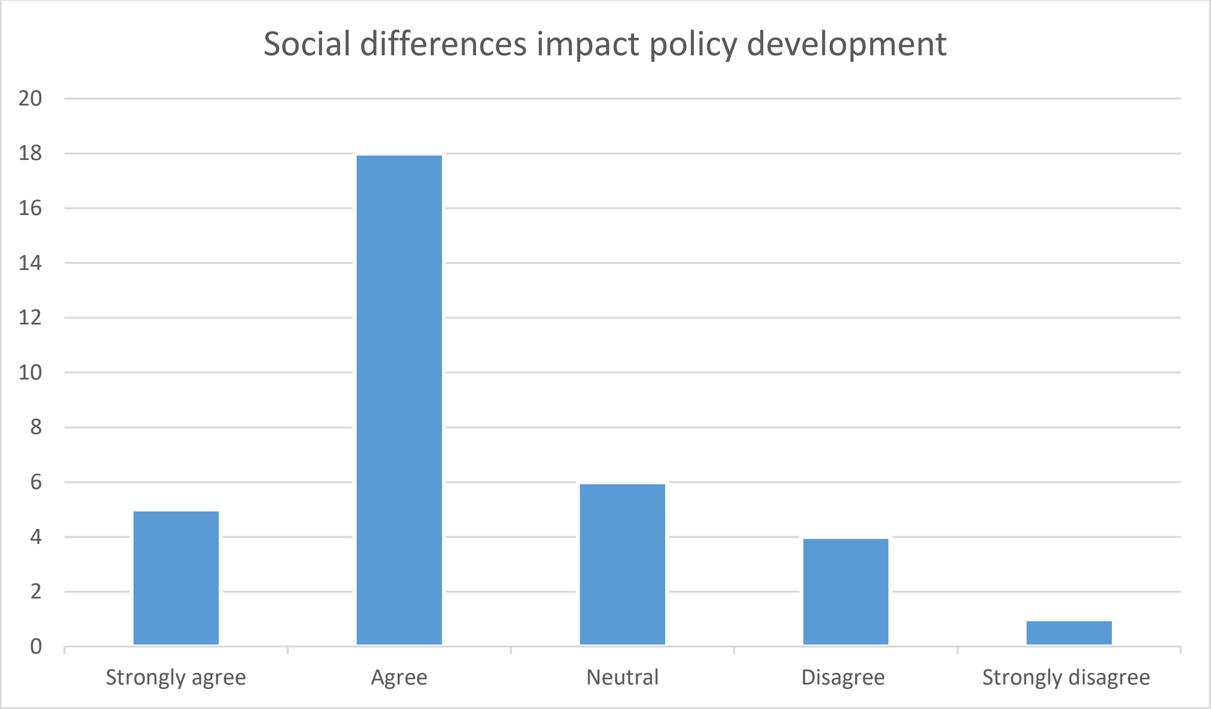


Figure D.46: Social differences impact policy development (Female)

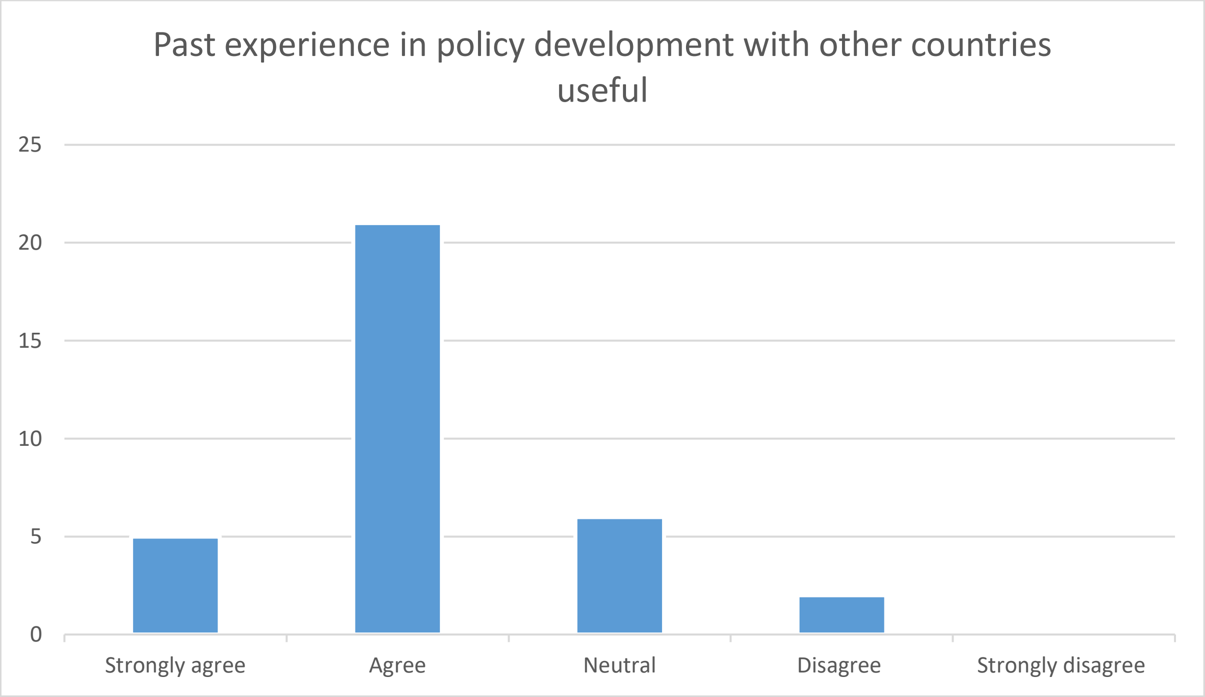


Figure D.47: Past experience in policy development with other countries useful (Female)

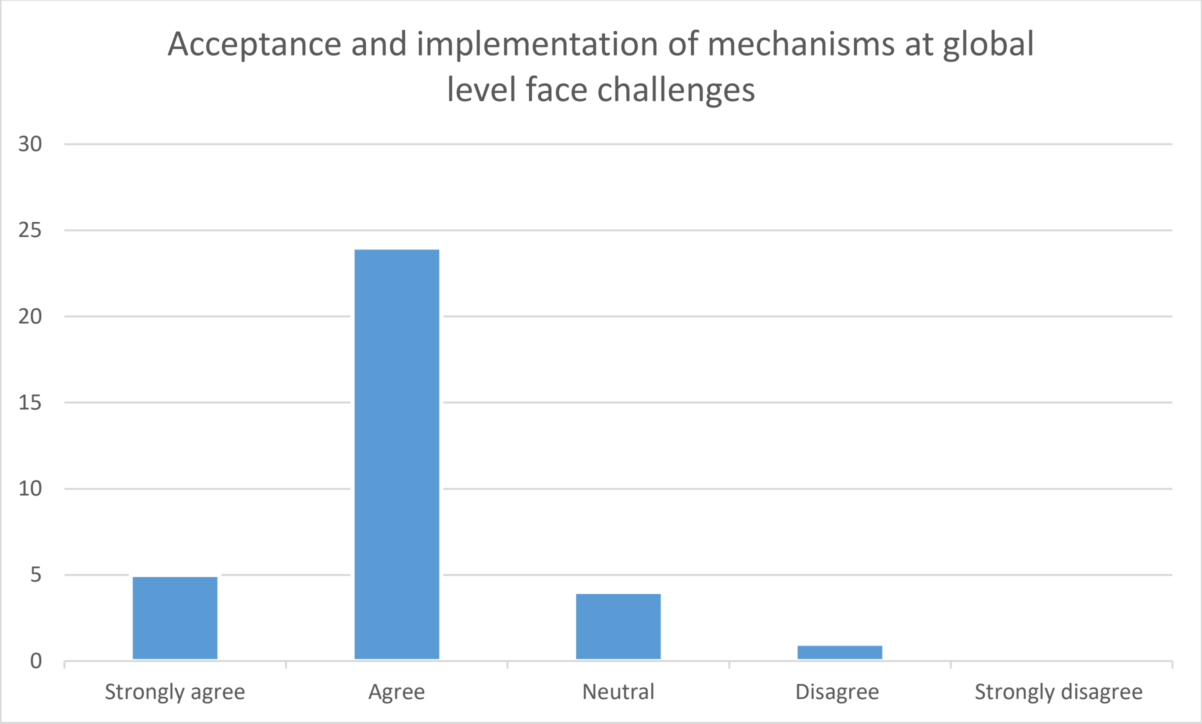


Figure D.48: Acceptance and implementation of mechanisms at global level face challenges (Female)

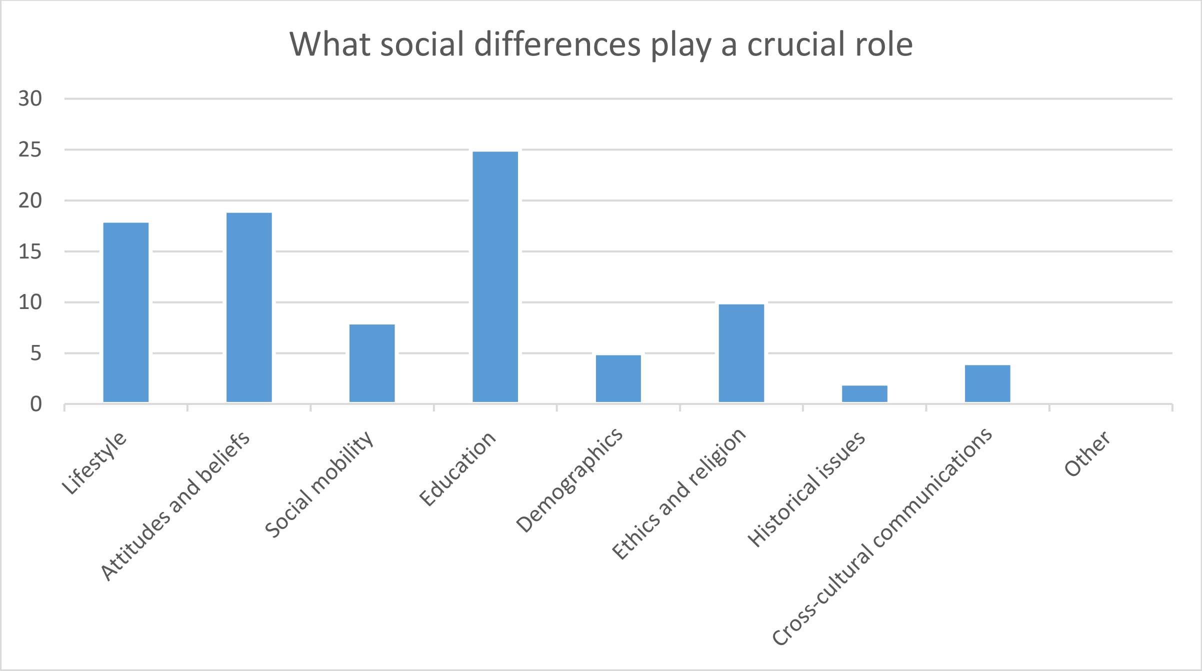


Figure D.49: What social differences play a crucial role (Female)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education (See figure D.49). Awareness of potential cyber threats and the impact on people and national security will be an important asset in terms of accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. Going back to the previous question about the provision of cybersecurity awareness training, proper security training had not been given. Therefore, it suggests that the majority of participants preferentially valued education than other social factors.

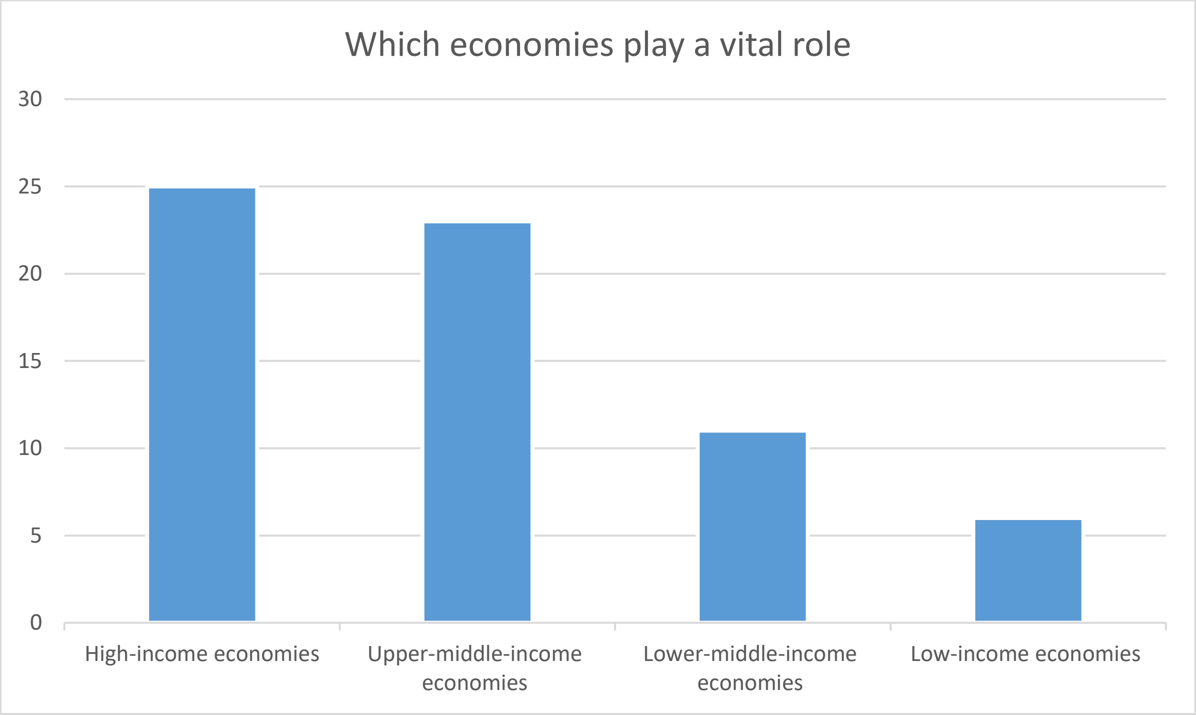


Figure D.50: Which economies play a vital role (Female)

In the questionnaire, the majority has stated that high-income countries and upper-middle-income countries play a vital role in the policymaking process (See figure D.50). The key stages in the policymaking process aim to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the resources necessary, implement, and finally evaluate the policy. These stages are time-consuming and require sufficient funding and resources. Therefore, the economic stability of the country is considered crucial to a large extent in achieving success in policymaking.

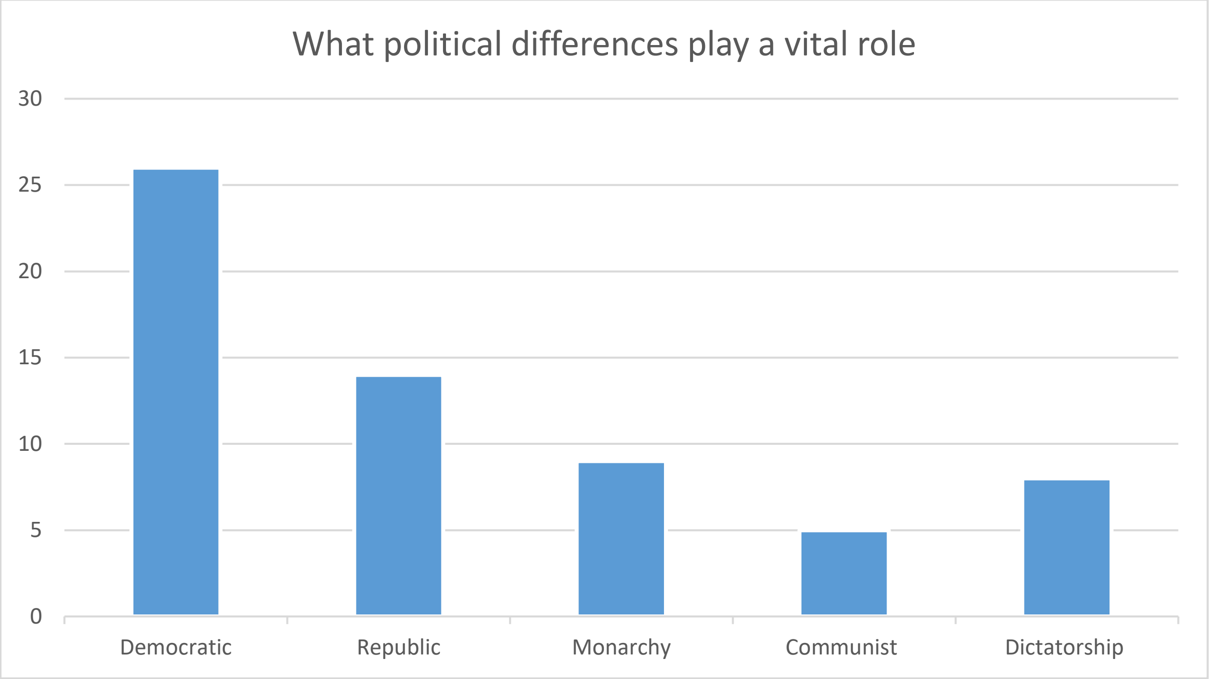


Figure D.51: What political differences play a vital role (Female)

The majority have chosen a democratic political system (See figure D.51), in preference to others because it allows the public an influential voice in policy development and encourages consensus and collective responsibility for their actions. These contribute to developing public trust between them and the organisations and ensure coherence and transparency in the policy development process.

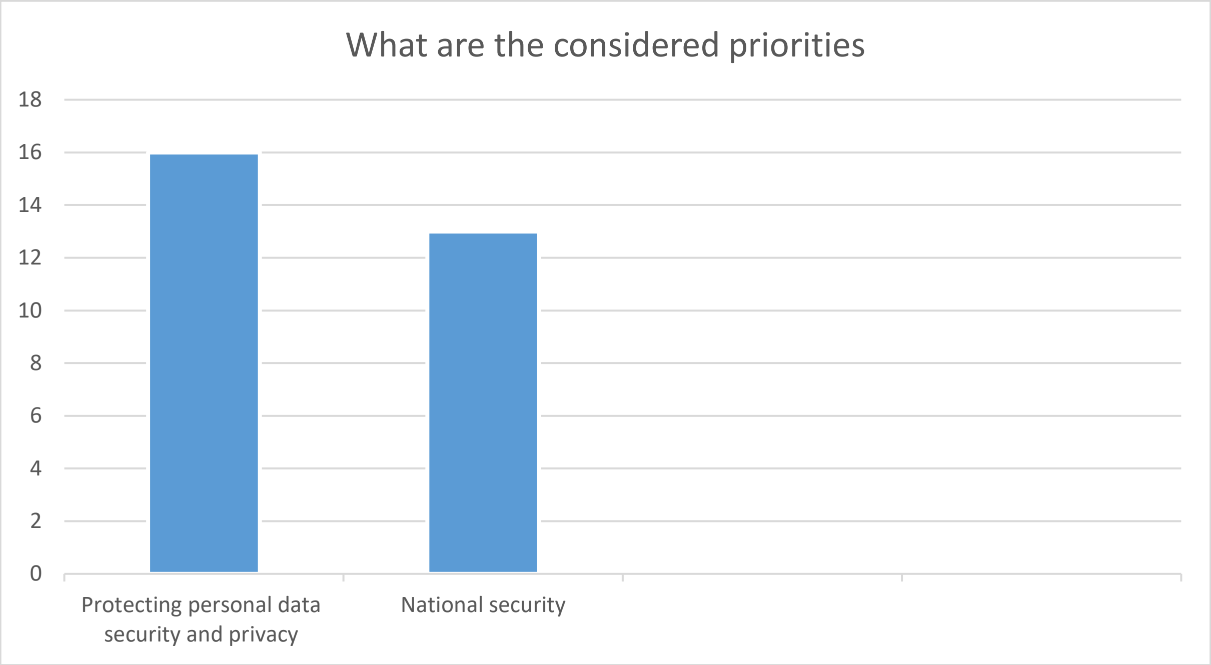


Figure D.52: What are the considered priorities (Female)

The majority does not give prominence to the importance of protection of personal data security and privacy nor protection of national security, in accepting and implementing a global data privacy and security policies (See figure D.52. In the event of a personal data breach, there will potentially be a knock-on effect on both personal data security and privacy and national security, and it will also be felt right across the groups as well as the community alike.

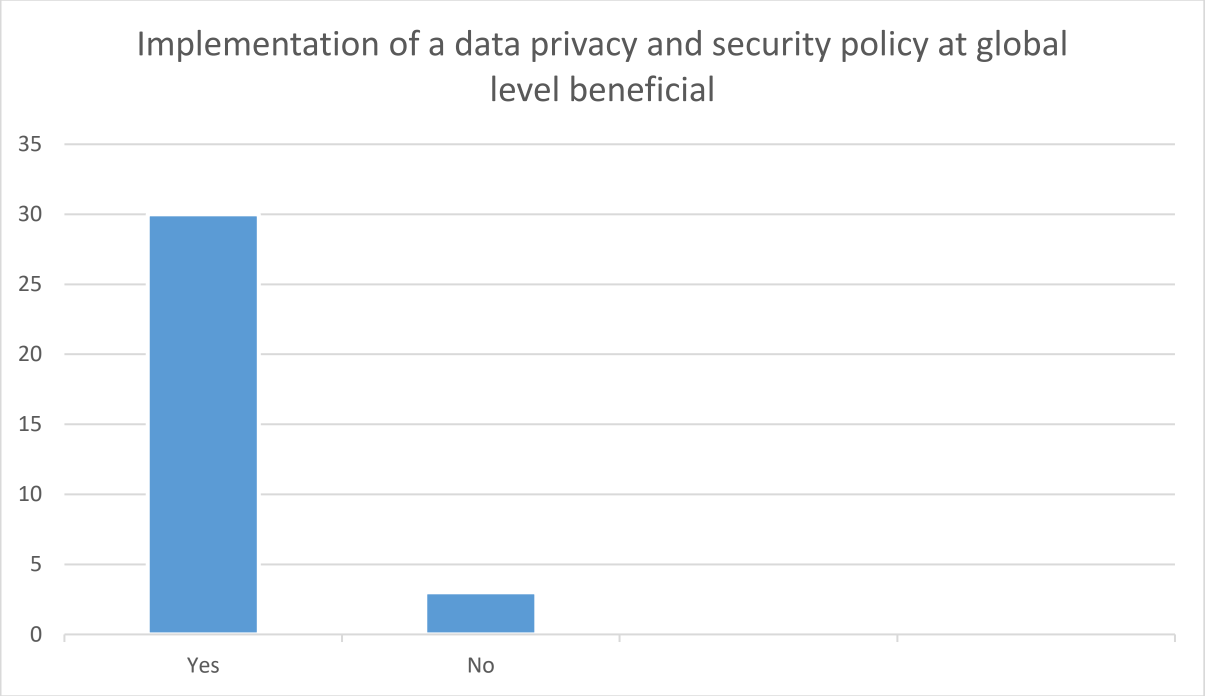


Figure D.53: Implementation of a data privacy and security policy at global level beneficial (Female)

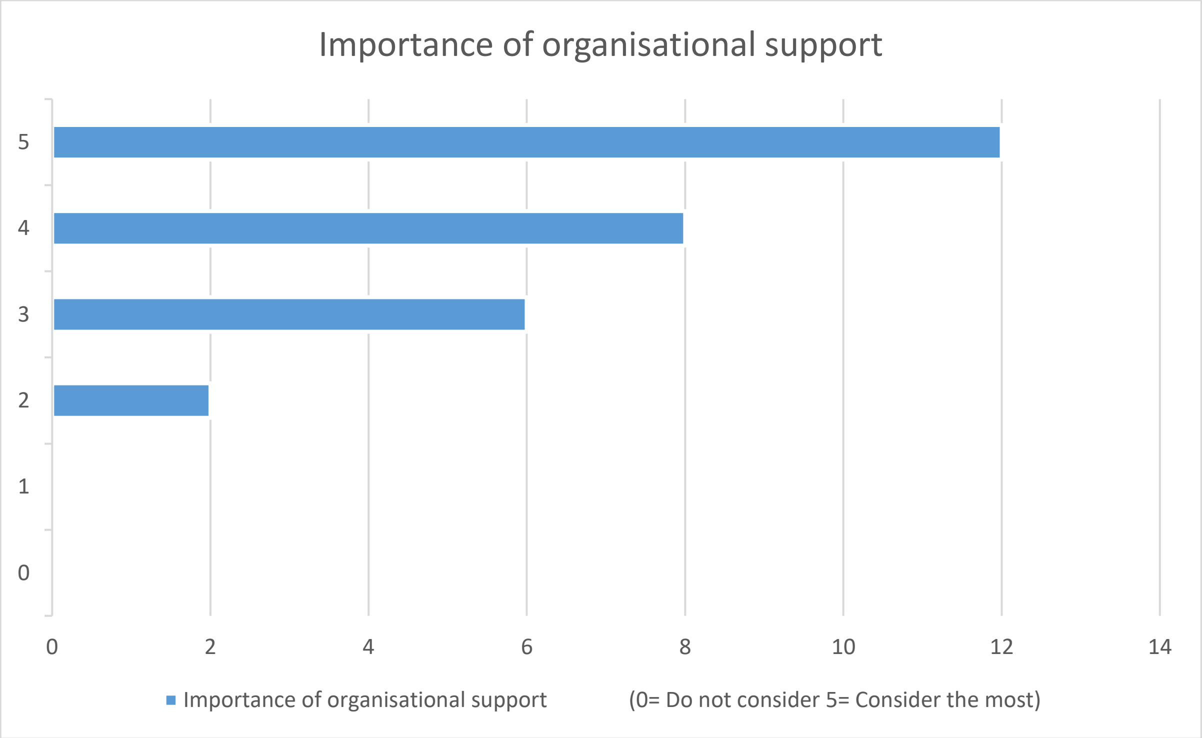


Figure D.54: Importance of organisational support (Female)

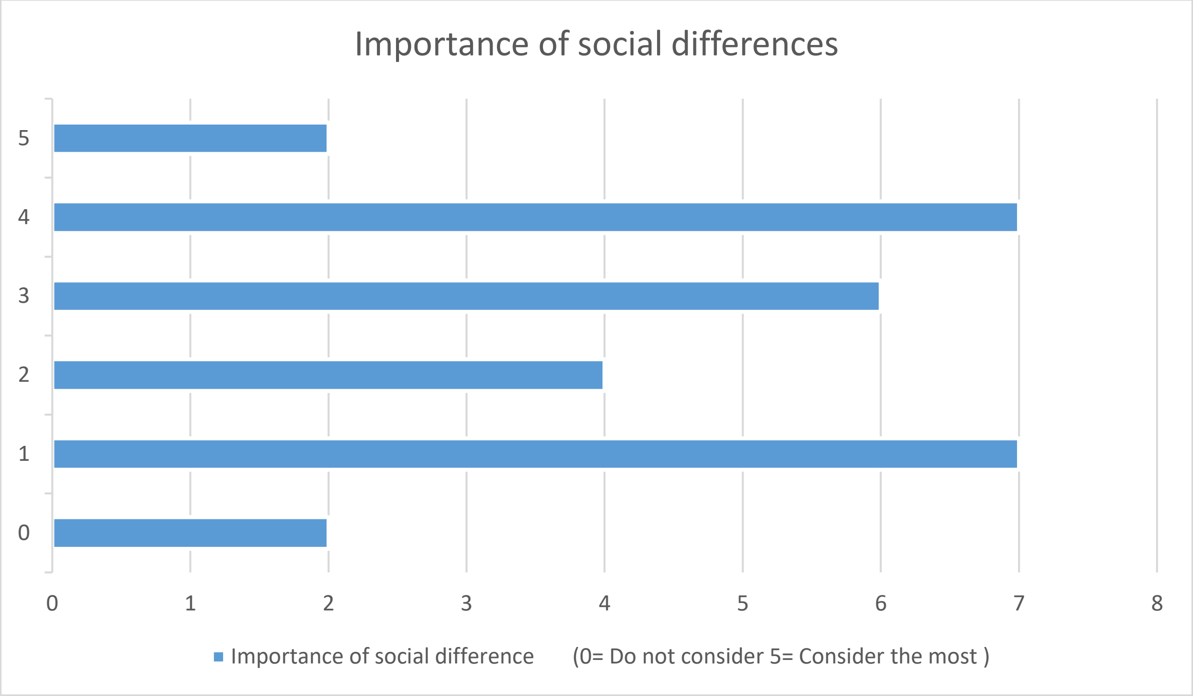


Figure D.55: Importance of social differences (Female)

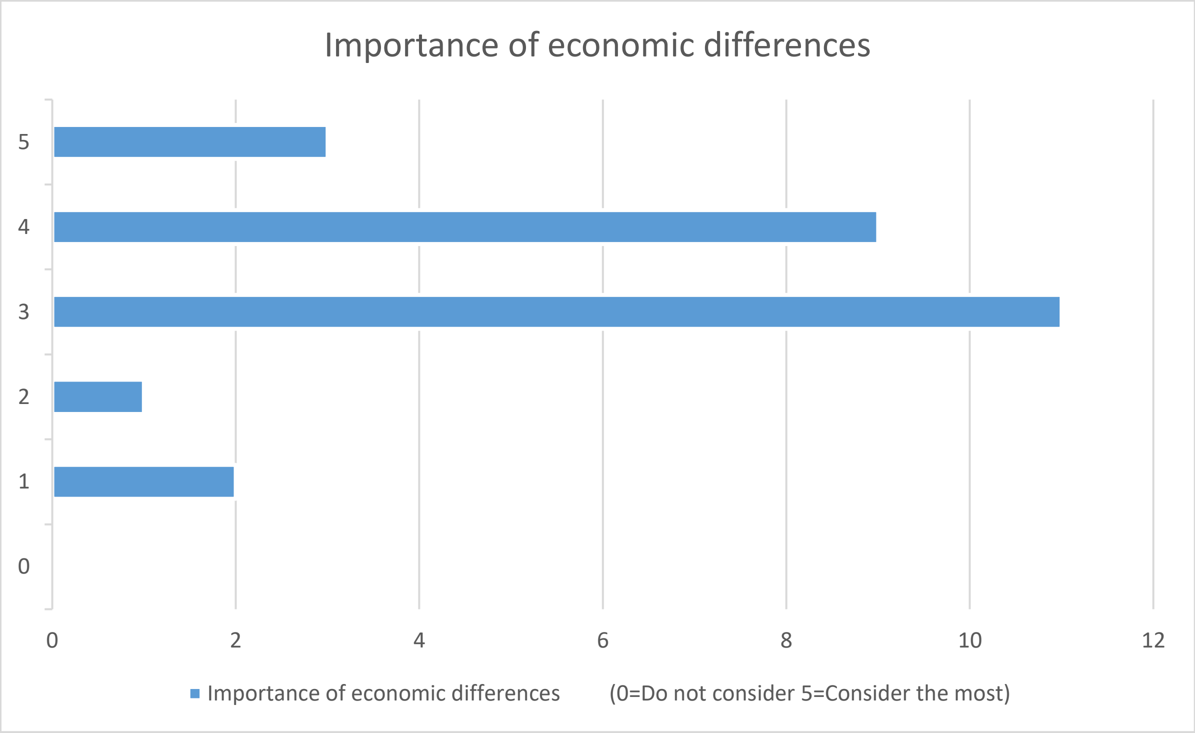


Figure D.56: Importance of economic differences (Female)

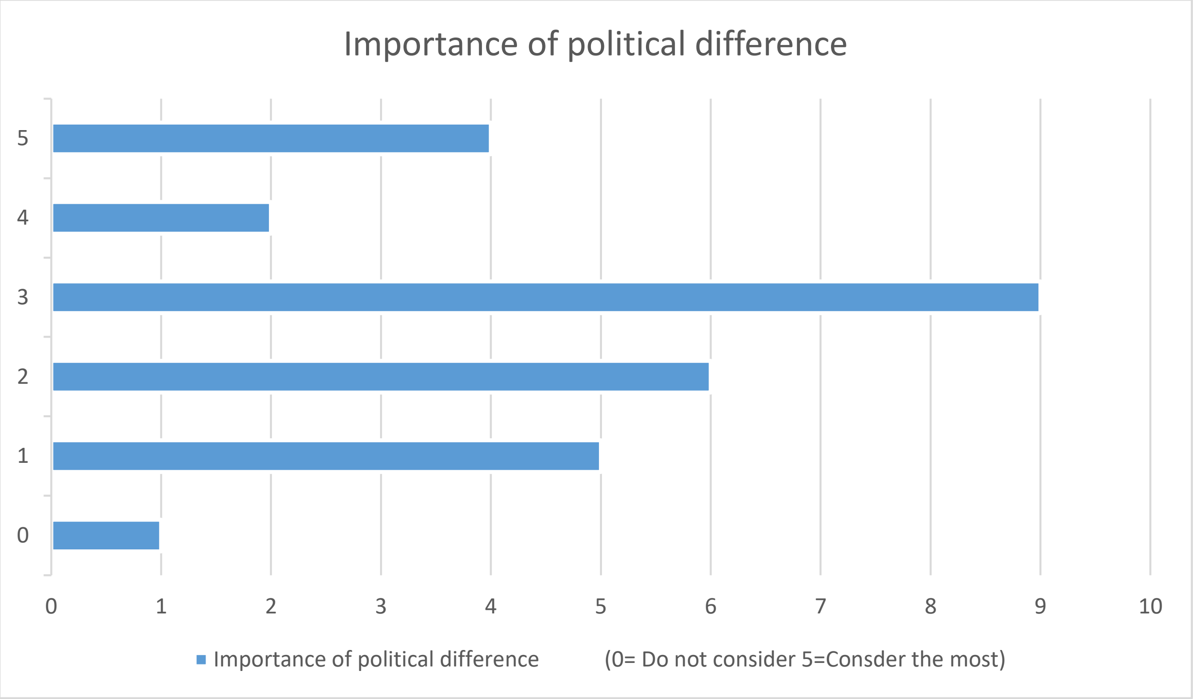


Figure D.57: Importance of political difference (Female)

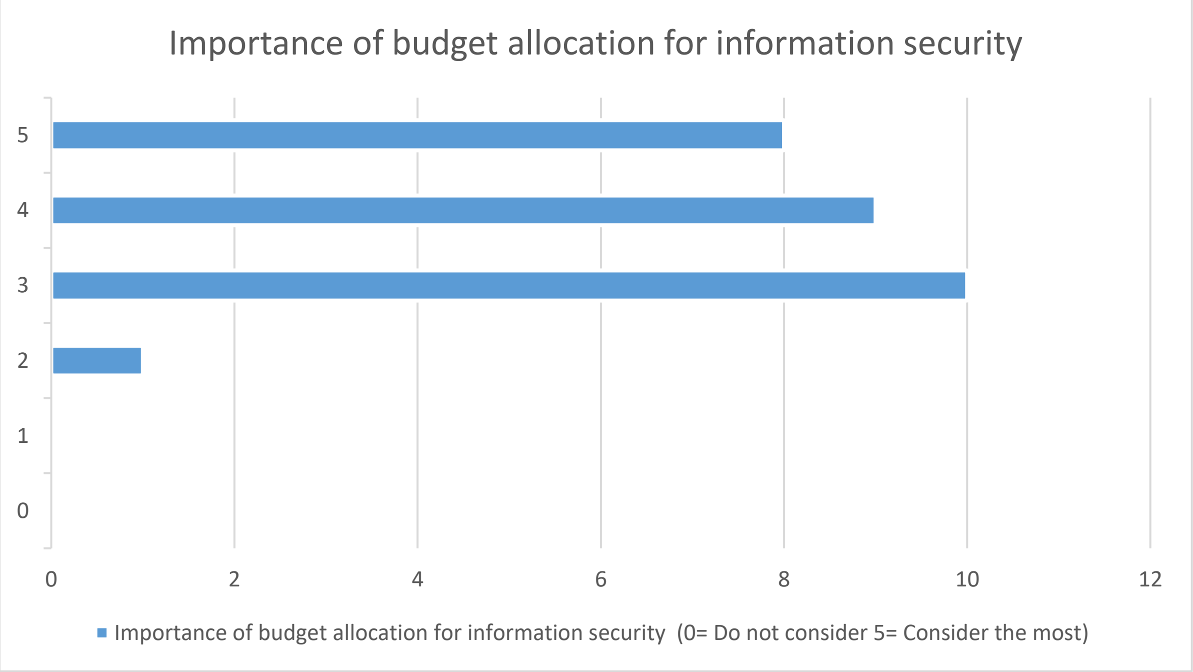


Figure D.58: Importance of budget allocation for information security (Female)

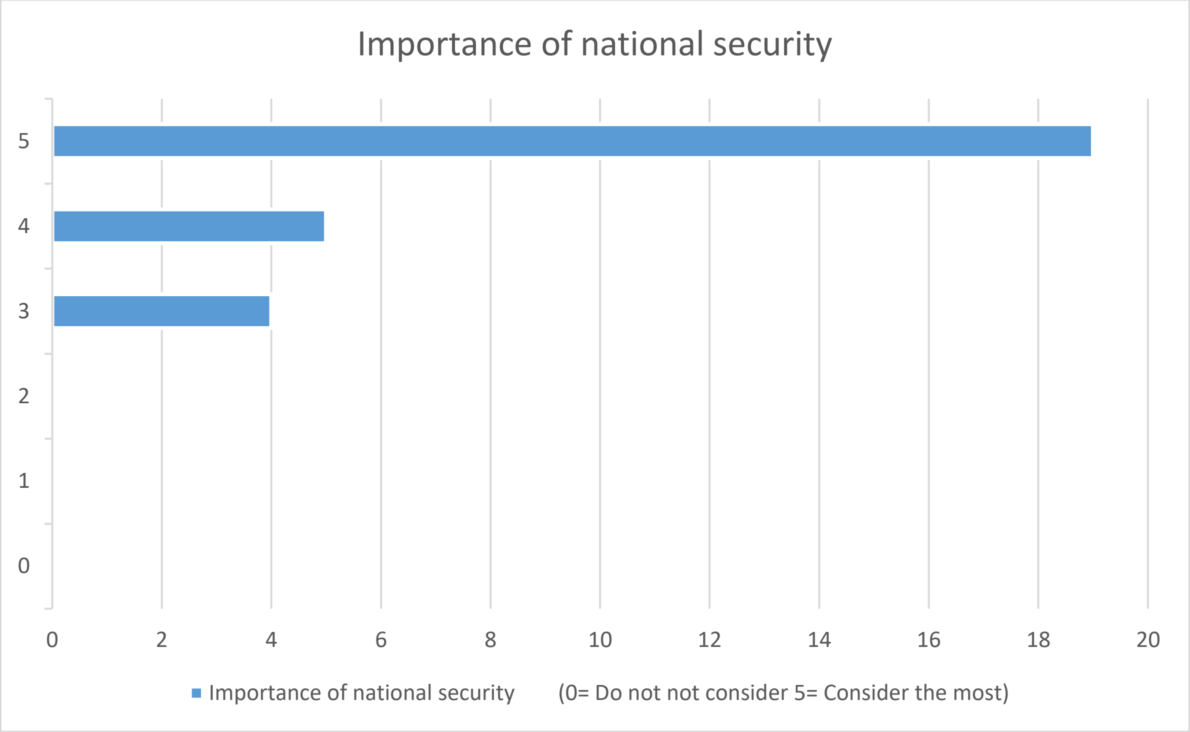


Figure D.59: Importance of national security (Female)

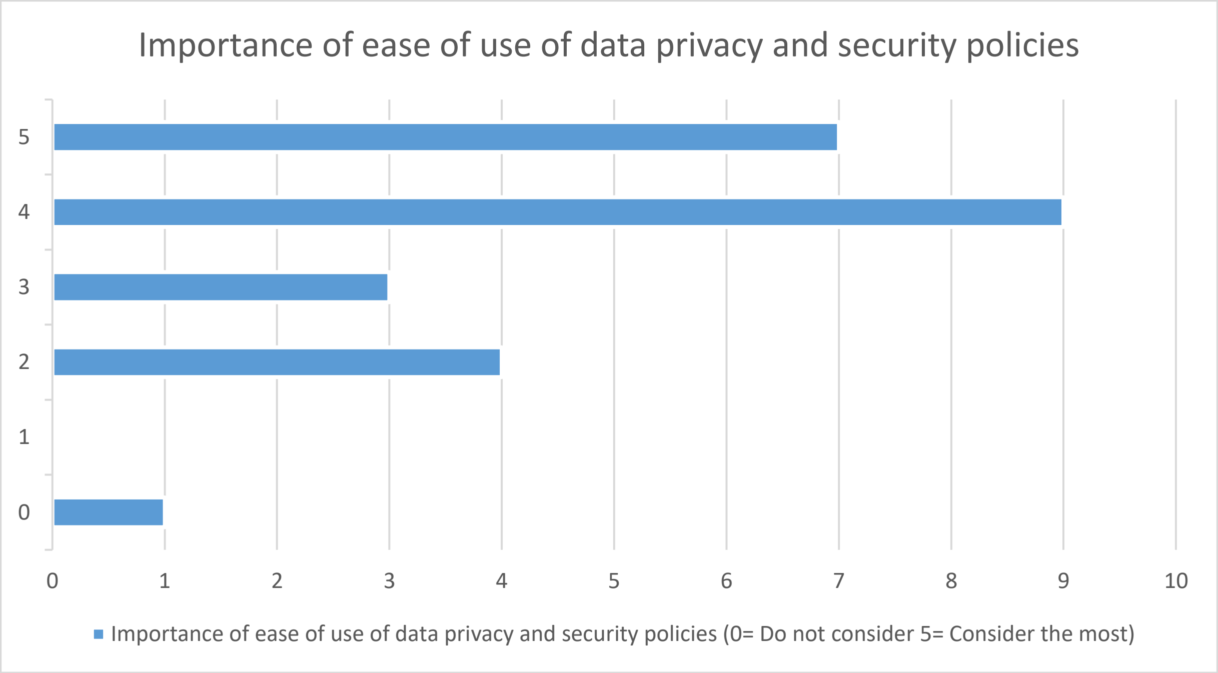


Figure D.60: Importance of ease of use of data privacy and security policies (Female)

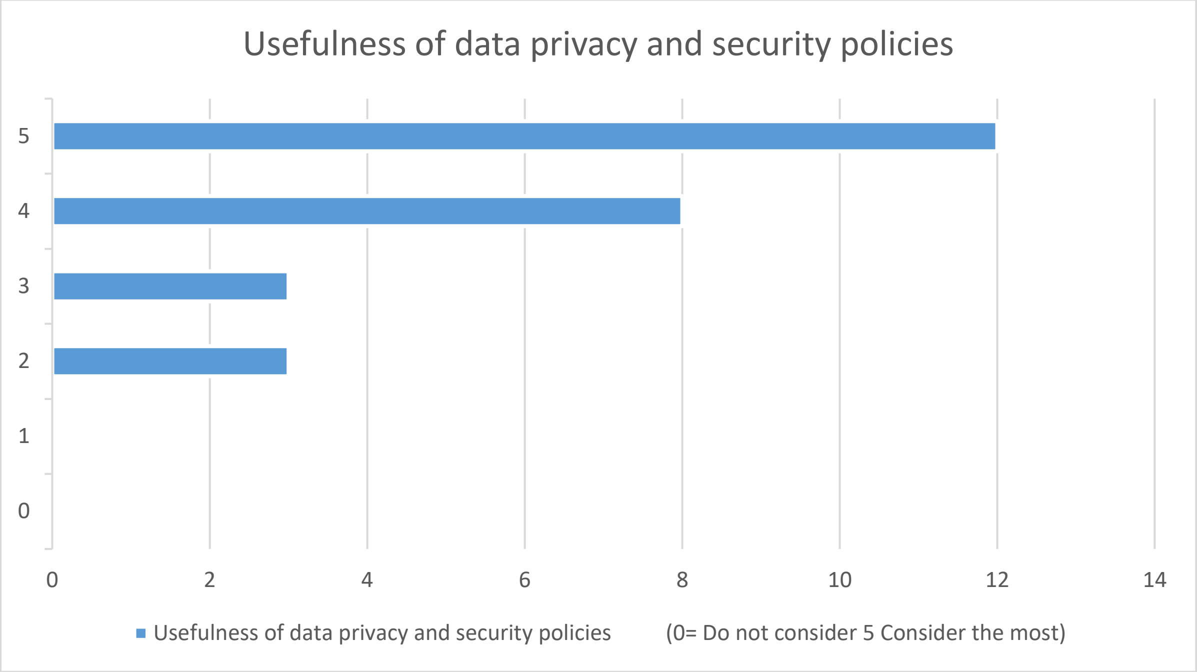


Figure 4.61: Usefulness of data privacy and security policies (Female)

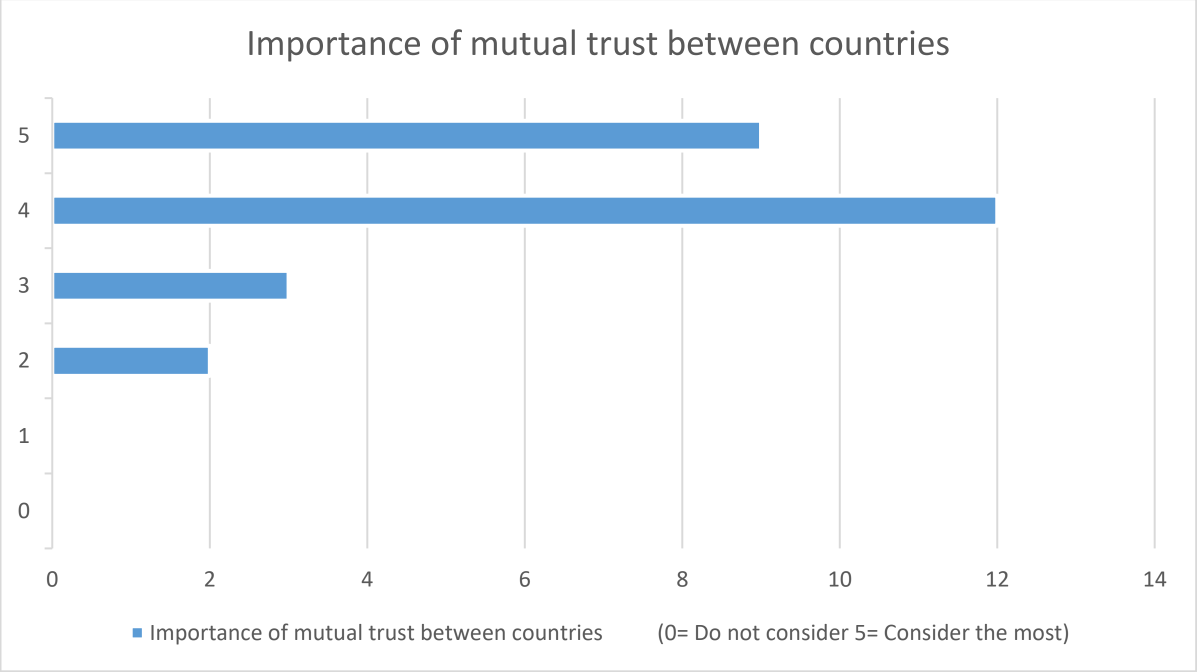


Figure 4.62 Importance of mutual trust between countries (Female)

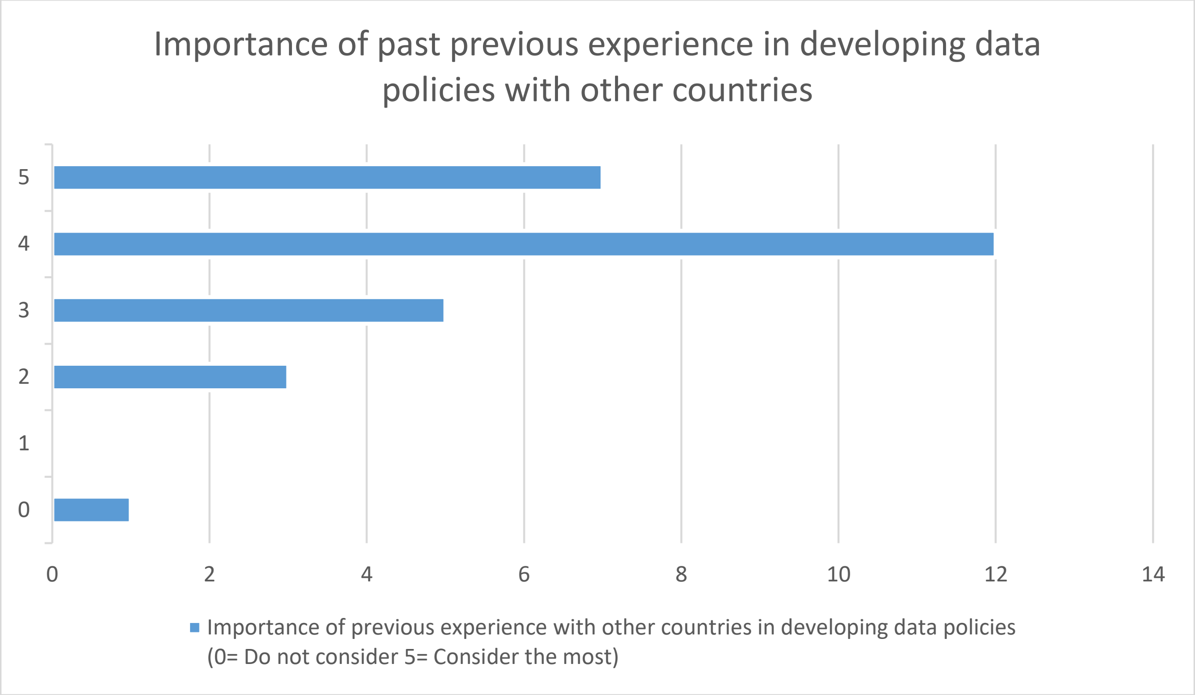


Figure 4.63: Importance of past experience in developing data policies with other counties (Female)

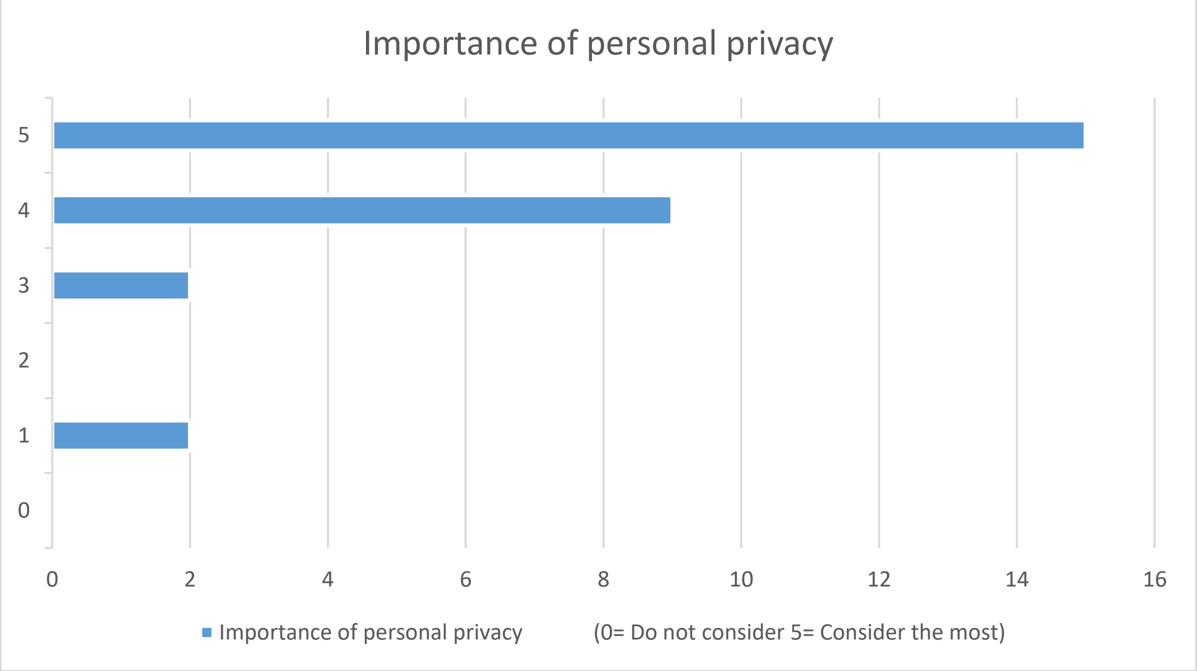


Figure 4.64: Importance of personal privacy (Female)

The message from the respondents is clear. The significance of this survey is 75 percent of the females are in support of a global level data protection mechanism (See figure D.53). The other prominent categories are organisational support, budget allocation, economical differences, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between countries previous experience in developing policies with other countries (See figure D.42-52) (See figure D.54-64)

Sri Lanka- 18-25

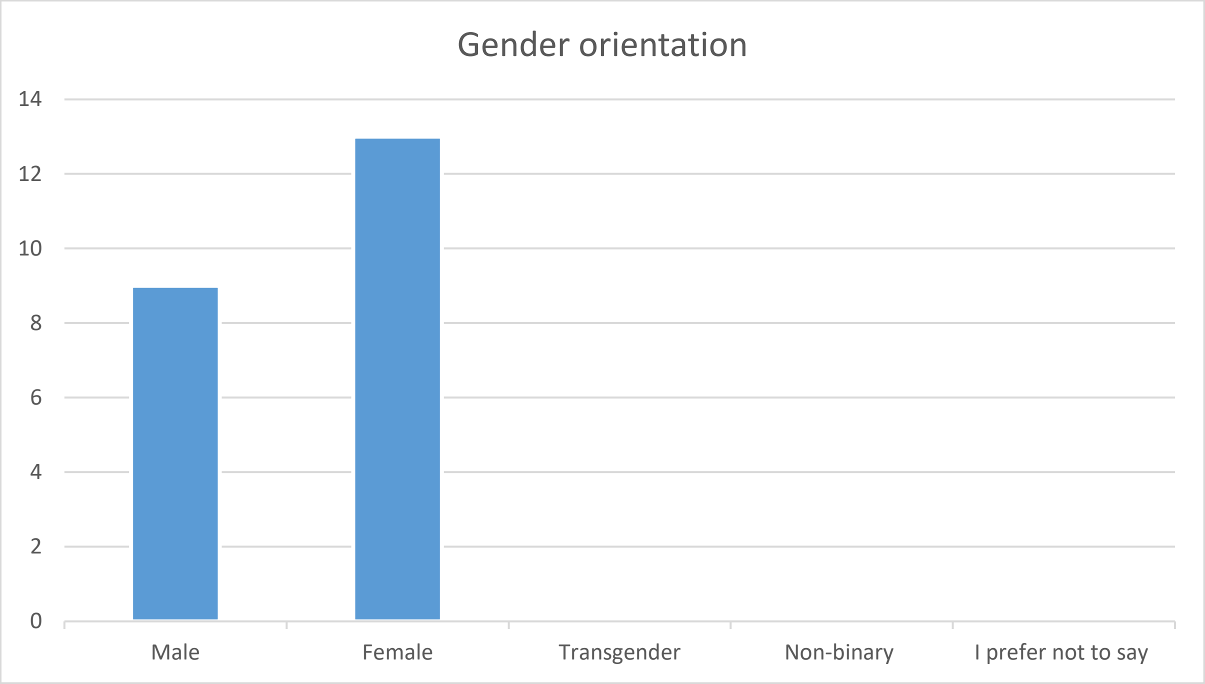


Figure D.65: Gender orientation (18-25)

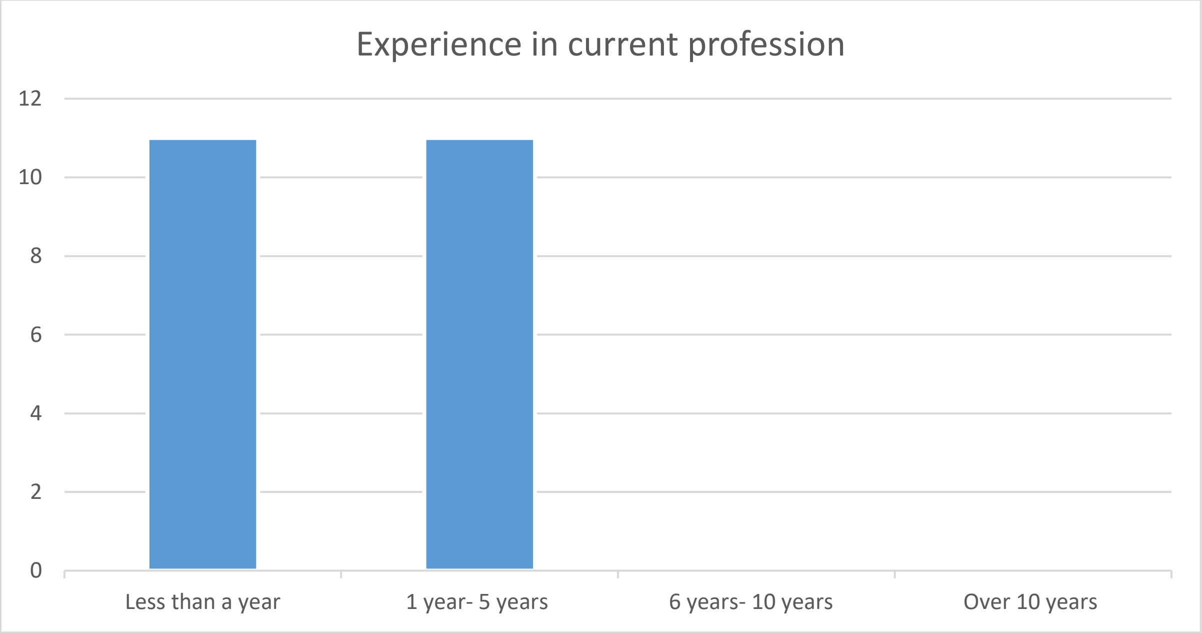


Figure D.66: Experience in current profession (18-25)

This analysis is based on the responses received from Sri Lankan participants aged 18-25. There were 22 participants, 9 males and 13 females (See figure D.65), all of them have been in employment for 5 years or less. Breaking down further, 11 out of the 22 less than a year, and the rest in the range of 1 to 5 years (See figure D.66).

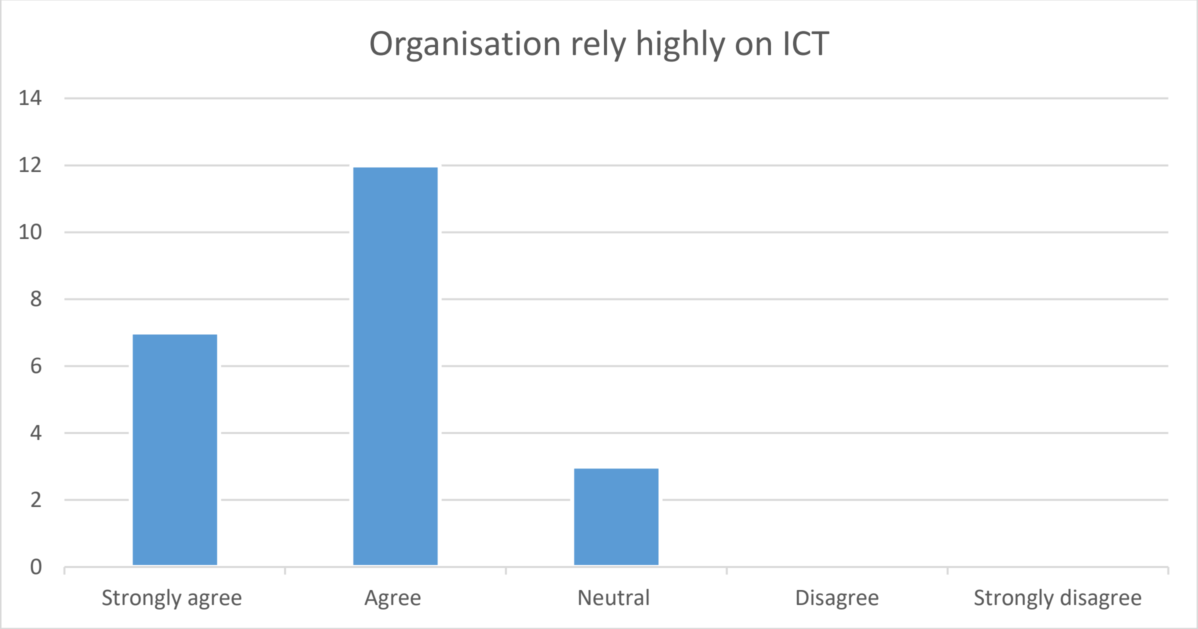


Figure D.67: Organisation rely highly on ICT (18-25)

19 out of the 22 have worked in a technology reliance working environment, 3 did not know about their working environment because of the nature of the work assigned to them (See figure D.67). This suggests that the majority of young people are dependent on technology to do their job.

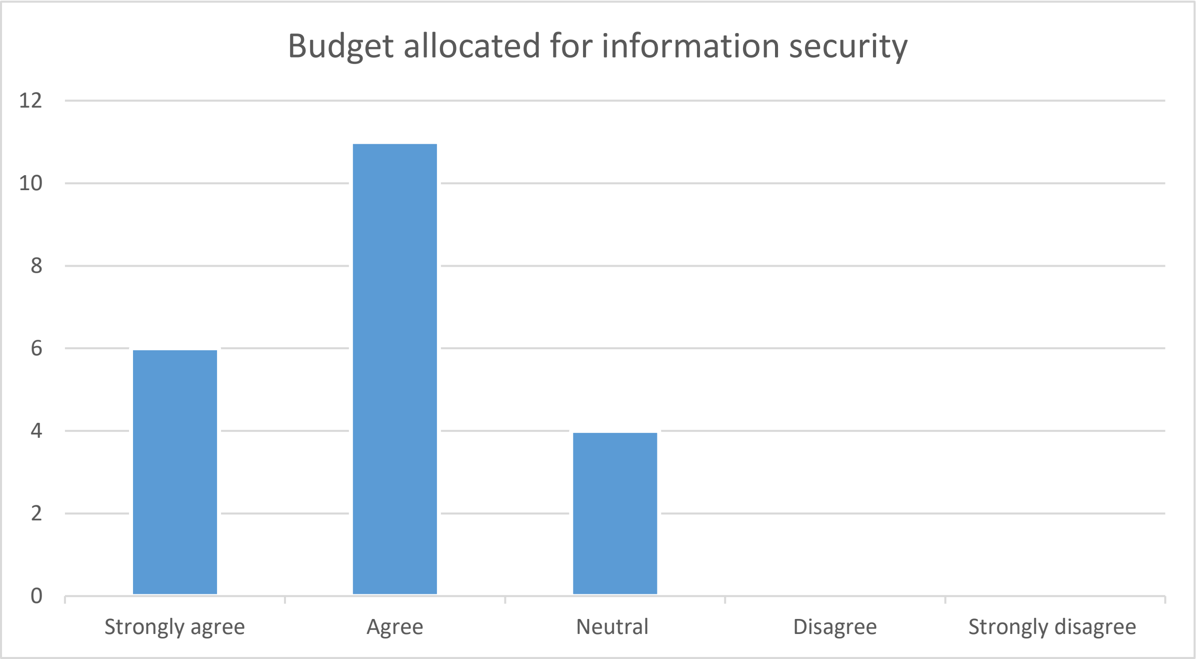


Figure D.68: Budget allocated for information security (18-25)

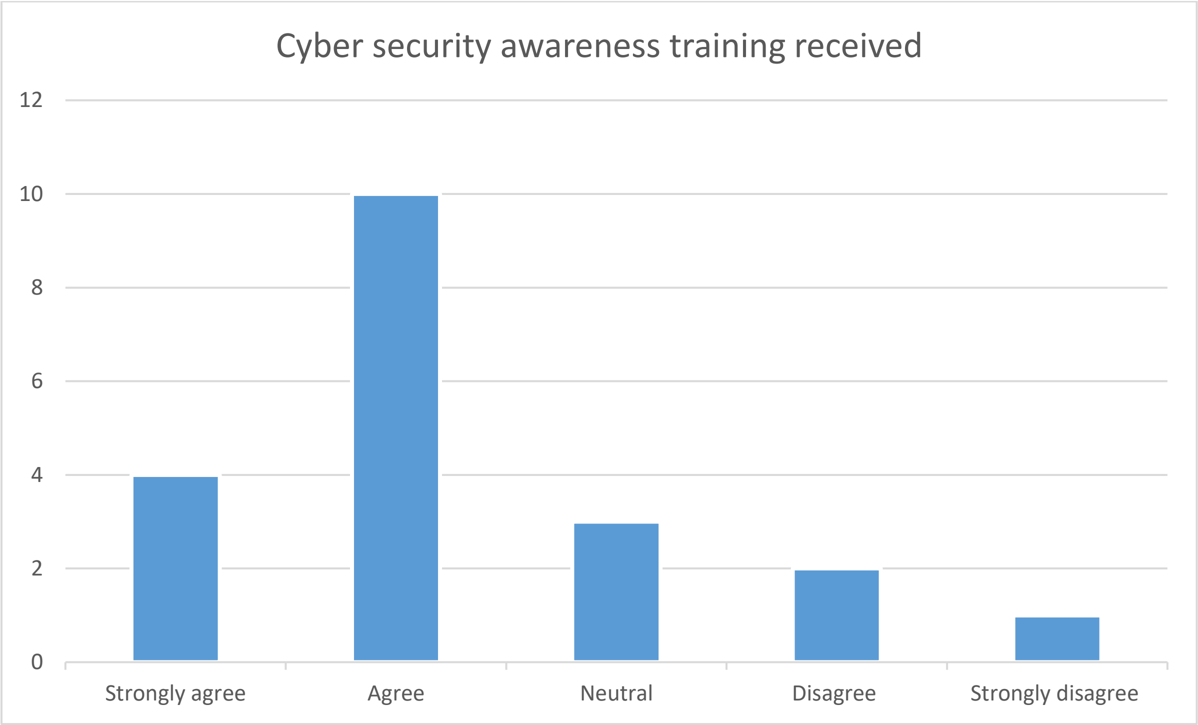


Figure D.69: Cyber security awareness training received (18-25)

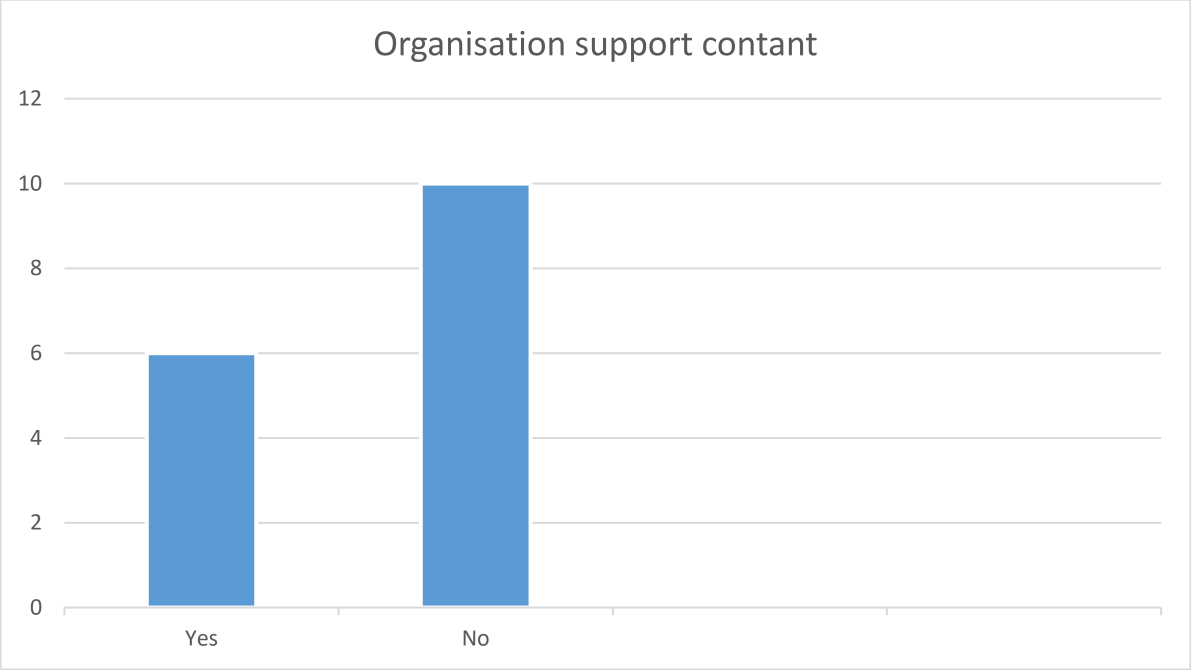


Figure D.70: Organisation support constant (18-25)

Funding has been sketchy. 17 out of the 22 have indicated that their organisations had an allocated budget for information security, whilst 4 had not expressed an opinion either way, and none disagreed (See figure D.68). Some of the participants have expressed satisfaction with the level of resources allocated for information security, and the level of regular security awareness training they received. 14 participants had received regular cybersecurity awareness training, and 3 had not received training regularly, 3 neither agreed nor disagreed with the question (See figure D.69). Significantly, 10 participants had not received support from the organisation to protect personal information and only 6 had support (See figure D.70). That suggests that the organisations did allocate funds for information security, although the level of training provided was satisfactory, the organisation support for the protection of personal information was low despite the high reliance on technology. These disparities can be seen as lack of emphasis on privacy training at the institutional level, in which case the onus will rest on them to outline their plans for addressing privacy protection necessities.

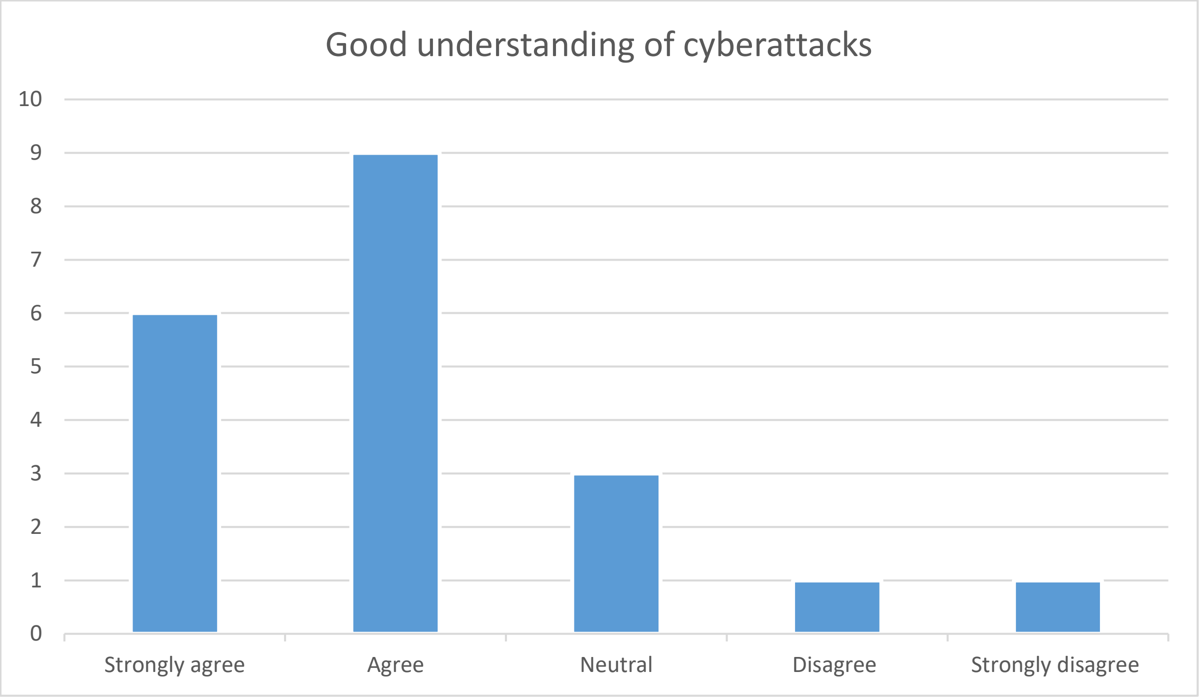


Figure D.71: Good understanding of cyberattacks (18-25)

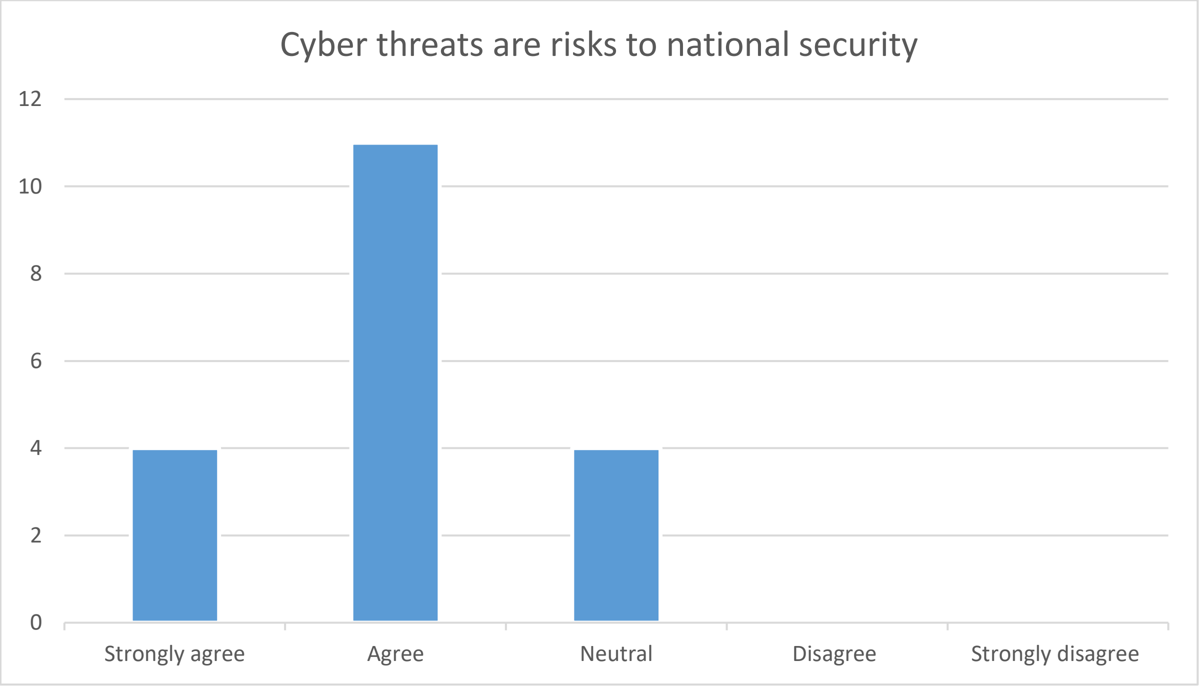


Figure D.72: Cyber threats are risks to national security (18-25)

The participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 15 participants do have, 3 have not expressed opinion either way, and only 2 participants had no understanding (See figure D.71). Furthermore, 68 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure D.72). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional, and global level mechanism.

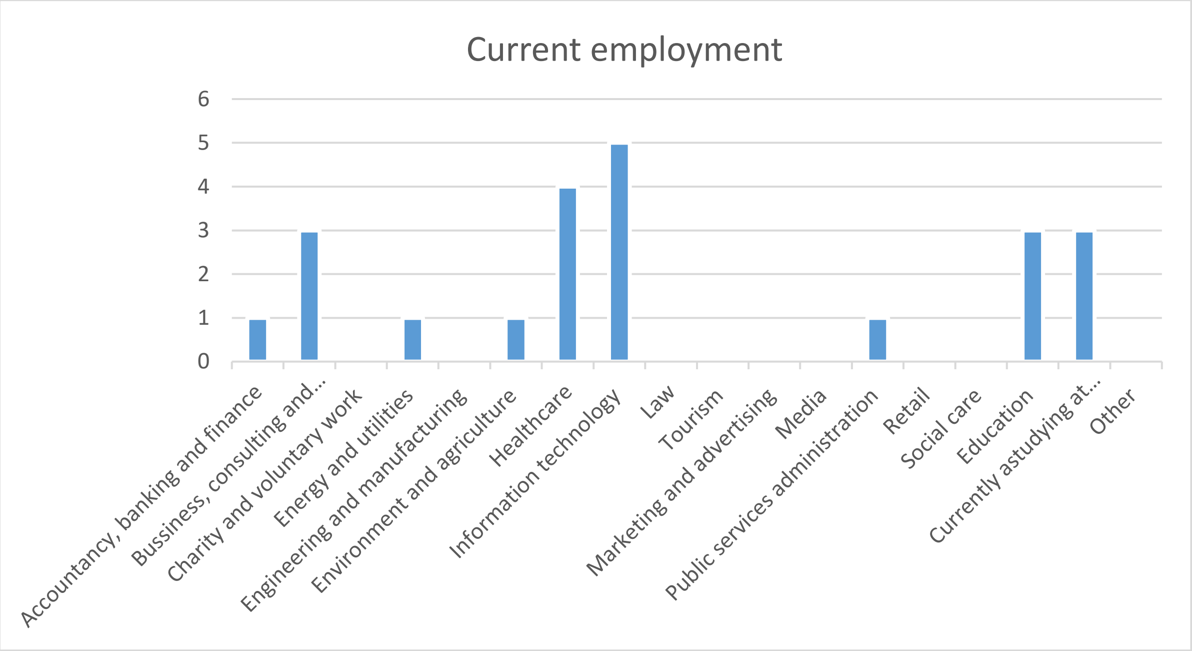


Figure D.73: Current employment (18-25)

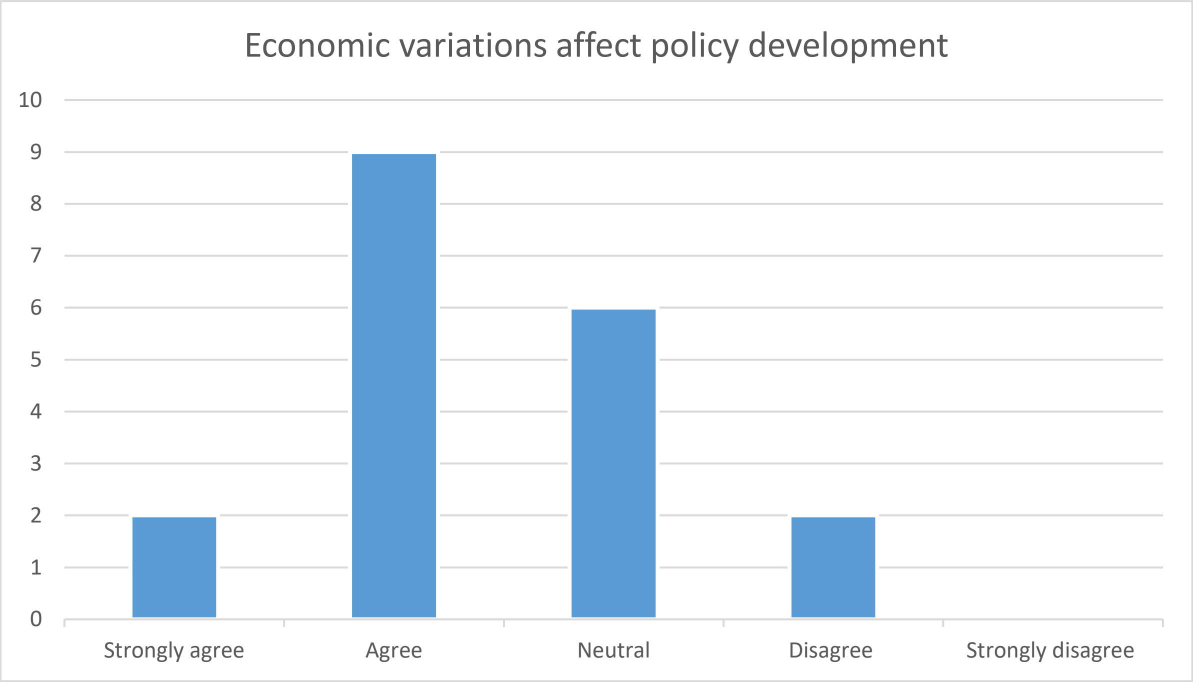


Figure D.74: Economic variations affect policy development (18-25)

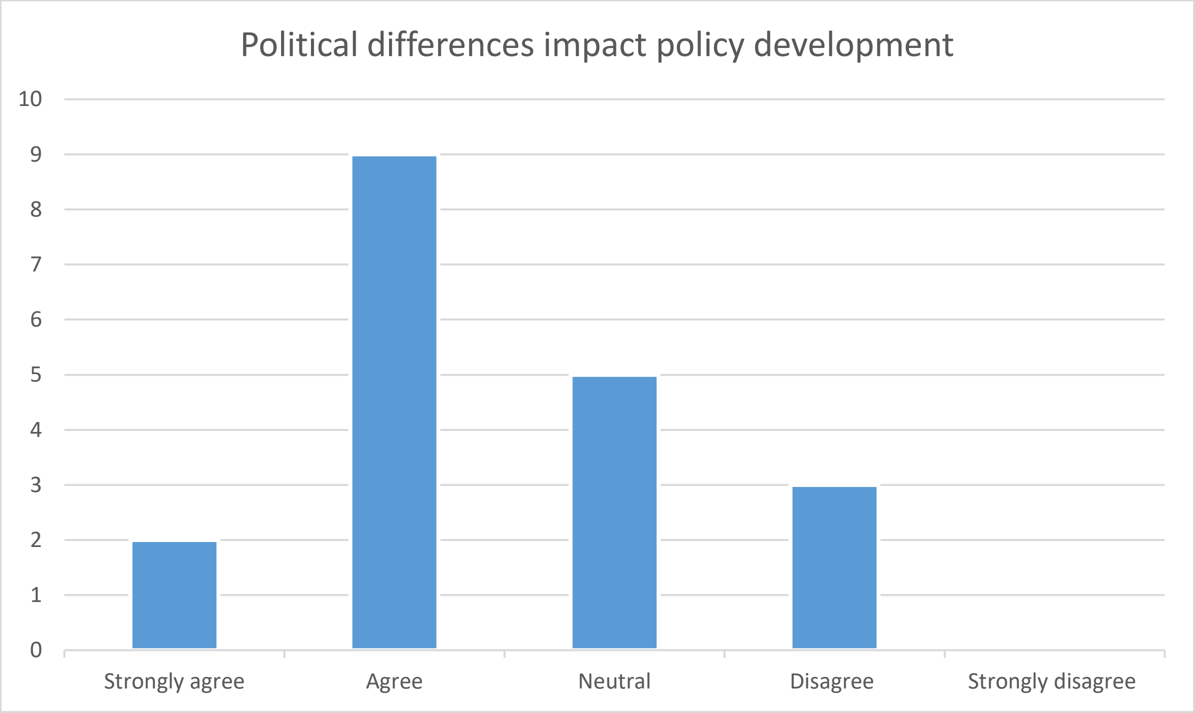


Figure D.75: Political differences impact policy development (18-25)

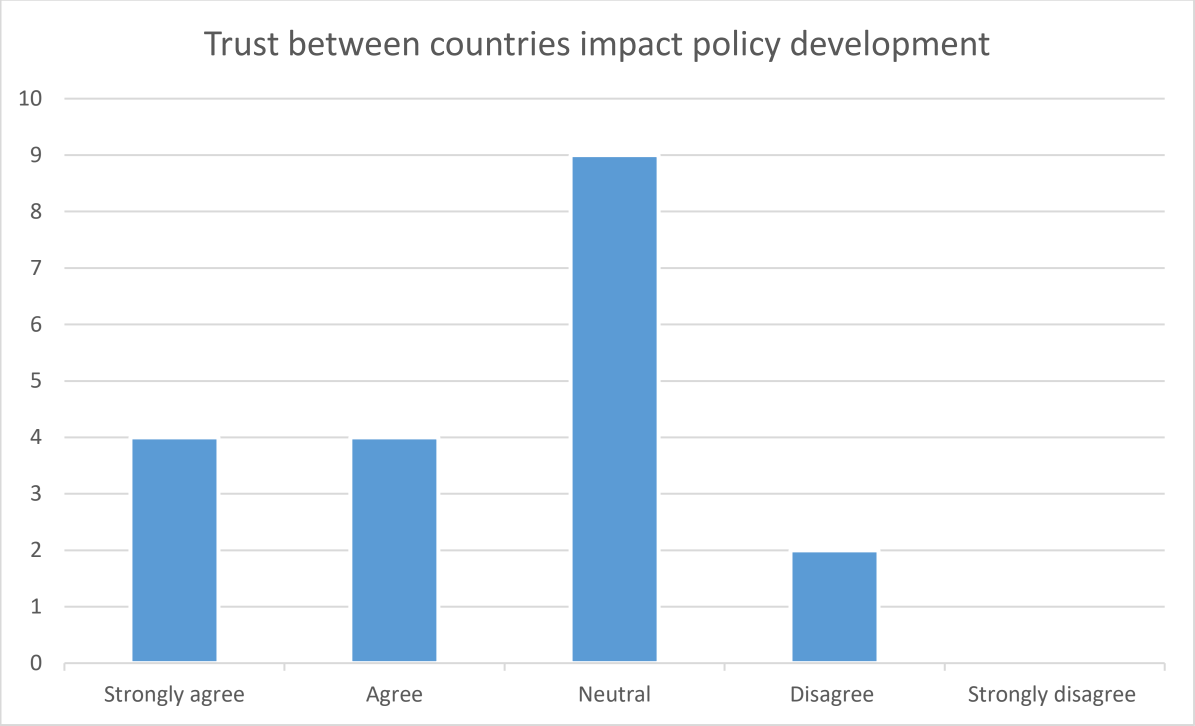


Figure D.76: Trust between countries impact policy development (18-25)

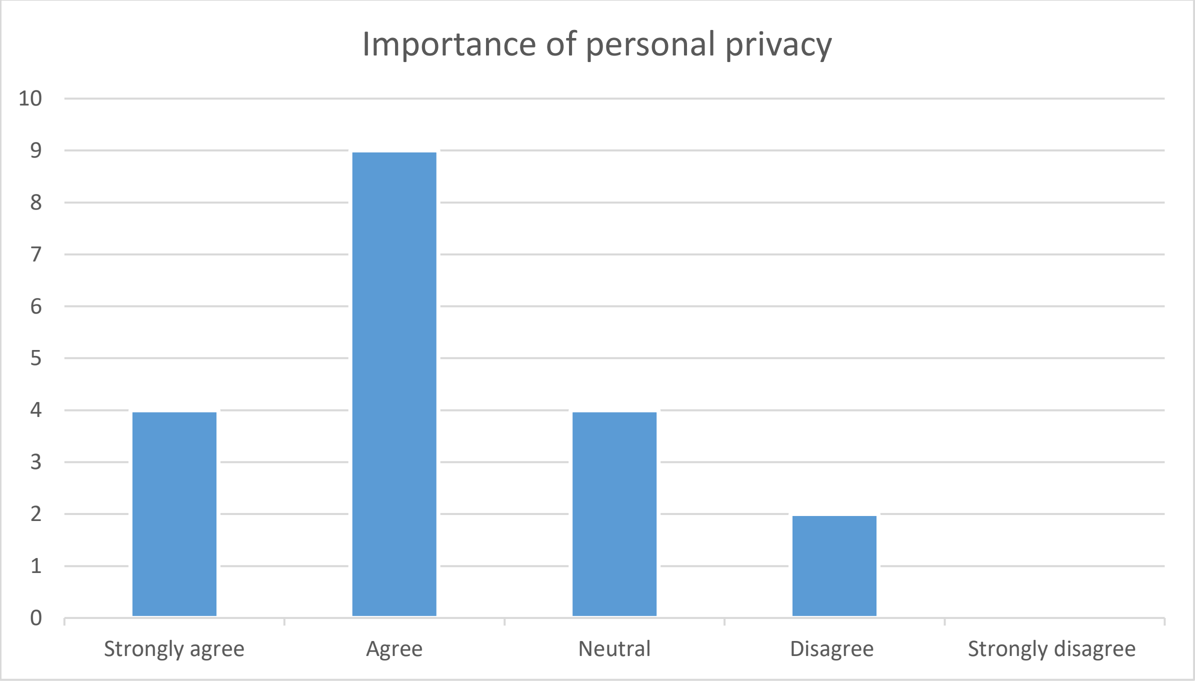


Figure D.77: Importance of personal privacy (18-25)

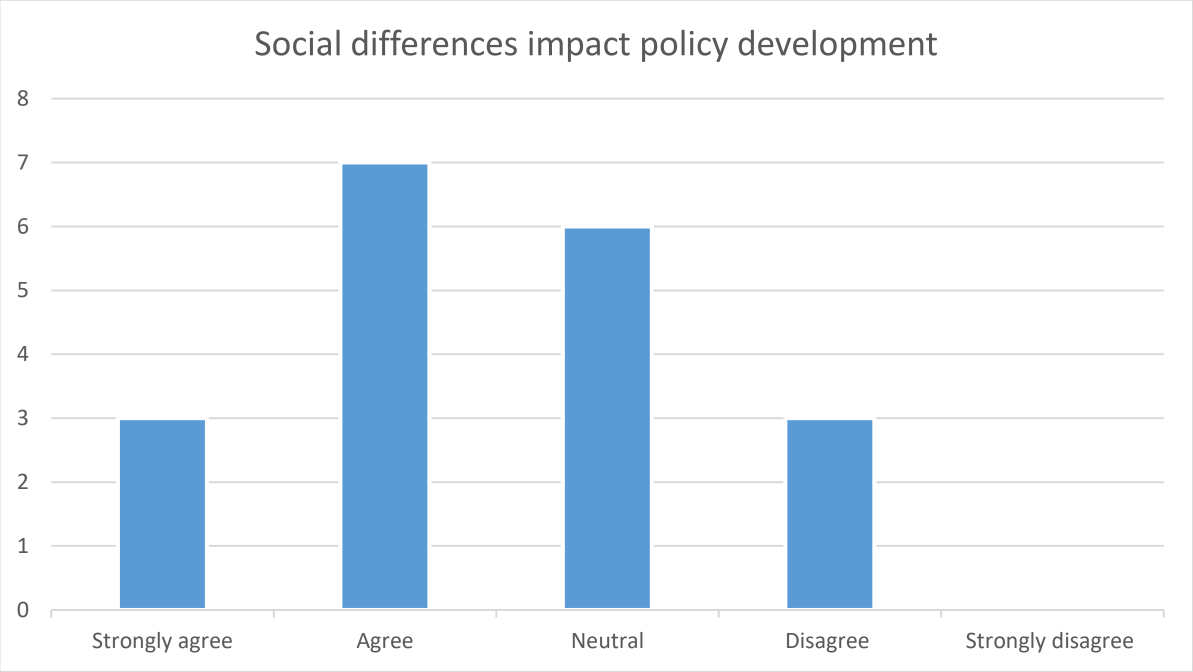


Figure D.78: Social differences impact policy development (18-25)

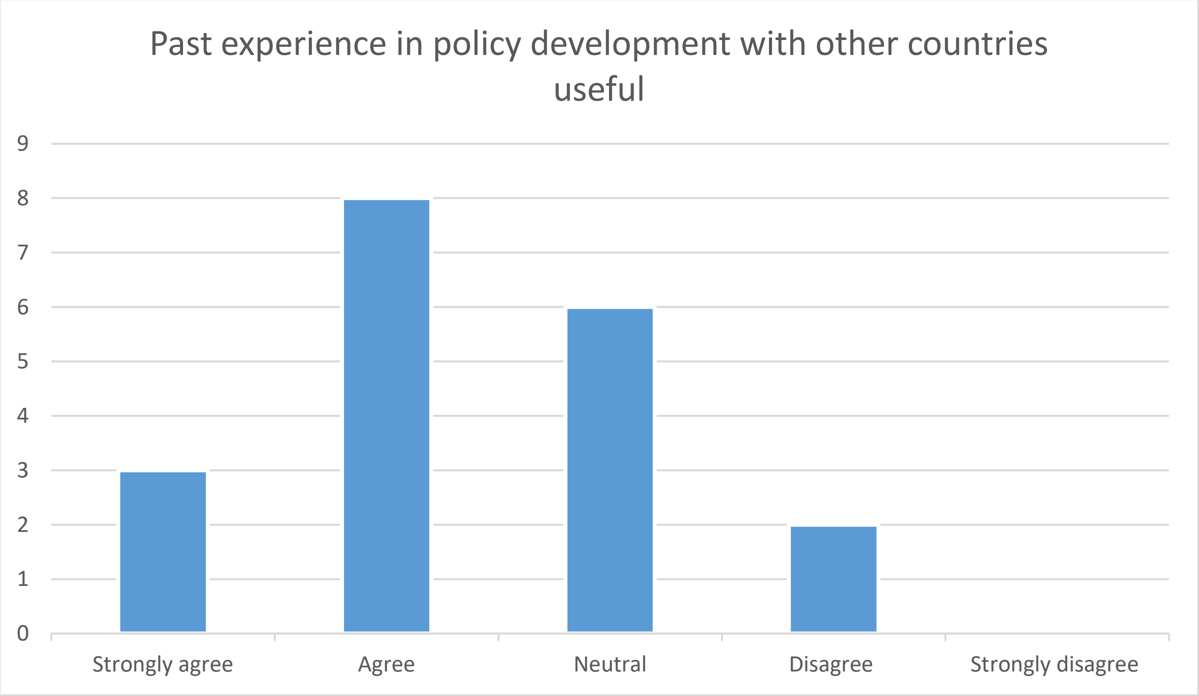


Figure D.79: Past experience in policy development with other countries useful (18-25)

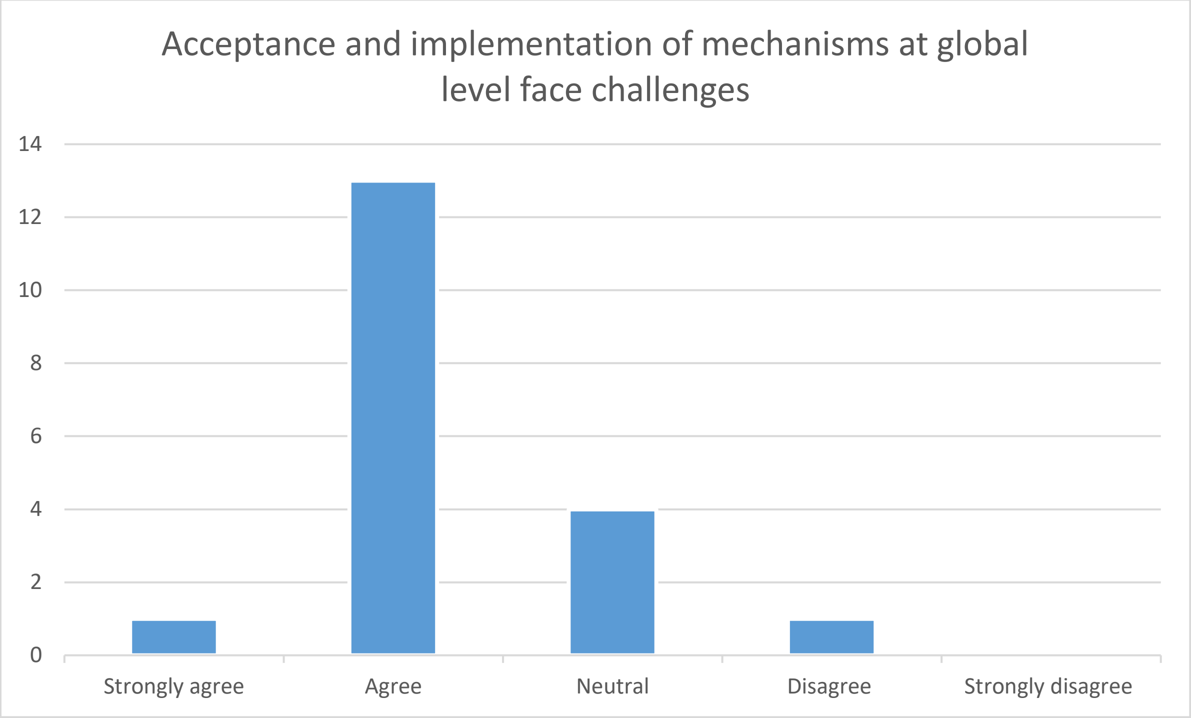


Figure D.80: Acceptance and implementation of mechanisms at global level face challenges (18-25)

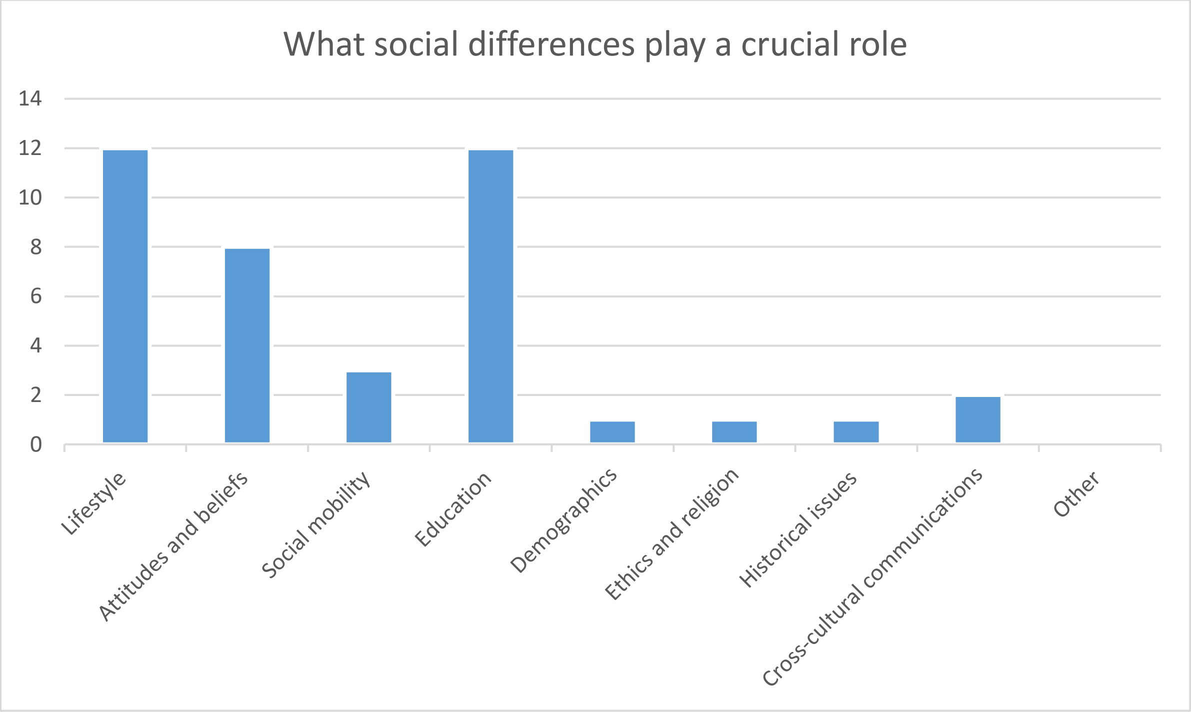


Figure D.81: What social differences play a crucial role (18-25)

The response to the social differences listed in the questionnaire, majority have highlighted the importance of both education and lifestyle (See figure D.81). It becomes clear that educational training can be an effective way to make people understand the importance of privacy and the implications associated with privacy violations. People will have to make a crucial choice in their lifestyles when considering reliance on technology at the workplace. If there is a high reliance on technology in sharing or handling personal information, the demand for accepting and implementing policies associated with data privacy and security also should be high. Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at organisational level.

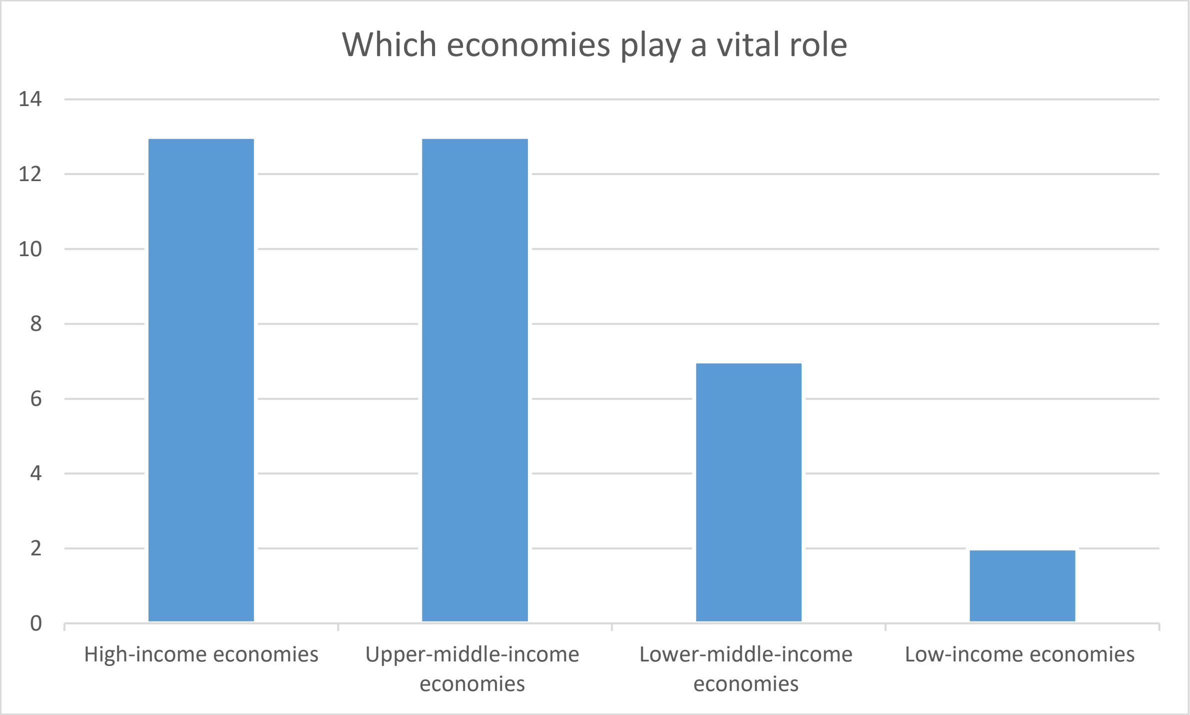


Figure D.82: Which economies play a vital role (18-25)

In the questionnaire, majority has stated that both the high income and upper-middle-income countries play a vital role (See figure D.82). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

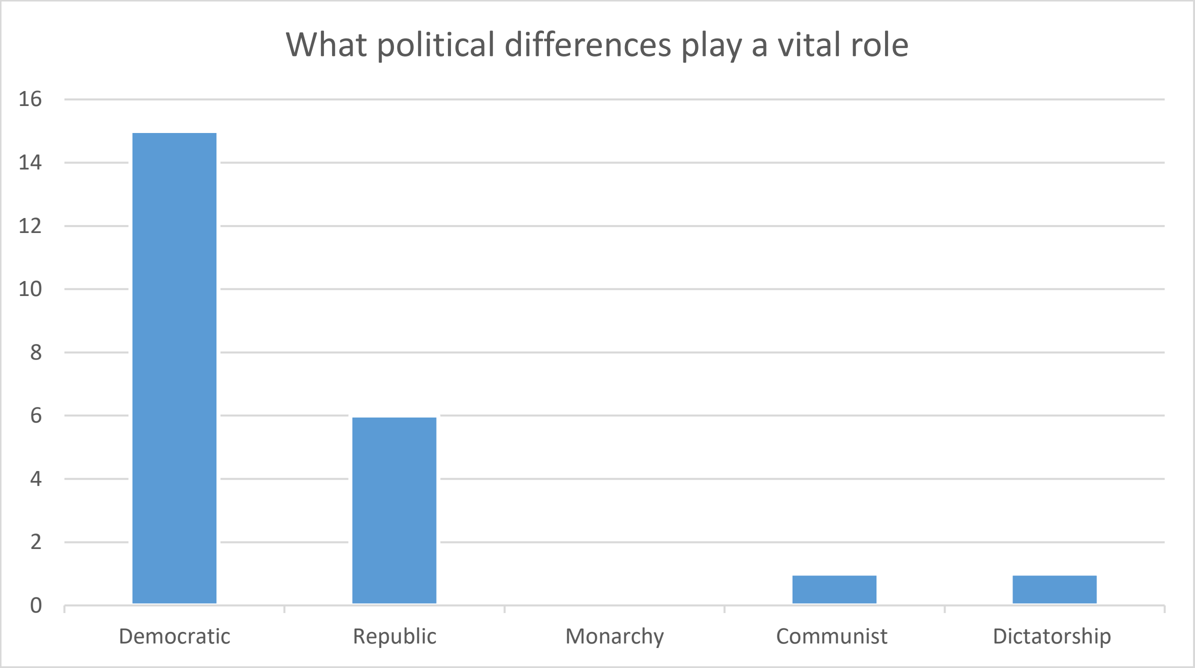


Figure D.83: What political differences play a vital role (18-25)

The majority have chosen democratic political system (See figure D.83), in preference to others as because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

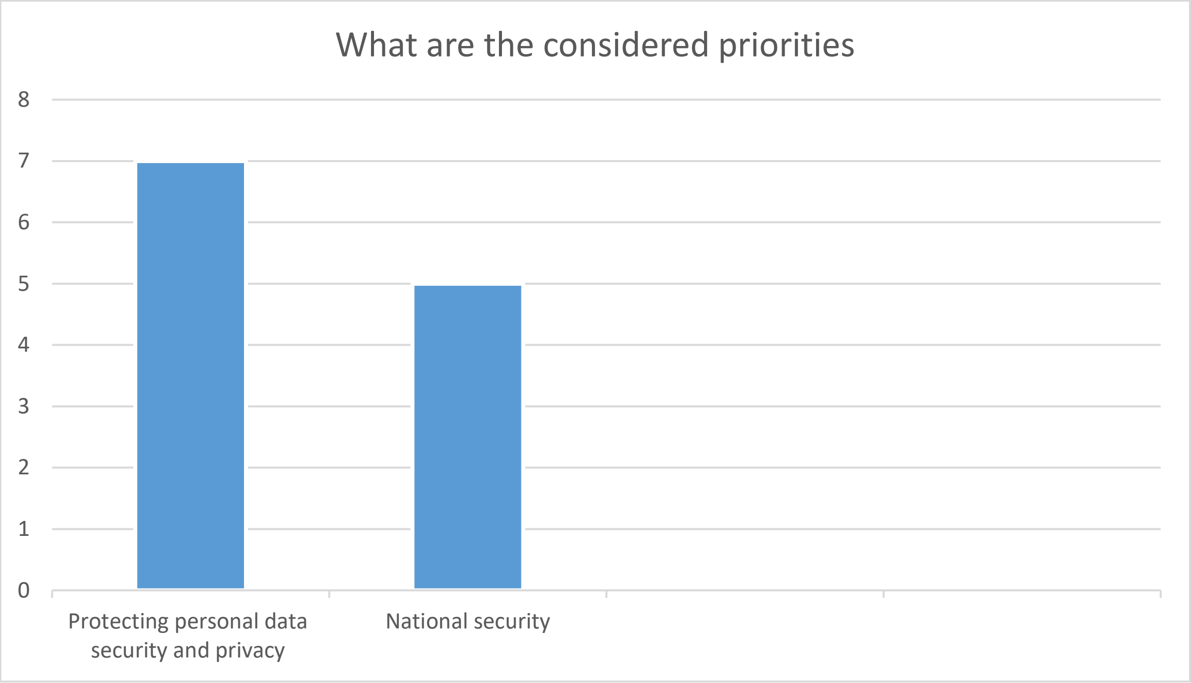


Figure D.84: What are the considered priorities (18-25)

In accepting and implementing a global framework of data privacy and security policies, the participants have not highlighted the importance of protecting personal data security and privacy, and national security to a satisfactory level, but they have not ignored their importance (See figure D.84). However, in an incident of a personal data breach, there will potentially be a knock-on effect on both personal data security and privacy, and national security, and it will also be felt right across the groups as well as the community alike.

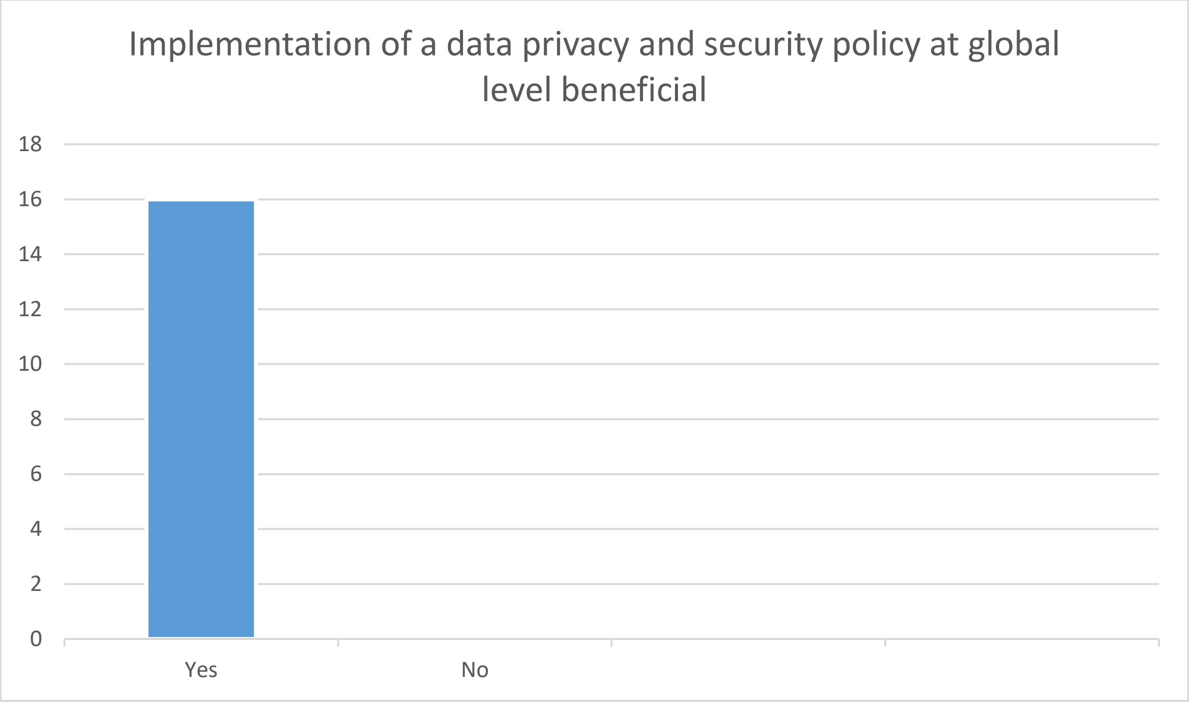


Figure D.85: Implementation of a data privacy and security policy at global level beneficial (18-25)

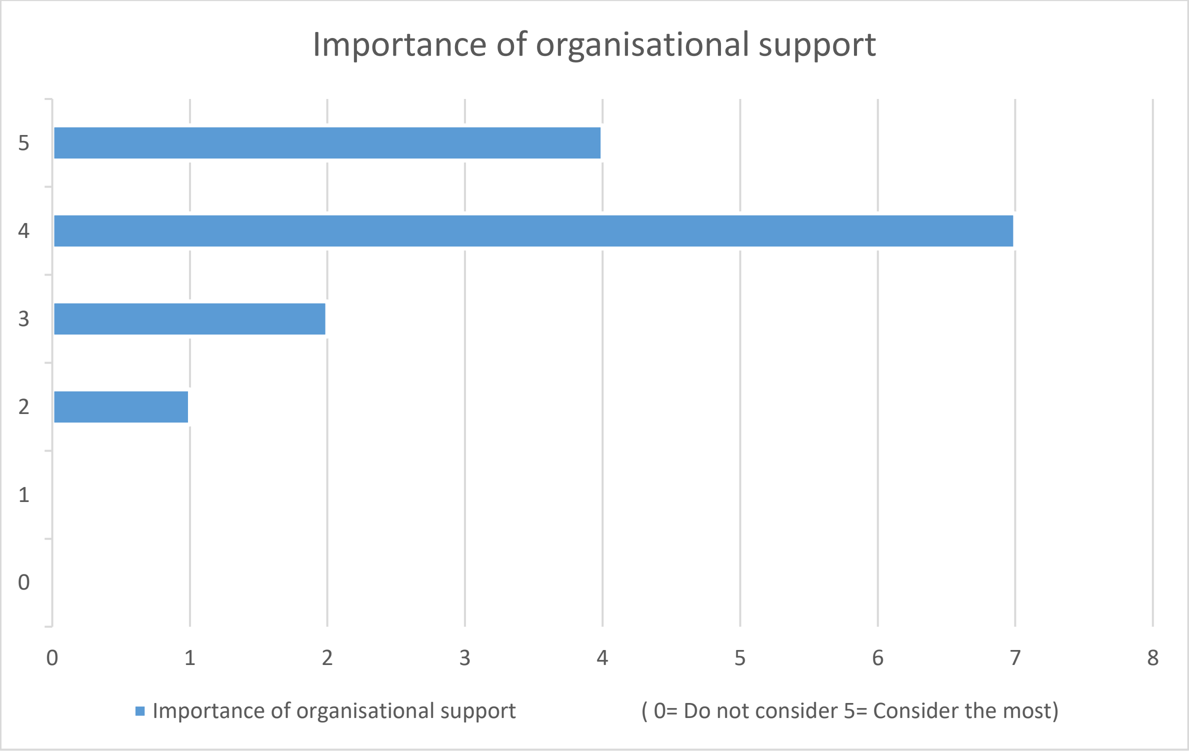


Figure D.86: Importance of organisational support (18-25)

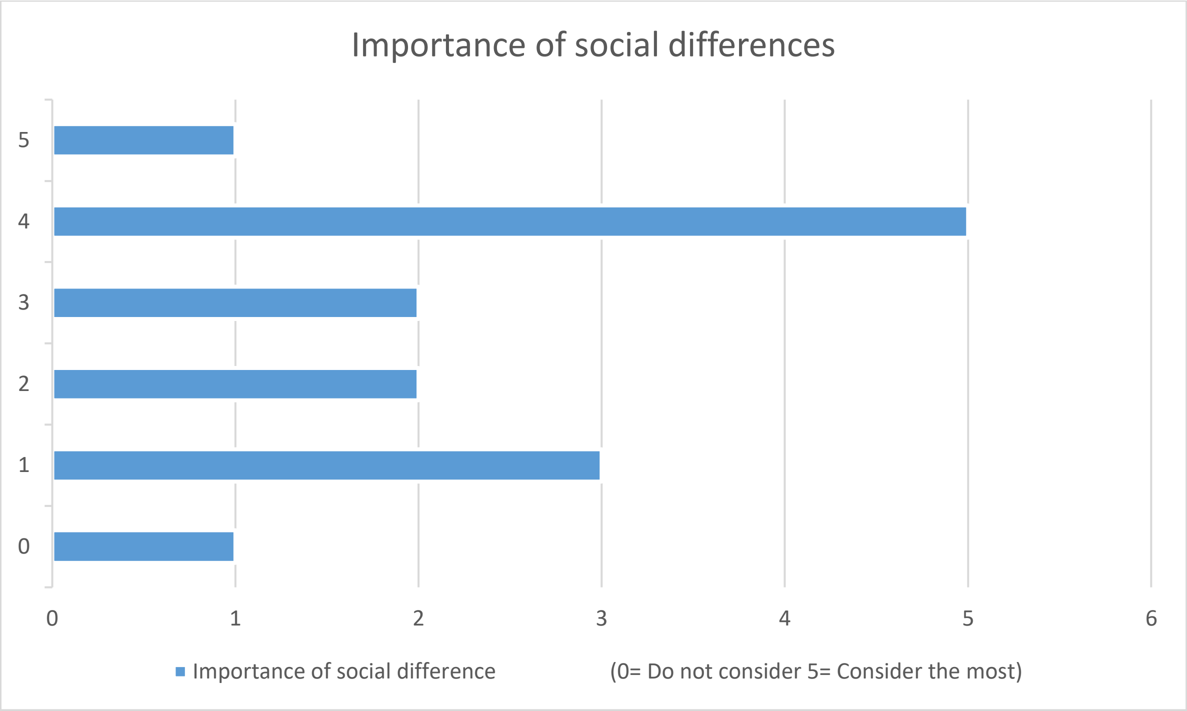


Figure D.87: Importance of social differences (18-25)

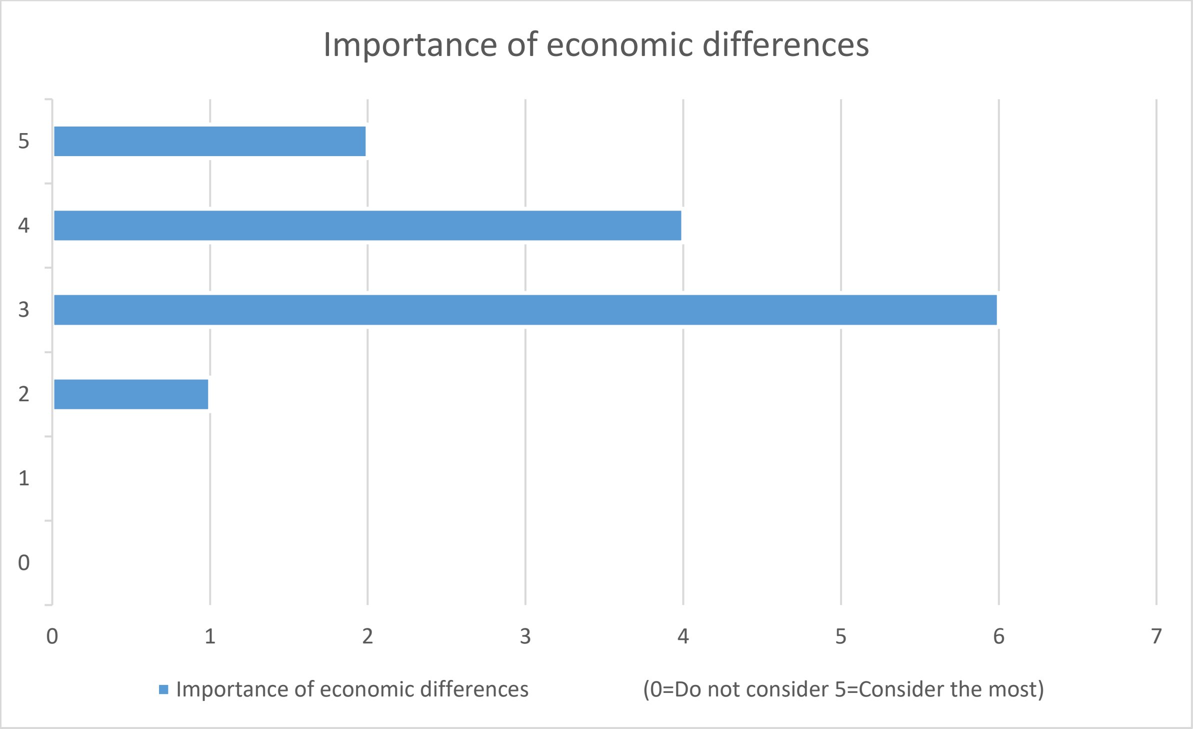


Figure D.88: Importance of economic differences (18-25)

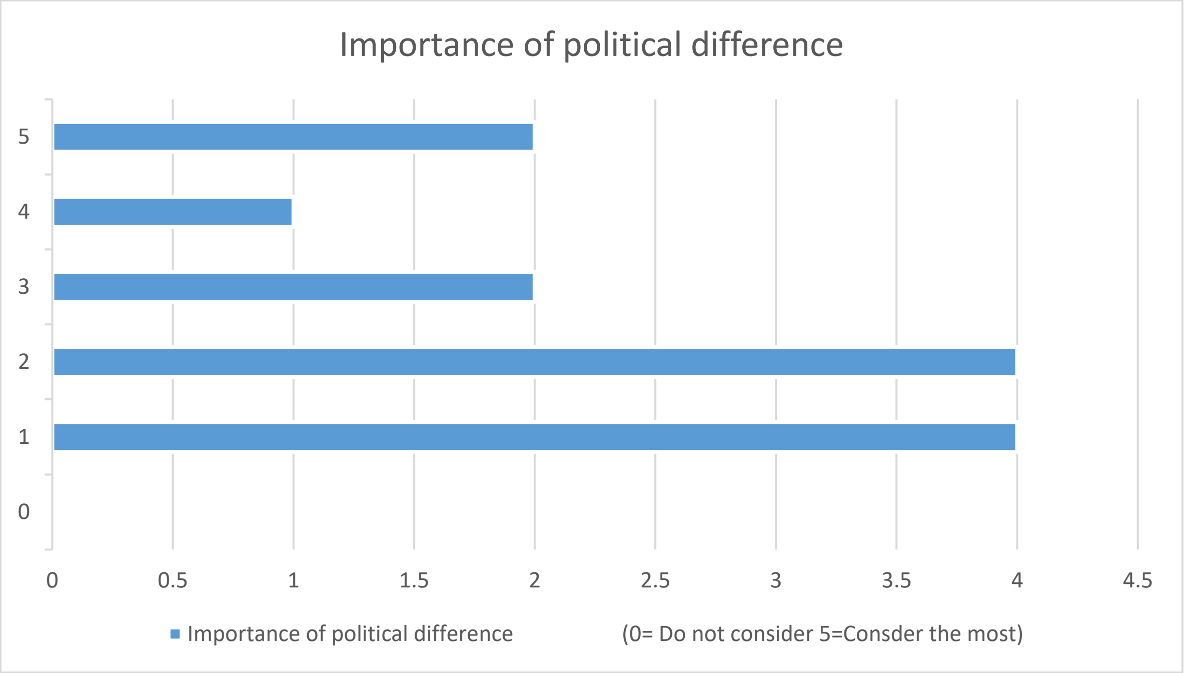


Figure D.89: Importance of political difference (18-25)

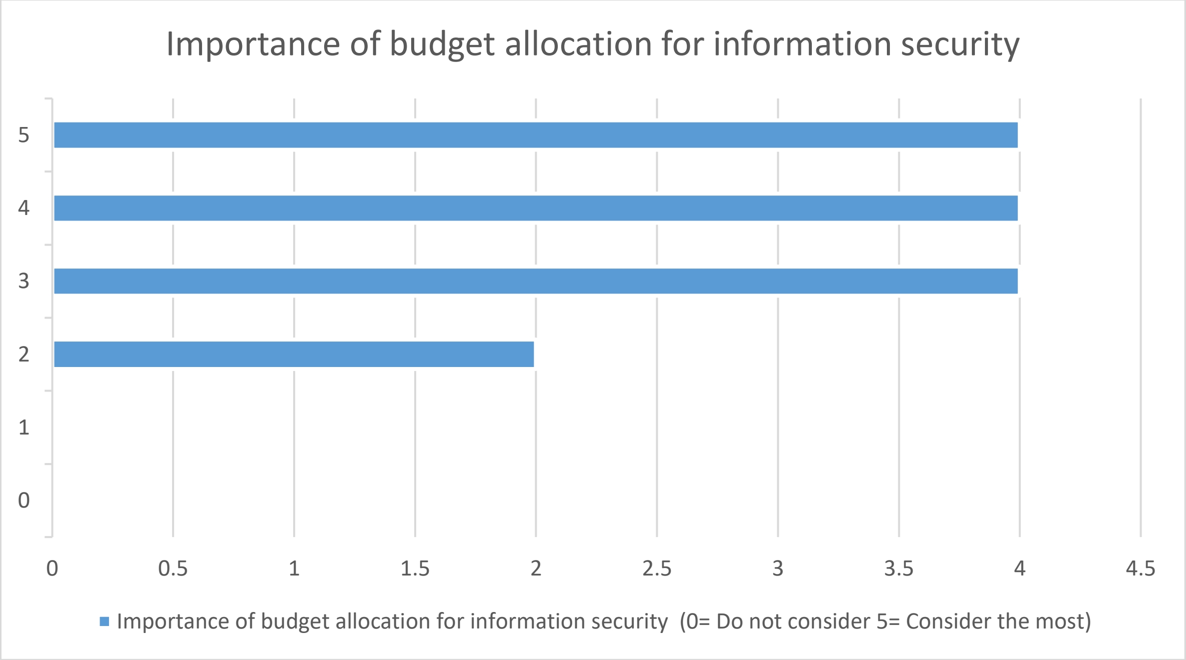


Figure D.90: Importance of budget allocation for information security (18-25)

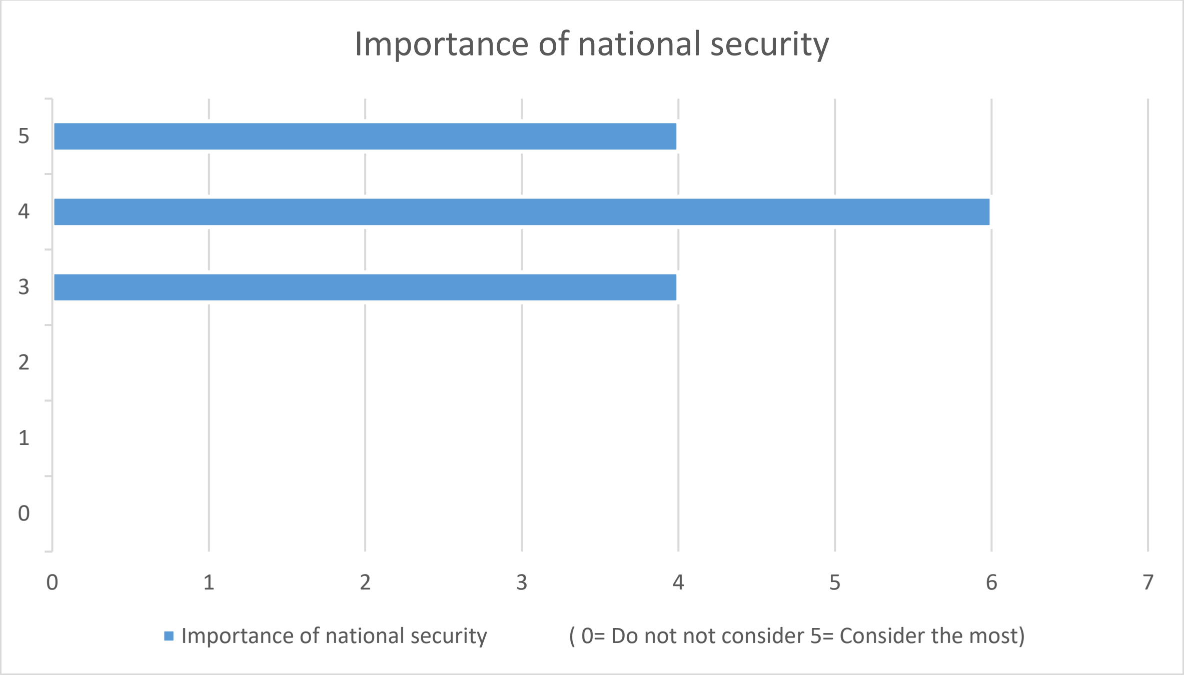


Figure D.91: Importance of national security (18-25)

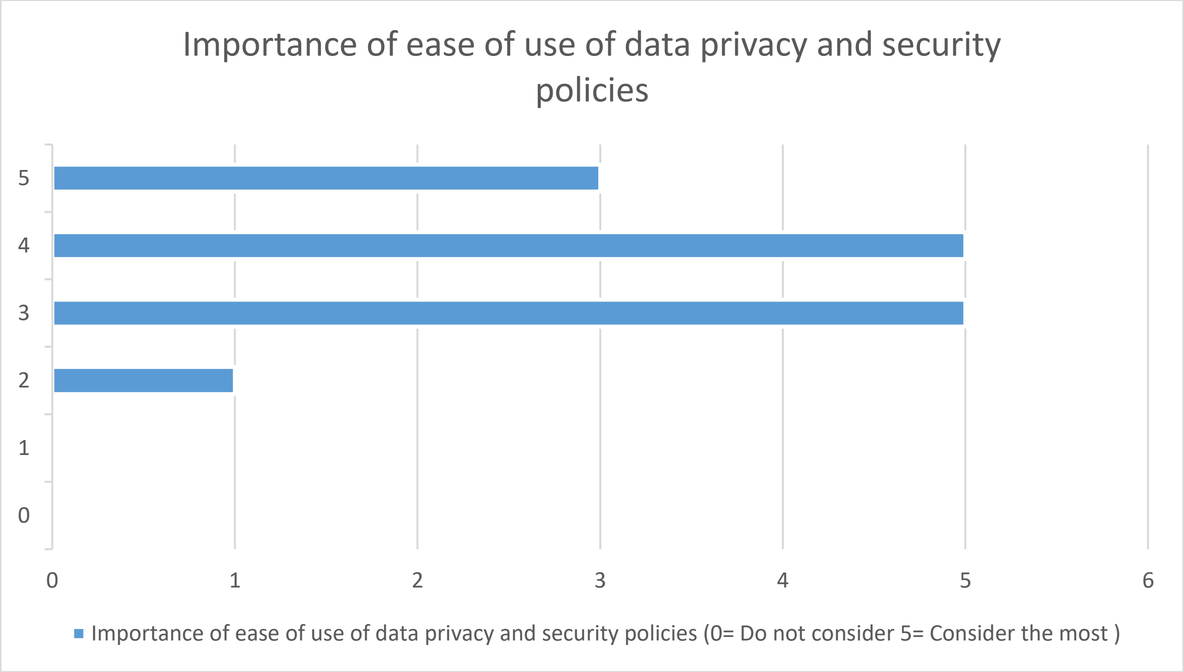


Figure D.92: Importance of ease of use of data privacy and security policies (18-25)

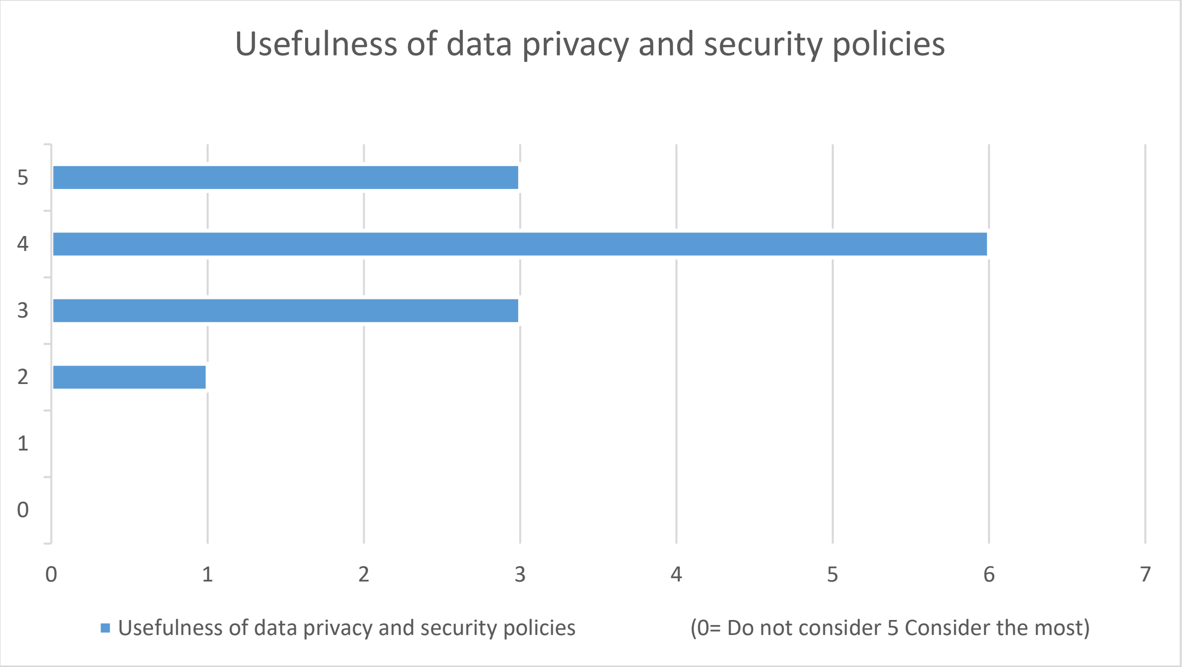


Figure D.93: Usefulness of data privacy and security policies (18-25)

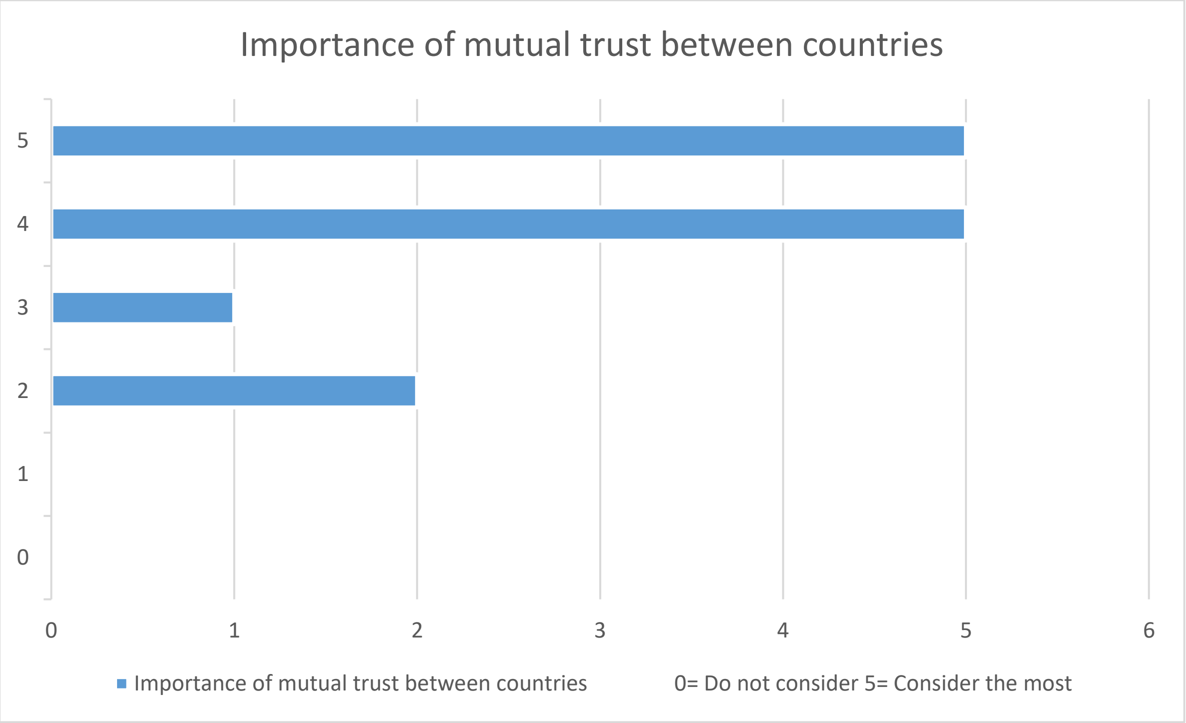


Figure D.94: Importance of mutual trust between countries (18-25)

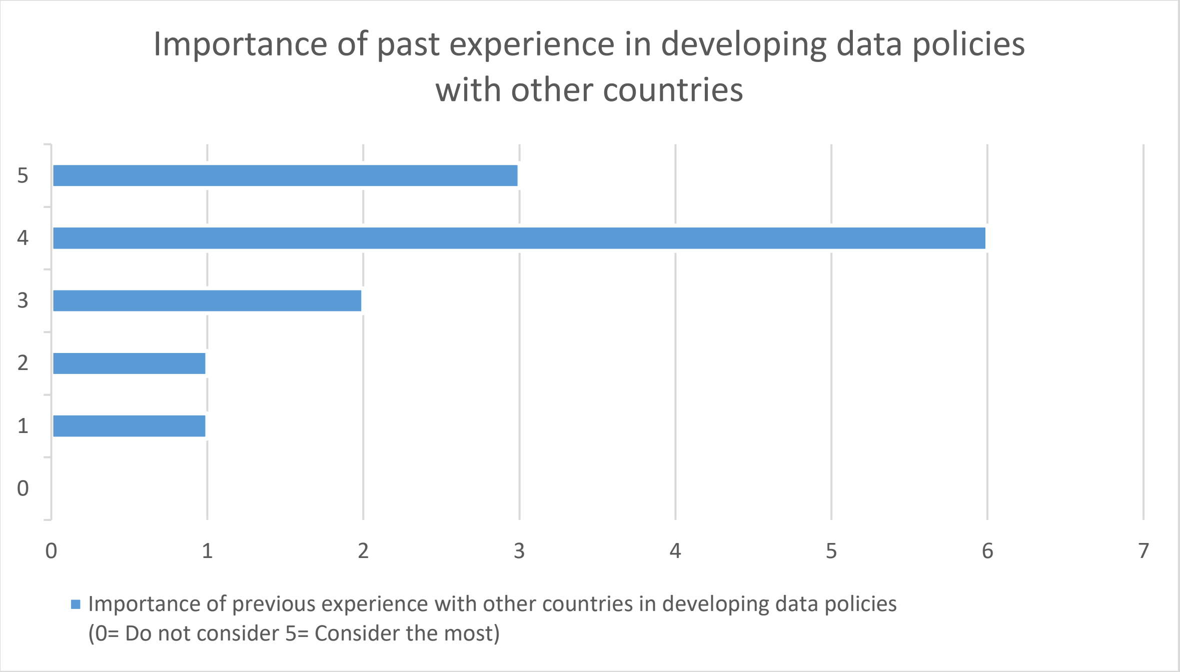


Figure D.95: Importance of past experience in developing data policies with other counties (18-25)

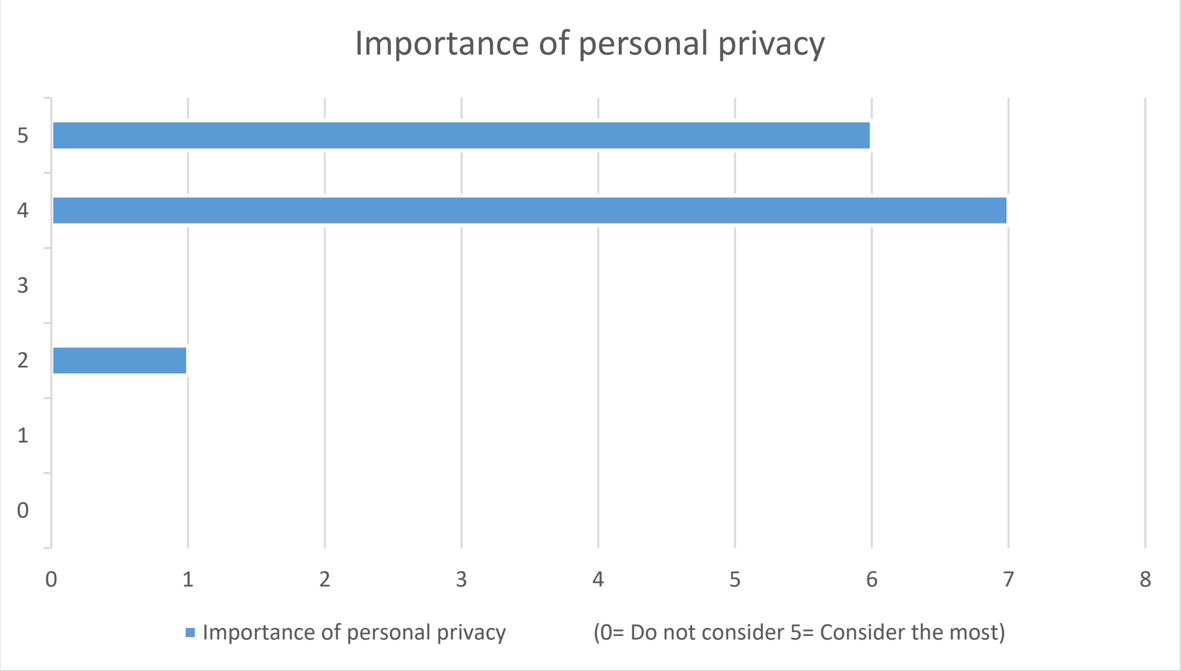


Figure D.96: Importance of personal privacy (18-25)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 75 percent of the respondents have endorsed (See figure D.85). The other notable factors that have come out of the survey are organisational support, budget allocation for information security, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure D.74-84) (See figure D.86-96)

Sri Lanka- 26-35

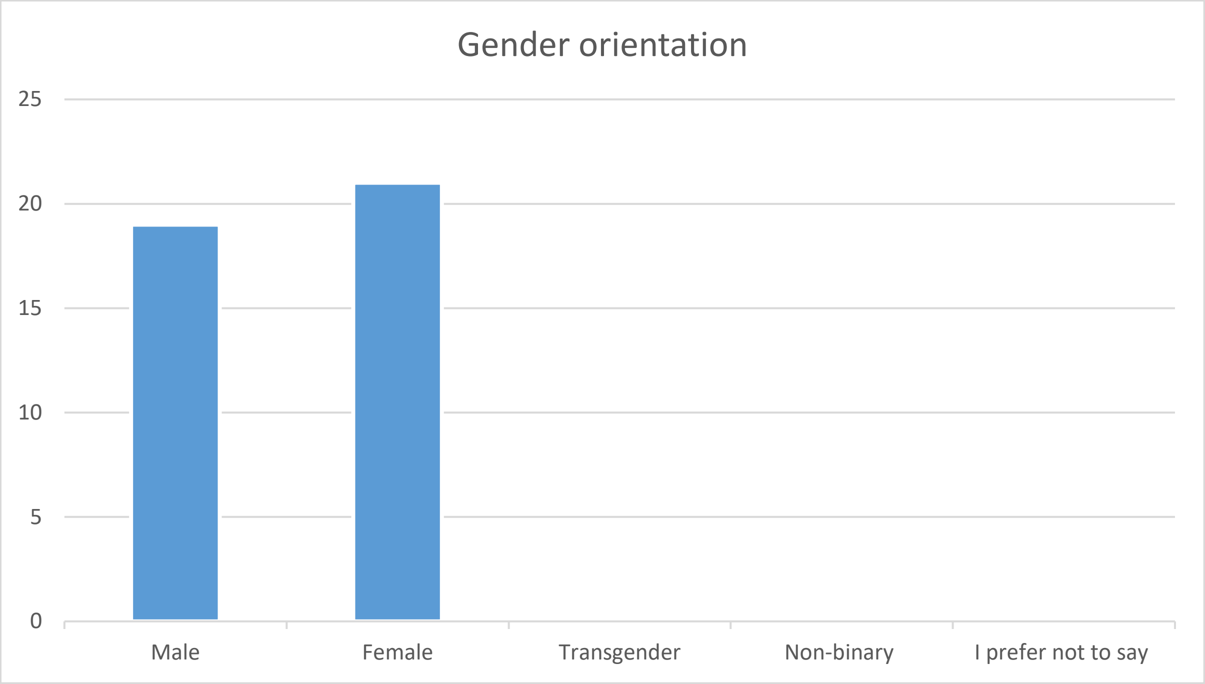


Figure D.97: Gender orientation (26-35)

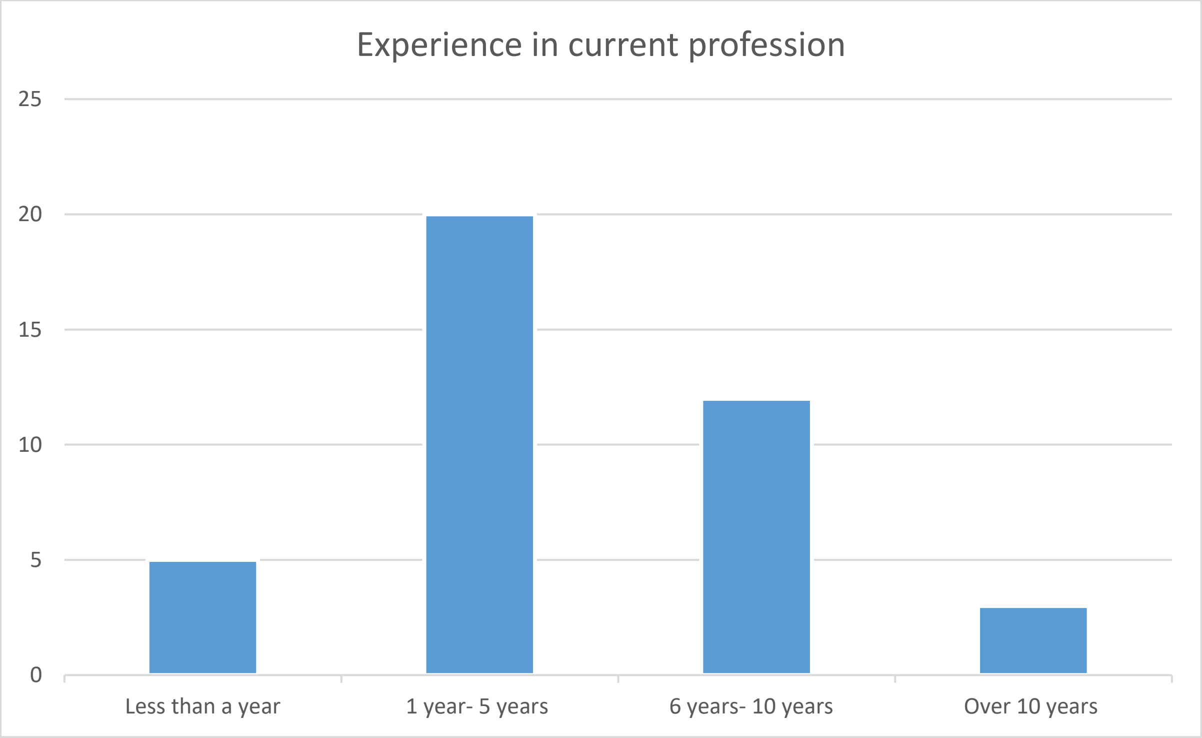


Figure D.98: Experience in current profession (26-35)

This analysis is based on the responses received from participants aged between 26 and 35. There were 40 participants, 19 males and 21 females (See figure D.97). The duration of their employment stretches from less than a year to 10 years or more. Out of the 40 participants, 5 employed in industry for less than one year; 20 between 1 and 5 years; 12 between 6 and 10 years; 3 more than 10 years (See figure D.98).

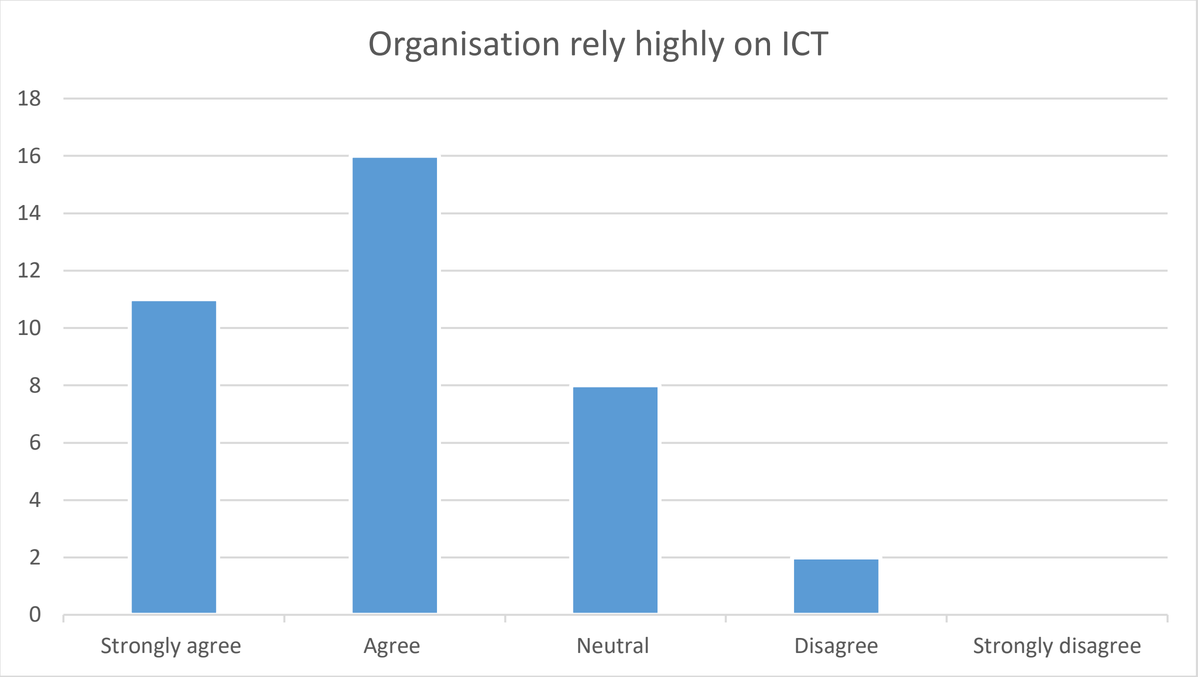


Figure D.99: Organisation rely highly on ICT (26-35)

27 out of the 40 respondents work in a technology reliance working environment, 8 unaware because of the nature of the work assigned to them, 2 'disagreed' on ICT. The majority of the employees within the 26-35 age range have a high reliance on ICT (See figure D.99).

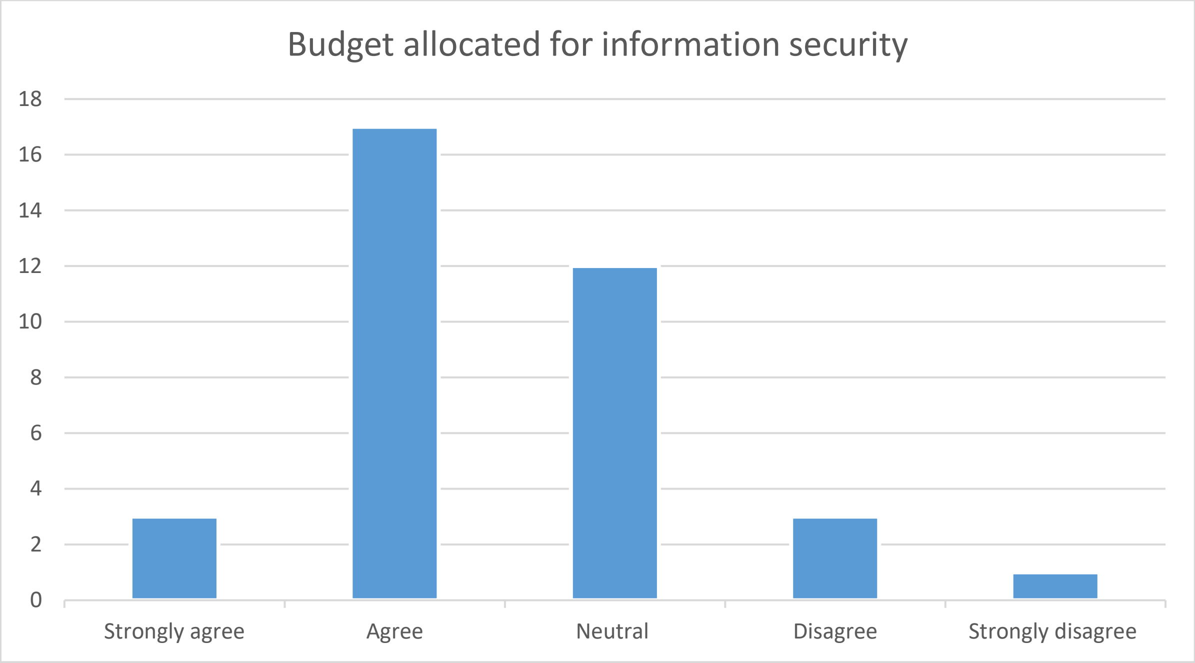


Figure D.100: Budget allocated for information security (26-35)

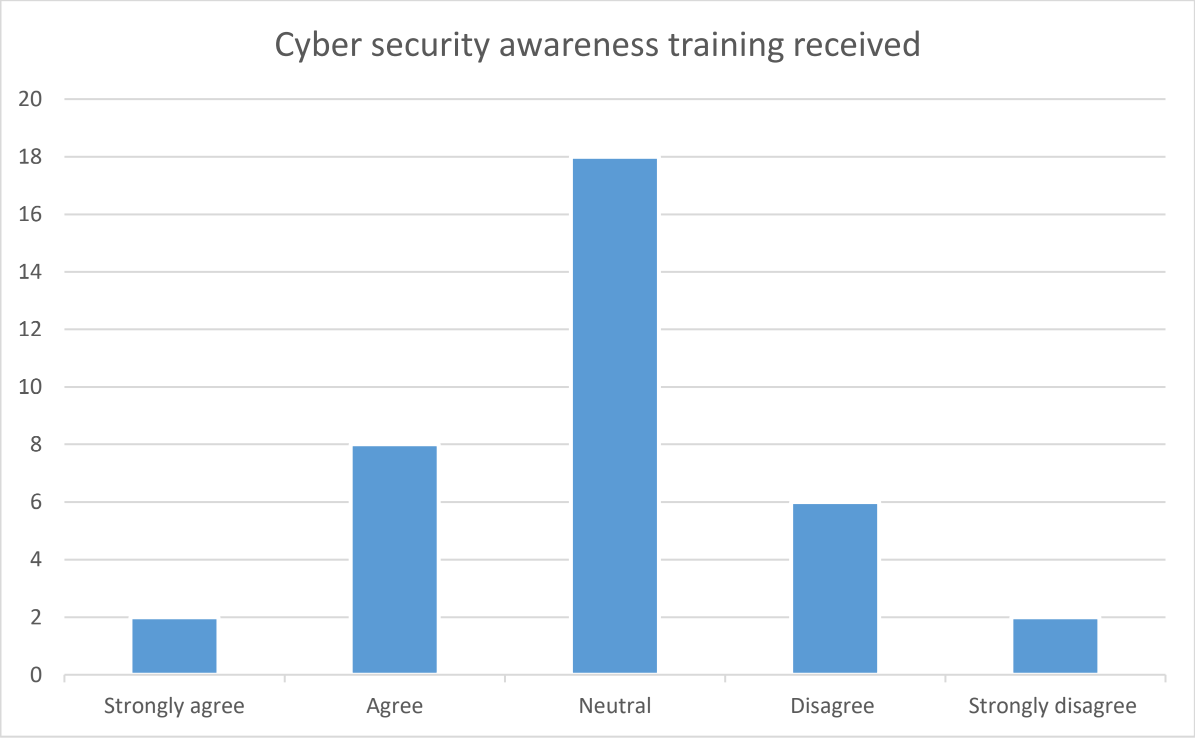


Figure D.101: Cyber security awareness training received (26-35)

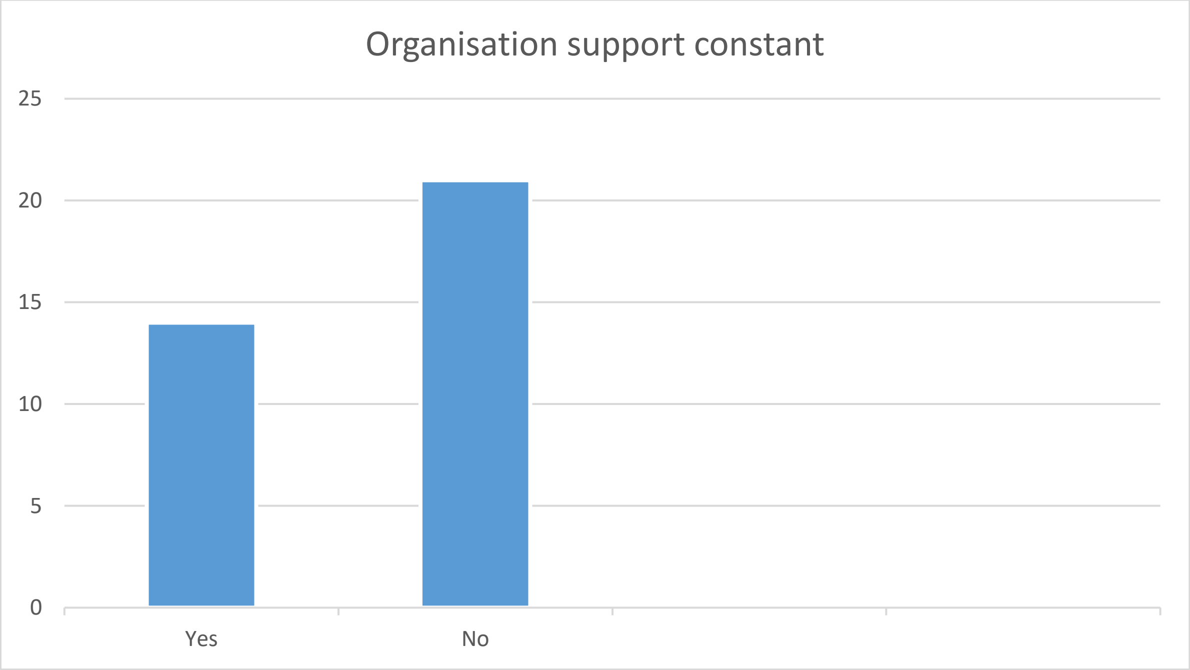


Figure D.102: Organisation support constant (26-35)

According to 20 respondents out of the 40, their organisations have a budget allocated for information security; 4 disagreed; notably, 12 had no opinion either way (See figure D.100). Some of the participants expressed satisfaction with the level of resources allocated for information security, but regular security awareness training received was inadequate. Only 10 participants received regular cybersecurity awareness training; 18 participants neither agreed nor disagreed, and 8 had none (See figure D.101). In addition, only 14 participants received support from the organisation to protect personal information, and 21 not received any (See figure D.102). The highlights clearly the inadequacy of organisational support for protecting personal information despite the budget allocated for information security and high reliance on technology.

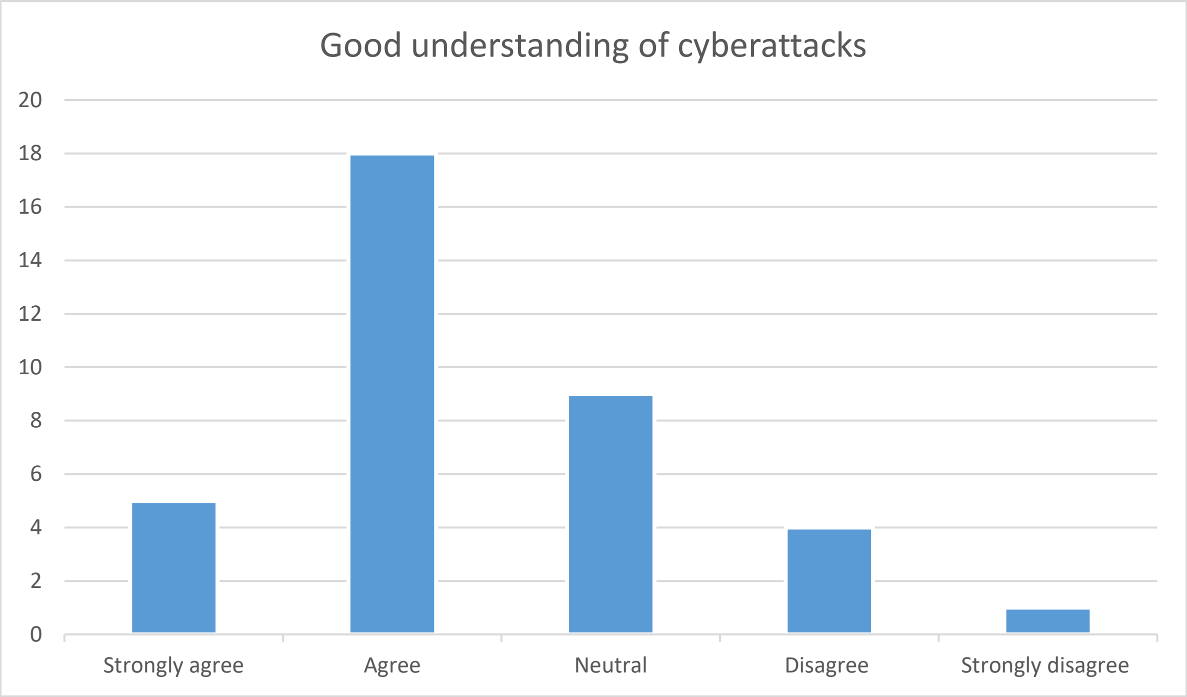


Figure D.103: Good understanding of cyberattacks (26-35)

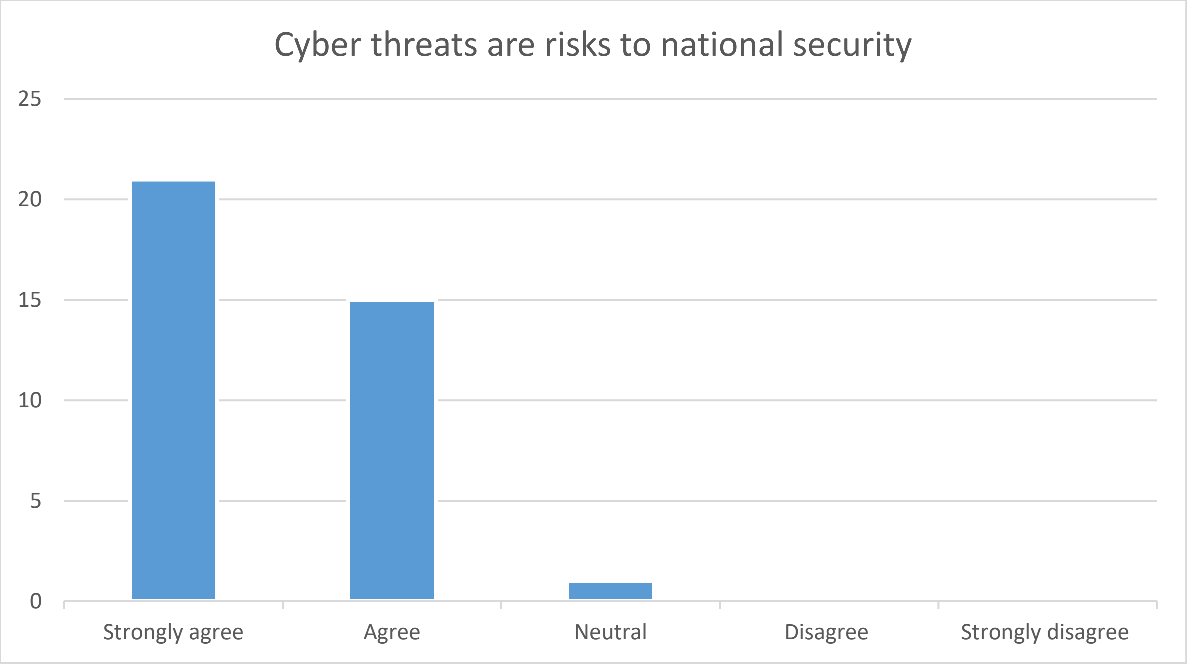


Figure D.104: Cyber threats are risks to national security (26-35)

The survey suggests that despite the lack of security awareness training, 23 participants have a high understanding of the impact of cyber-attacks on the public and the organisation; 5 no understanding; 9 did not express an opinion either way (See figure D.103). Significantly, 90 percent of the participants do realise the potential threats to national security from cyber-attacks (See figure D.104). In general, understanding cyber threats and their impact on national security should encourage people to act responsibly to minimise end-user errors, and in time, they will be in a strong position to influence the process in accepting and implementing a national, regional, and global level mechanism.

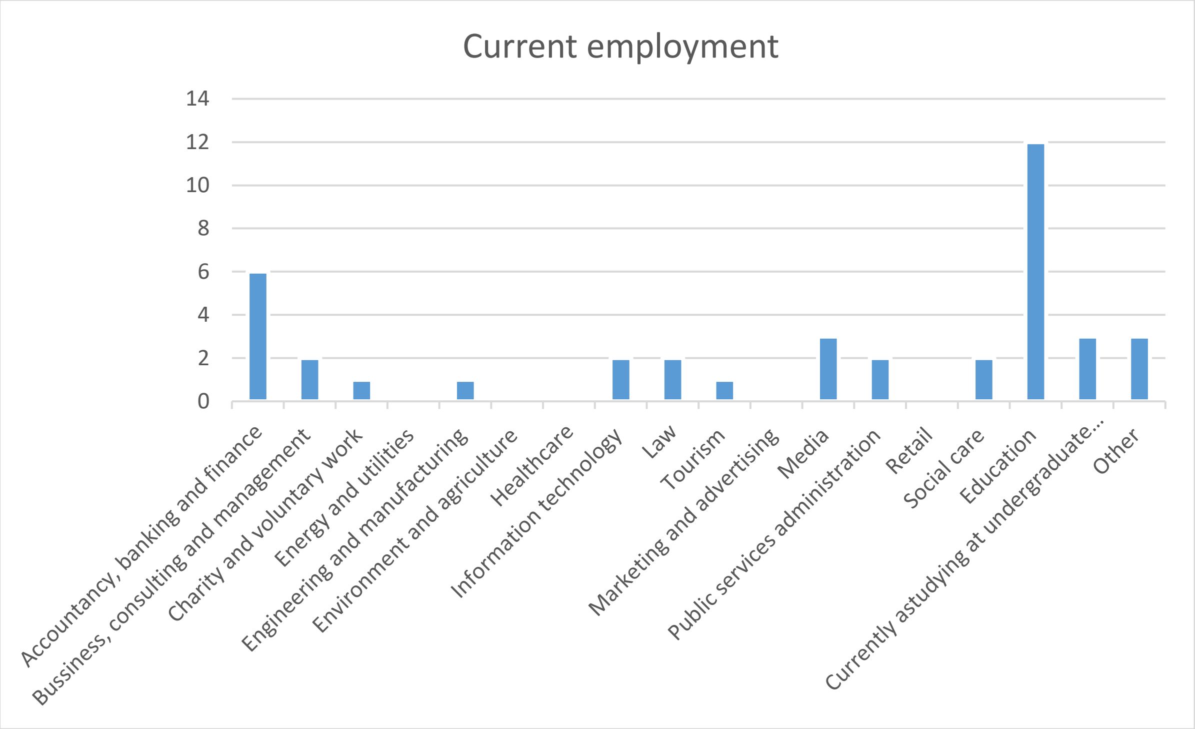


Figure D.105: Current employment (26-35)

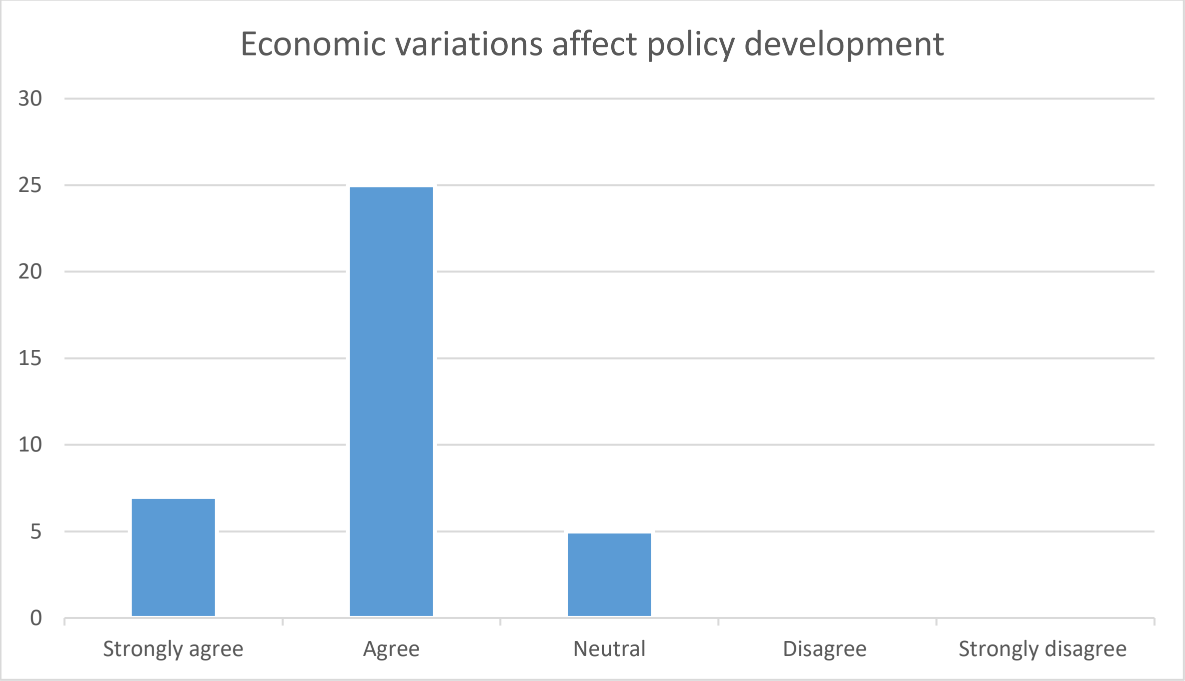


Figure D.106: Economic variations affect policy development (26-35)

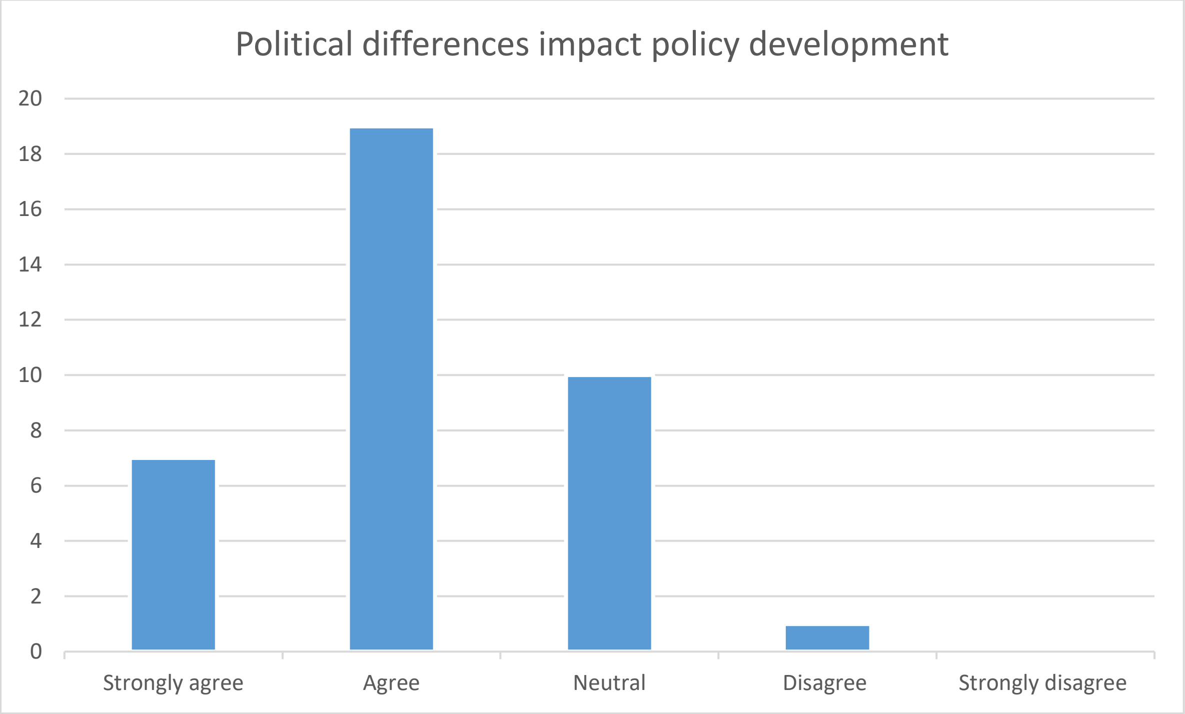


Figure D.107: Political differences impact policy development (26-35)

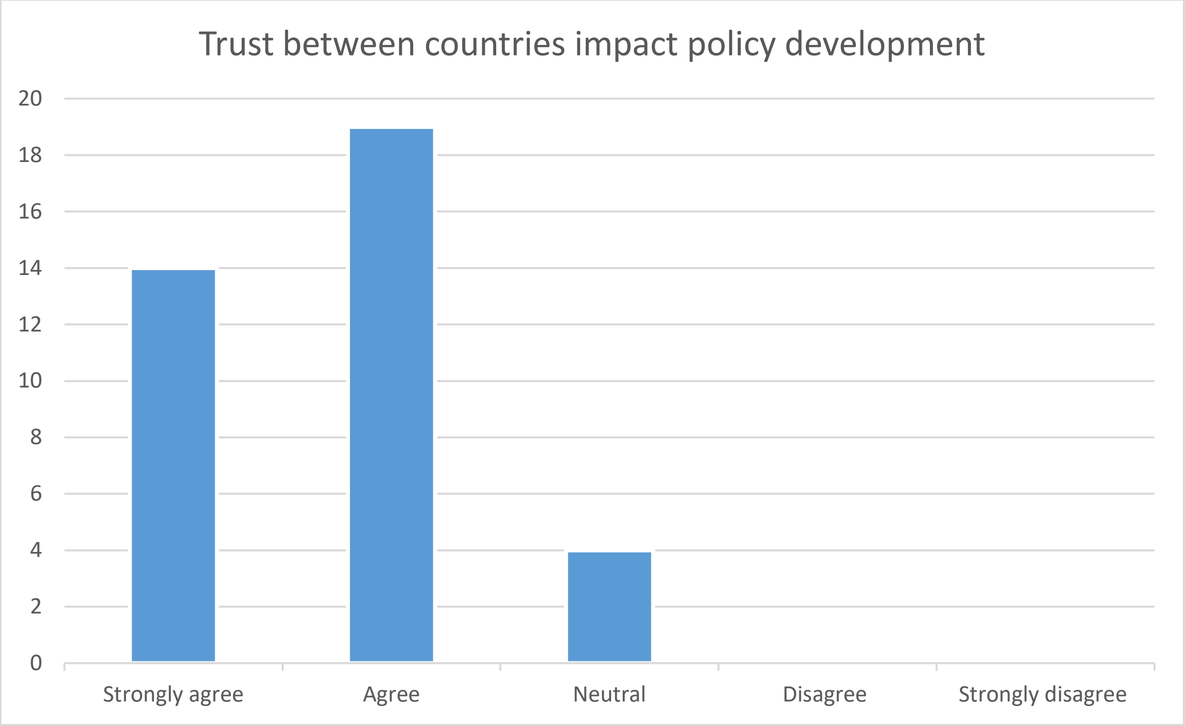


Figure D.108: Trust between countries impact policy development (26-35)

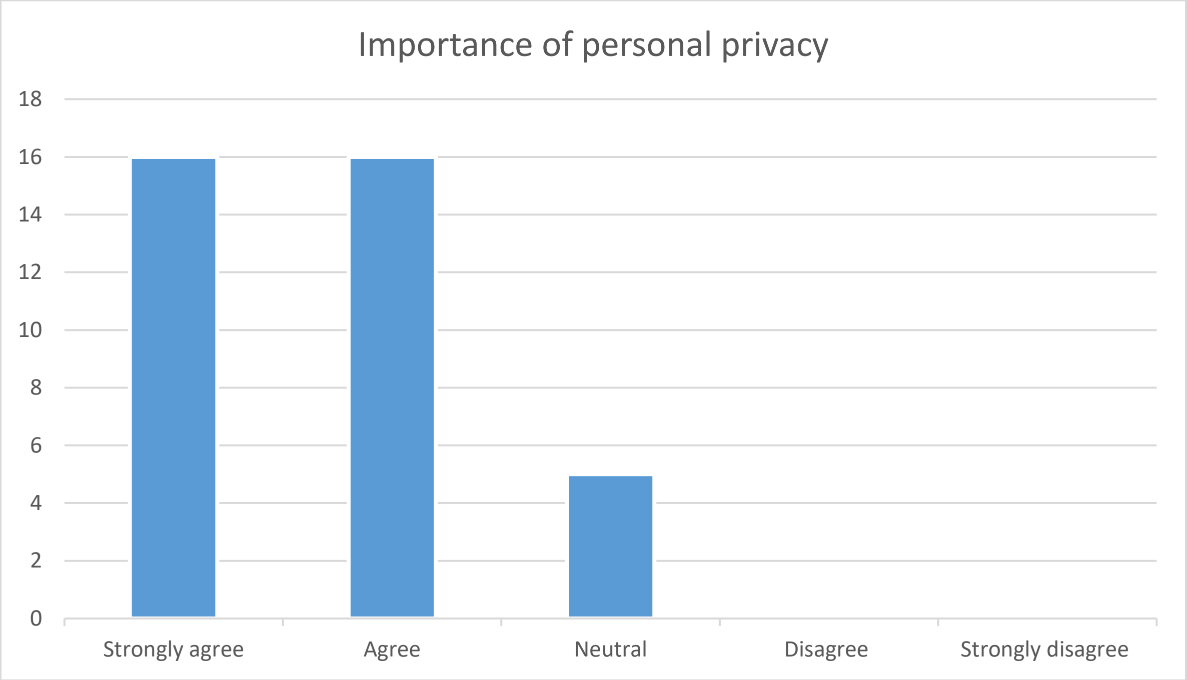


Figure D.109: Importance of personal privacy (26-35)

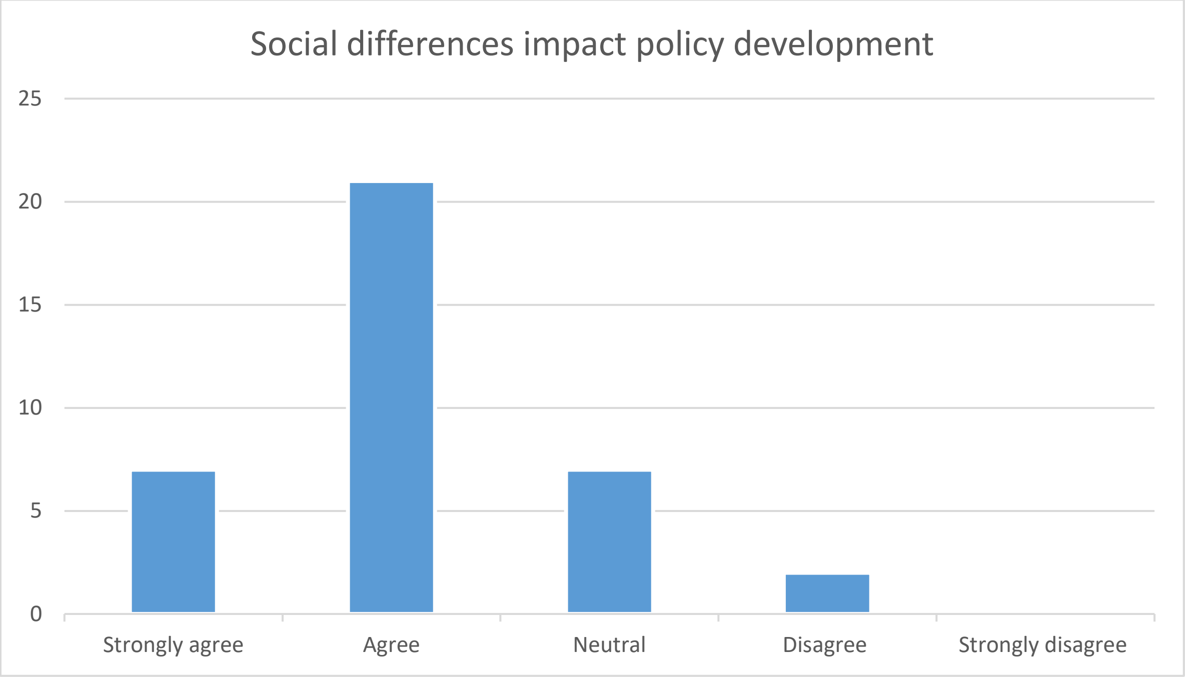


Figure D.110: Social differences impact policy development (26-35)

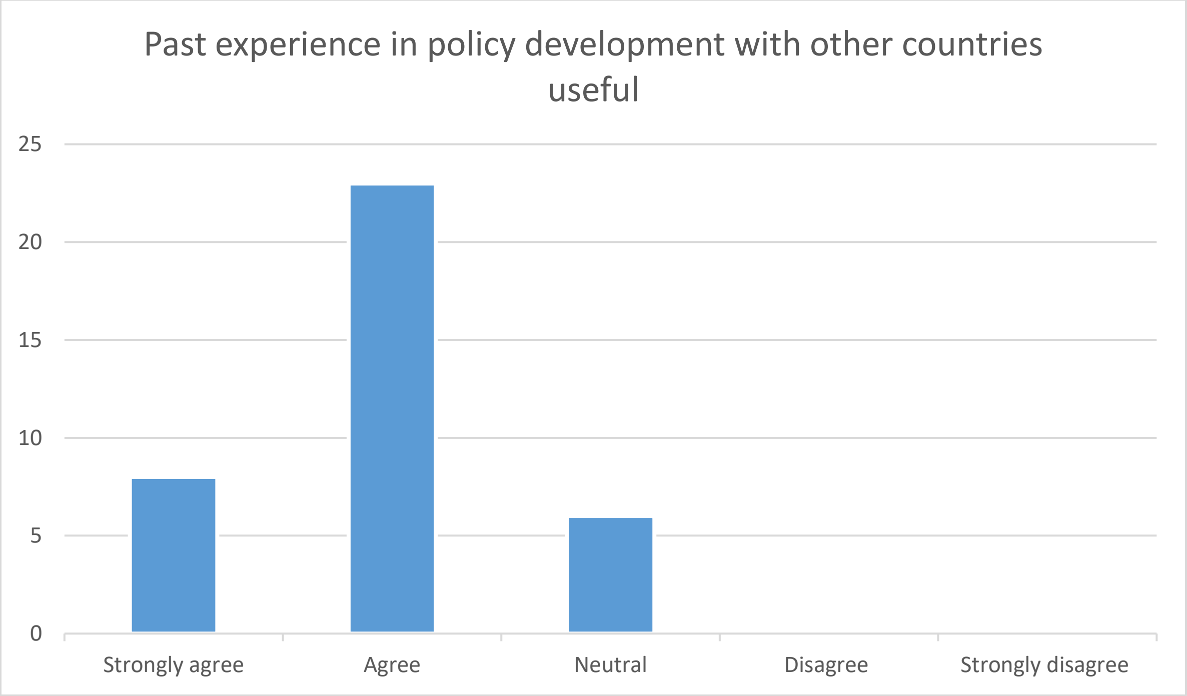


Figure D.111: Past experience in policy development with other countries useful (26-35)

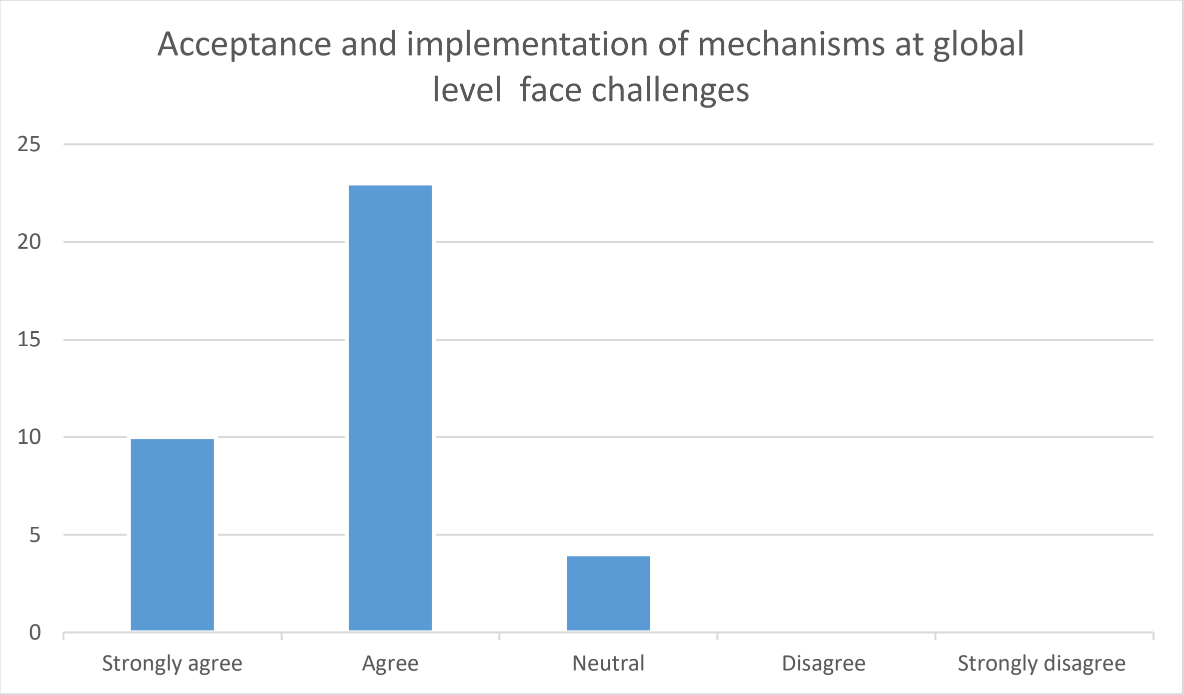


Figure D.112: Acceptance and implementation of mechanisms at global level face challenges (26-35)

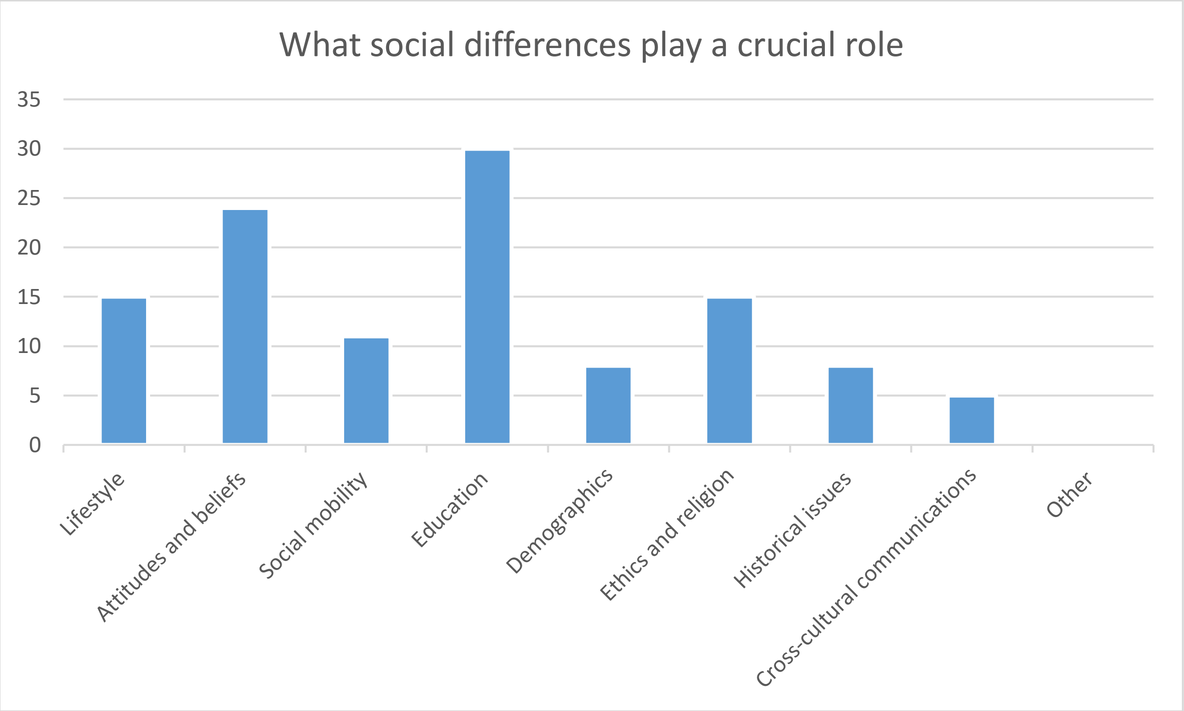


Figure D.113: What social differences play a crucial role (26-35)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure D.113). Awareness of potential cyber threats and the impact on people and national security will be important assets in terms of accepting and implementing data privacy and security policies. Therefore, it is important to provide cybersecurity awareness training at the school and organisational level. There is consensus on the need for knowledge and awareness of potential cyber threats, and the impact on people and national security is crucial to accepting and implementing data privacy and security policies. Therefore, it is important to deliver cybersecurity awareness training at the school and organisational level. Going back to the previous question about the provision of cybersecurity awareness training, proper security training had not been given. Therefore, it becomes clear that the majority of participants prefer education to social factors.

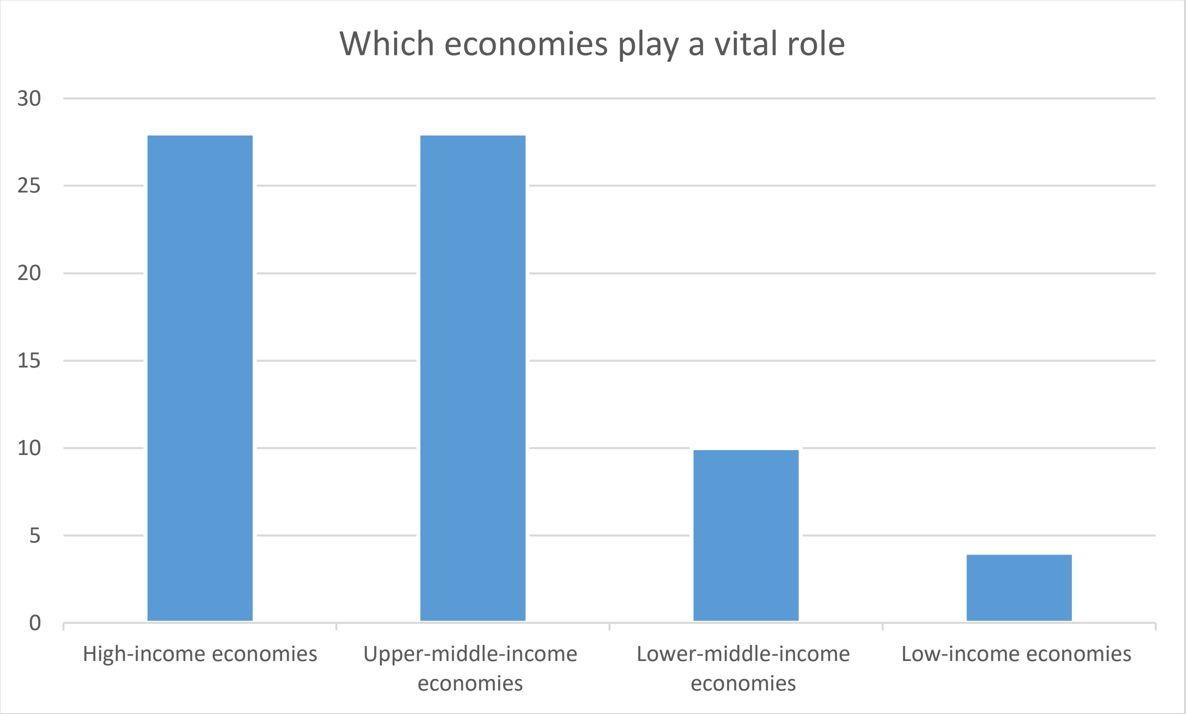


Figure D.114: Which economies play a vital role (26-35)

In the questionnaire, majority has stated that the high income and upper-middle-income countries play a vital role (See figure D.114). The key stages in policymaking are to identify policymaker aims, identify the policies to achieve those aims, select a policy measure, identify the necessary resources, implement, and then evaluate the policy. These stages are time-consuming and need to be resourced and funded. Therefore, the economic stability of the country is considered crucial to a large extent in achieving success in policymaking.

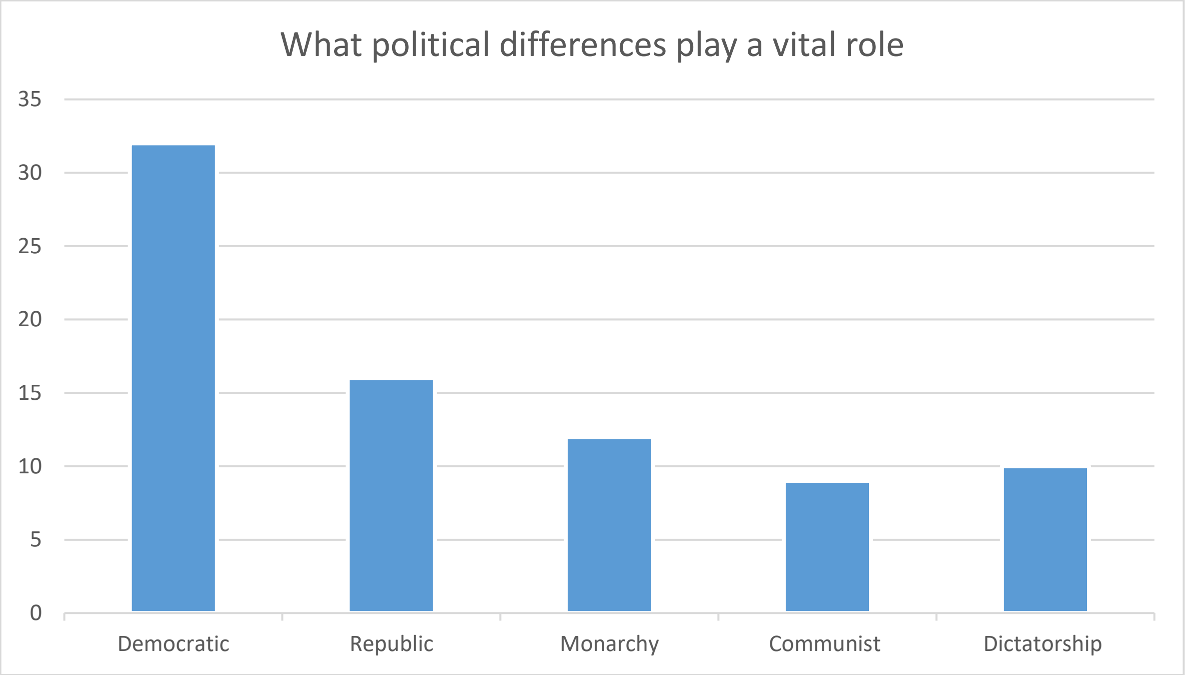


Figure D.115: What political differences play a vital role (26-35)

The majority of this age group have chosen democratic political system (See figure D.115), in preference to others because it allows the public an influential voice in policy development and encourage consensus and collective responsibility for their actions. These contribute to developing trust between the organisations, and coherence and transparency in the policy development process.

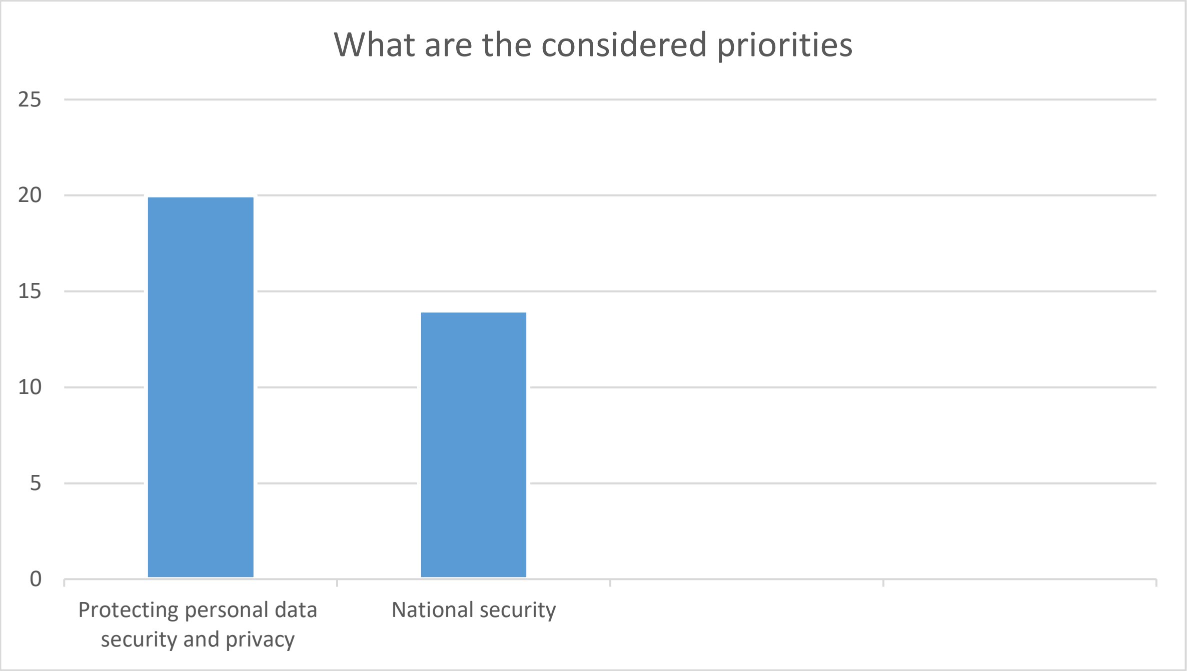


Figure D.116: What are the considered priorities (26-35)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy is placed above the protection of national security (See figure D.116). The implications of a personal data breach incident will have a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

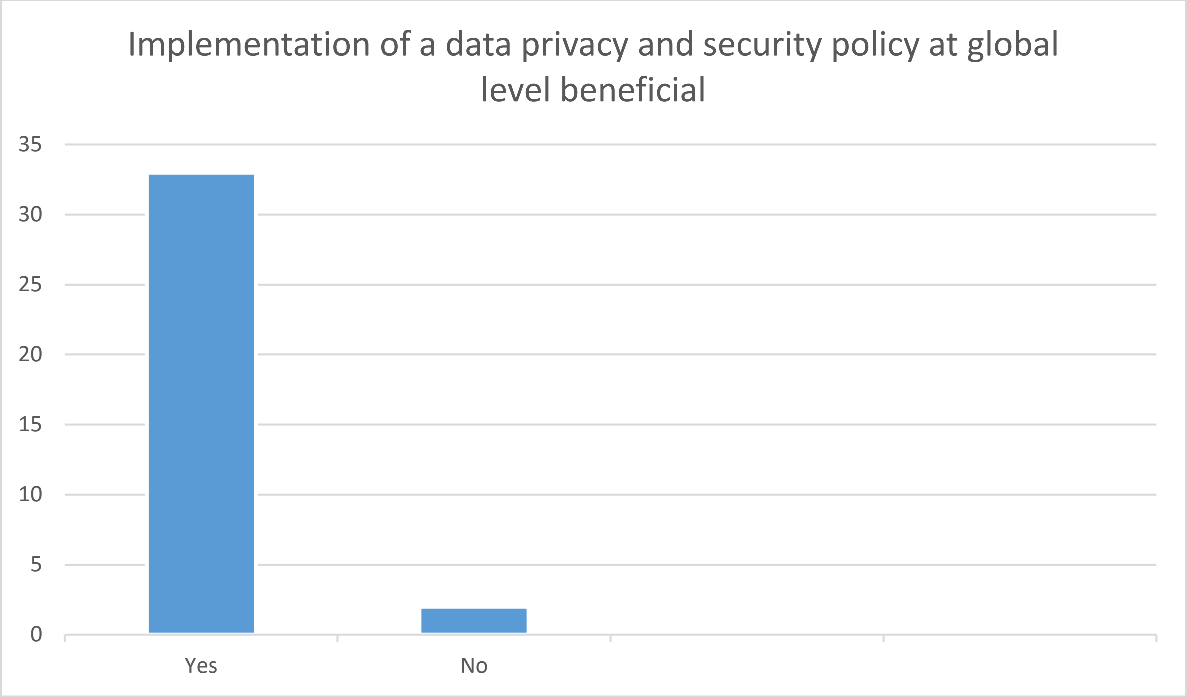


Figure D.117: Implementation of a data privacy and security policy at global level beneficial (26-35)

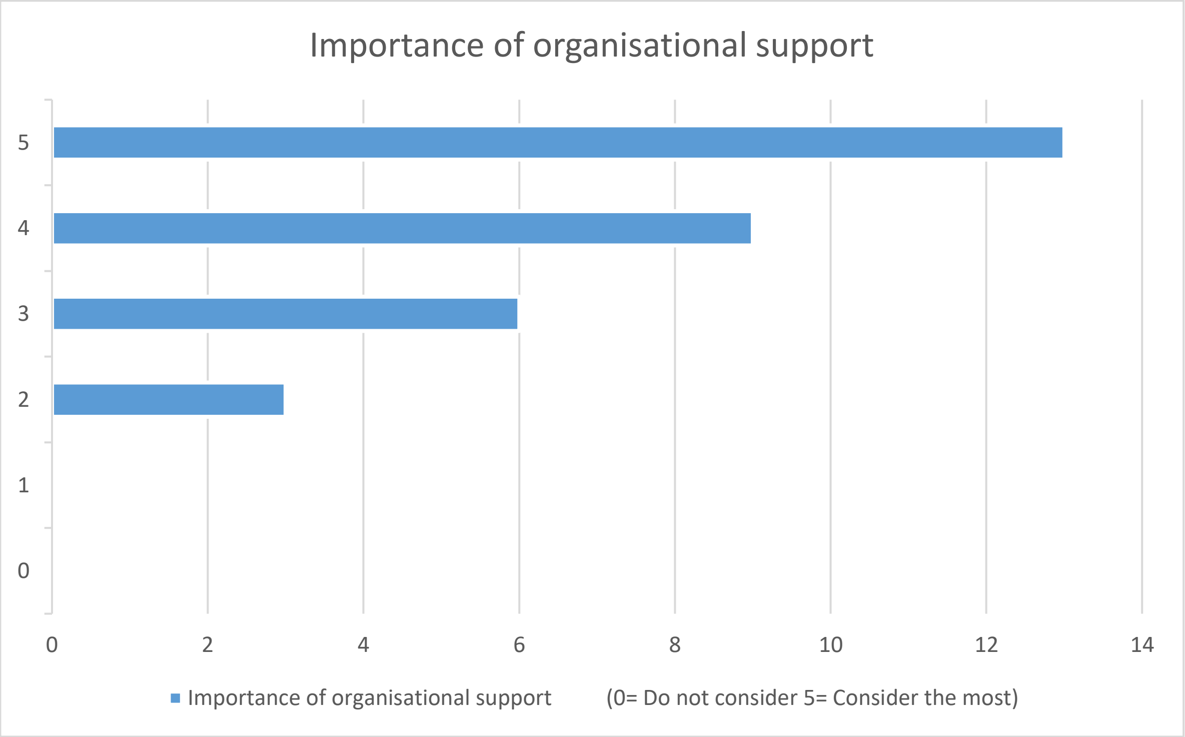


Figure D.118: Importance of organisational support (26-35)

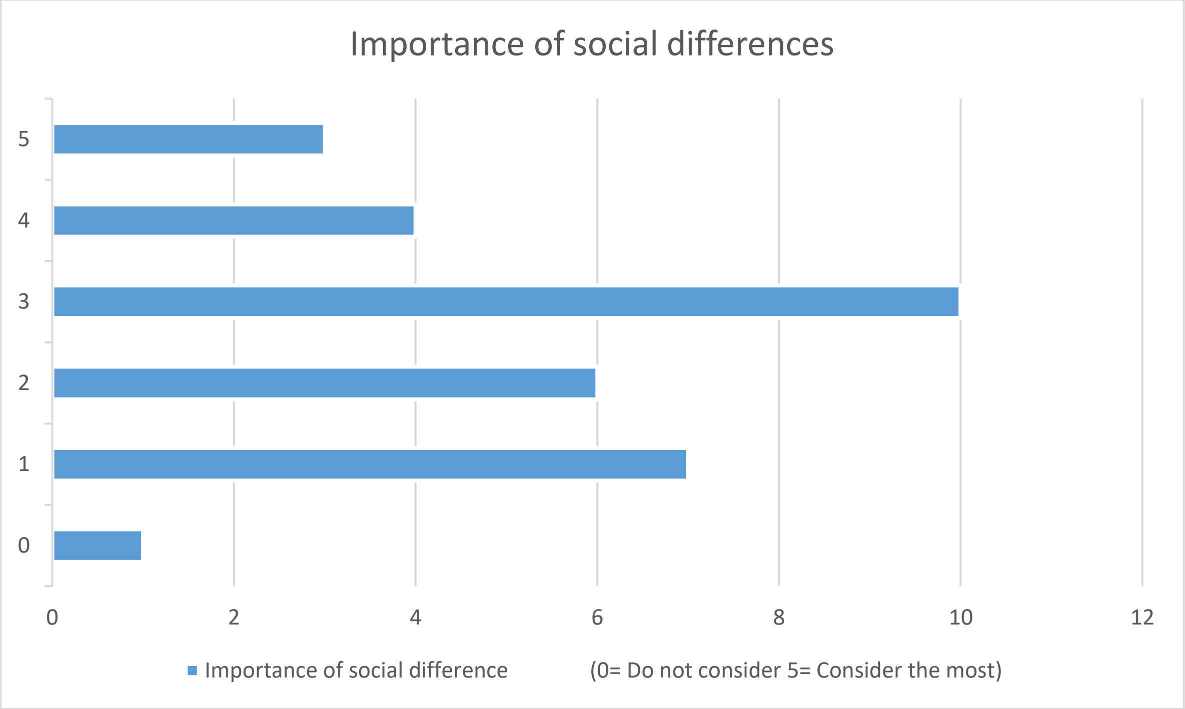


Figure D.119: Importance of social differences (26-35)

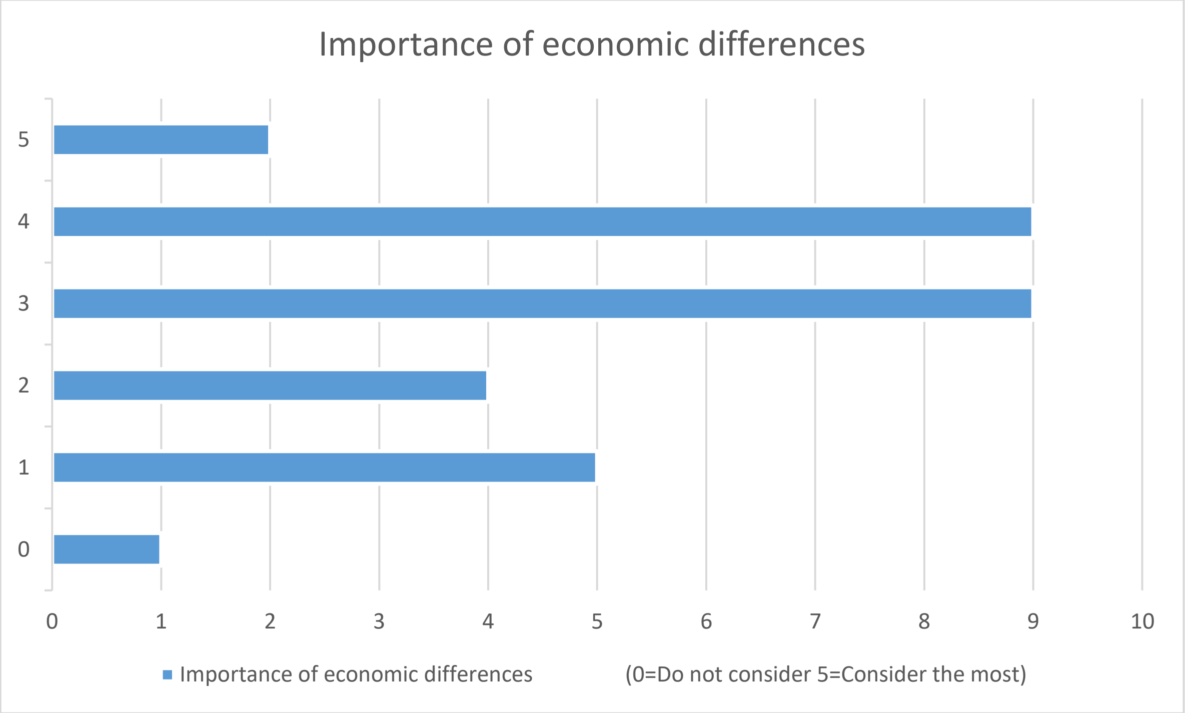


Figure D.120: Importance of economic differences (26-35)

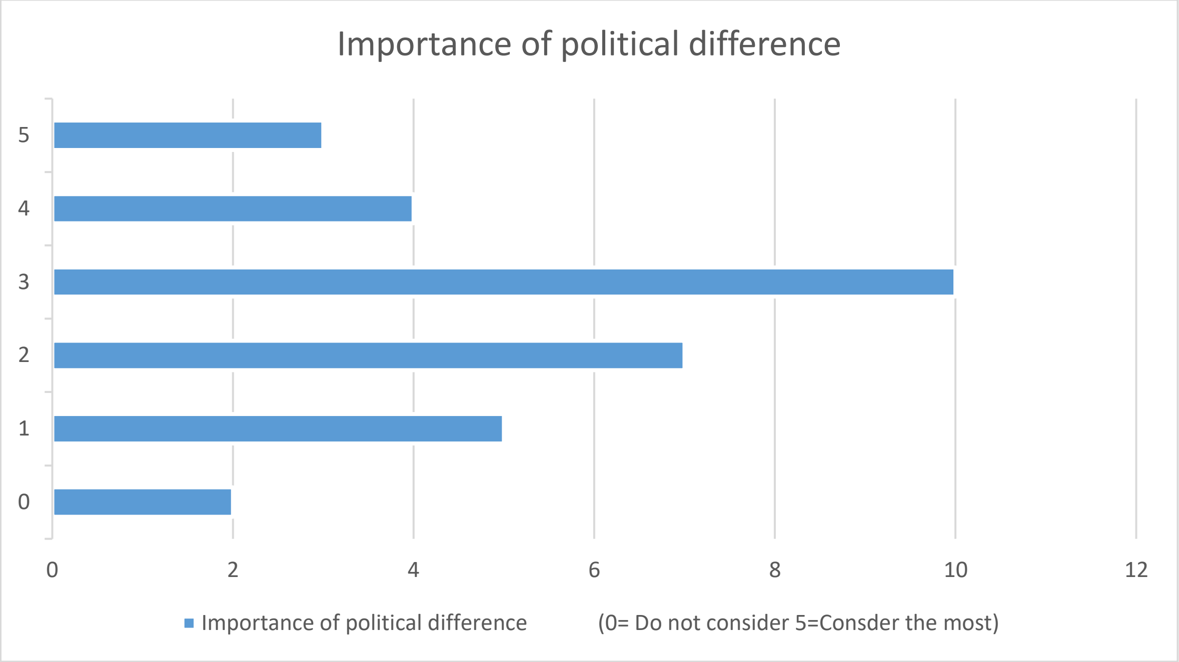


Figure D.121: Importance of political difference (26-35)

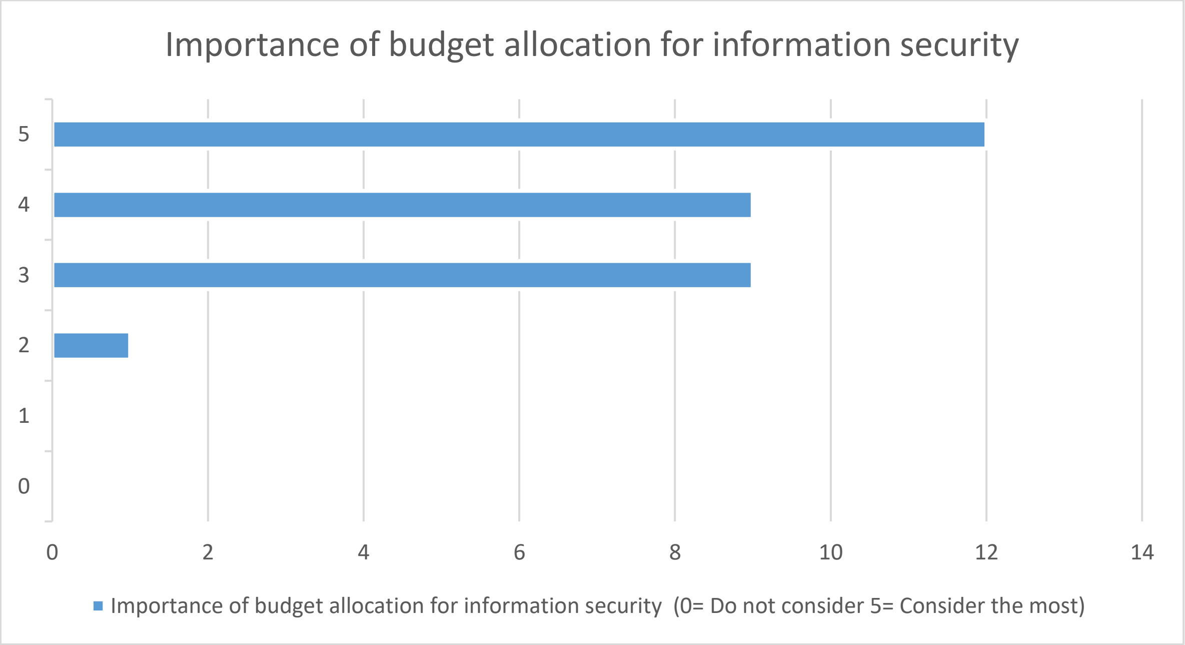


Figure D.122: Importance of budget allocation for information security (26-35)

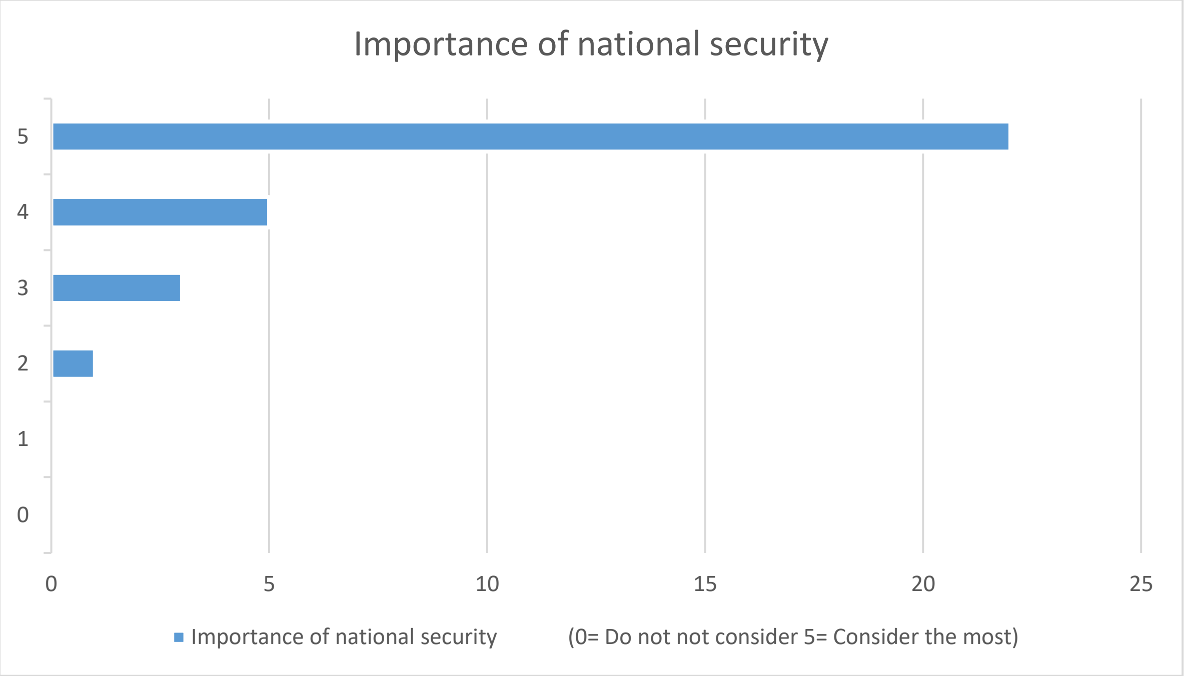


Figure D.123: Importance of national security (26-35)

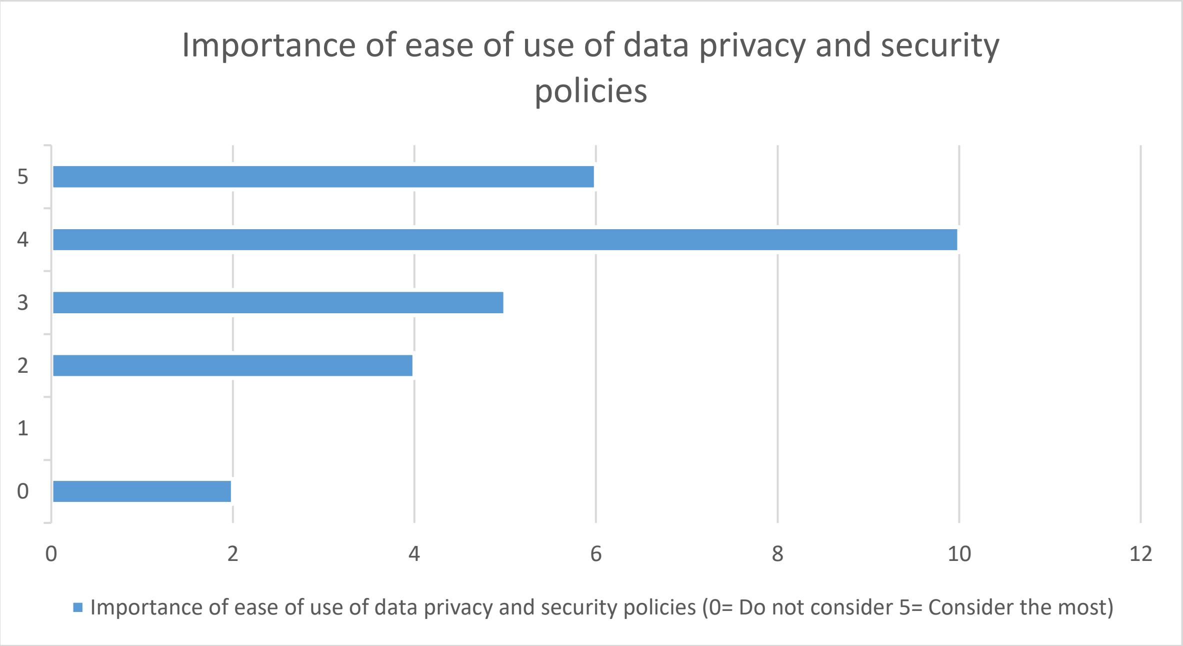


Figure D.124: Importance of ease of use of data privacy and security policies (26-35)

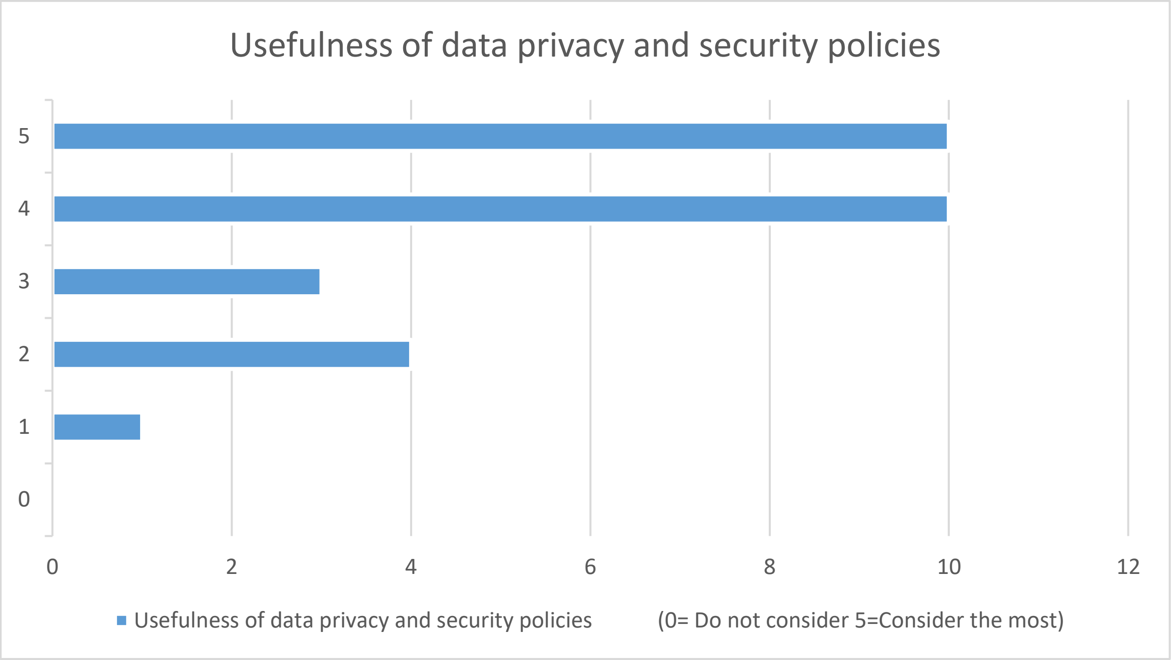


Figure D.125: Usefulness of data privacy and security policies (26-35)

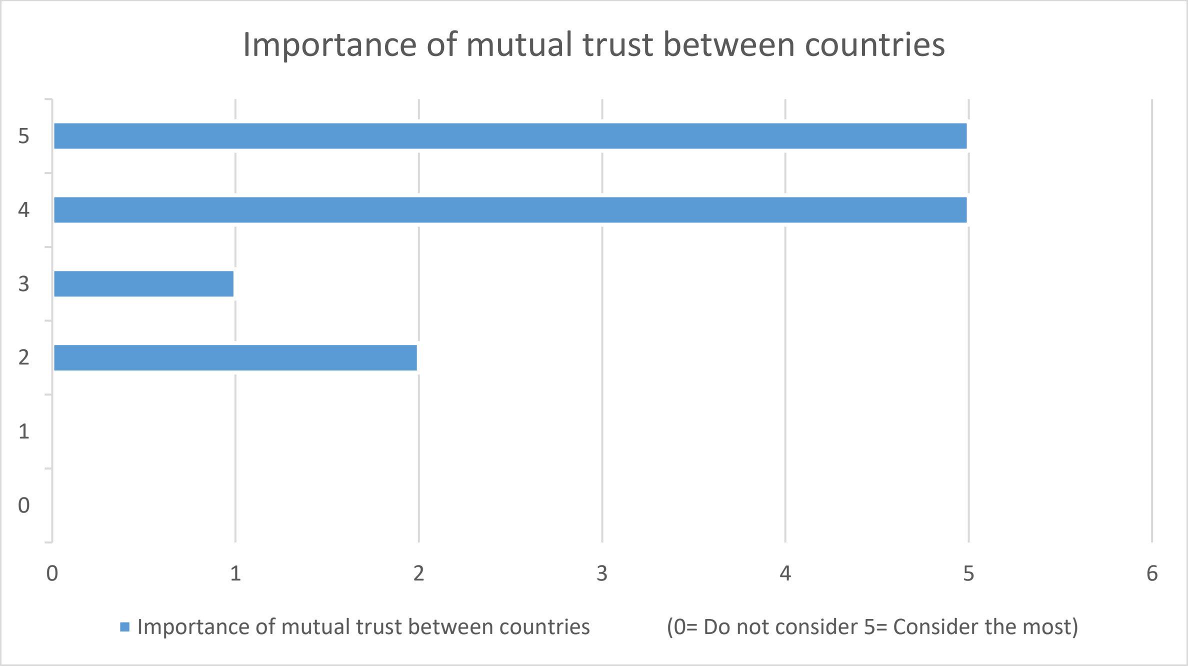


Figure D.126 Importance of mutual trust between countries (26-35)

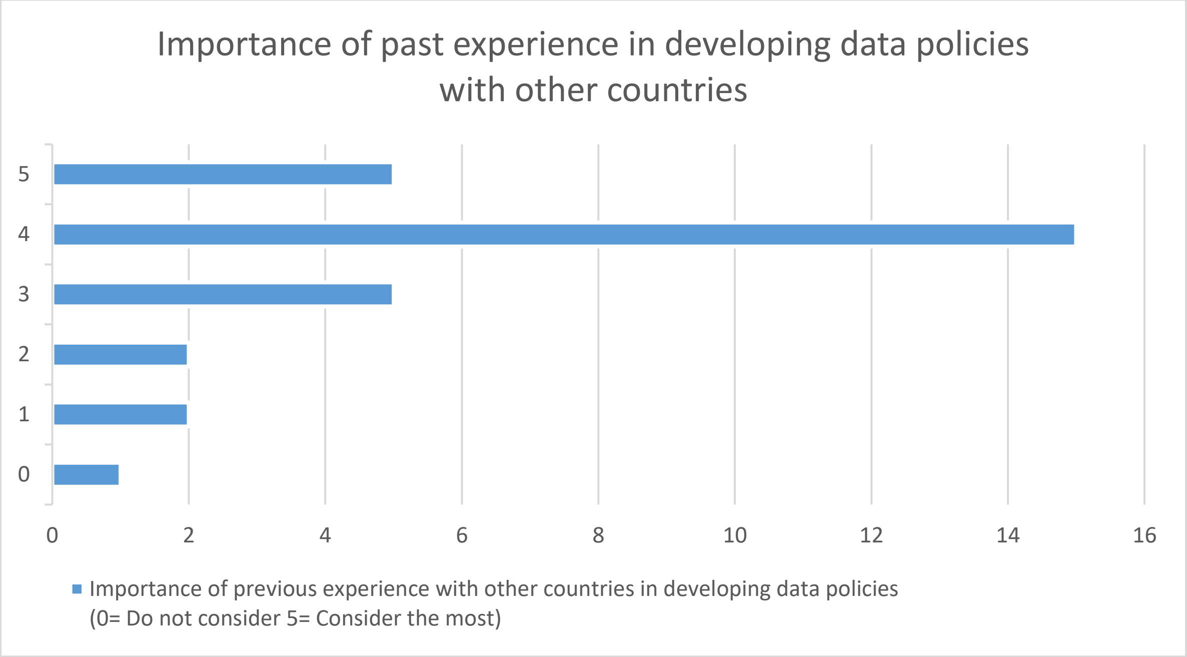


Figure 4.127: Importance of past experience in developing data policies with other counties (26-35)

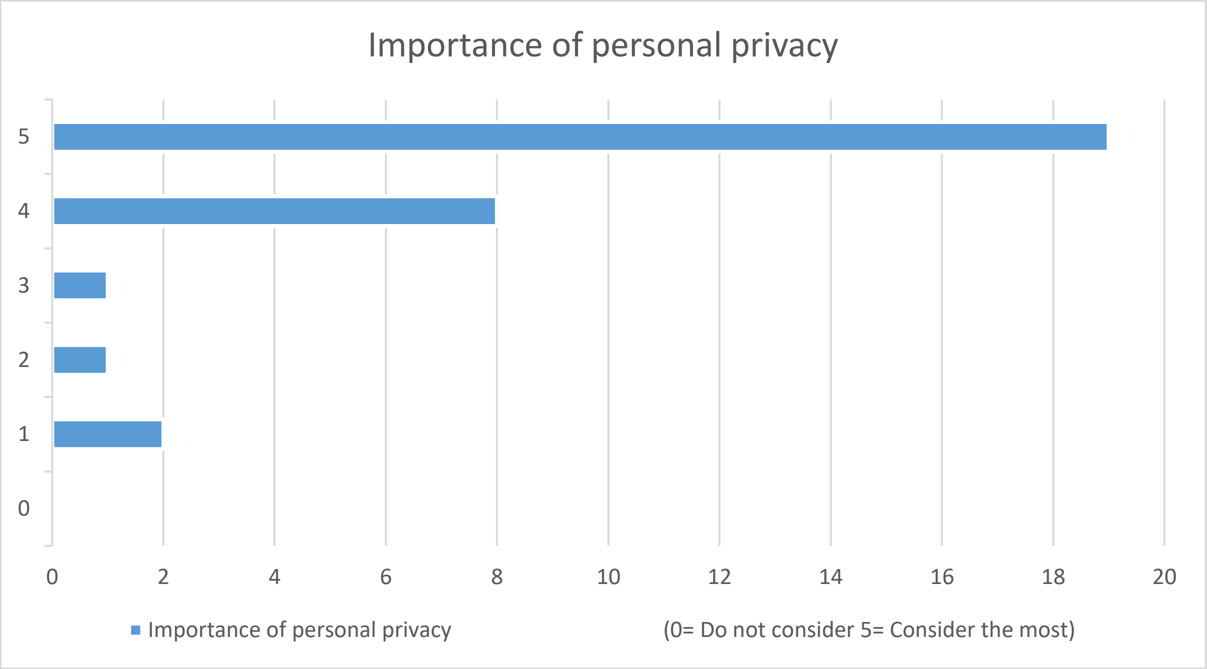


Figure 4.128: Importance of personal privacy (26-35)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 83 percent of the respondents have endorsed (See figure D.117). The other notable factors are organisational support, budget allocation for information security, economic differences, personal privacy, national security, user-friendly data privacy and security policies, the usefulness of data privacy and security policies, previous experience in developing policies with other countries (See figure D.106-116) (See figure D.118-128).

Sri Lanka- 36-45

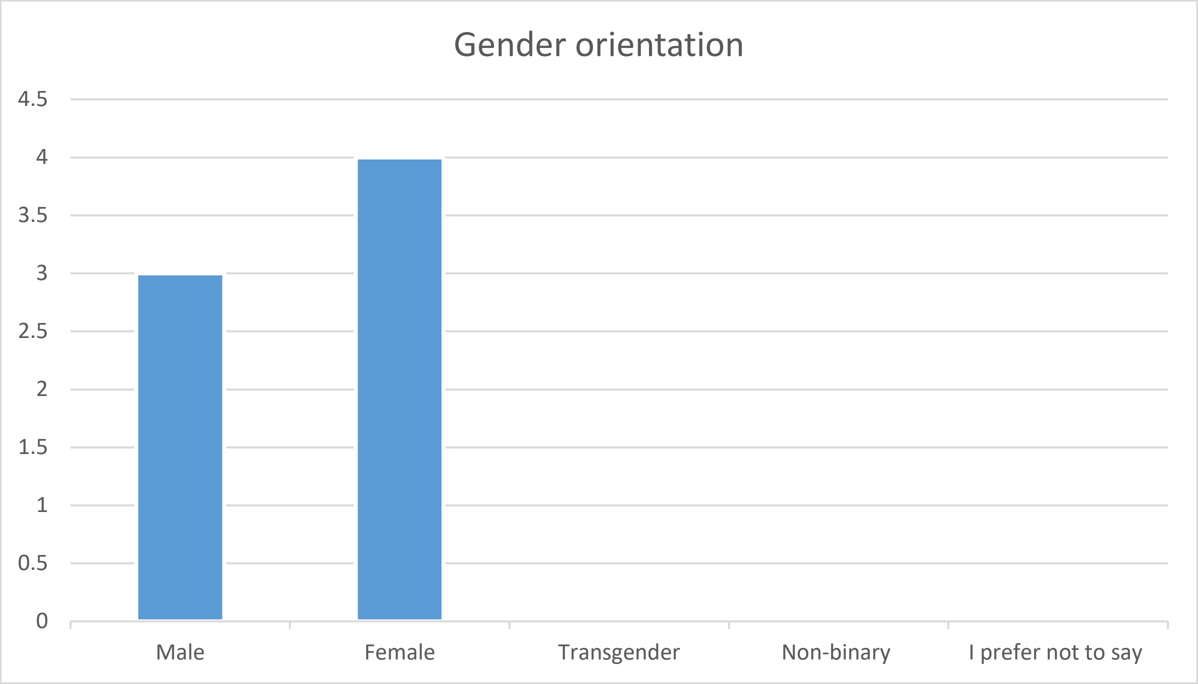


Figure D.129: Gender orientation (36-45)

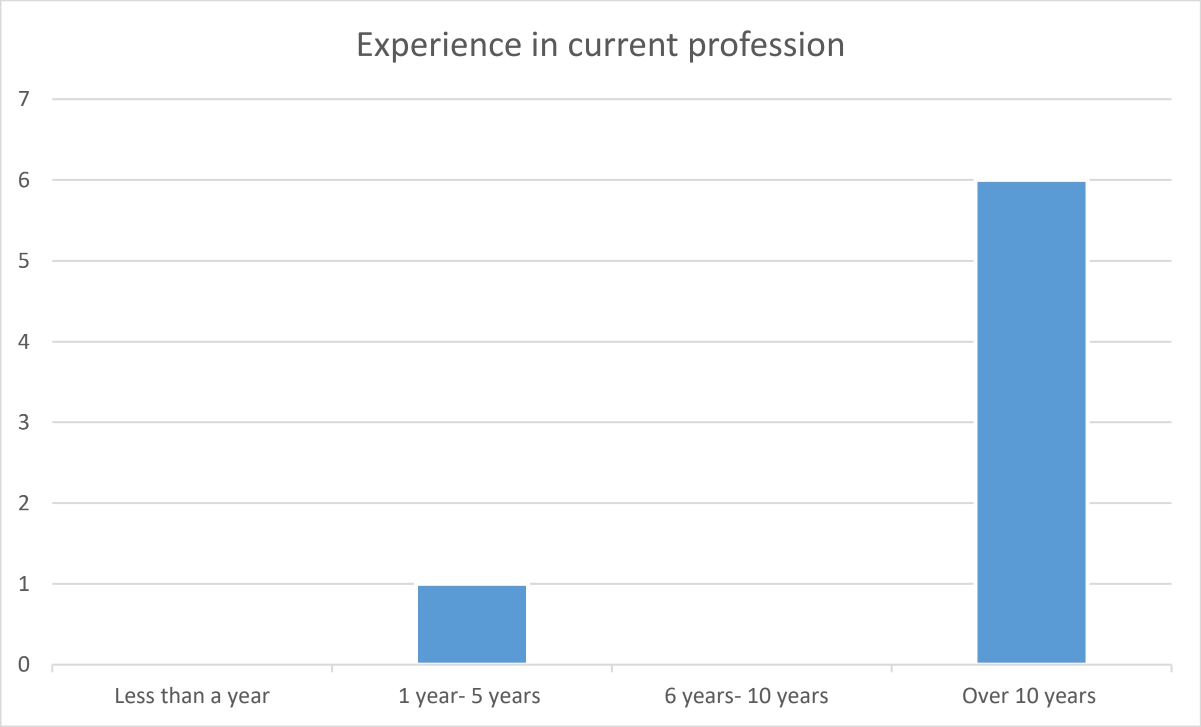


Figure D.130: Experience in current profession (36-45)

This analysis is based on the responses received from Sri Lankan participants between the 36-45 age range. Of the 7 participants who responded, 3 were males, and 4 females (See figure D.129), all employed in the industry over a duration of 1 to 10 years (See figure D.130).

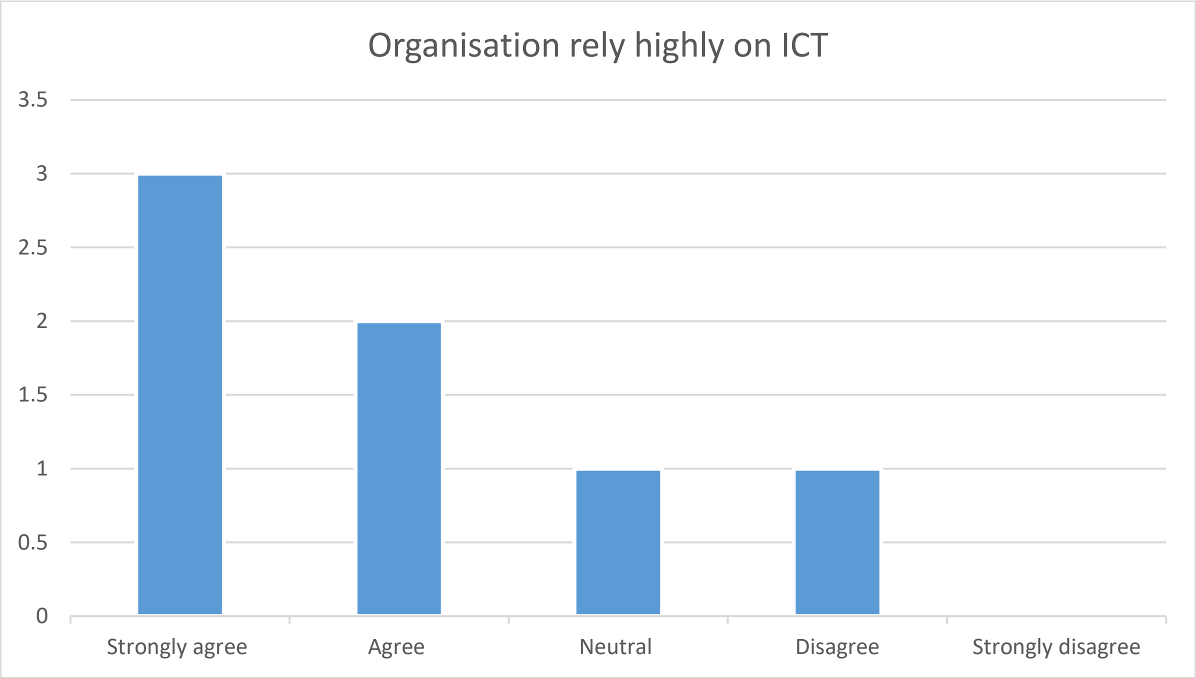


Figure D.131: Organisation rely highly on ICT (36-45)

Technology reliance working environment: 5 in technology reliance working environment; 1 unable to specify because of the nature of the work assigned to them; 1 chose to 'disagree' on ICT (See figure D.131). The majority of the employees within the 36-45 age range have a high reliance on ICT.

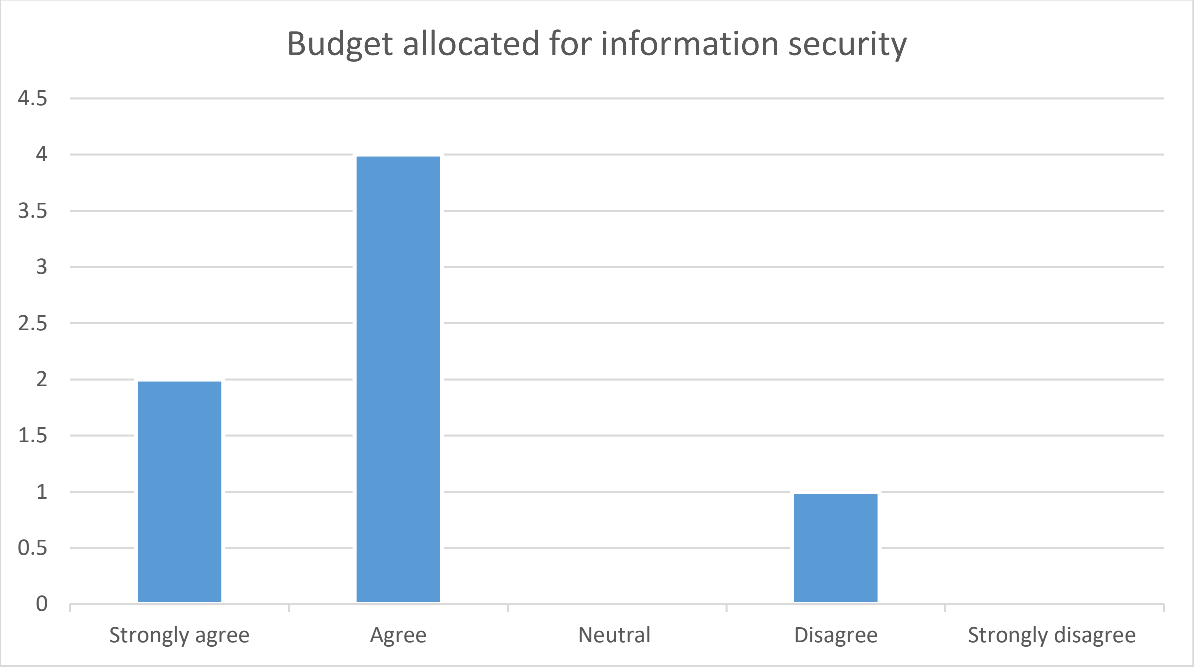


Figure D.132: Budget allocated for information security (36-45)

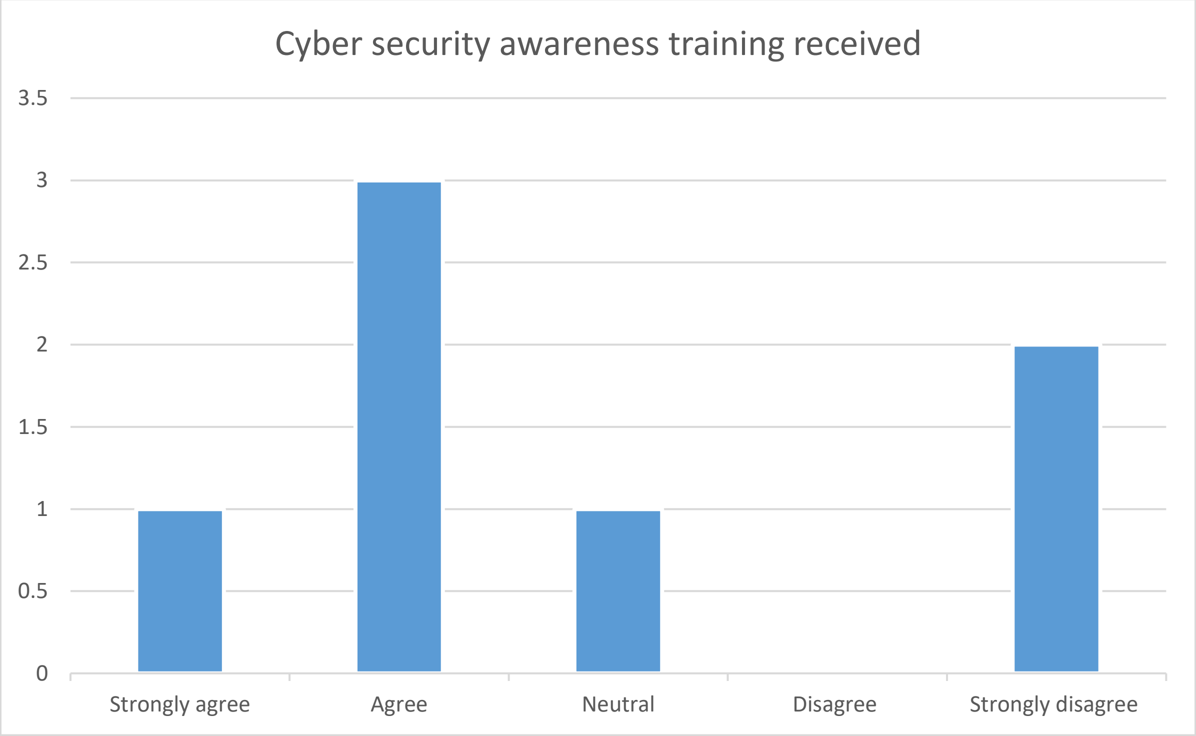


Figure D.133: Cyber security awareness training received (36-45)

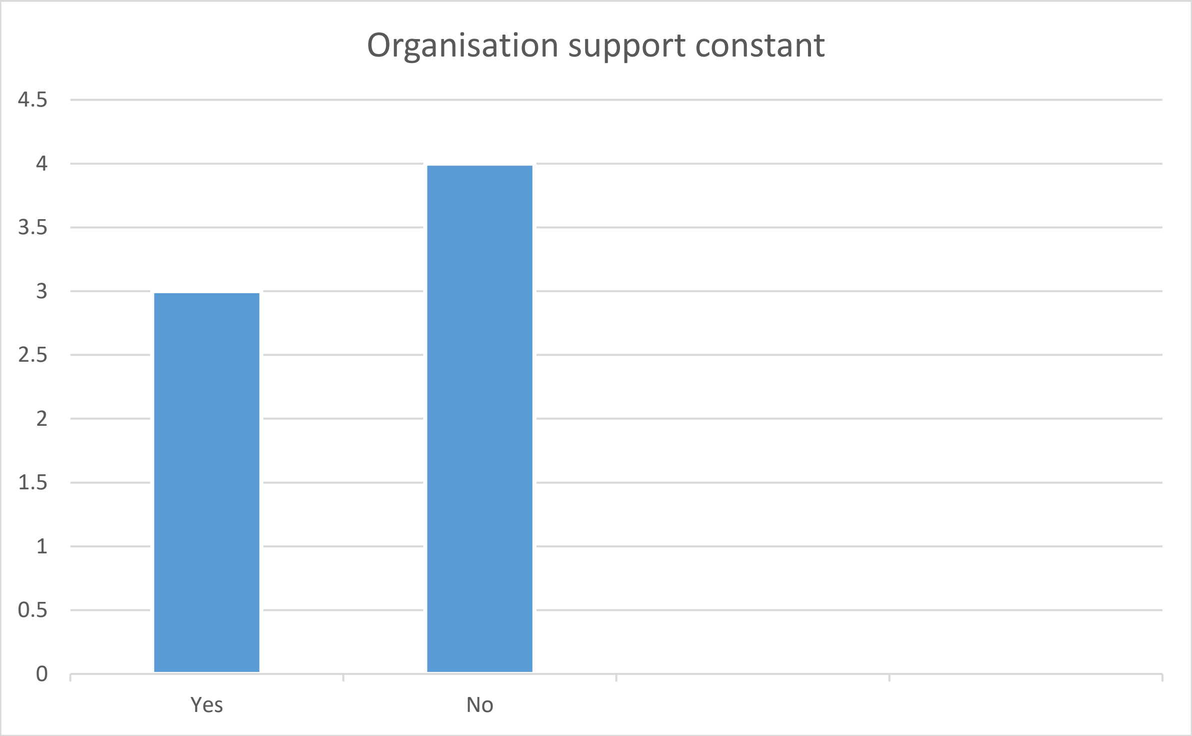


Figure D.134: Organisation support constant (36-45)

Mixed response from the participants, and according to 6 out of the 7, the organisations had an allocated budget for information security, and notably according to the 1 disagreed, the organisation had no budget allocation for information security (See figure D.132). According to some of the participants, regular security awareness training they received was inadequate despite the satisfactory level of resources allocated for information security and regular security awareness training. 4 participants received regular cybersecurity awareness training; 2 did not; one neither agreed nor disagreed (See figure D.133). In addition, 4 participants did not receive support from the organisation to protect personal information; only 3 did (See figure D.134). This represents lack of organisational support to protect personal information despite the budget allocated for information security and high reliance on technology.

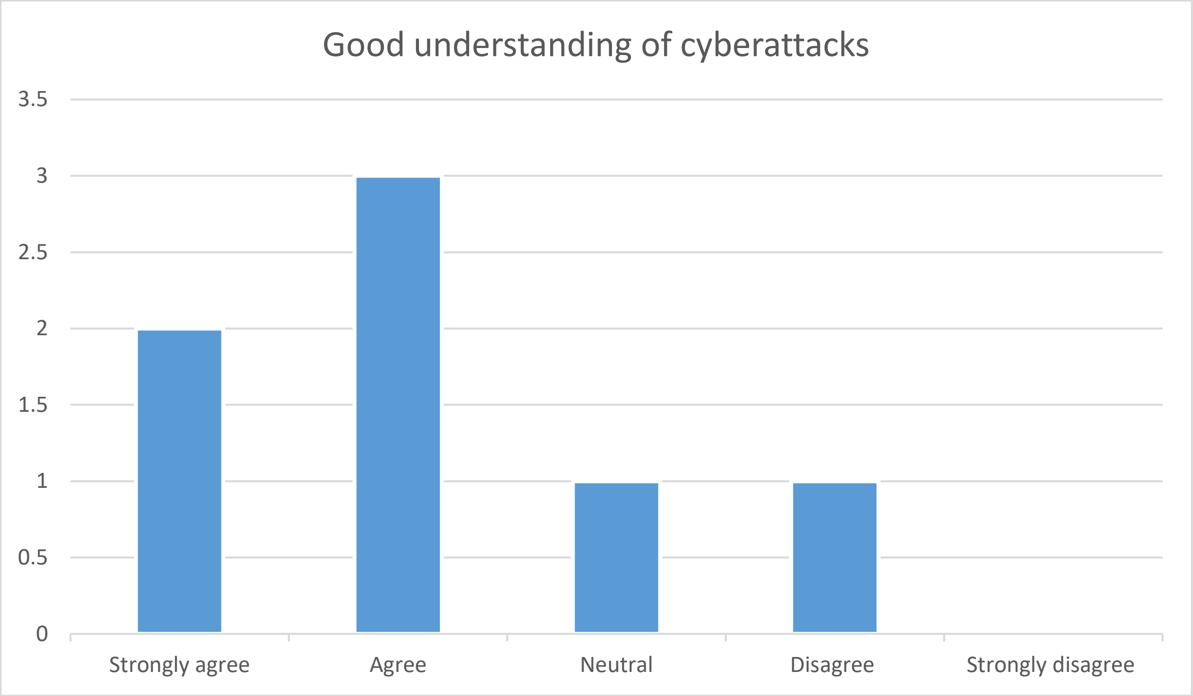


Figure D.135: Good understanding of cyberattacks (36-45)

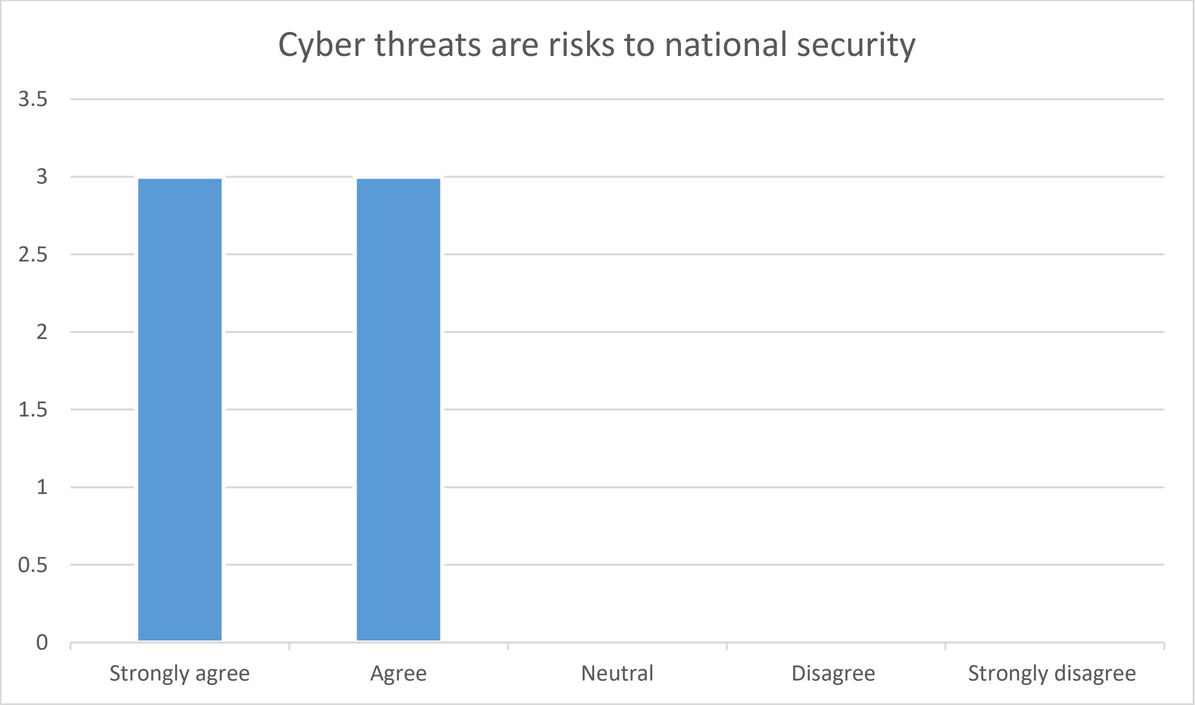


Figure D.136: Cyber threats are risks to national security (36-45)

Despite the level of security awareness training, the participants have a comparatively high understanding of the impact of cyber-attacks on the public and the organisation. Except for the 5 who have, 1 has no understanding, and 1 other did not say either way (See figure D.135). Furthermore, 86 percent of the participants have knowledge of the potential threats to national security from cyber-attacks (See figure D.136). Generally, understanding cyber threats and their impact on national security prompt people to act responsibly to minimise end-user errors; also, their engagement would influence acceptance and implementation of a national, regional, and global level mechanism.

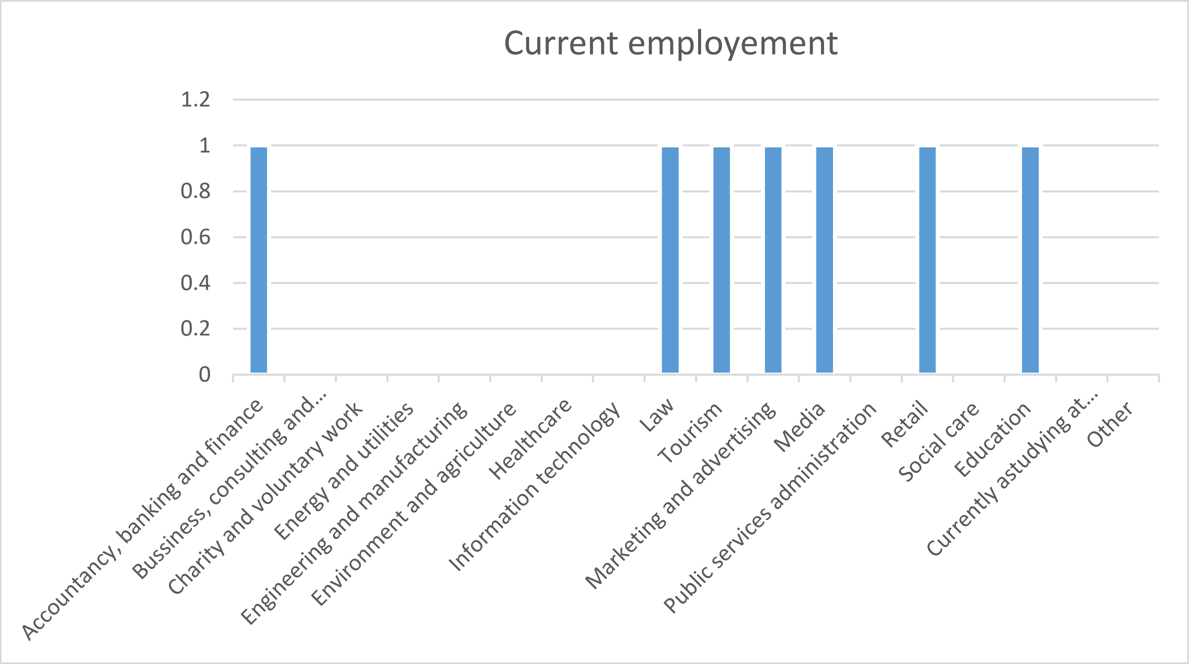


Figure D.137: Current employment (36-45)

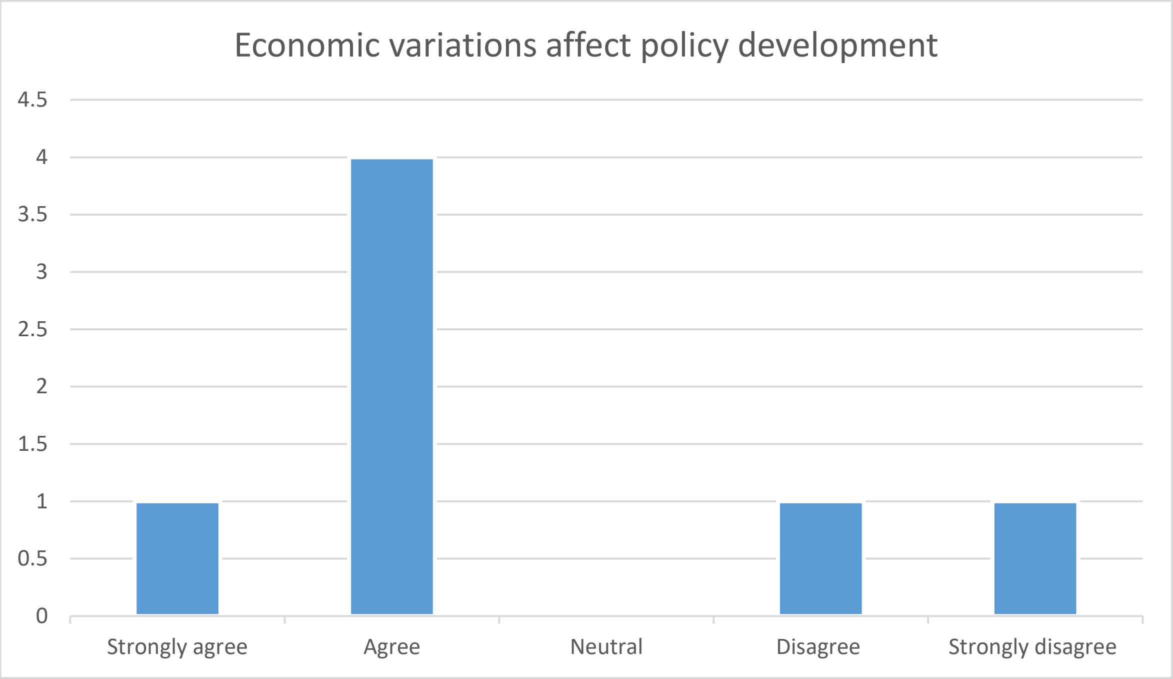


Figure D.138: Economic variations affect policy development (36-45)

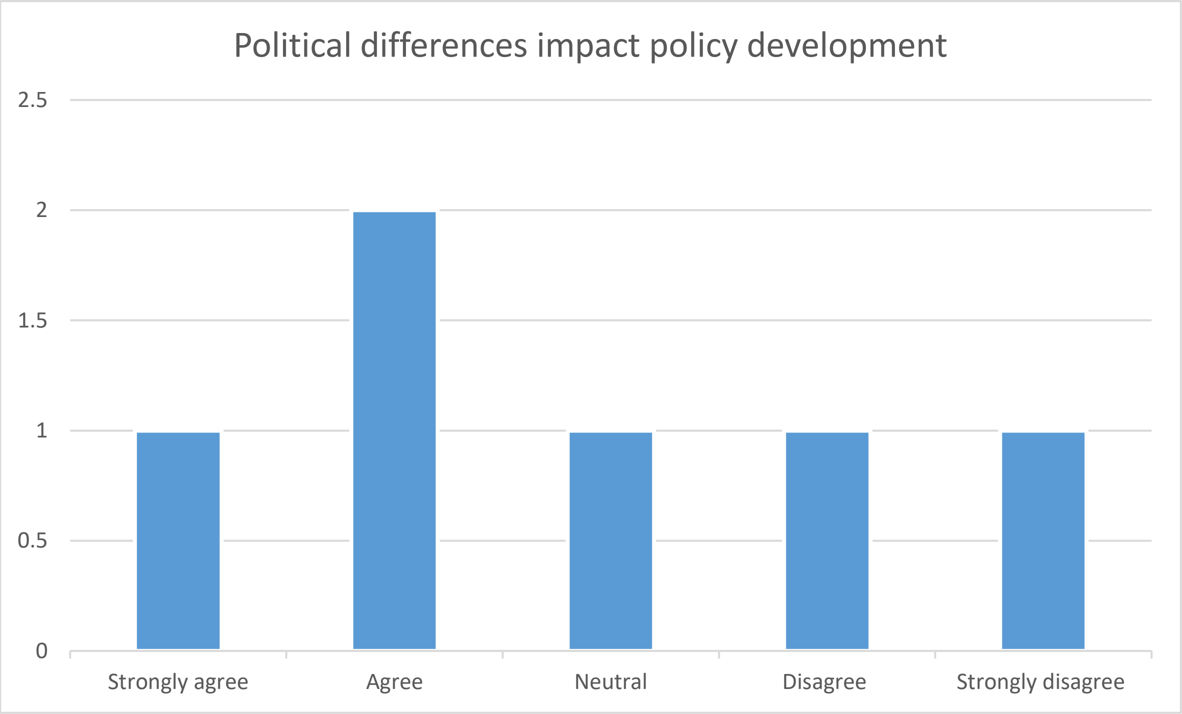


Figure D.139: Political differences impact policy development (36-45)

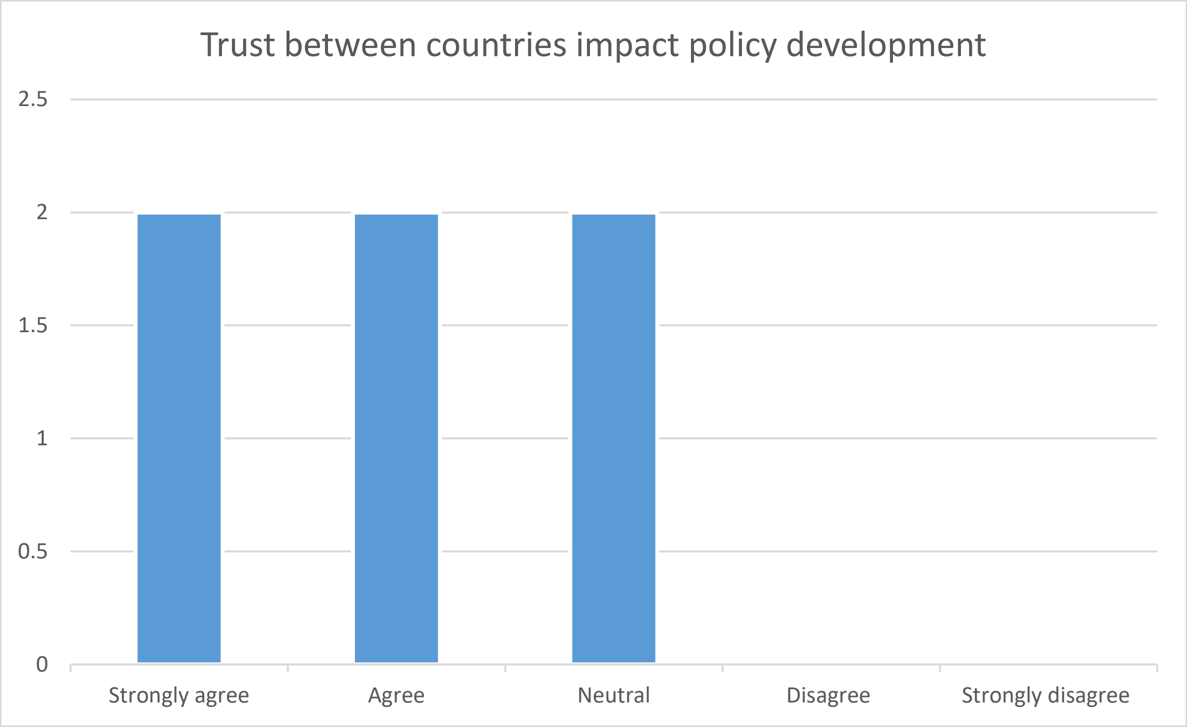


Figure D.140: Trust between countries impact policy development (36-45)

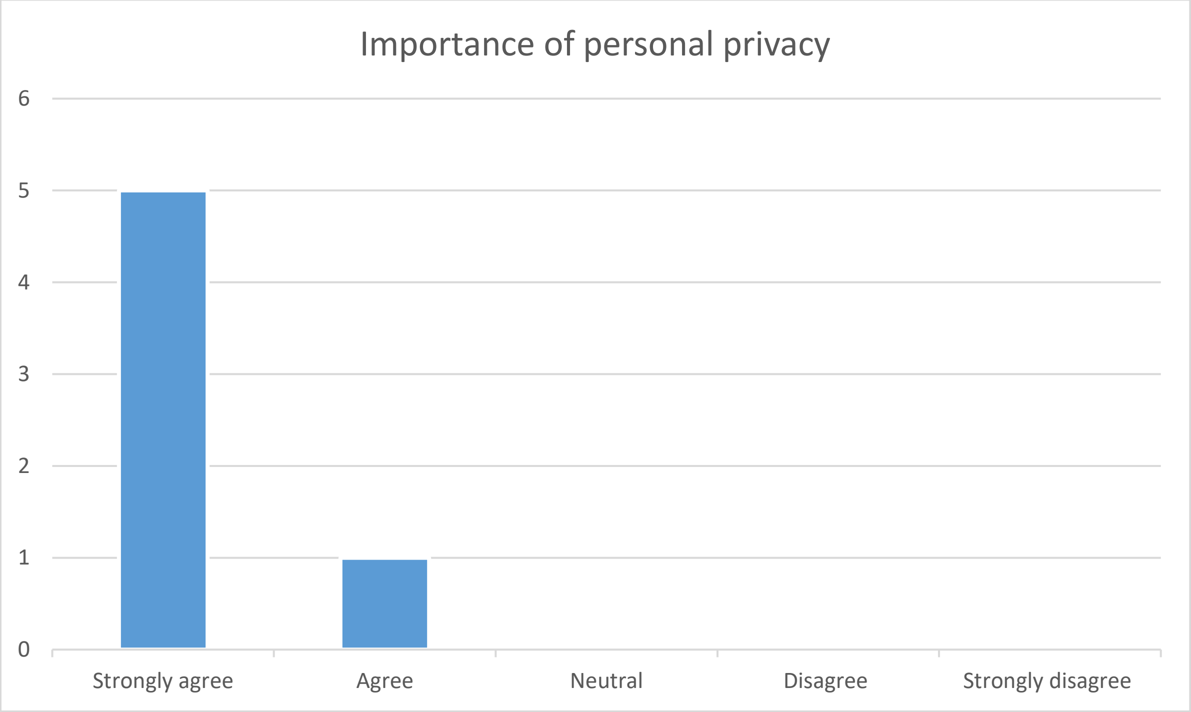


Figure D.141: Importance of personal privacy (36-45)

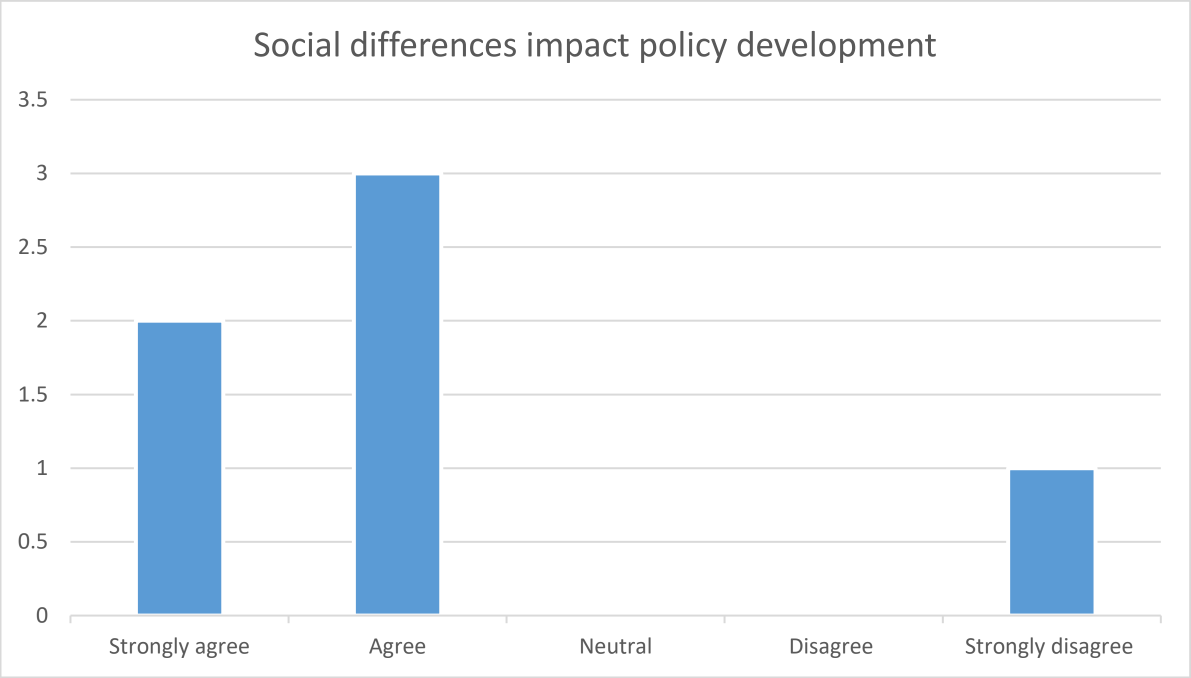


Figure D.142: Social differences impact policy development (36-45)

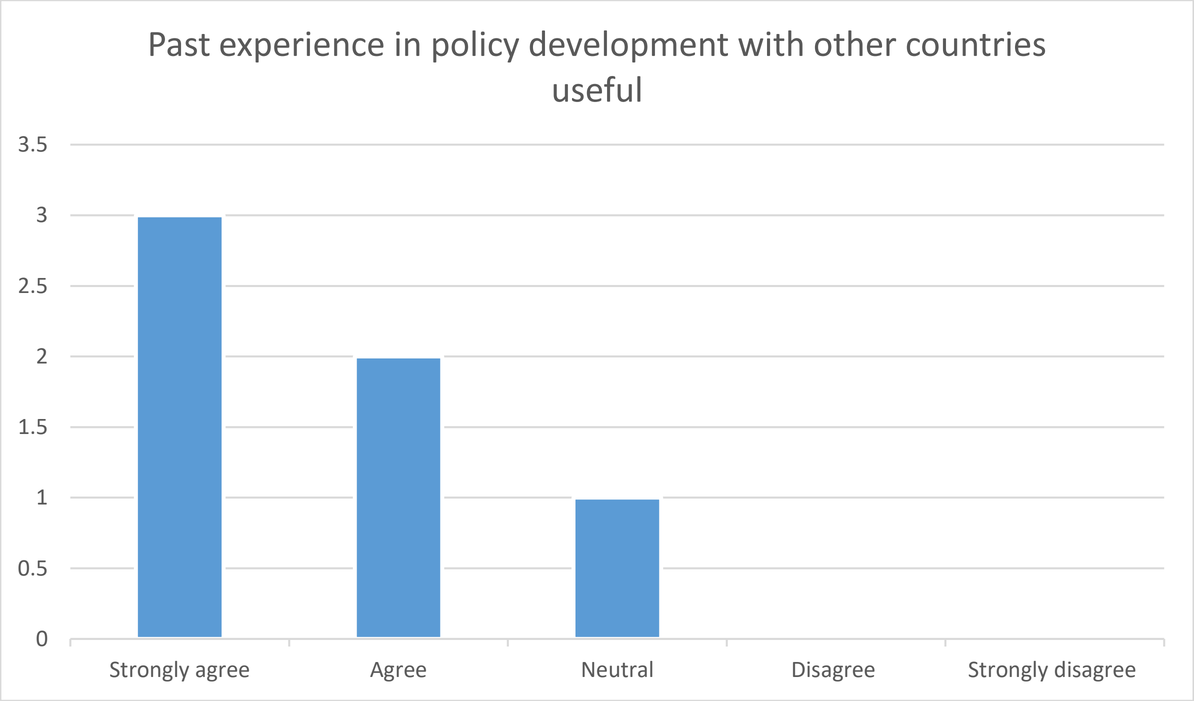


Figure D.143: Past experience in policy development with other countries useful (36-45)

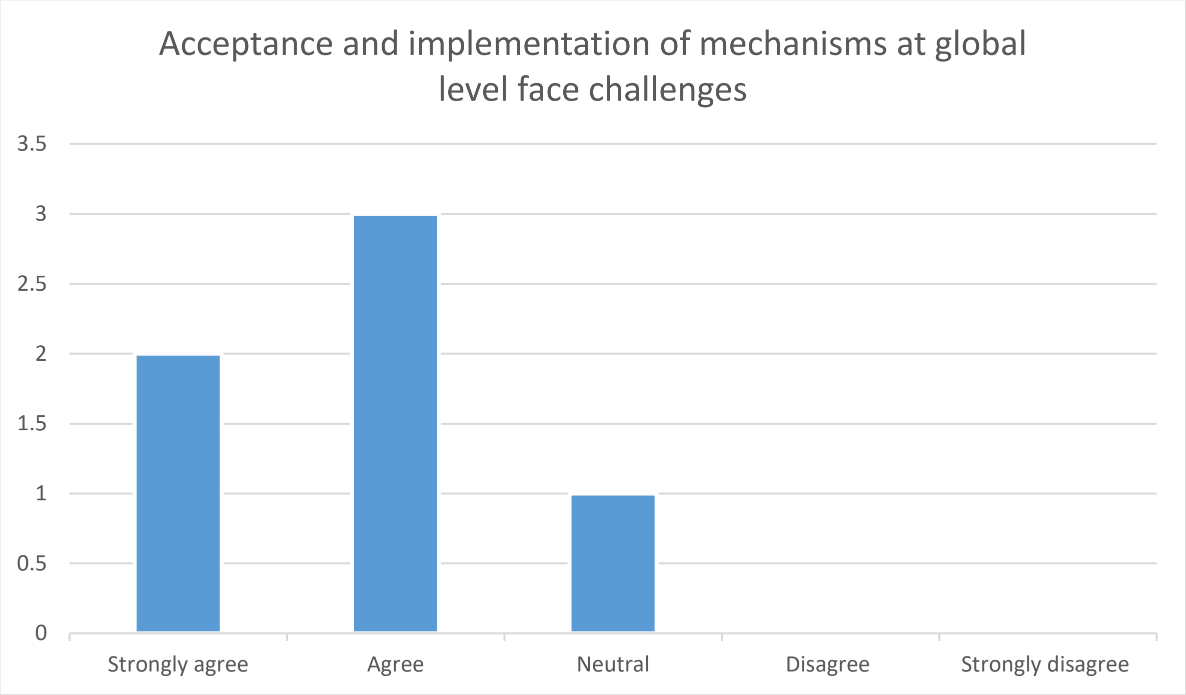


Figure D.144: Acceptance and implementation of mechanisms at global level face challenges (36-45)

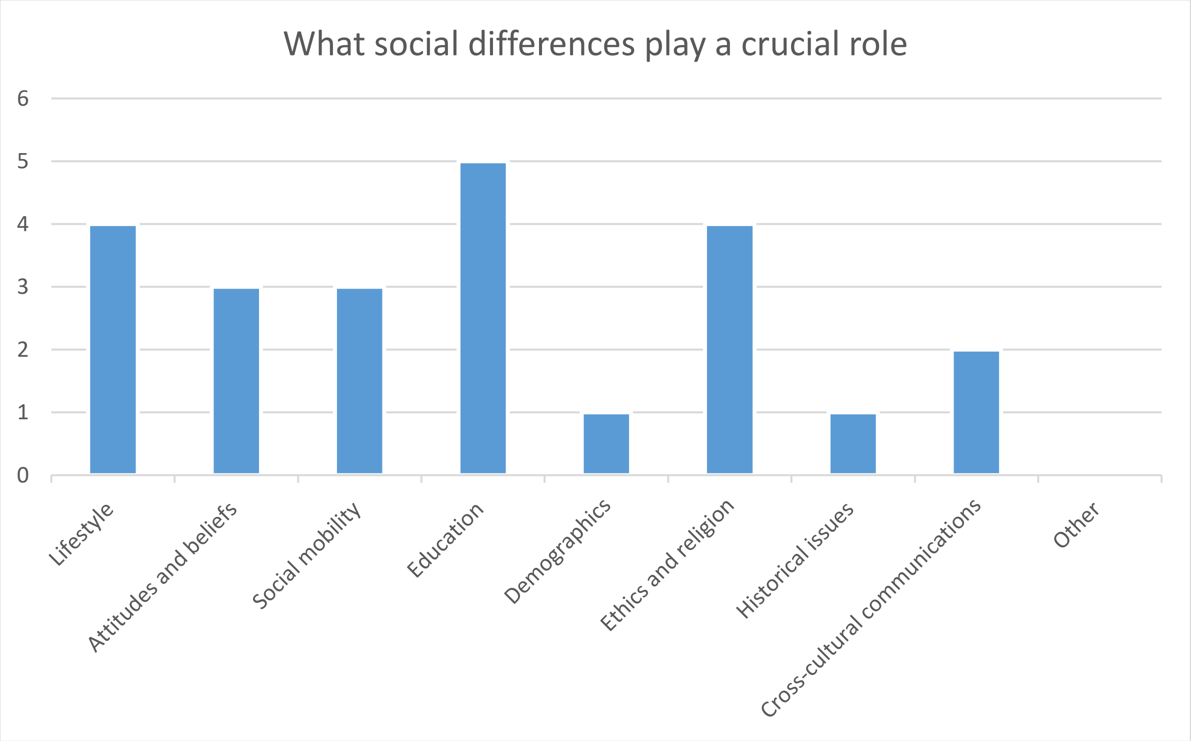


Figure D.145: What social differences play a crucial role (36-45)

In response to the social difference, the majority scores the importance of education, attitudes and beliefs, ethnicity, and religious preferences (See figure D.145). These evaluations indicate the importance of awareness of potential cyber threats, and their impact on people and national security in accepting and implementing data privacy and security policies. That makes the delivery of cybersecurity awareness training at the school and organisational level an essential requirement. The desirability of placing faith in privacy, respecting the privacy of self and others have been discussed under attitude and beliefs. It is intriguing to note the importance of ethics and religion given prominence. The reasonable assumption to make is that the perception of the participants living in a mixture of cultural, religious, and social environment are not integrated into a coherent diverse lifestyle to an appreciative level.

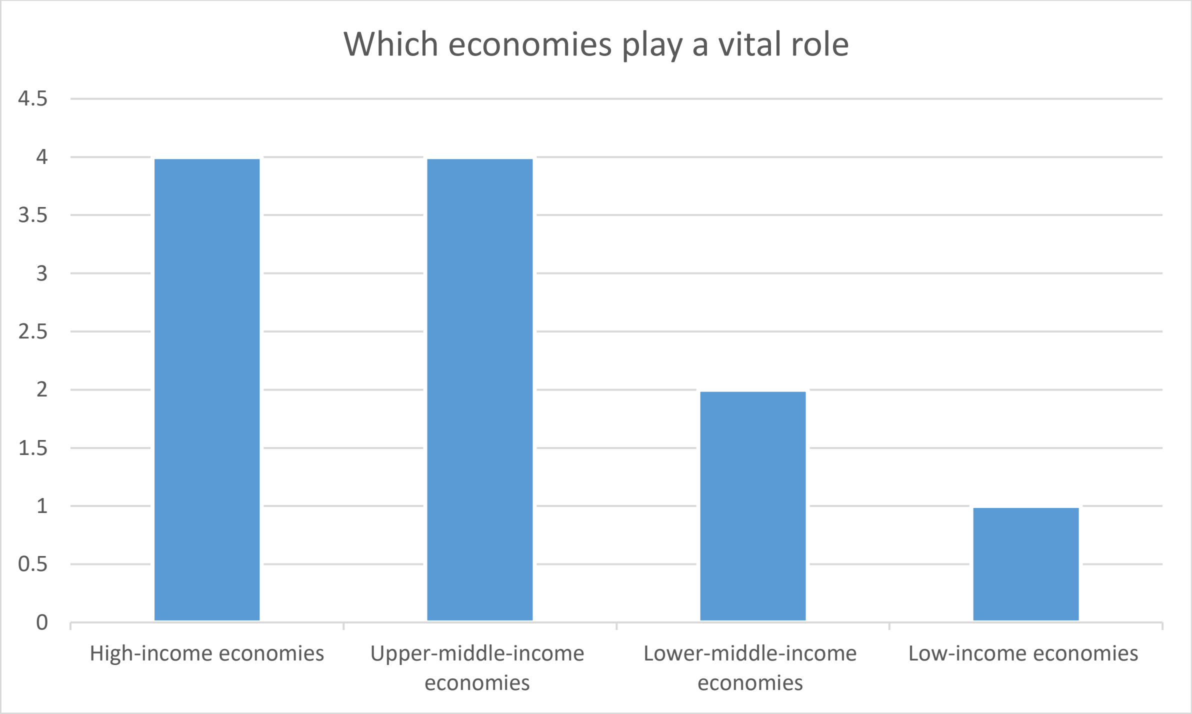


Figure D.146: Which economies play a vital role (36-45)

The majority of the respondents suggest that both high income and upper-middle-income countries play a vital role in the policymaking process (See figure D.146). The key stages in the policymaking process aim to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the resources necessary, implement, and finally evaluate the policy. These stages are time-consuming and require sufficient funding and resources. Therefore, achieving success to a large extent depends on the economic stability of the country, and is considered crucial in the policymaking process.

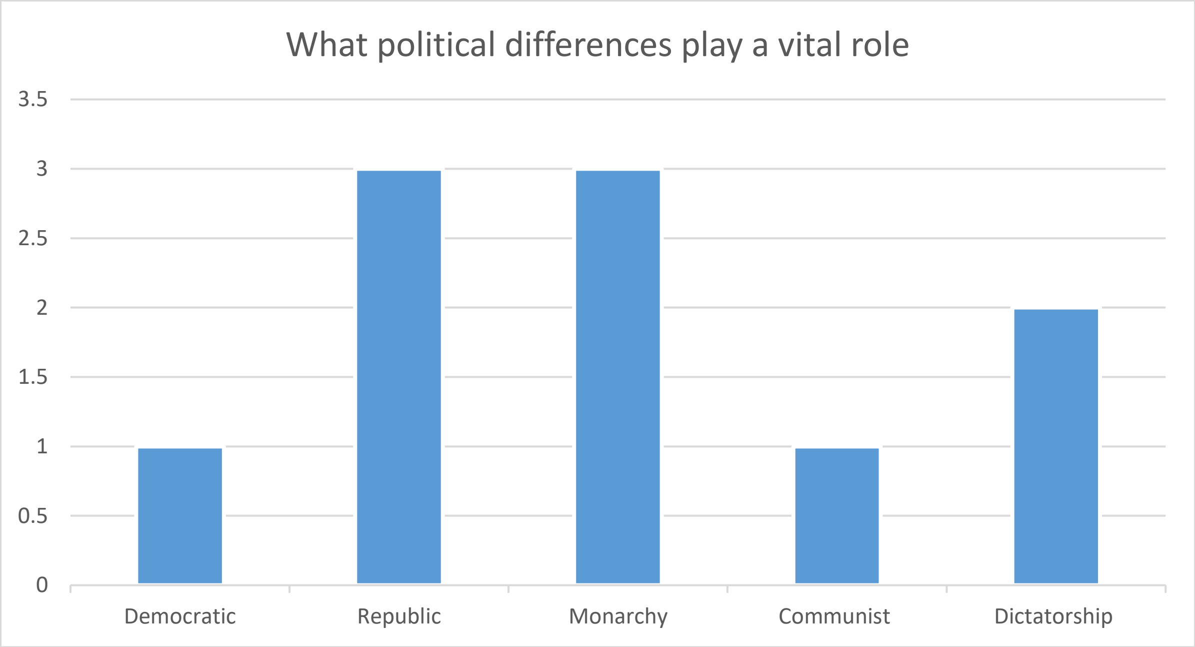


Figure D.147: What political differences play a vital role (36-45)

Unlike the participants in other age groups, a specific political system not chosen by a majority in 36-45 age range (See figure D.147). Only 43 percent selected both republic and monarchist system. In a Republican Model Administration, it is common practice for the public to contribute to policy development. That is an effective way to ensures collective responsibility for their actions. This forms the basis for developing trust between the organisations and ensured transparency and coherence in the policy development process. Also, the constitutional rights of the public give assurance that the organisations collecting, storing, and sharing personal information will not be compromised for any reason. The monarchist system has an individual ruler as head of state having functional power to sustain his/or her hereditary status. This system does not provide space for public participation and expression of opinions prohibited, and the power of the ruler is unquestionable. The reason for choosing Monarchist system is likely to be the failures and shortcomings of democratic systems of governance.

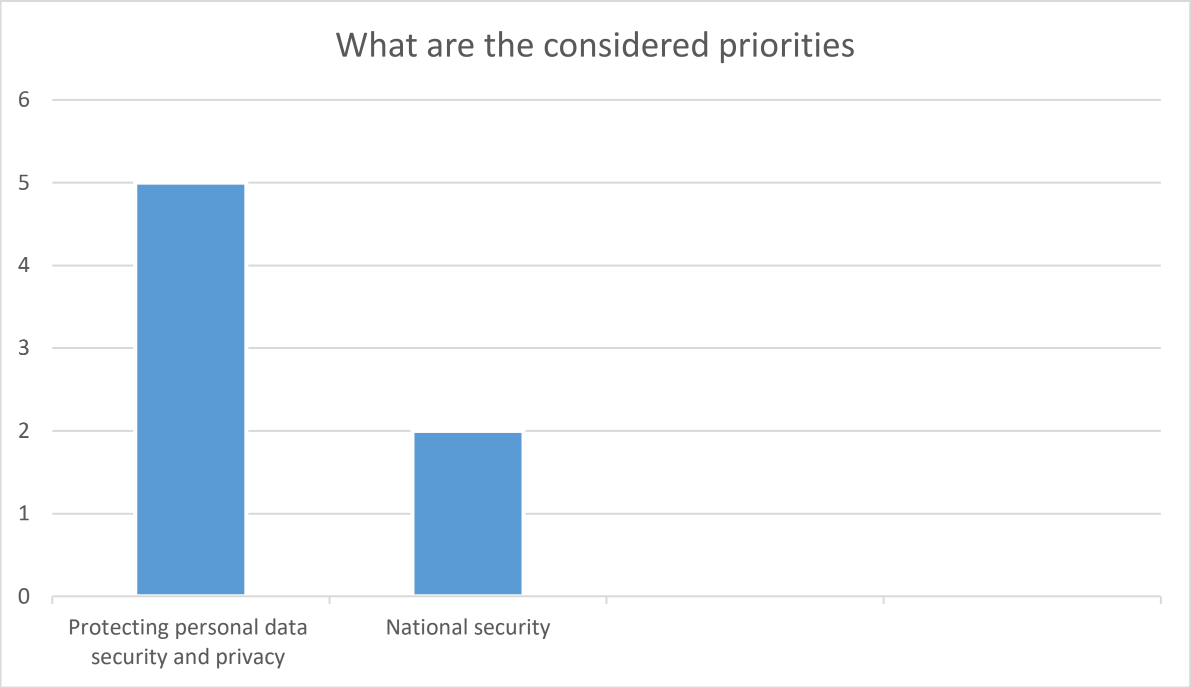


Figure D.148: What are the considered priorities (36-45)

In accepting and implementing a global data privacy and security policies, the participants focus far more on the importance of protecting personal data security and privacy and less on protecting national security but without discounting the importance of national security altogether (See figure D.148). These participants are not teenagers but people with previous experience. They have learned from their lifetime background experience not to risk personal privacy, and the awareness that potential privacy breaches would impact badly on them and their families, in term of damage to their reputation and standing in the community, mental trauma, and suffering financial losses.

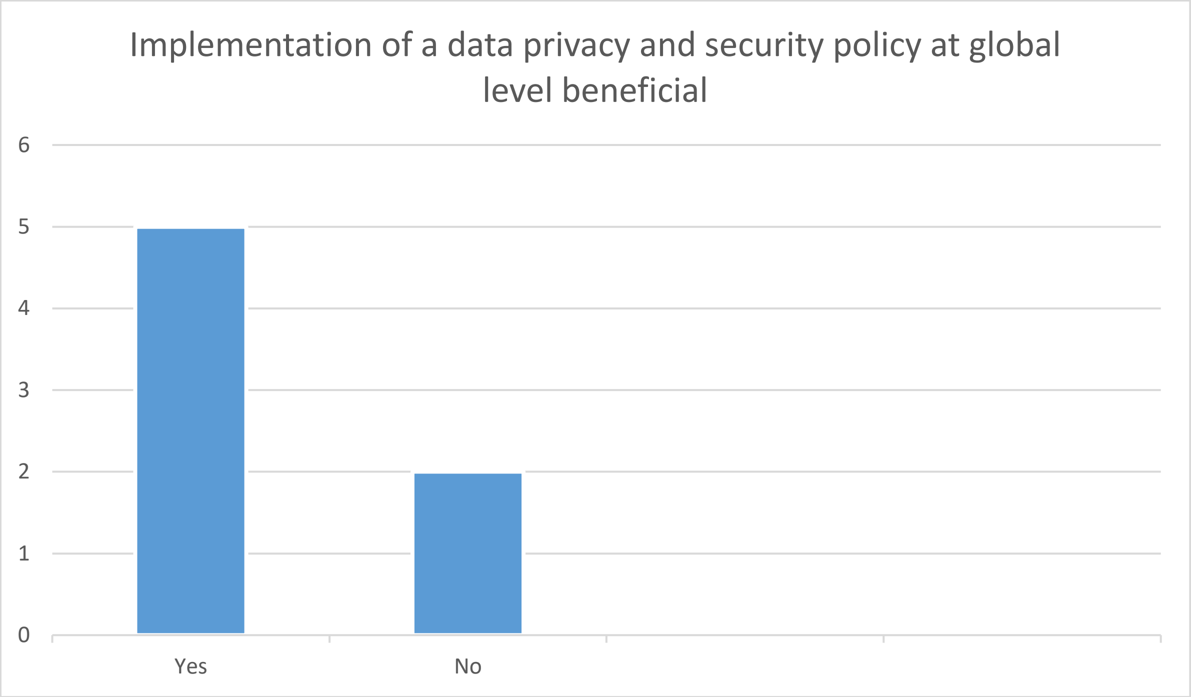


Figure D.149: Implementation of a data privacy and security policy at global level beneficial (36-45)

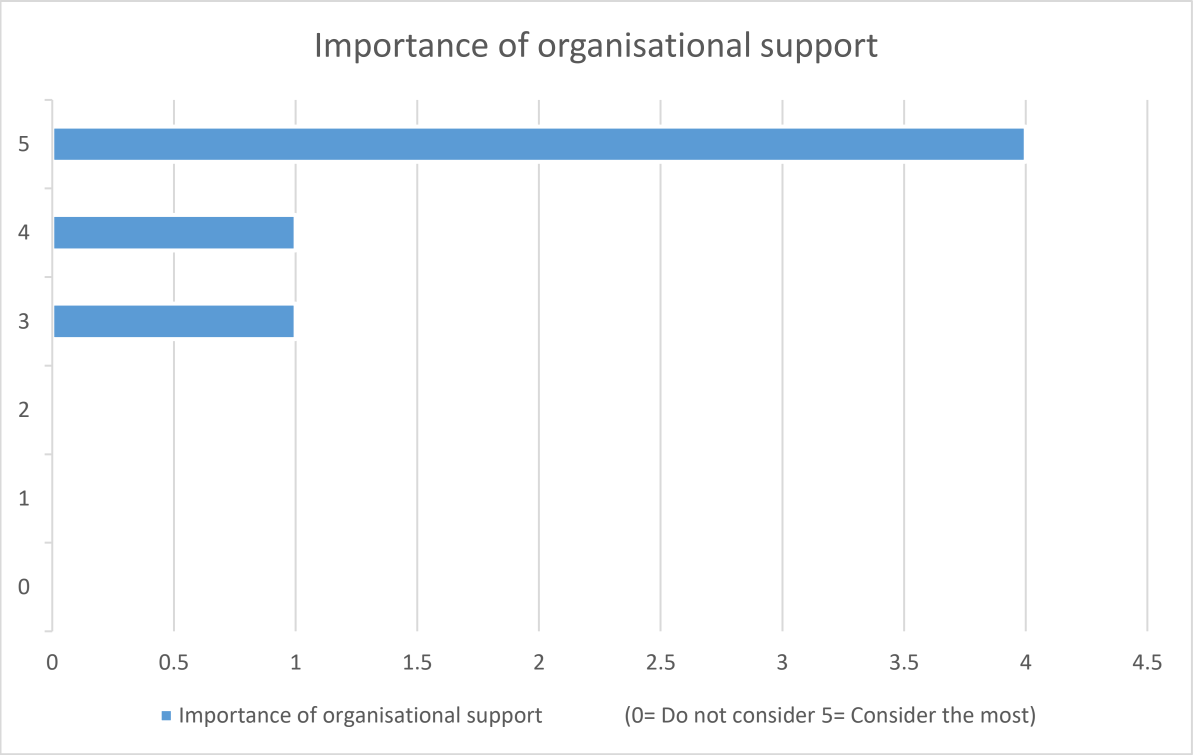


Figure D.150: Importance of organisational support (36-45)

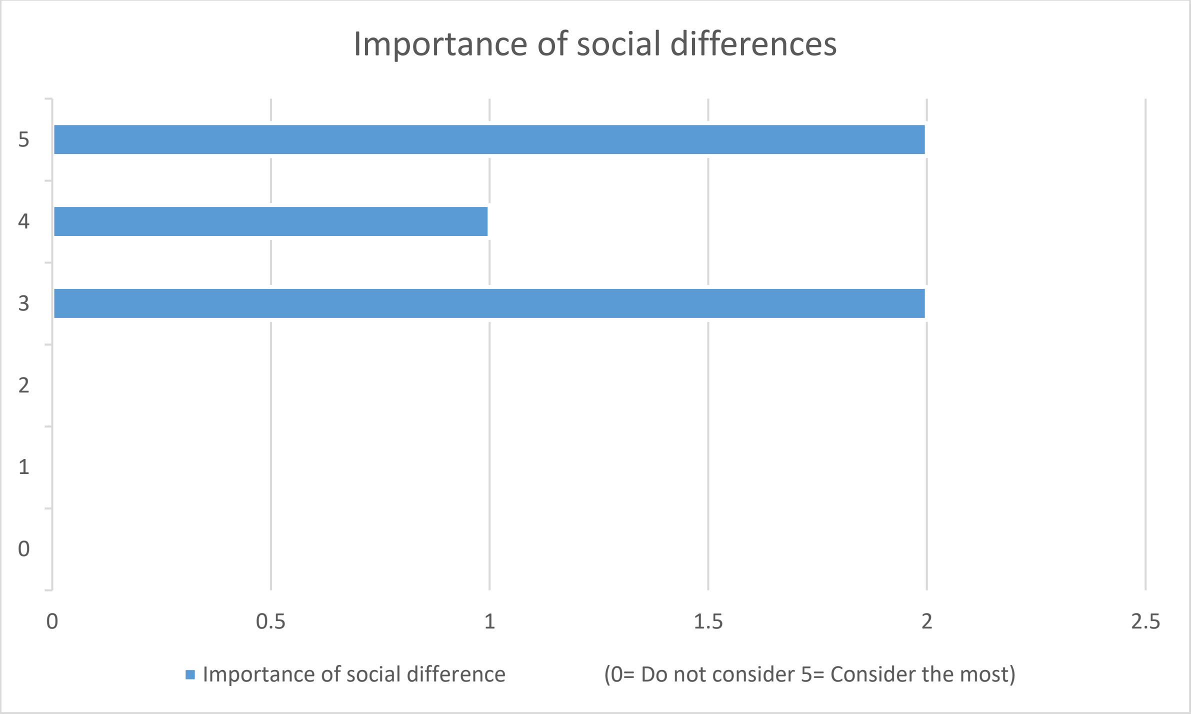


Figure D.151: Importance of social differences (36-45)

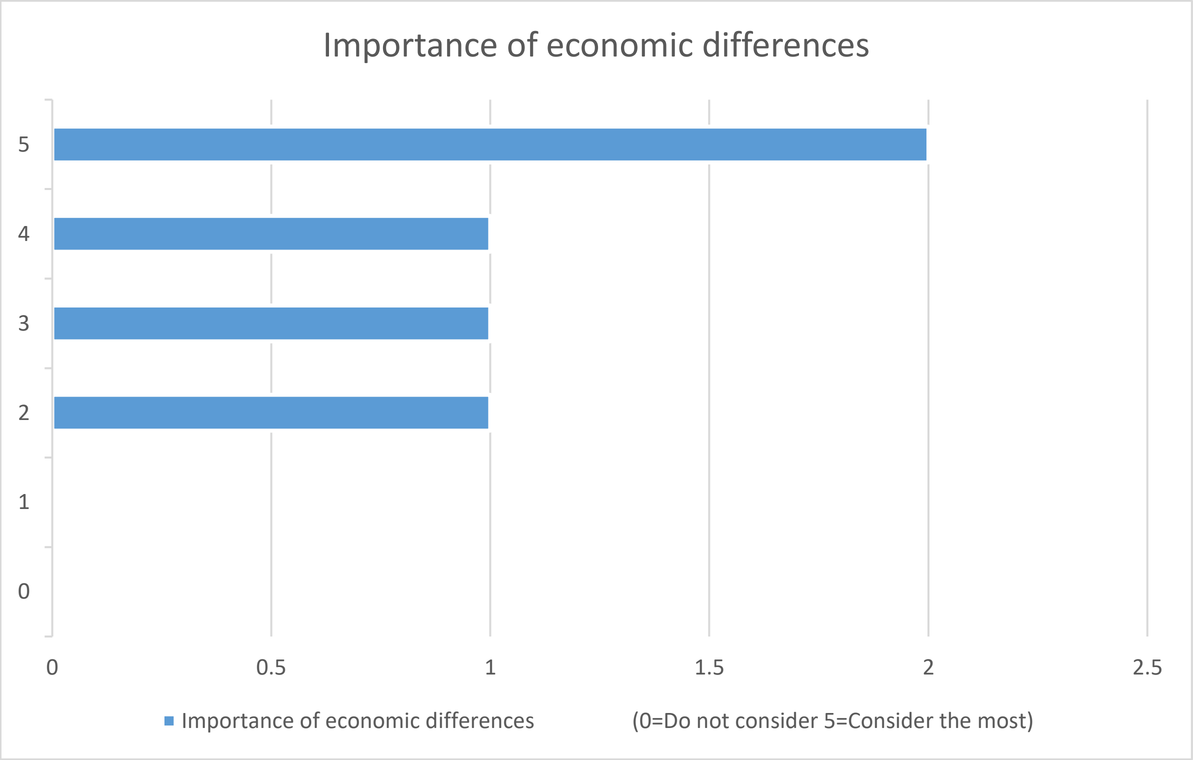


Figure D.152: Importance of economic differences (36-45)

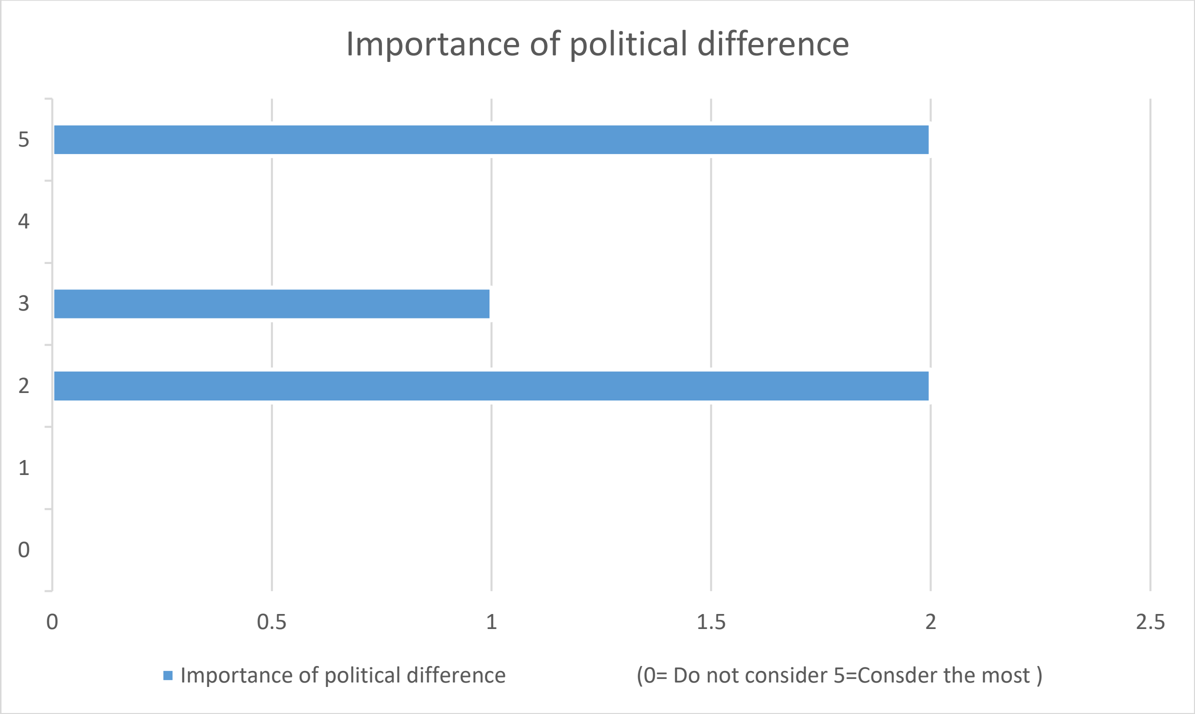


Figure D.153: Importance of political difference (36-45)

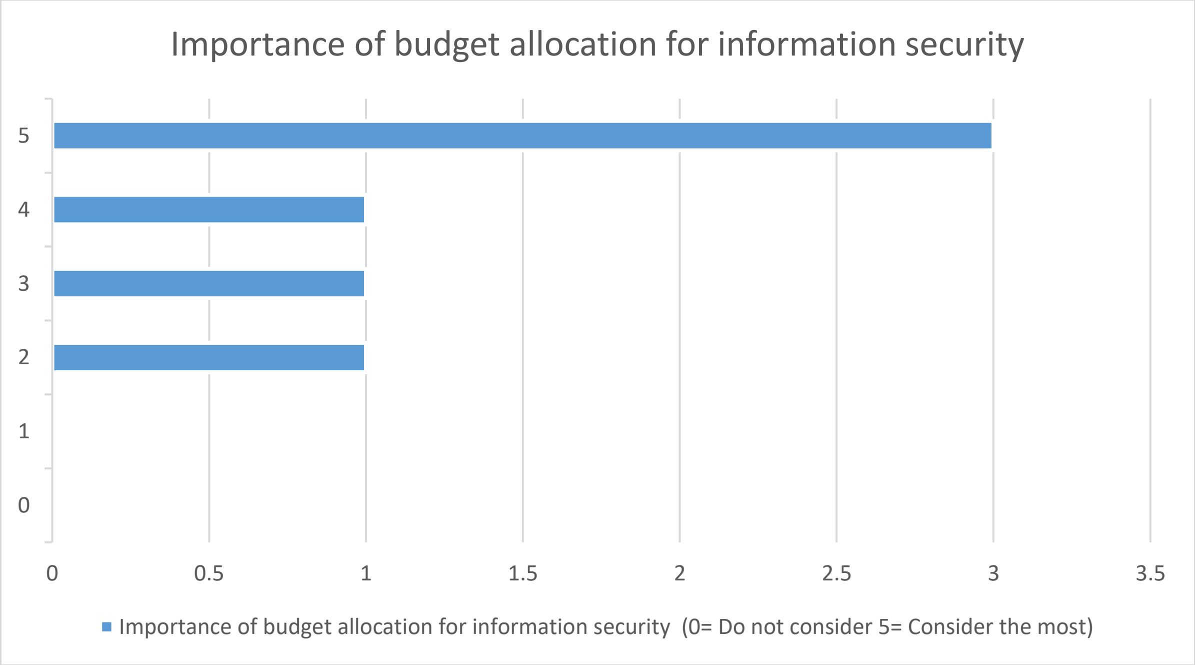


Figure 4.154: Importance of budget allocation for information security (36-45)

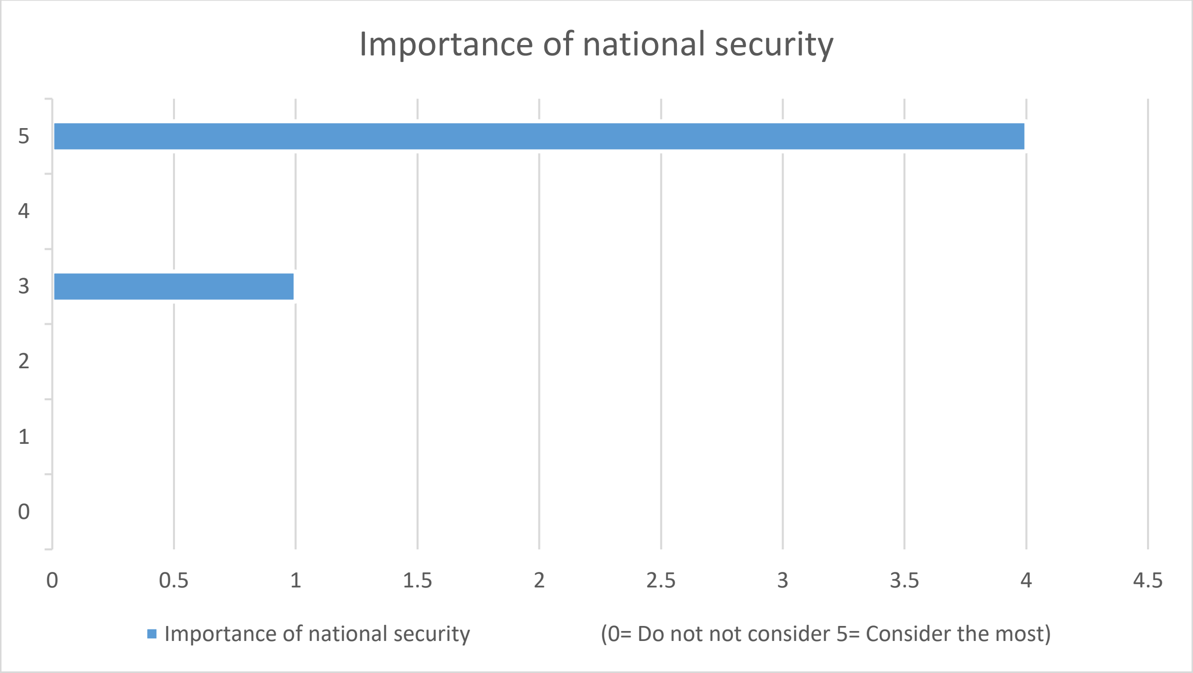


Figure D.155: Importance of national security (36-45)

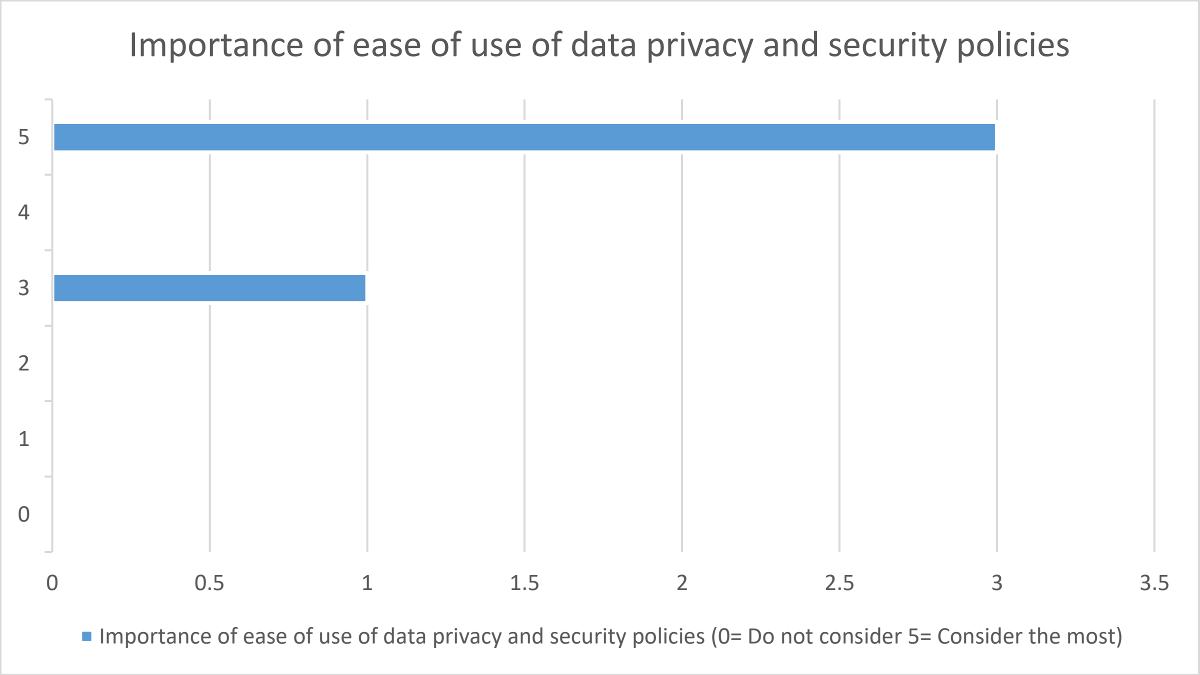


Figure 4.156: Importance of ease of use of data privacy and security policies (36-45)

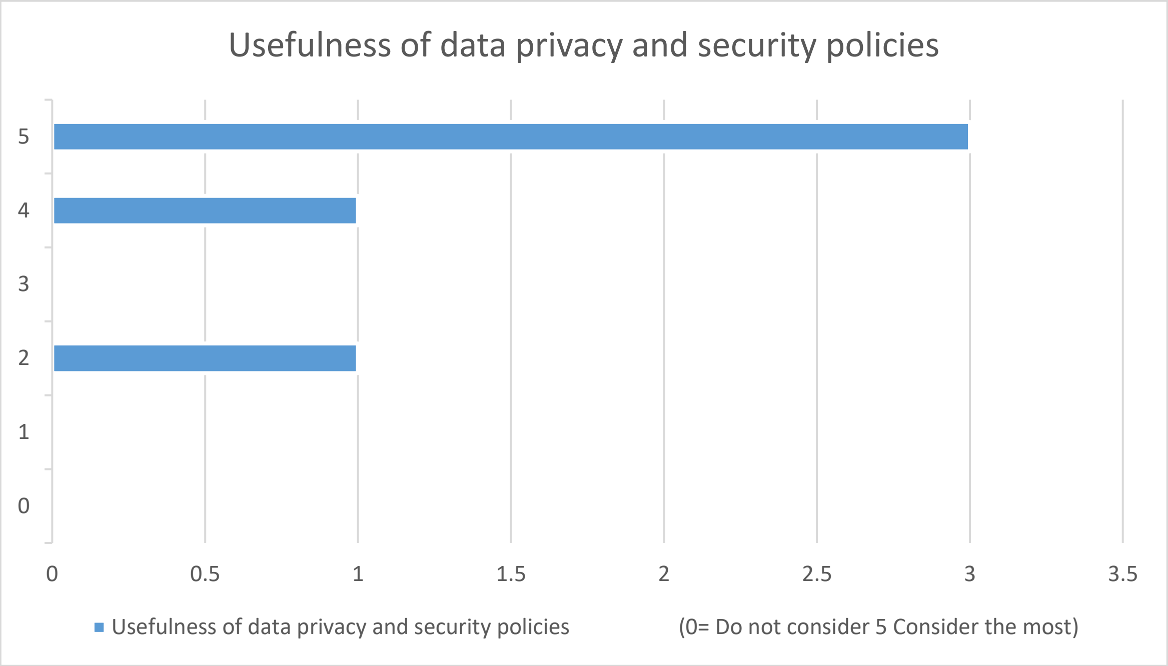


Figure 4.157: Usefulness of data privacy and security policies (36-45)

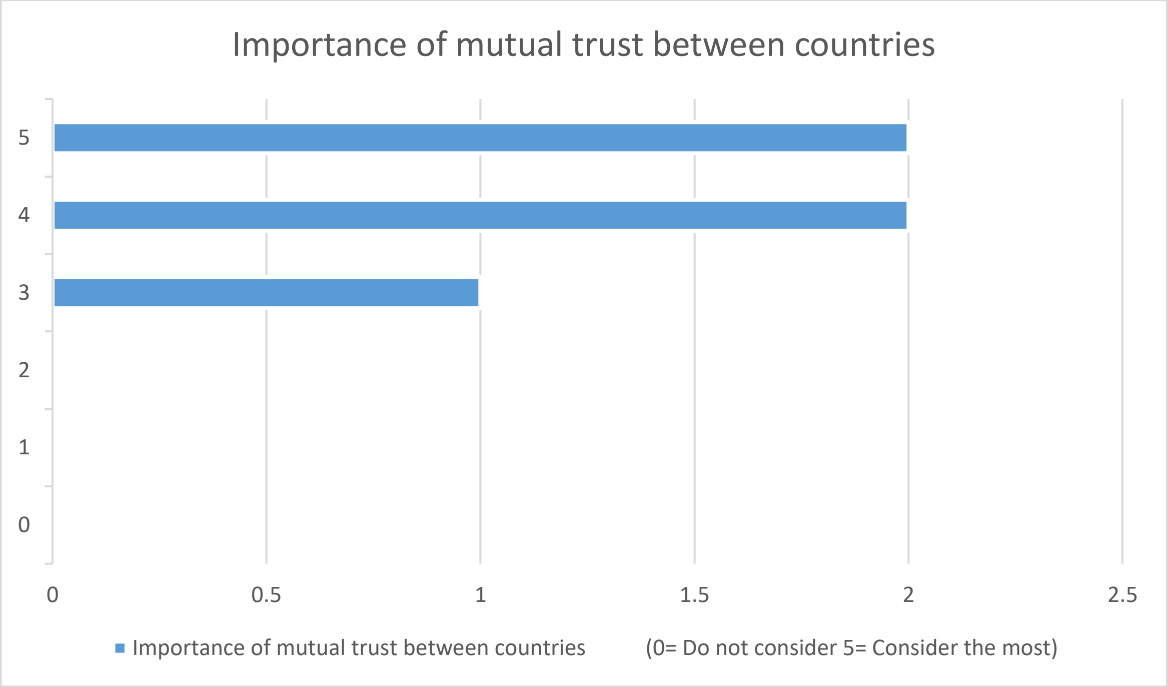


Figure 4.158 Importance of mutual trust between countries (36-45)

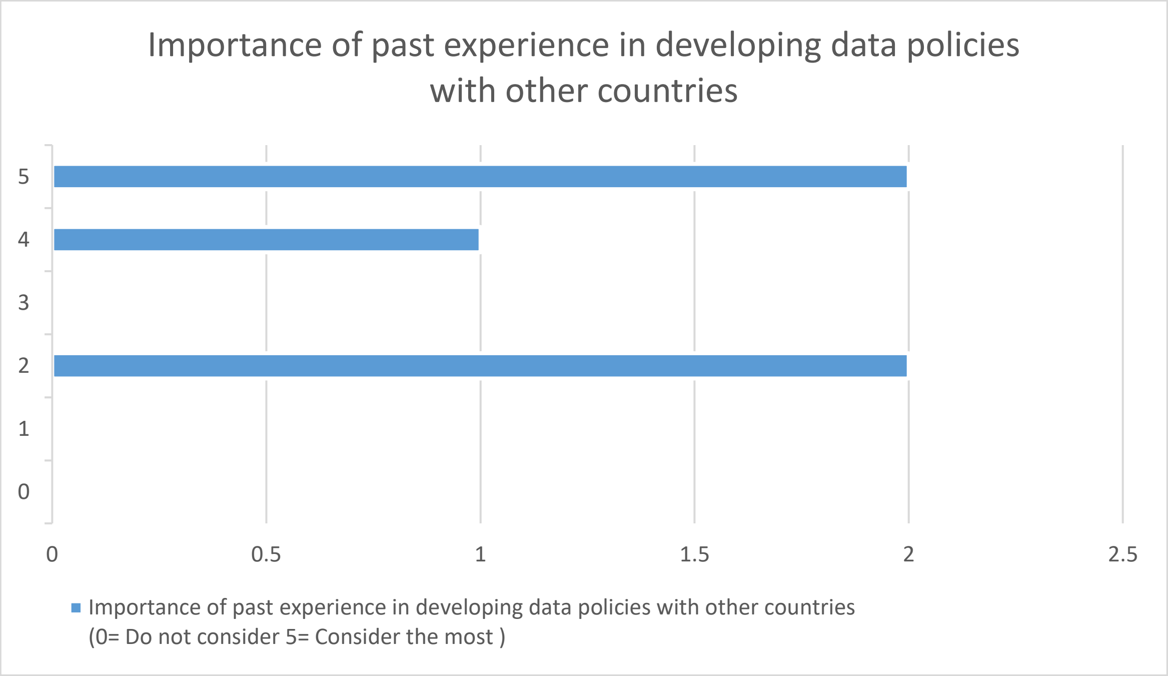


Figure D.159: Importance of past experience in developing data policies with other counties (36-45)

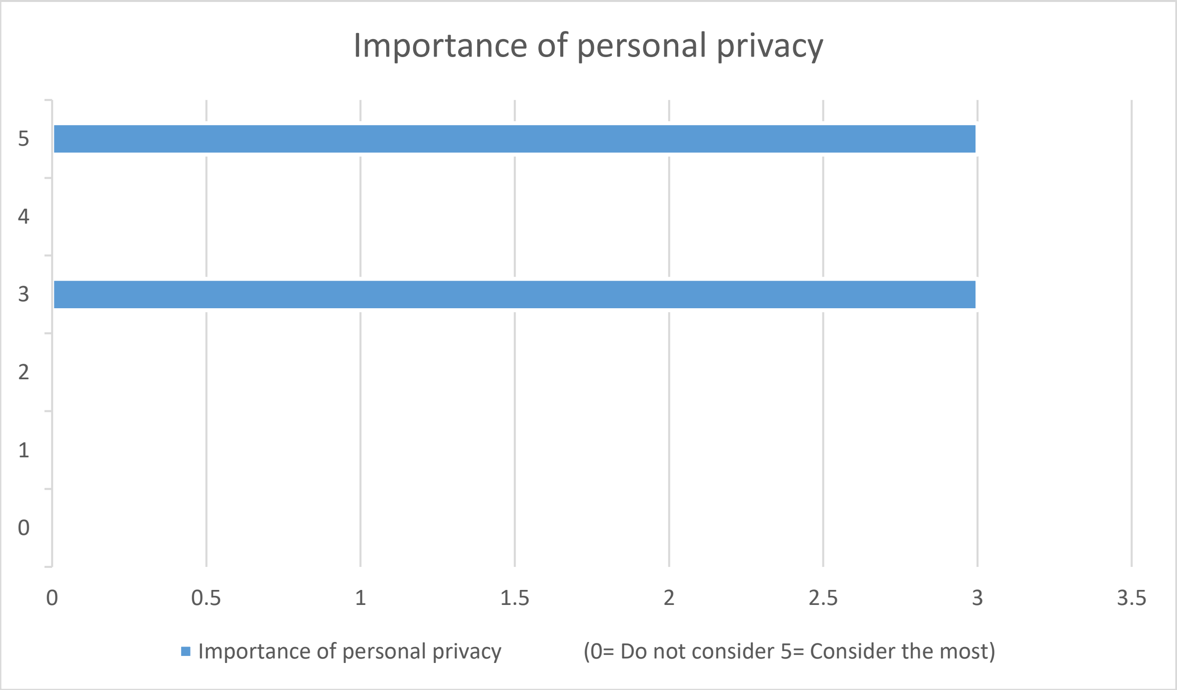


Figure 4.160: Importance of personal privacy (36-45)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 71 percent of the respondents have endorsed (See figure D.149). The other notable factors coming out of the survey are organisational support, budget allocation for information security, social differences, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies and mutual trust between countries (See D.138-D.148) (See figure D.150-160).

Sri Lanka- 46+

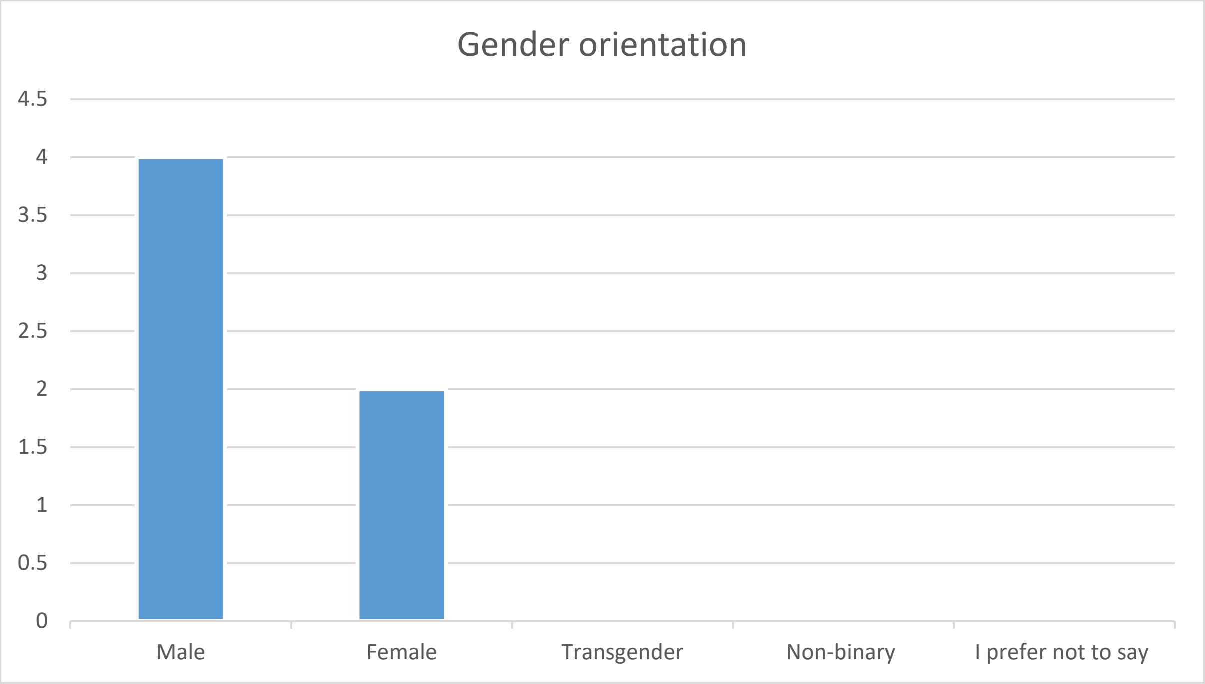


Figure D.161: Gender orientation (46+)

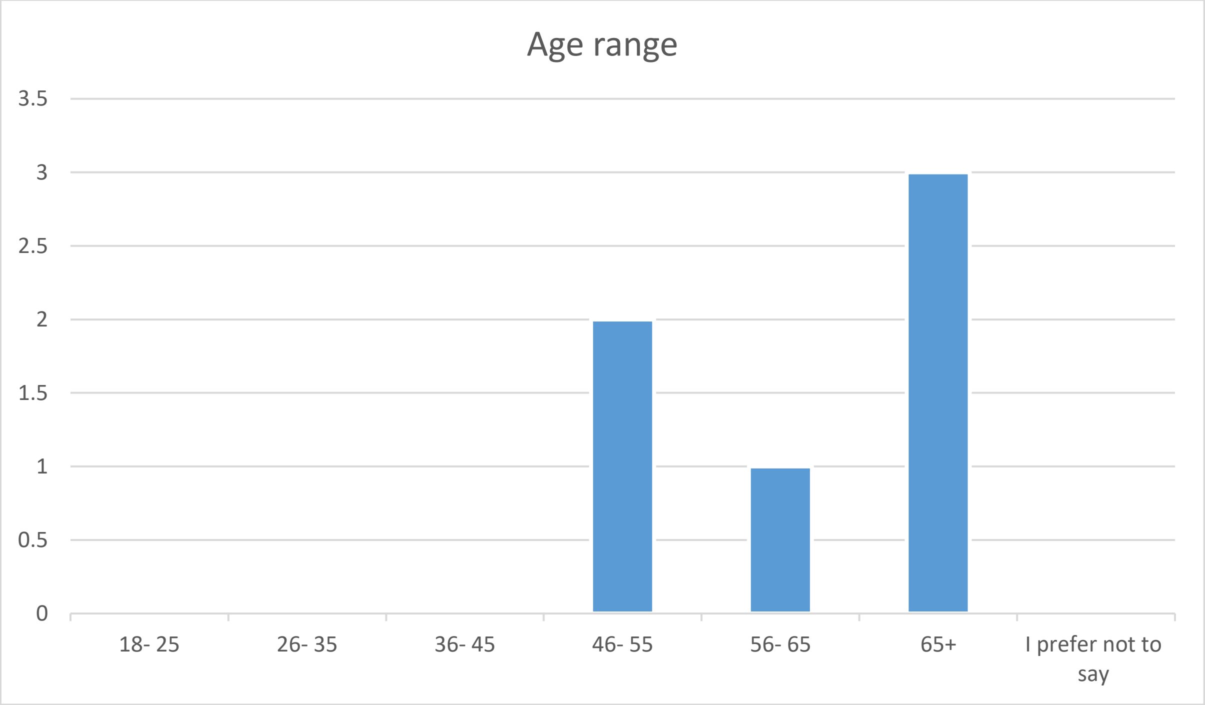


Figure D.162: Age range (46+)

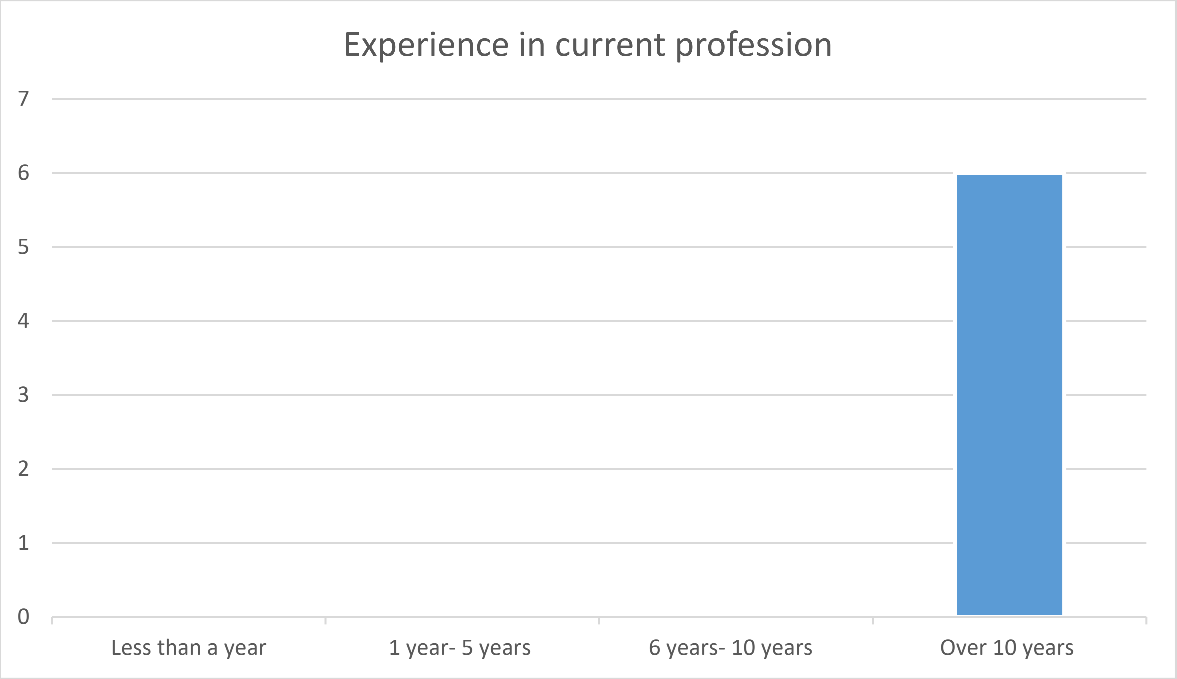


Figure D.163: Experience in current profession (46+)

This analysis is based on the responses received from Sri Lankan participants who are aged above 46 plus range. There were 6 participants, 4 males and 2 females (See figure D.161); categorised into 2 in 46-55, 1 in 56-65, 3 over 65 plus range (See figure D.162). 100 percent of the participants have been working in the industry for over 10 years (See figure D.163).

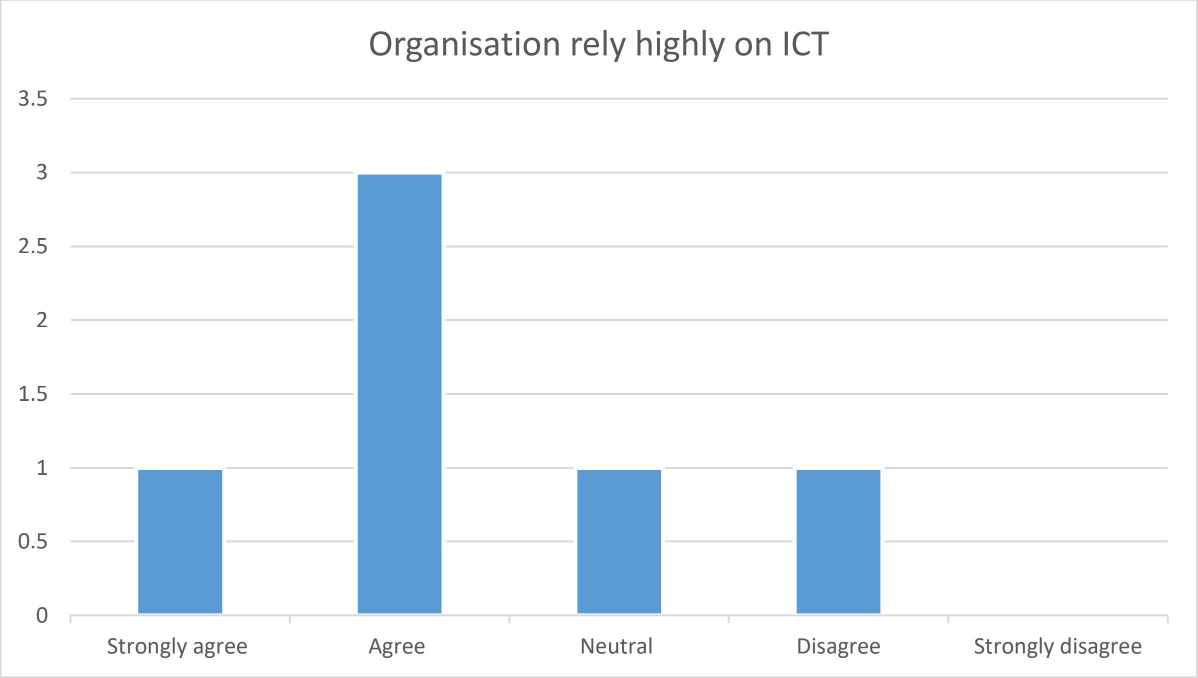


Figure D.164: Organisation rely highly on ICT (46+)

Out of the 6 respondents, 4 have worked in a technology reliance working environment, 1 unaware of reliance on technology because of the nature of the work assigned to them, 1 have marked ‘disagree’ on ICT (See figure D.164). This indicates a majority (4 out of 6) have been working for over 10 years in an organisation with high reliance on ICT.

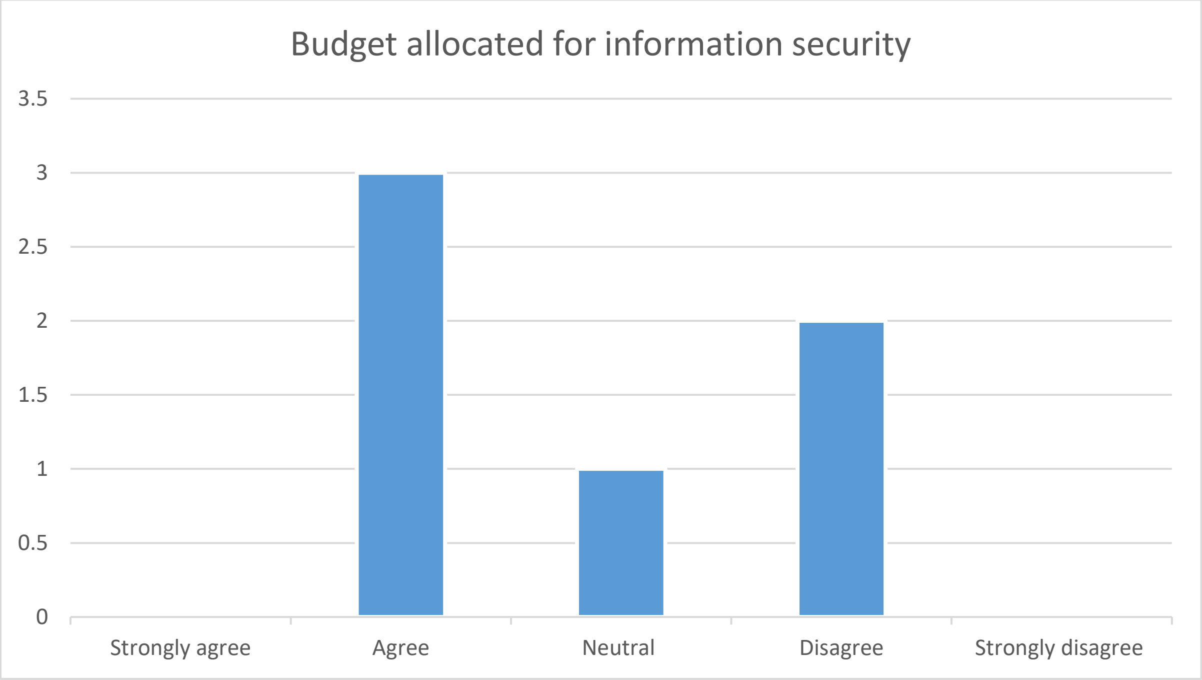


Figure D.165: Budget allocated for information security (46+)

3 out of the 6 have indicated that their organisations had a budget allocation for information security; 1 did not express an opinion either way; notably, according to the 2 disagreed, their organisations had no budget allocation for information security (See figure D.165).

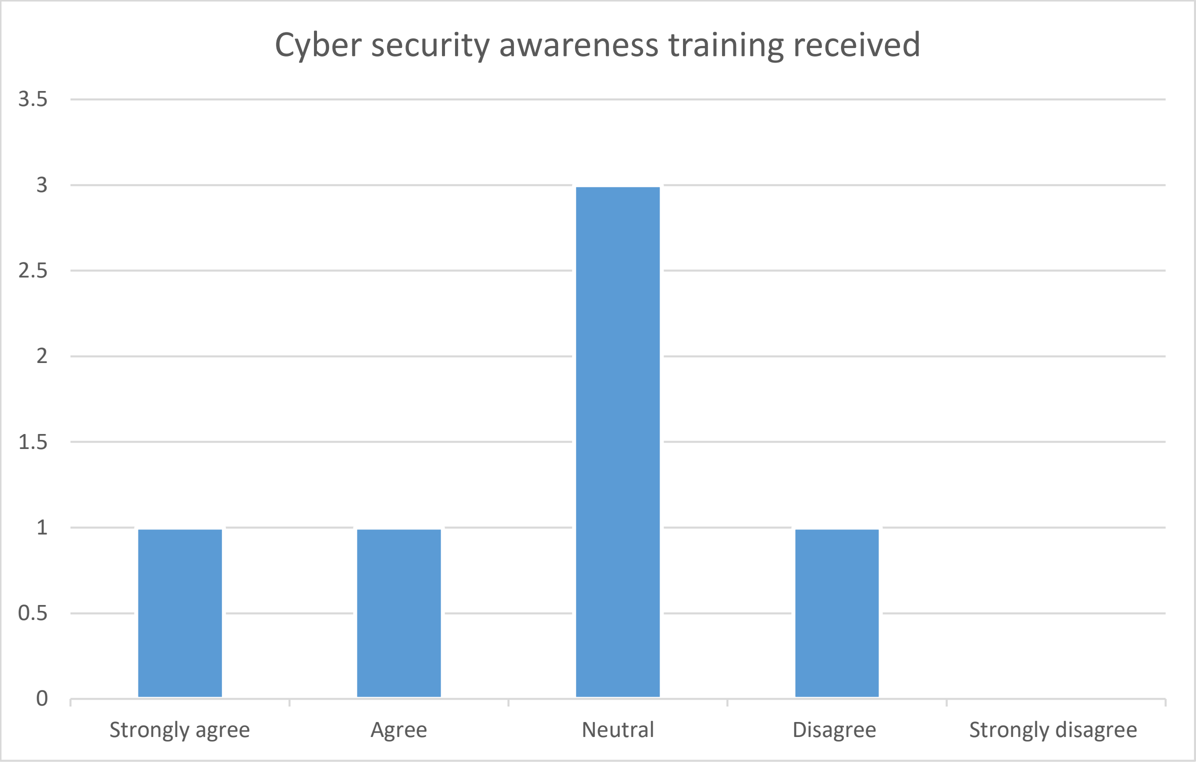


Figure D.166: Cyber security awareness training received (46+)

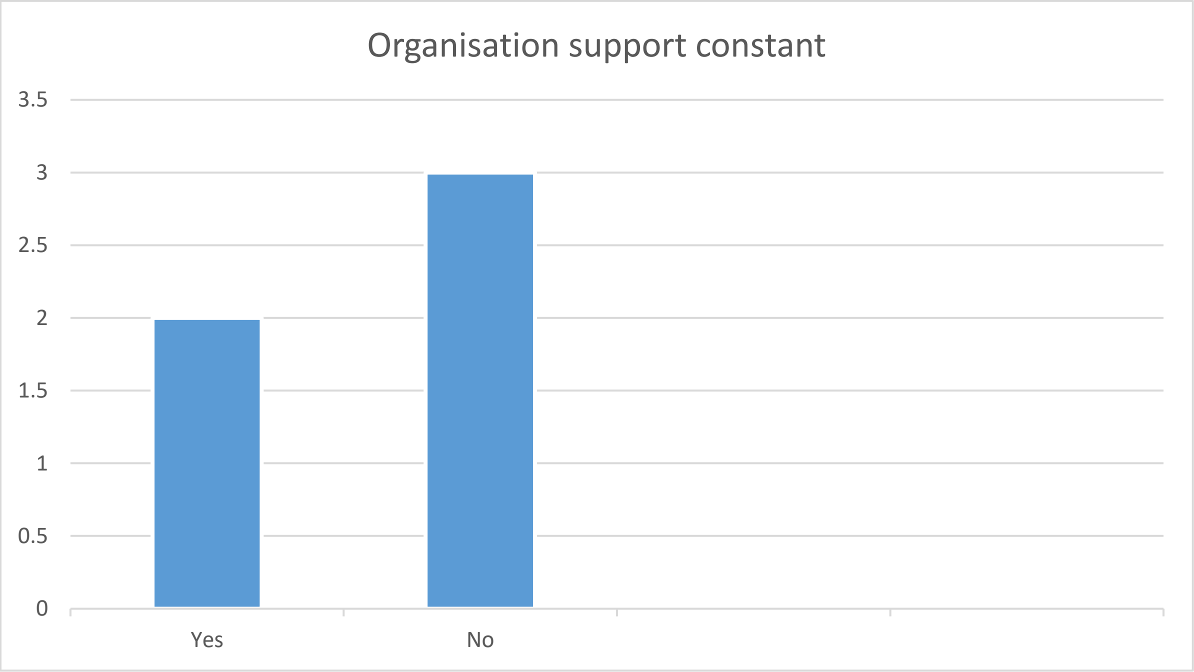


Figure D.167: Organisation support constant (46+)

According to some of the participants, despite the satisfactory level of resources allocated for information security, regular security awareness training they received was inadequate, Only 2 participants have received regular cybersecurity awareness training; 3 neither agreed nor disagreed; 1 participant had not received security awareness training regularly (See figure D.166). In addition, 3 participants had not received support from the organisation to protect personal information and only 2 did (See figure D.167). This represents lack of organisational support to protect personal information despite the budget allocated for information security and high reliance on technology.

Considering the history of technology and the age range of the participants, it is not surprising to note the variation in the responses. Also, it is likely that the nature of the work assigned to them did not want extensive training and in-depth knowledge of ICT, and for that reason, the organisation would have used available resource in a selective and cost-effective way. It is also the case that the employers themselves had little understanding of the threats and did not see the importance of providing training to every employee, except for those engaged in areas with high dependency on ICT.

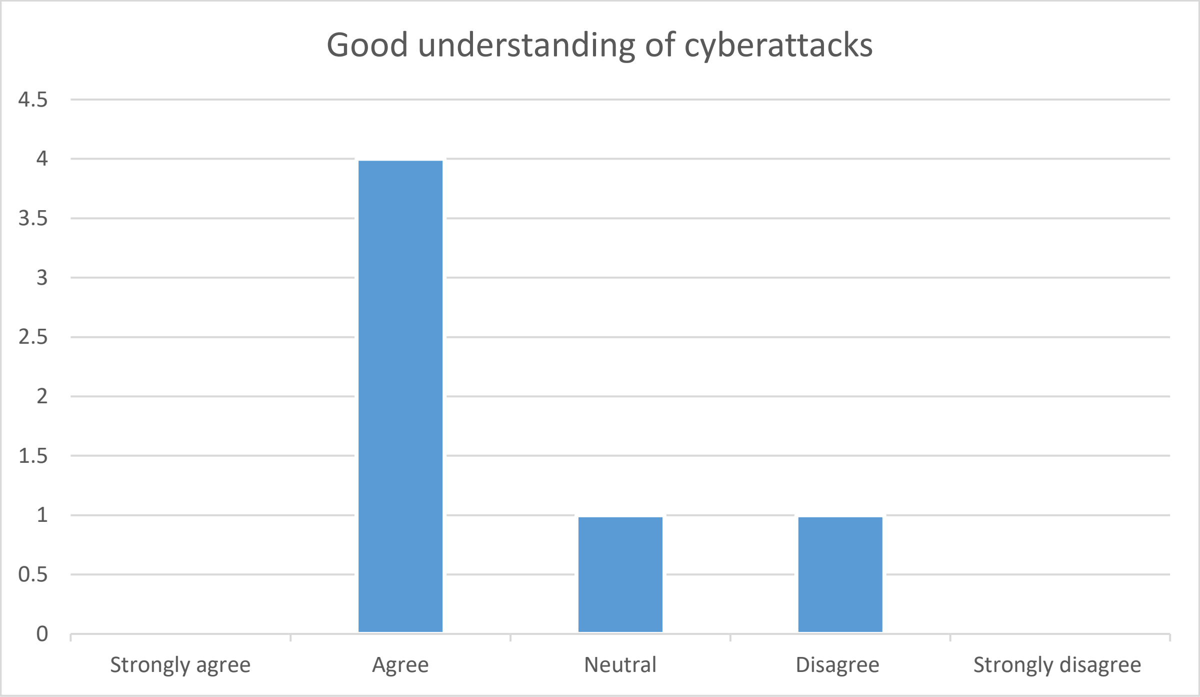


Figure D.168: Good understanding of cyberattacks (46+)

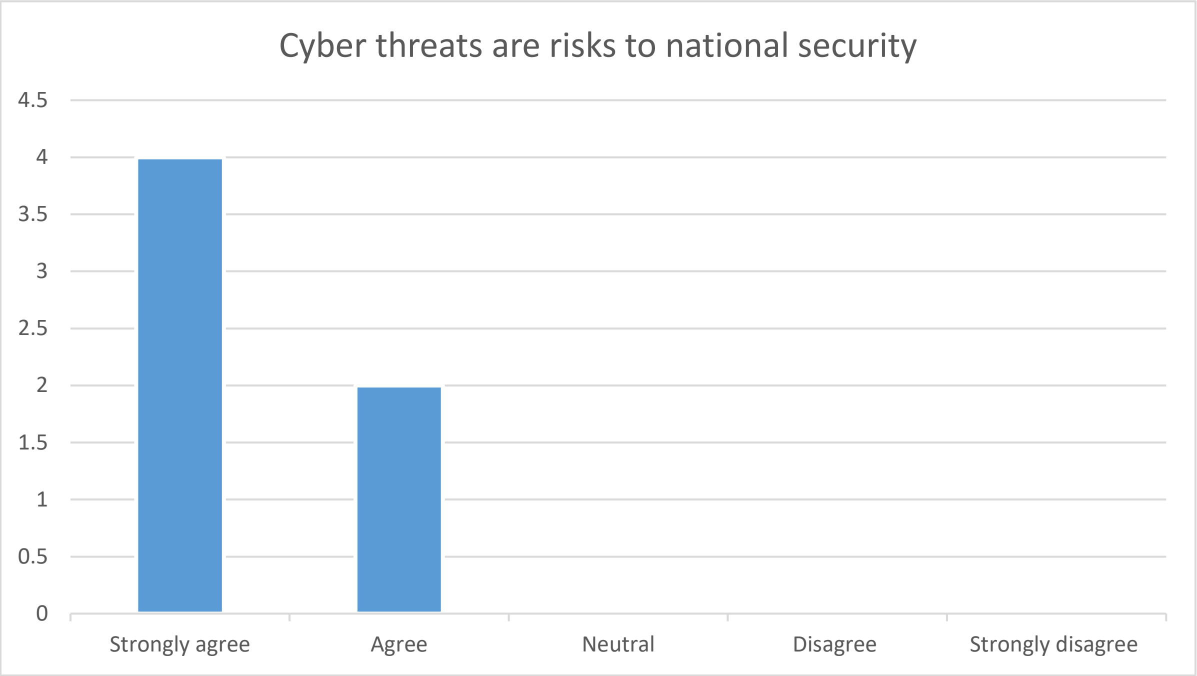


Figure D.169: Cyber threats are risks to national security (46+)

The participants have given a mixed response, and in respect of understanding the impact of cyber-attacks on the public and the organisation (See figure D.168), 1 has none; 1 choosing neither, despite security awareness training available to 4 participants. Furthermore, all 6 participants also recognise the potential threats to national security from cyber-attacks (See figure D.169). General understanding of cyber threats and their impact on national security contributes to making people act responsibly to minimise end-user errors, and over time, their voice would make a difference in influencing acceptance and implementation of a national, regional, and global level mechanism.

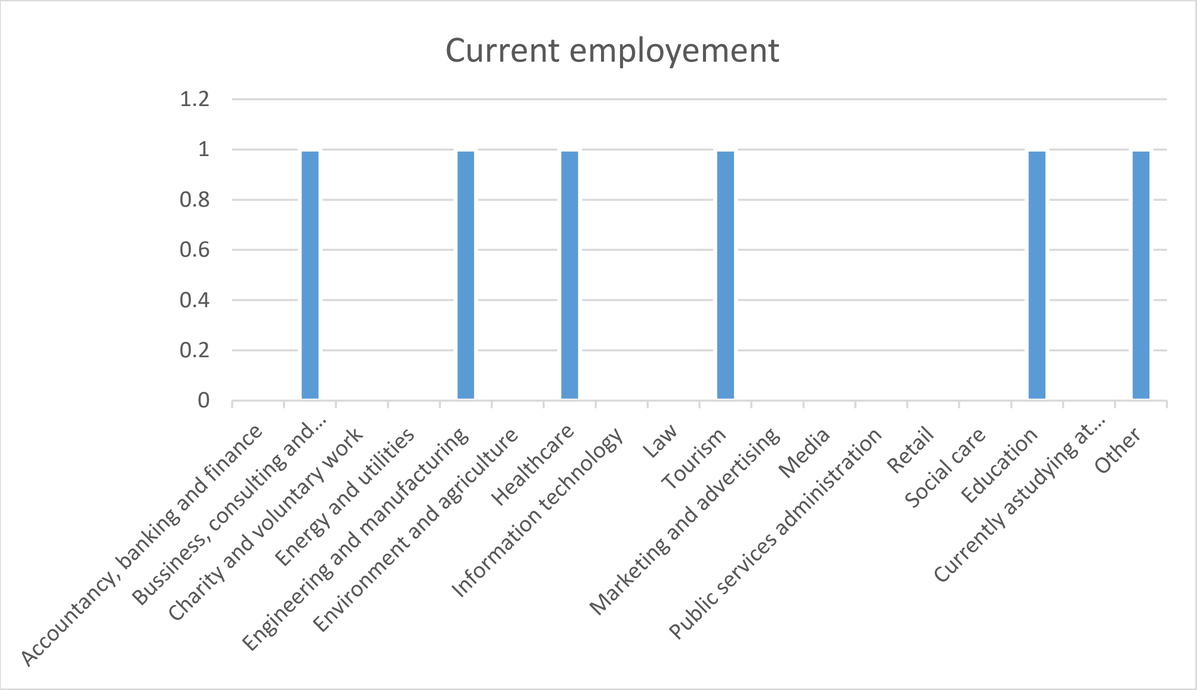


Figure D.170: Current employment (46+)

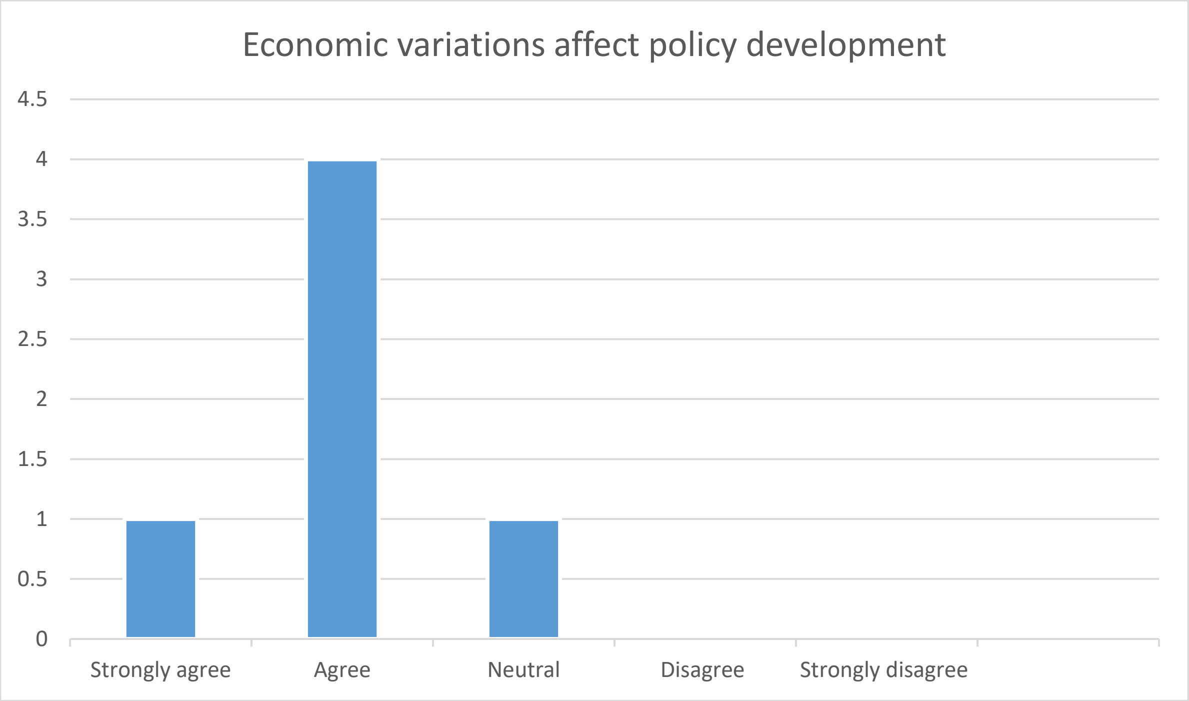


Figure D.171: Economic variations affect policy development (46+)

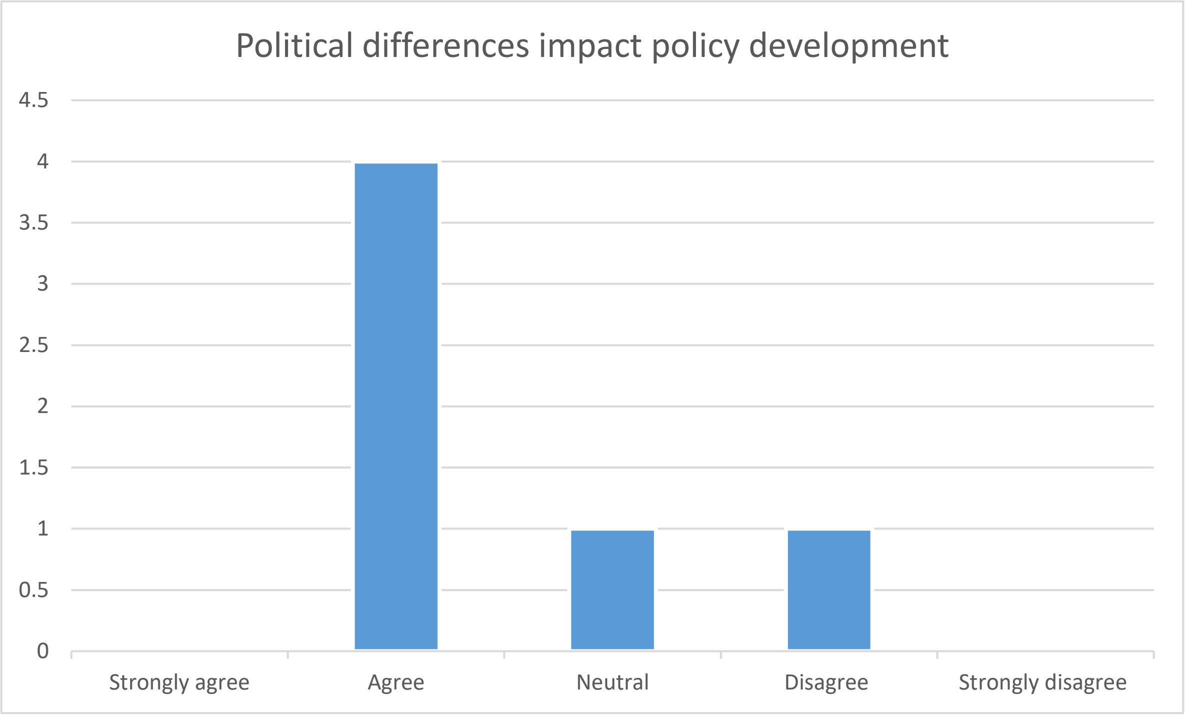


Figure D.172: Political differences impact policy development (46+)

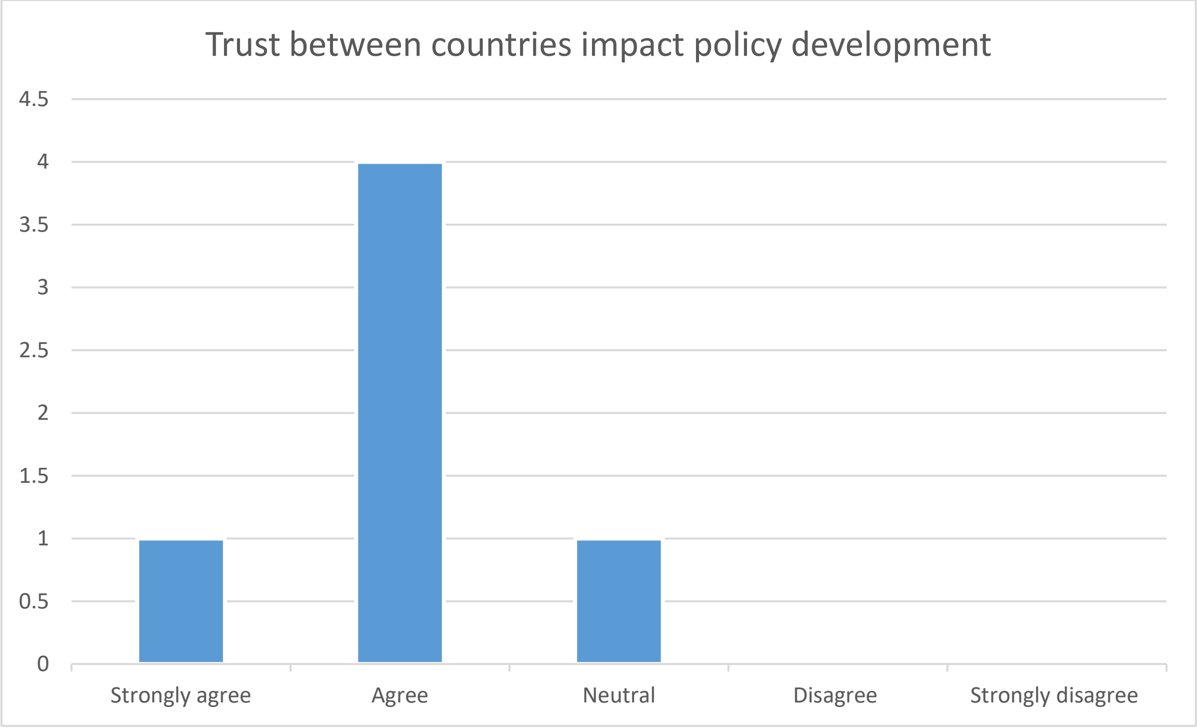


Figure D.173: Trust between countries impact policy development (46+)

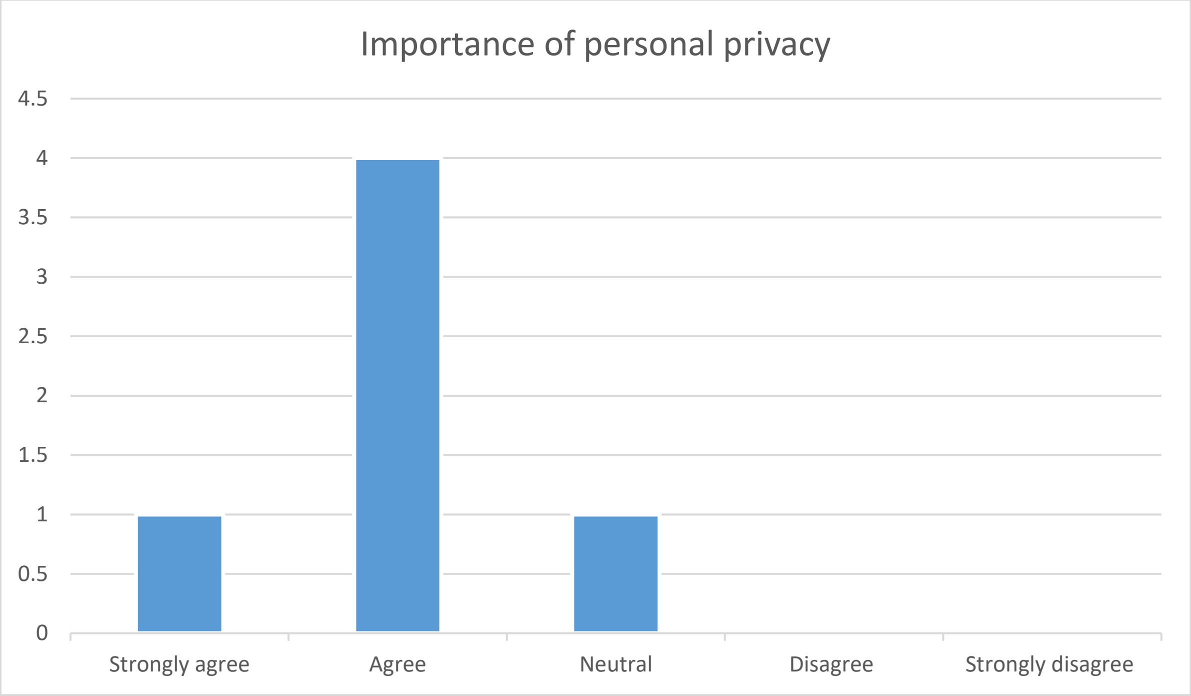


Figure D.174: Importance of personal privacy (46+)

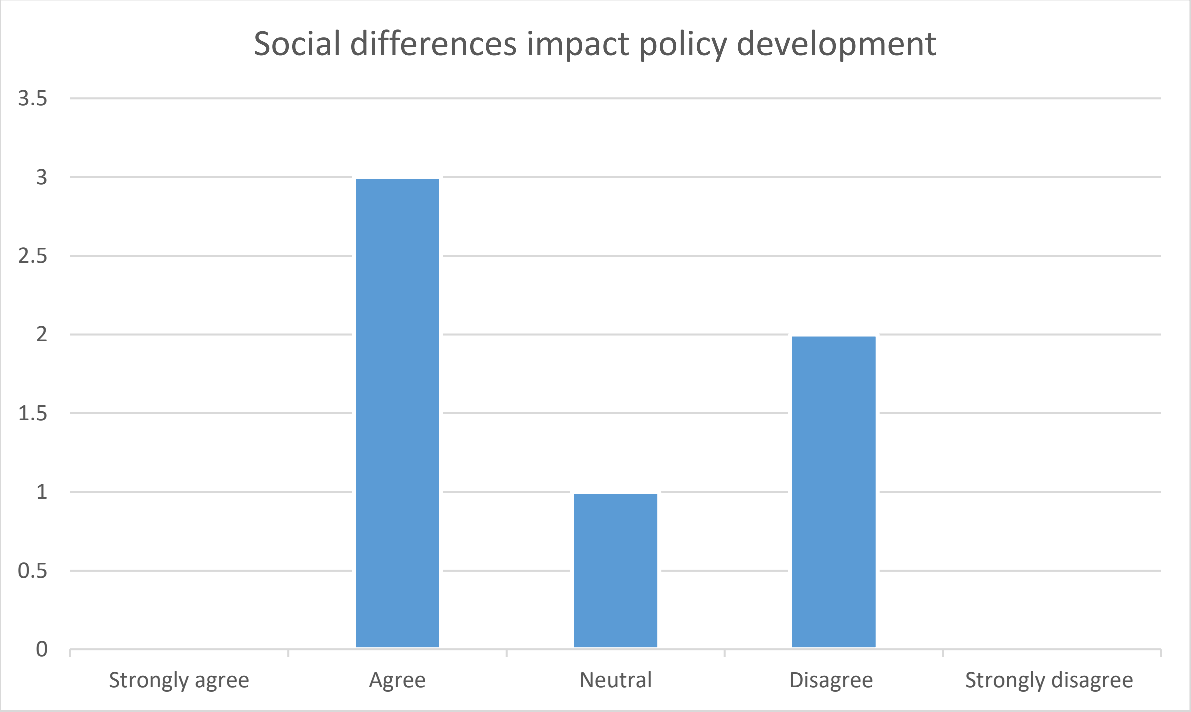


Figure D.175: Social differences impact policy development (46+)

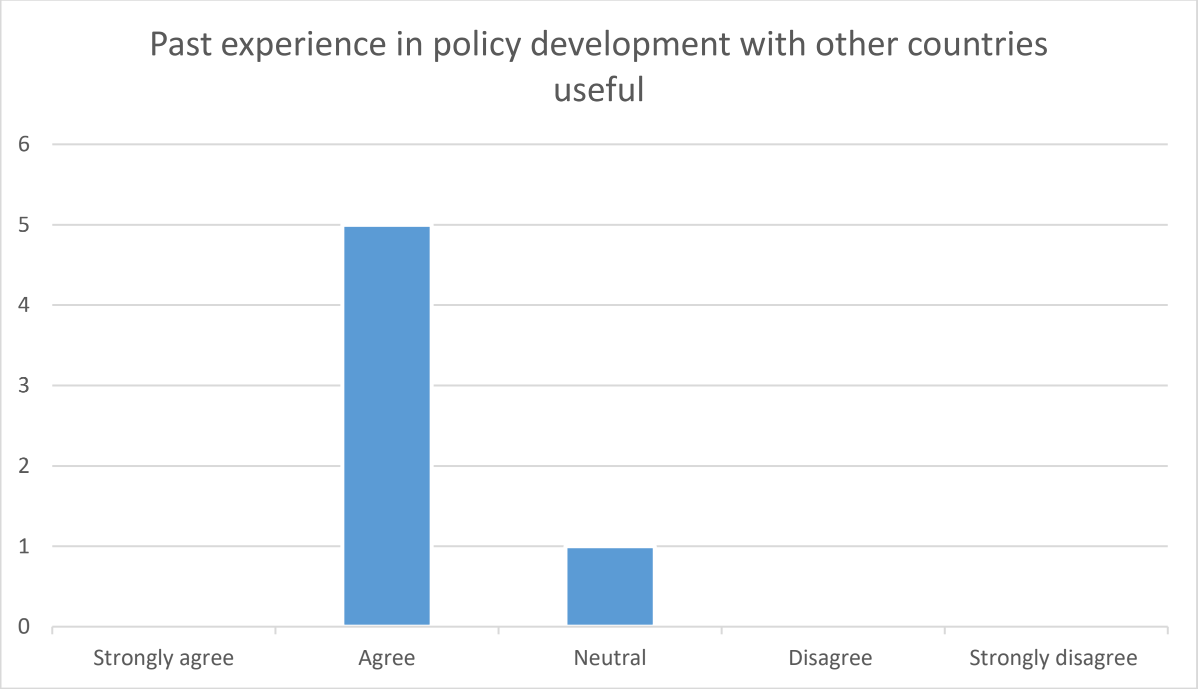


Figure D.176: Past experience in policy development with other countries useful (46+)

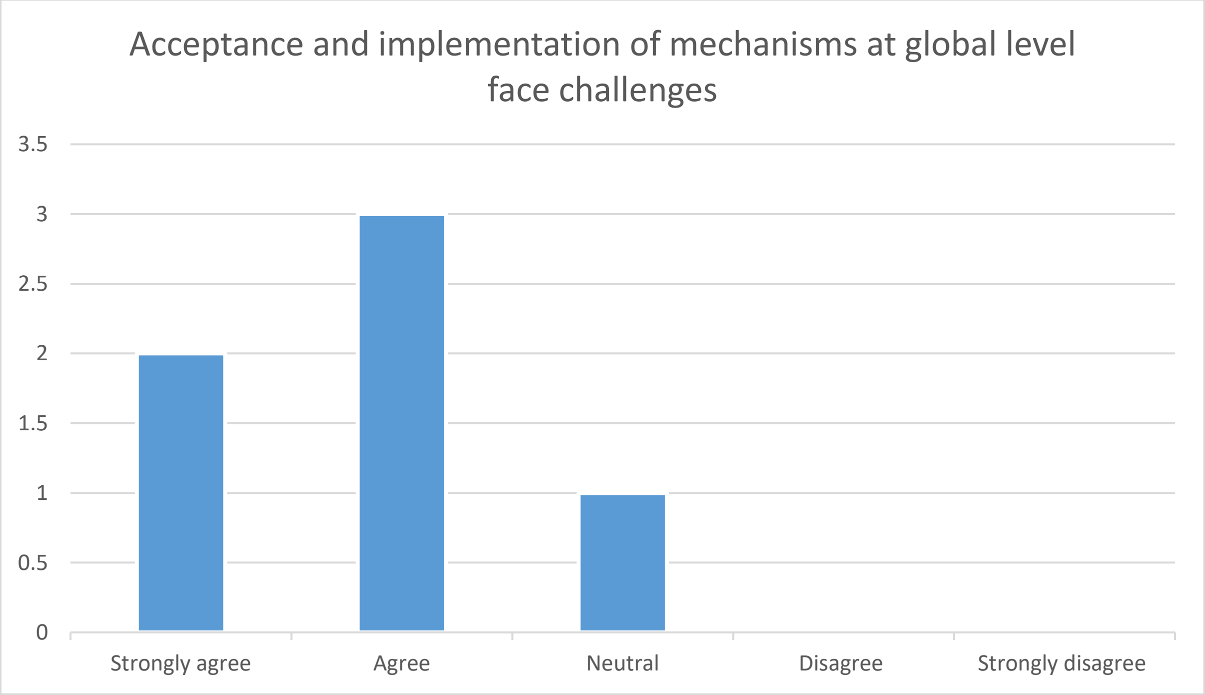


Figure D.177: Acceptance and implementation of mechanisms at global level face challenges (46+)

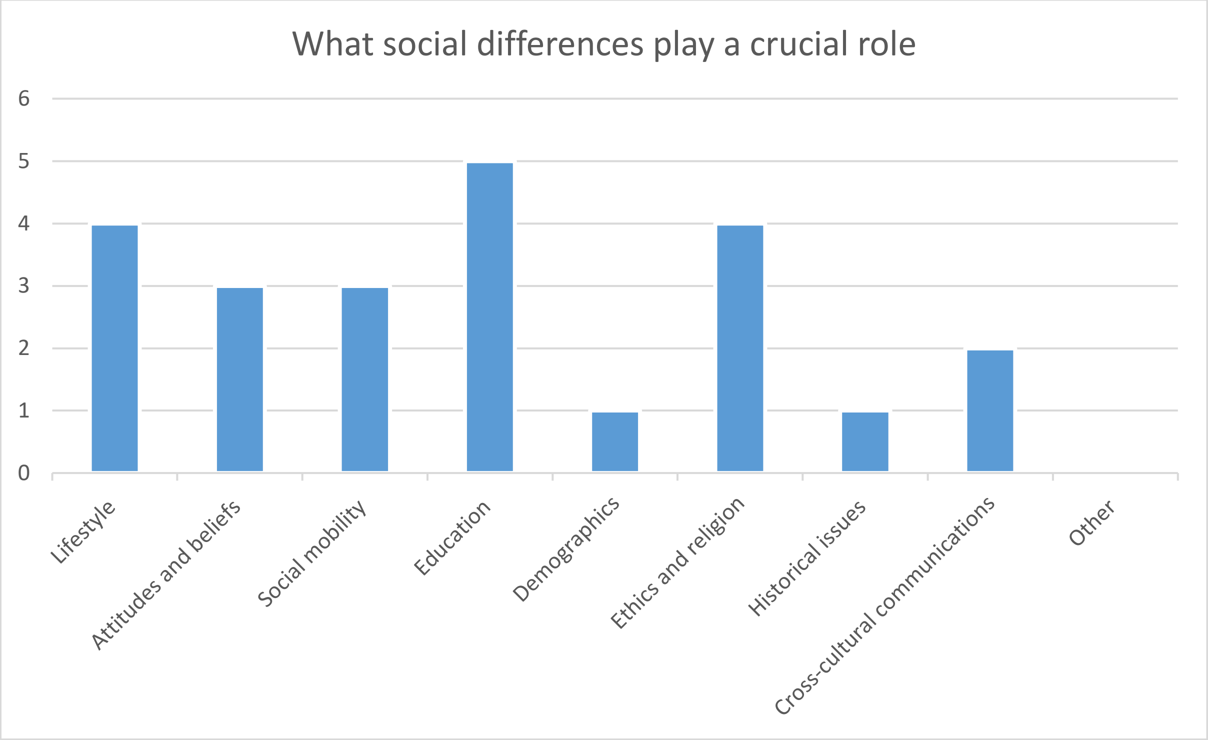


Figure D.178: What social differences play a crucial role (46+)

In respect of social differences, the majority has highlighted the importance of education (See figure D.178). That reflects the importance of awareness and familiarity with potential cyber threats, and their impact on people and national security in accepting and implementing data privacy and security policies. Therefore, it makes the delivery of cybersecurity awareness training at the organisational level an essential requirement. Because of the challenges they faced in their professional life, the rating for education is higher than others.

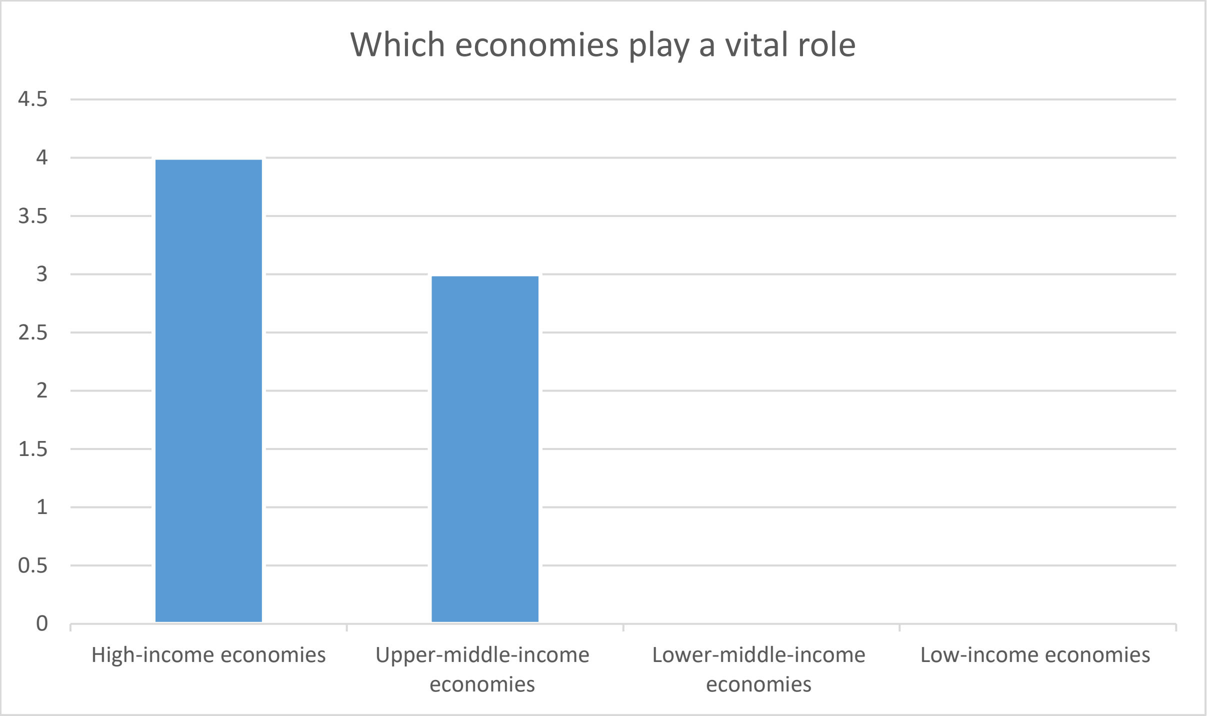


Figure D.179: Which economies play a vital role (46+)

In the questionnaire, majority has stated that the high income and upper-middle-income countries play a vital role (See figure D.179). The stages in the policymaking process aim to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the resources necessary, implement, and finally evaluate the policy. These stages are time-consuming and, require sufficient funding and resources. Therefore, achieving success to a large extent depends on the economic stability of the country, which counts as a crucial factor in policymaking.

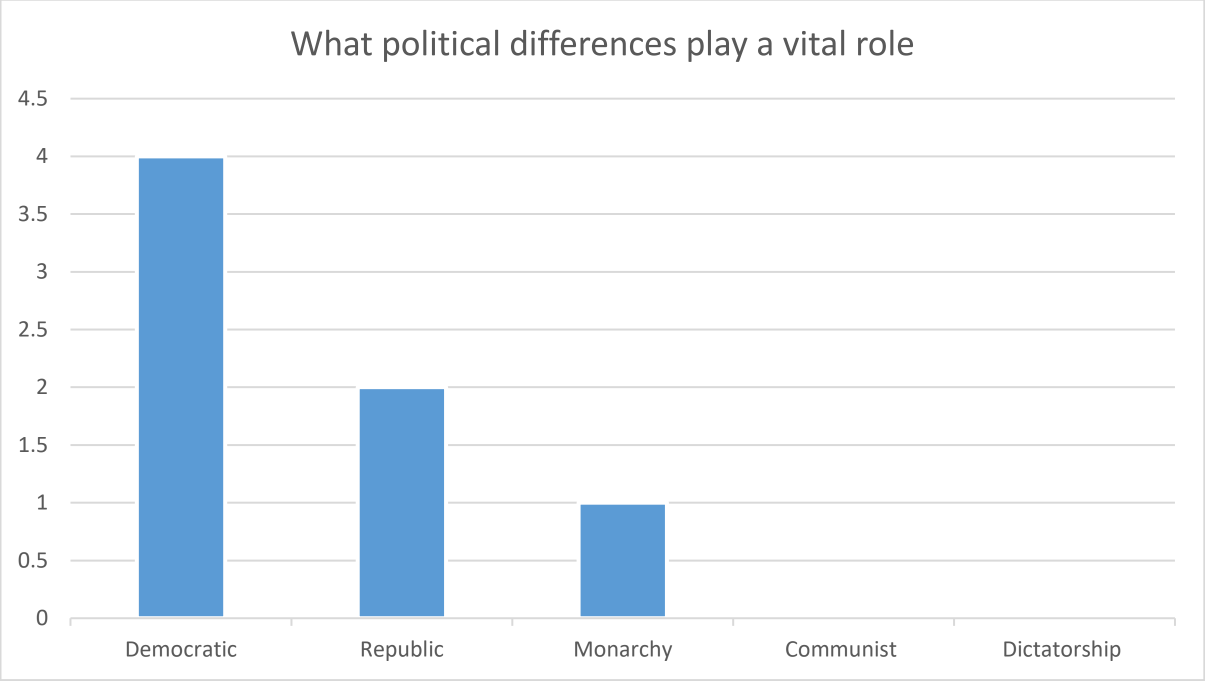


Figure D.180: What political differences play a vital role (46+)

The majority prefers democratic political system (See figure D.180), over others because it allows an influential public voice in the process of policy development and, encourages consensus and collective responsibility for their actions. These contribute to developing trust between the organisations, and coherence and transparency in the policy development process.

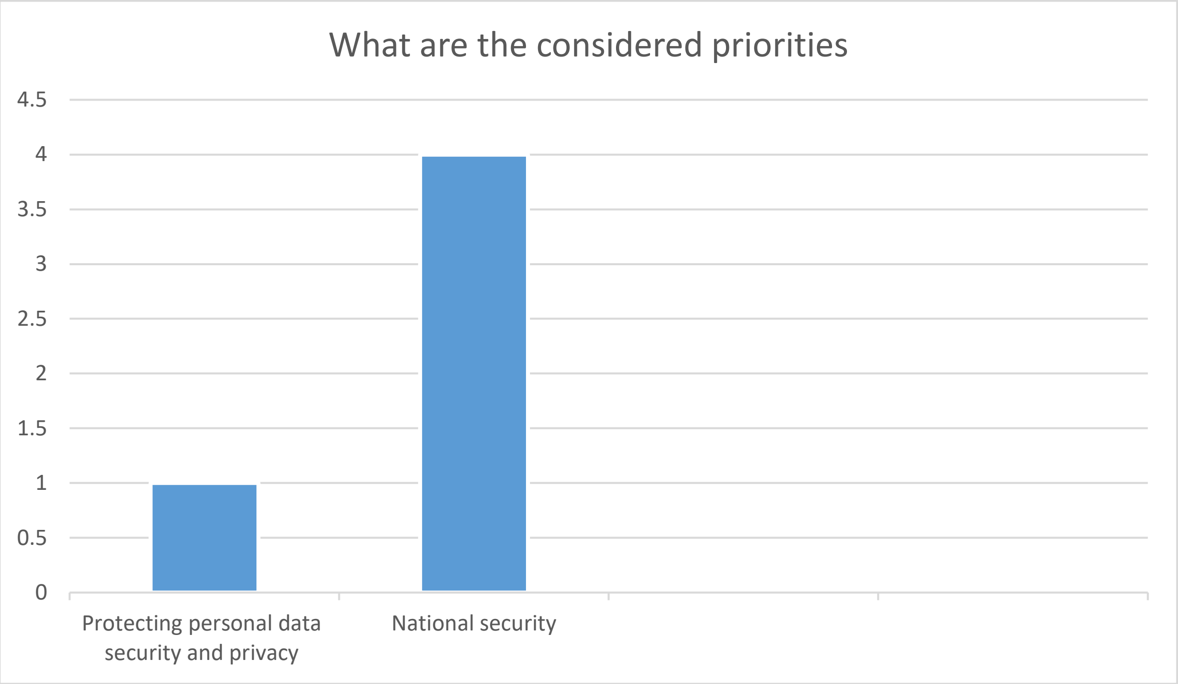


Figure D.181: What are the considered priorities (46+)

Although protection of personal data security and privacy national security is of utmost importance, this age group places the importance of national security above it in accepting and implementing a global data privacy and security policies (See figure D.181). However, in a data breach incident, there may be potential consequential effect on personal data security and privacy will be felt right across the groups as well as the community alike. Therefore in such circumstances, the importance of protection of personal data and security cannot be ignored.

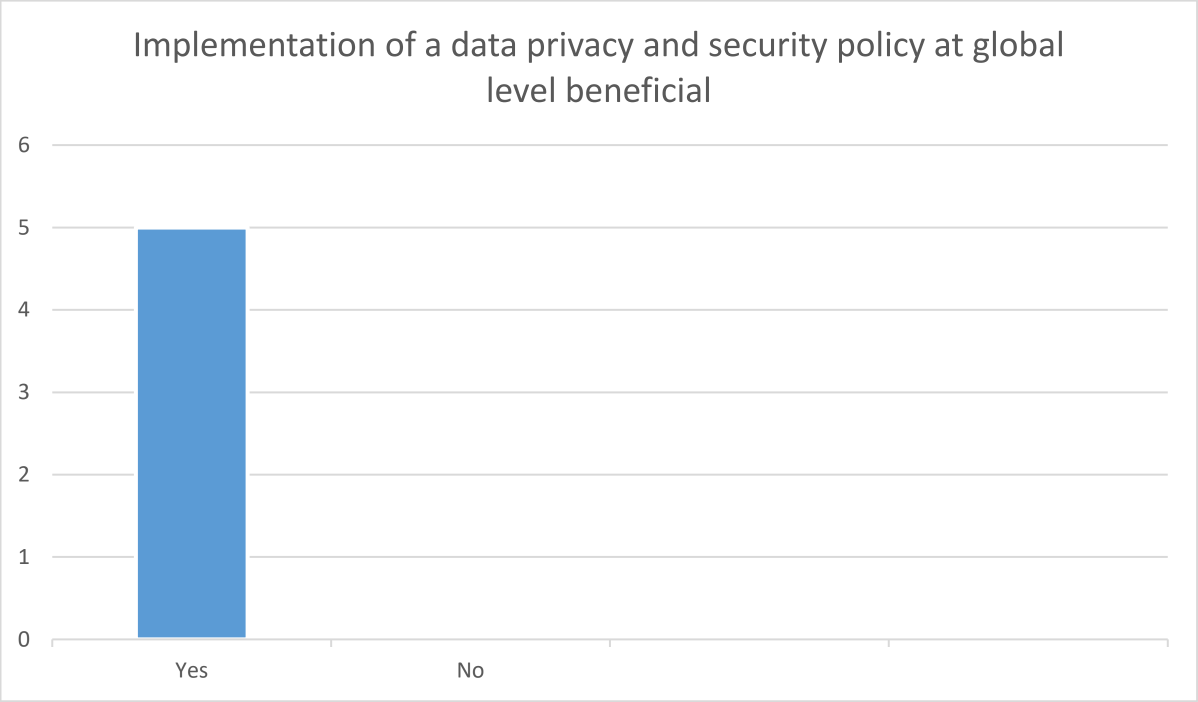


Figure D.182: Implementation of a data privacy and security policy at global level beneficial (46+)

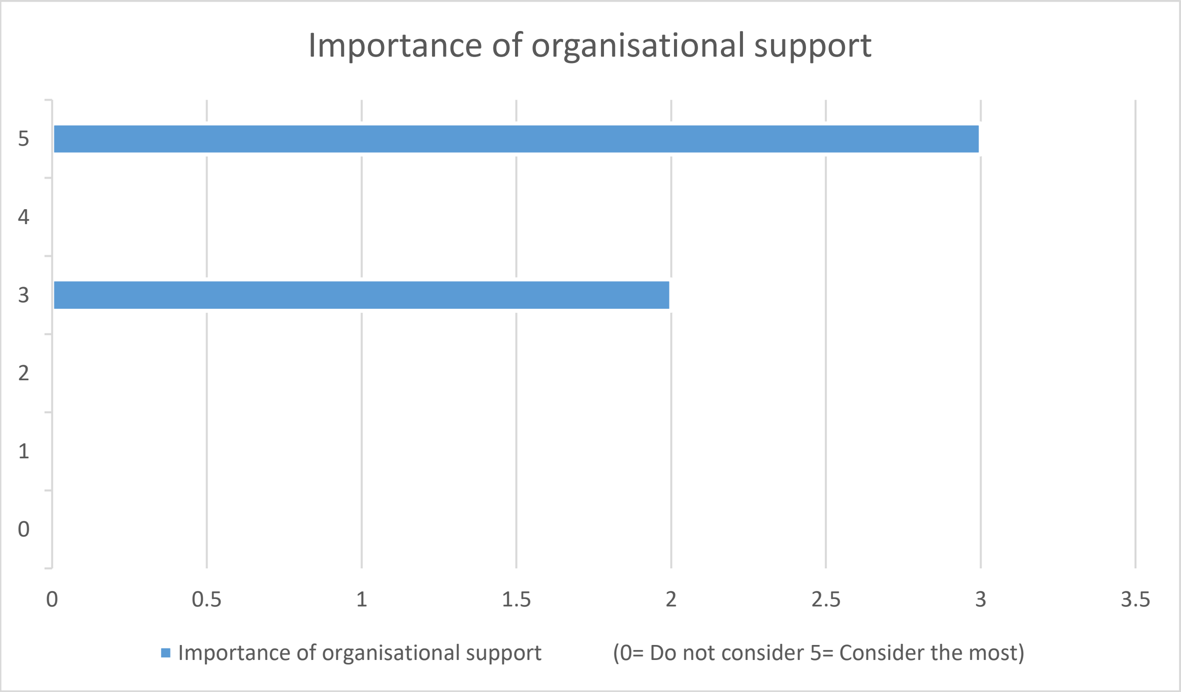


Figure D.183: Importance of organisational support (46+)

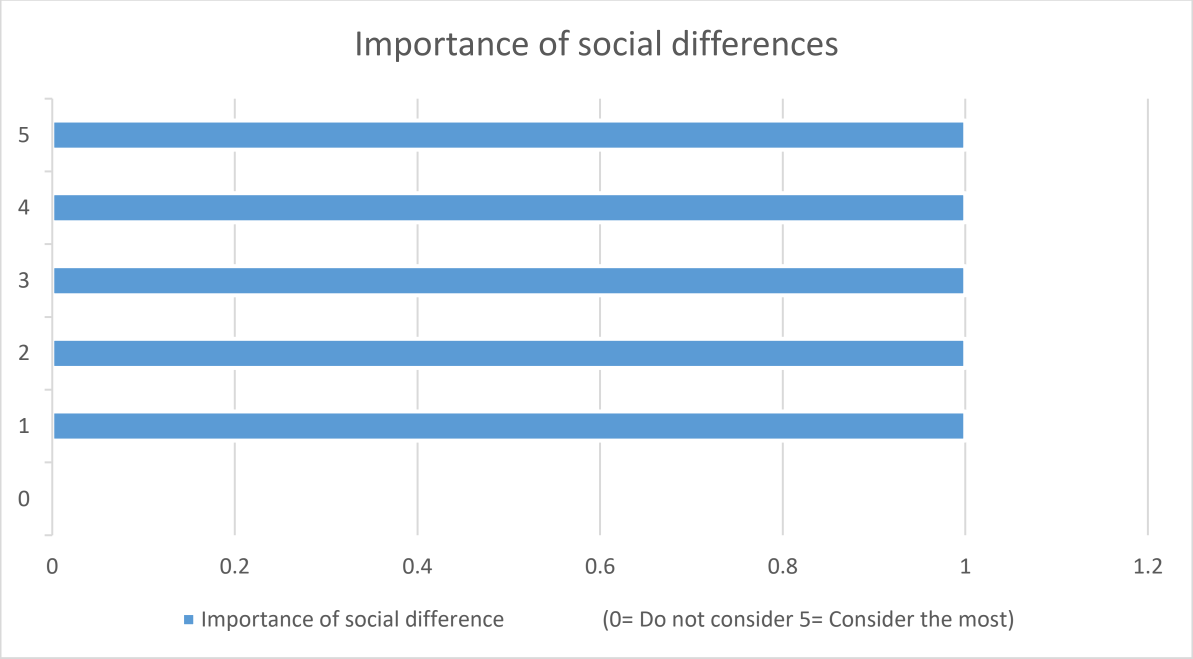


Figure D.184: Importance of social differences (46+)

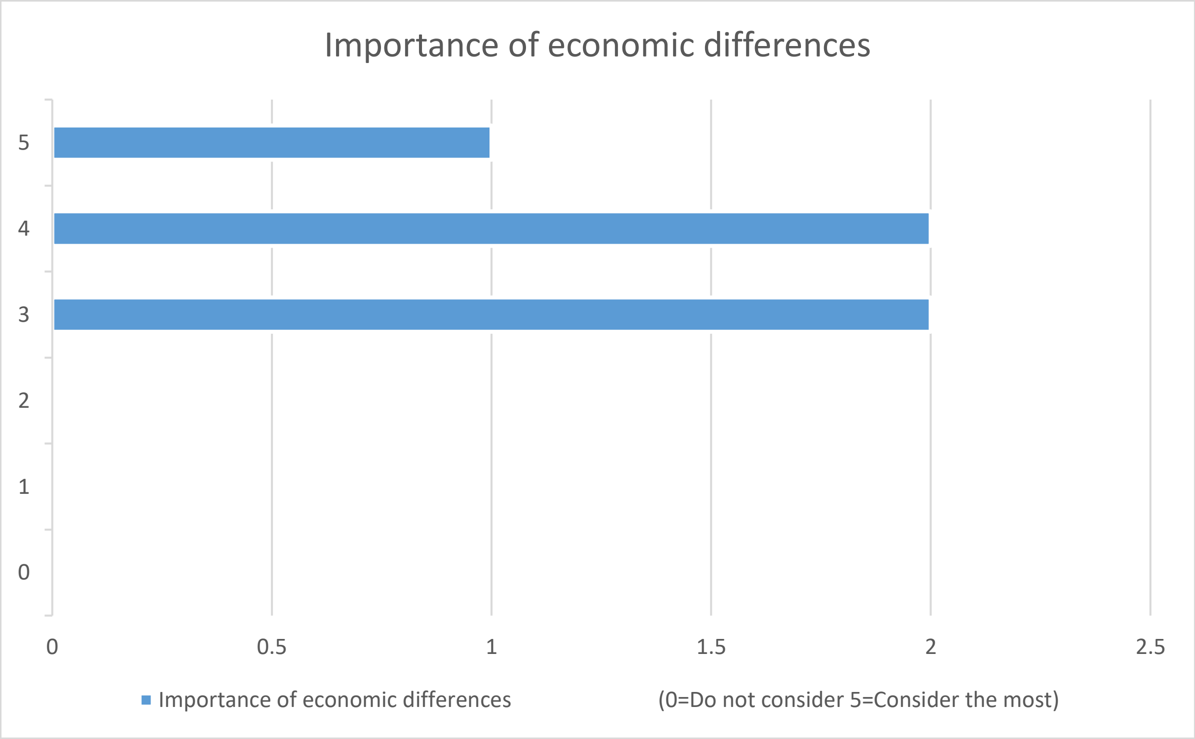


Figure D.185: Importance of economic differences (46+)

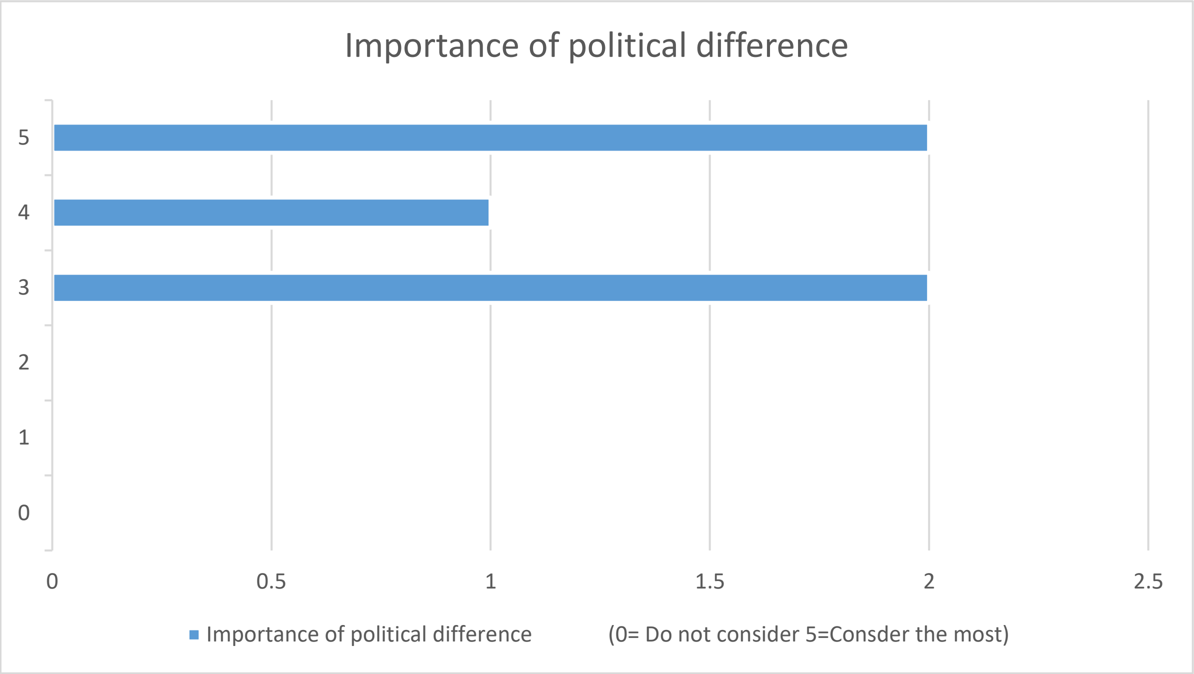


Figure D.186: Importance of political difference (46+)

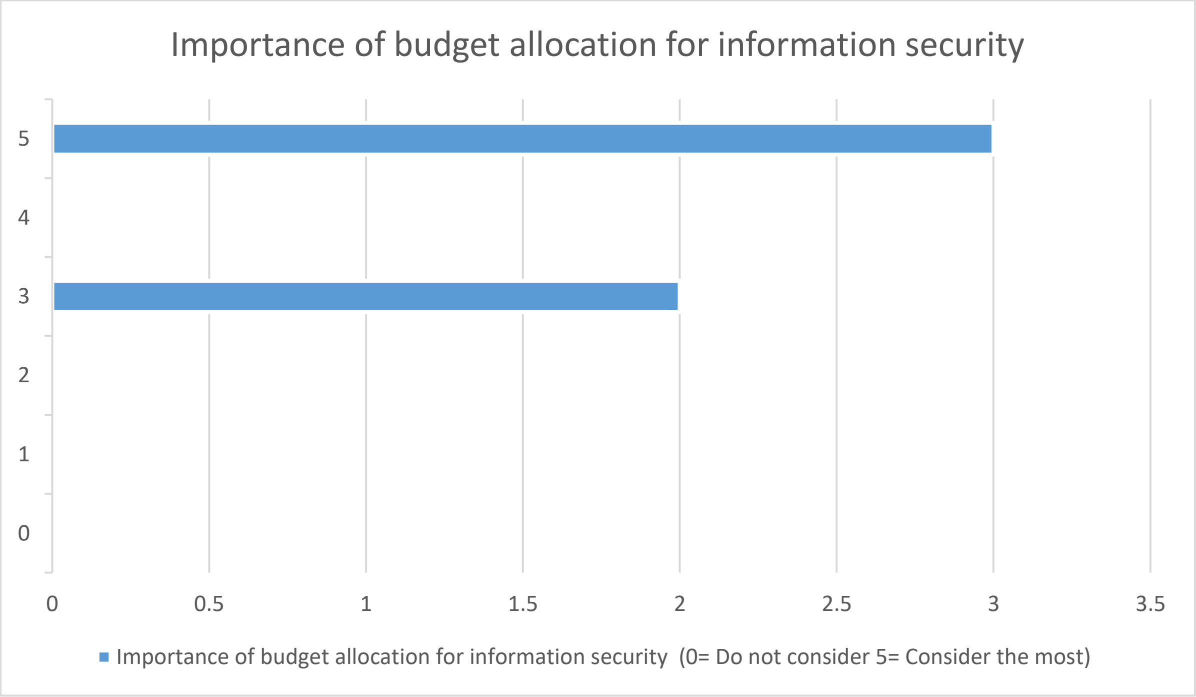


Figure D.187: Importance of budget allocation for information security (46+)

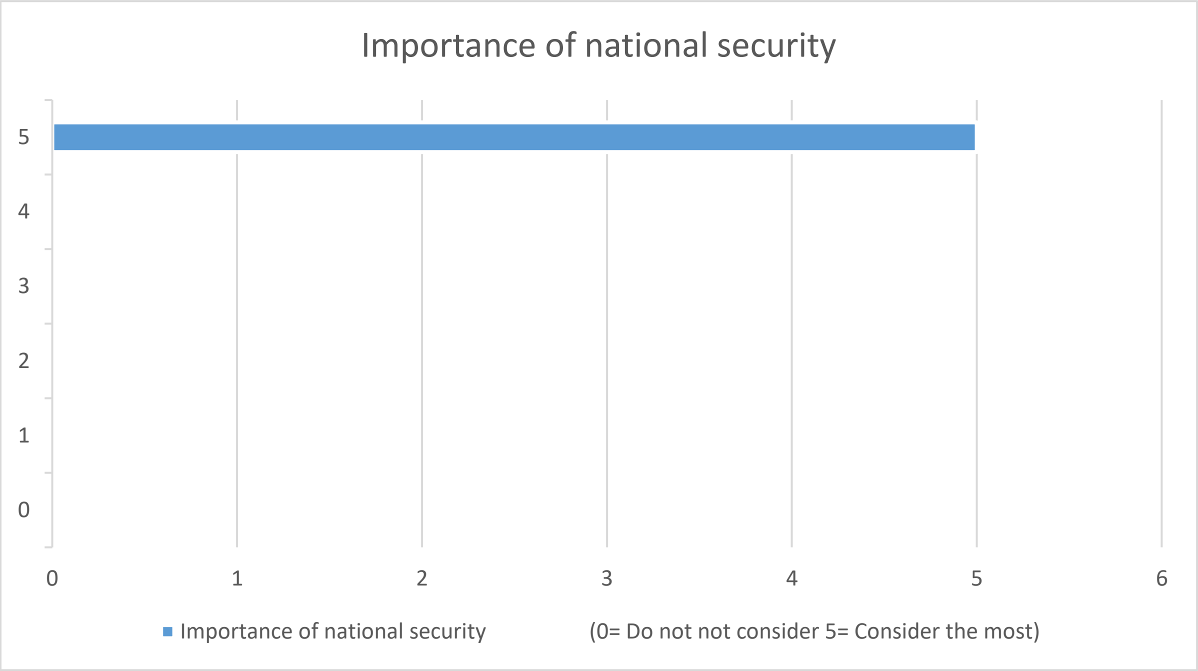


Figure D.188: Importance of national security (46+)

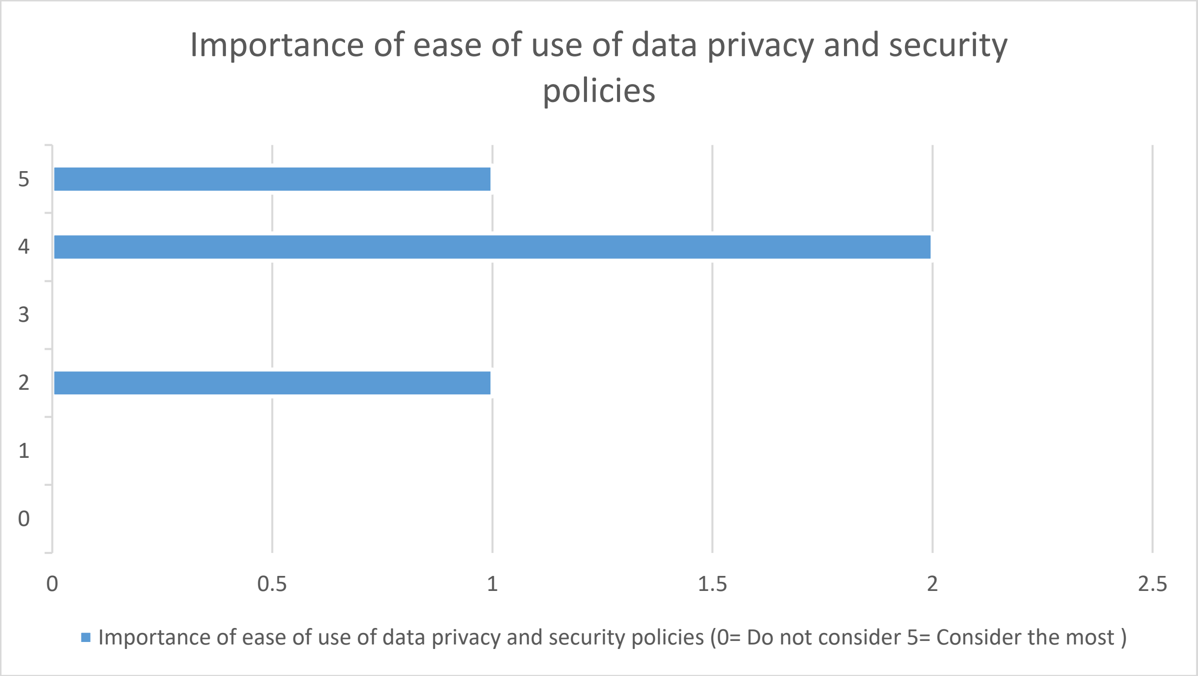


Figure D.189: Importance of ease of use of data privacy and security policies (46+)

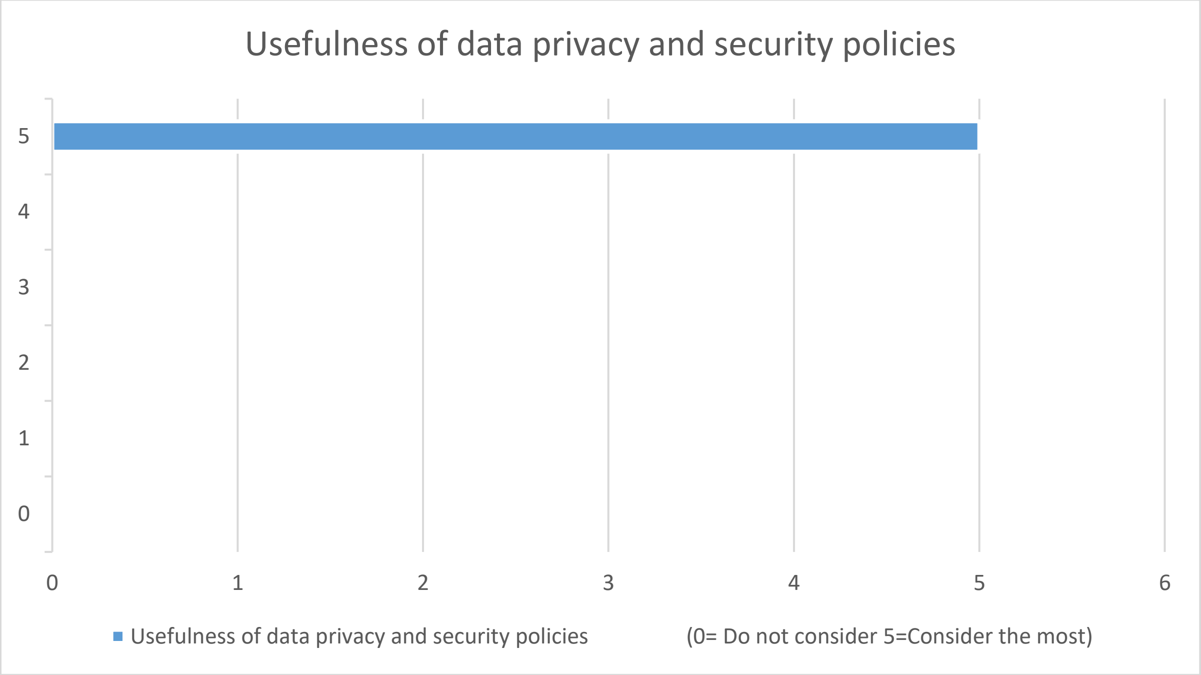


Figure D.190: Usefulness of data privacy and security policies (46+)

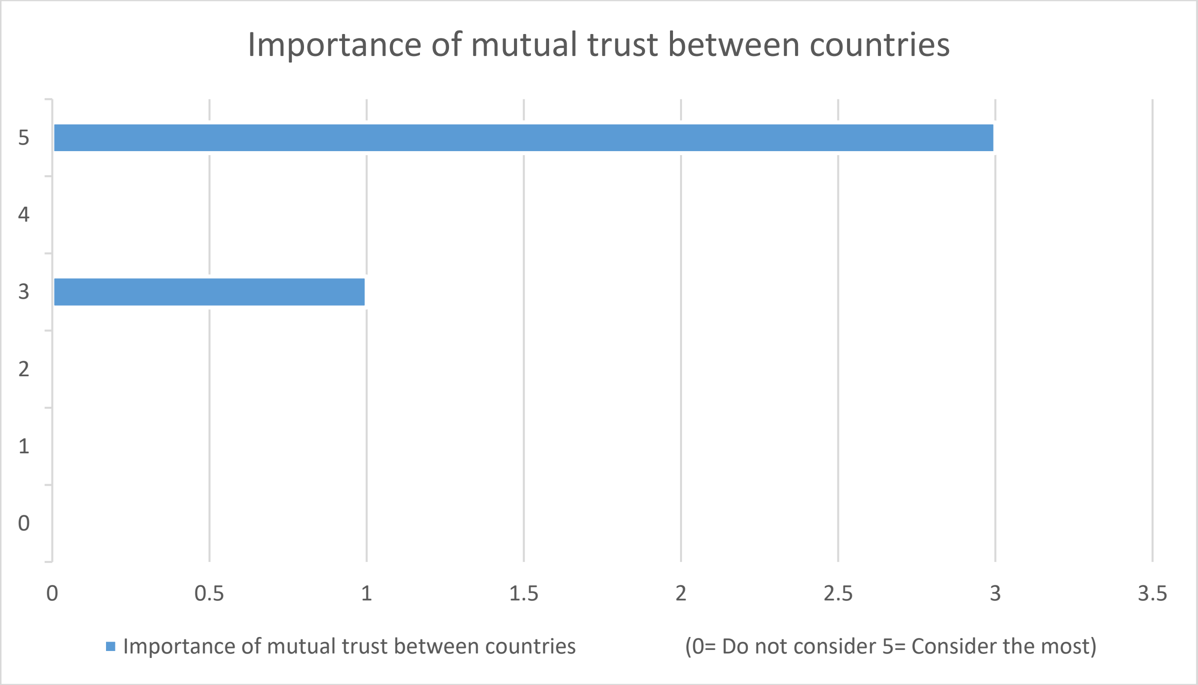


Figure D.191 Importance of mutual trust between countries (46+)

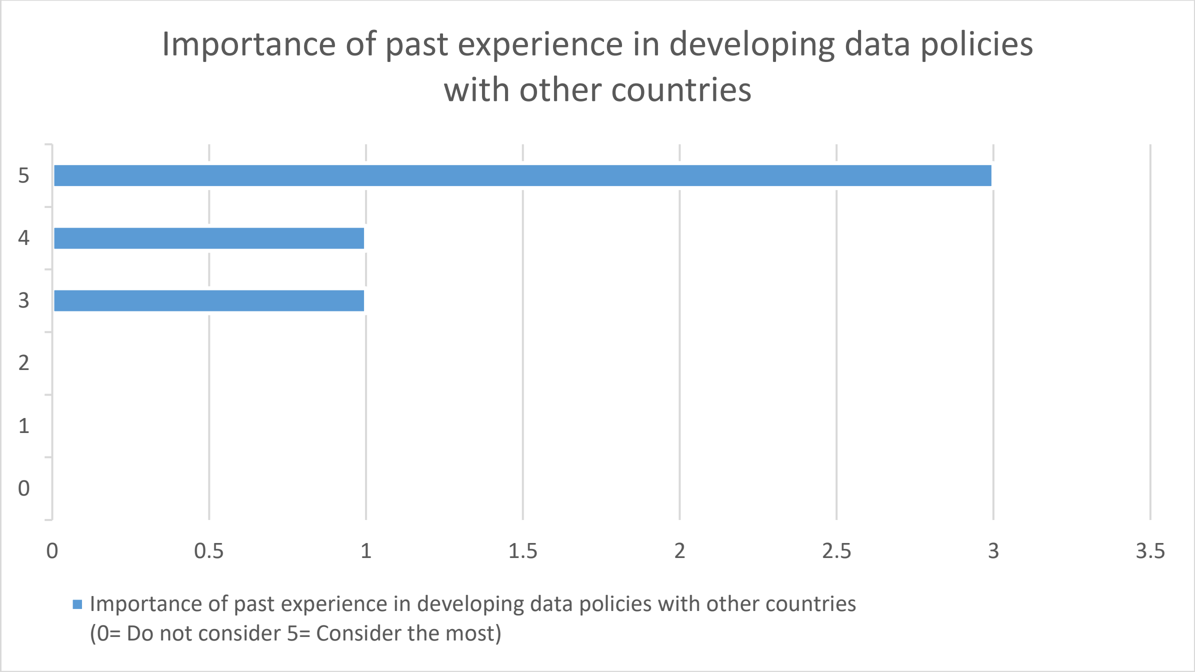


Figure D.192: Importance of past experience in developing data policies with other counties (46+)

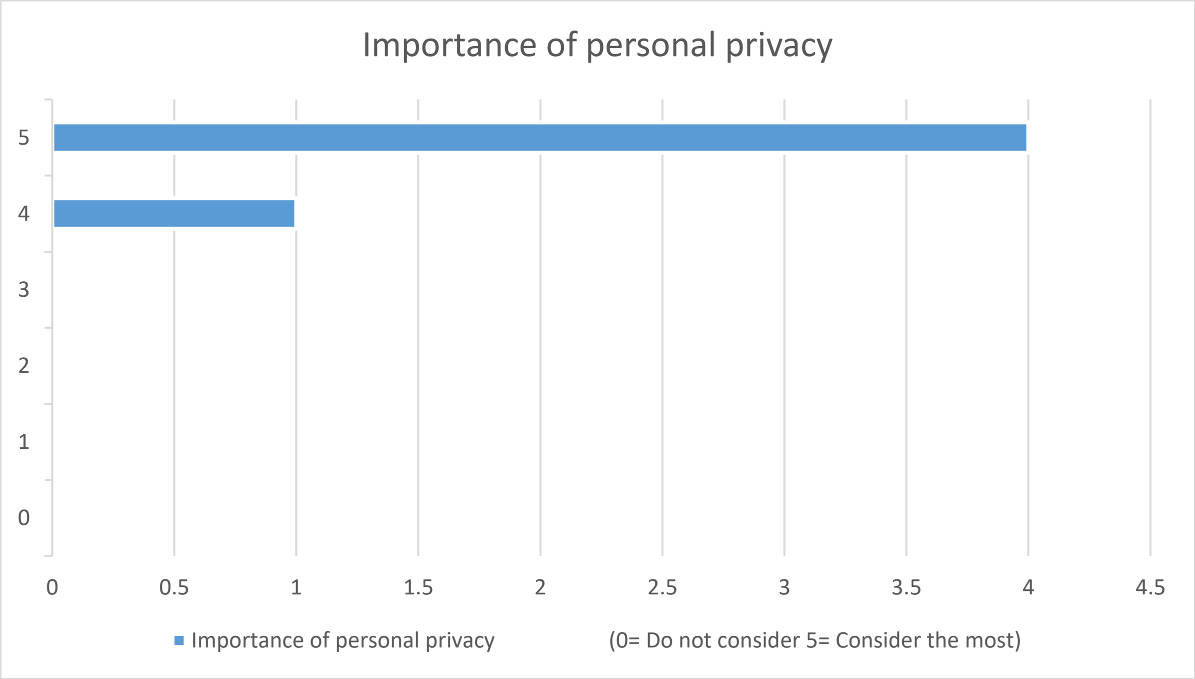


Figure D.193: Importance of personal privacy (46+)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 83 percent of the respondents have endorsed (See figure D.182). The other notable cross-cutting factors that have come out of the survey are organisational support, budget allocation, social differences, economical differences, political differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure D.171-181) (See figure D.183-193).

Sri Lanka – Less than a year

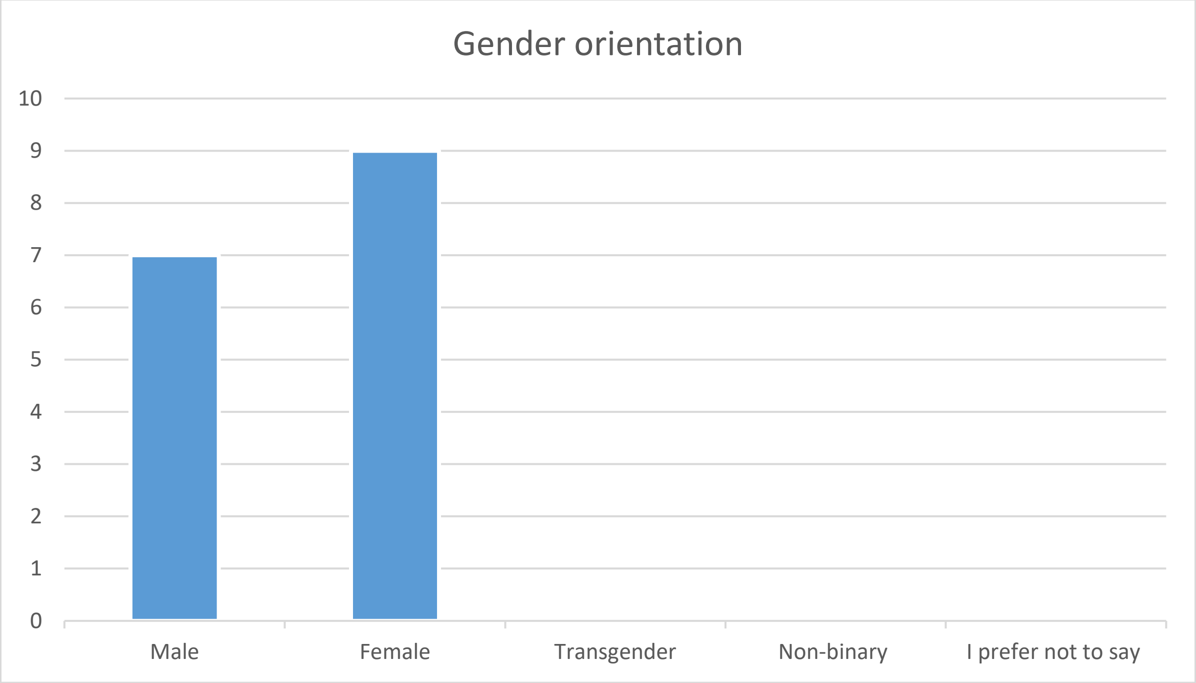


Figure D.194: Gender orientation (Less than a year)

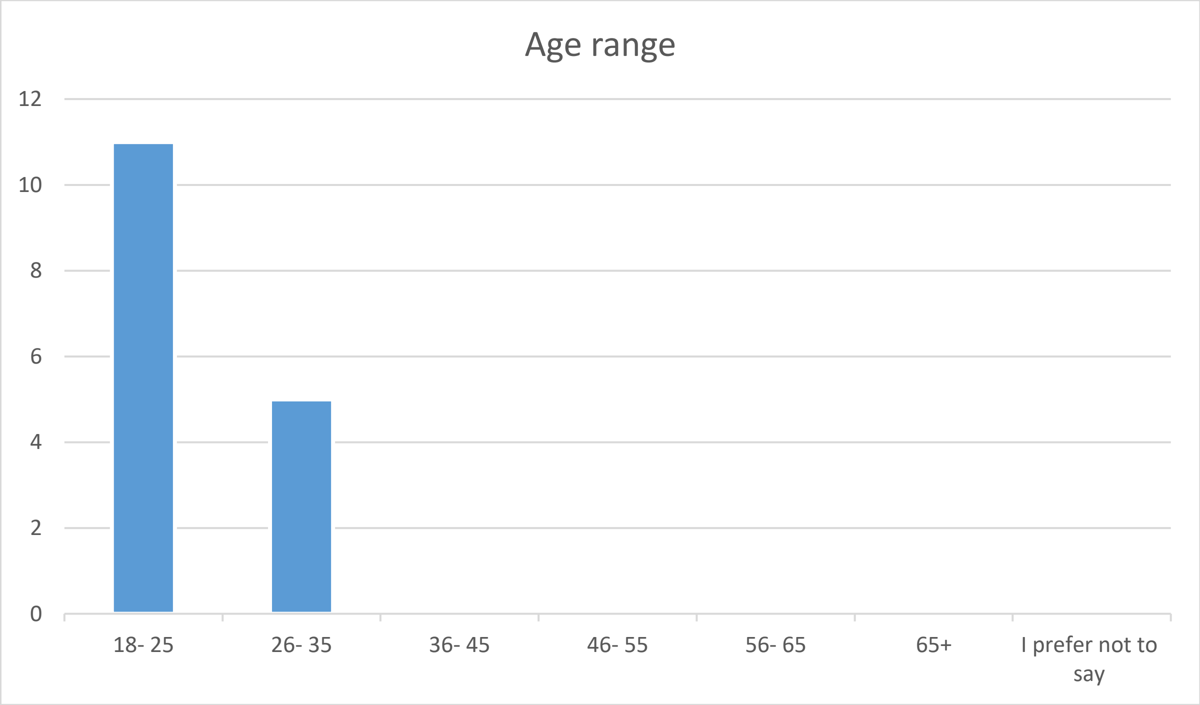


Figure D.195: Age range (Less than a year)

This analysis is based on the responses received from Sri Lankan participants in the industry for less than one year. Responses received from 16 made up of 7 males 9 females (See figure D.194), all in the age range between 18-35. Breaking down groups of 11 in the 18-25 and 5 in the 26-35 age range (See figure D.195). In this category, the majority of employees with less than a year of service is below 35 years.

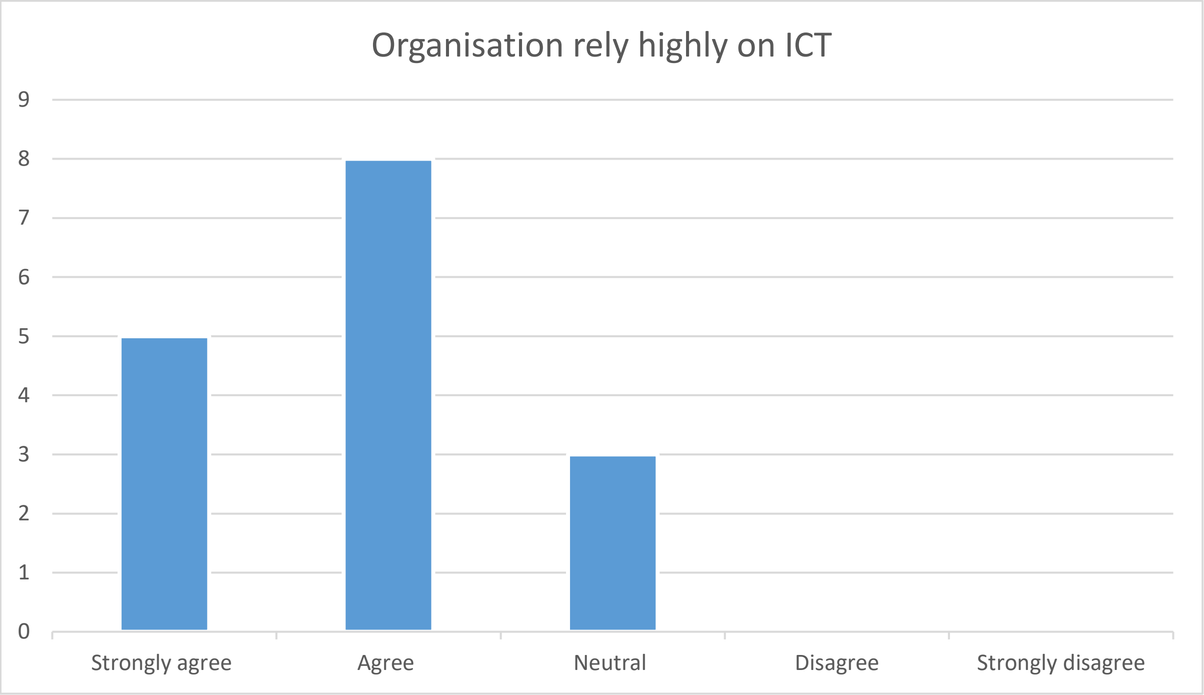


Figure D.196: Organisation rely highly on ICT (Less than a year)

Of the 16 respondents, 13 employed in a technology reliance working environment, and 3 not aware of reliance on technology because of the nature of the work assigned to them (See figure D.196). The distinct responses here is that majority with less than one year in employment (in an organisation) have a high reliance on ICT.

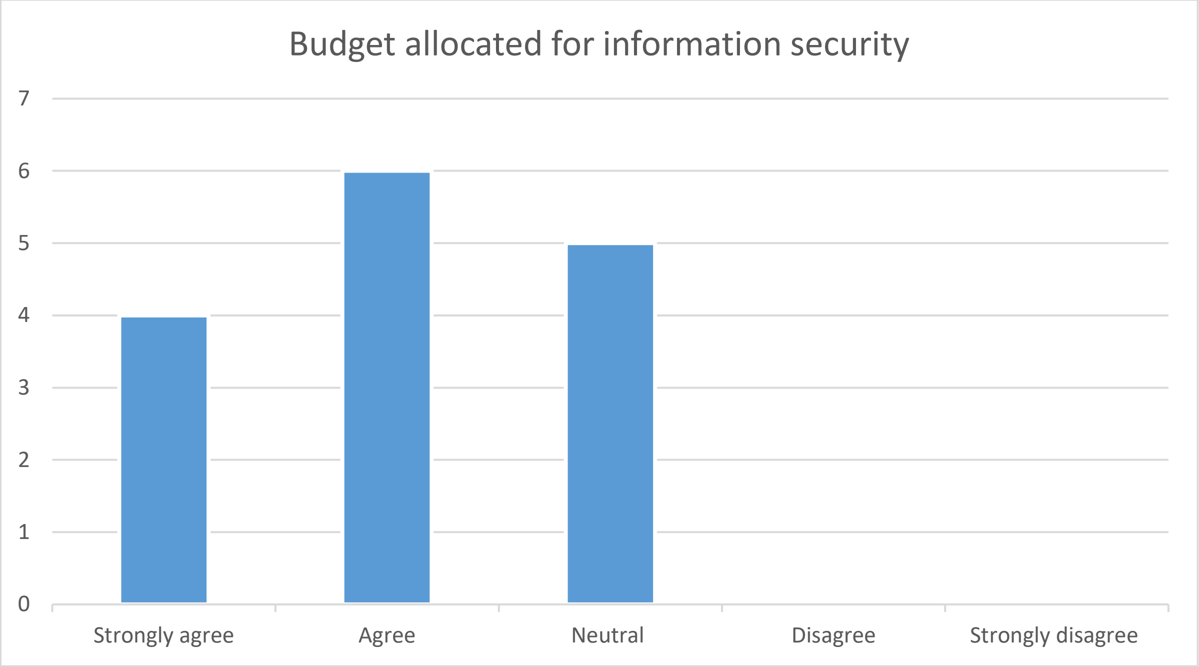


Figure D.197: Budget allocated for information security (Less than a year)

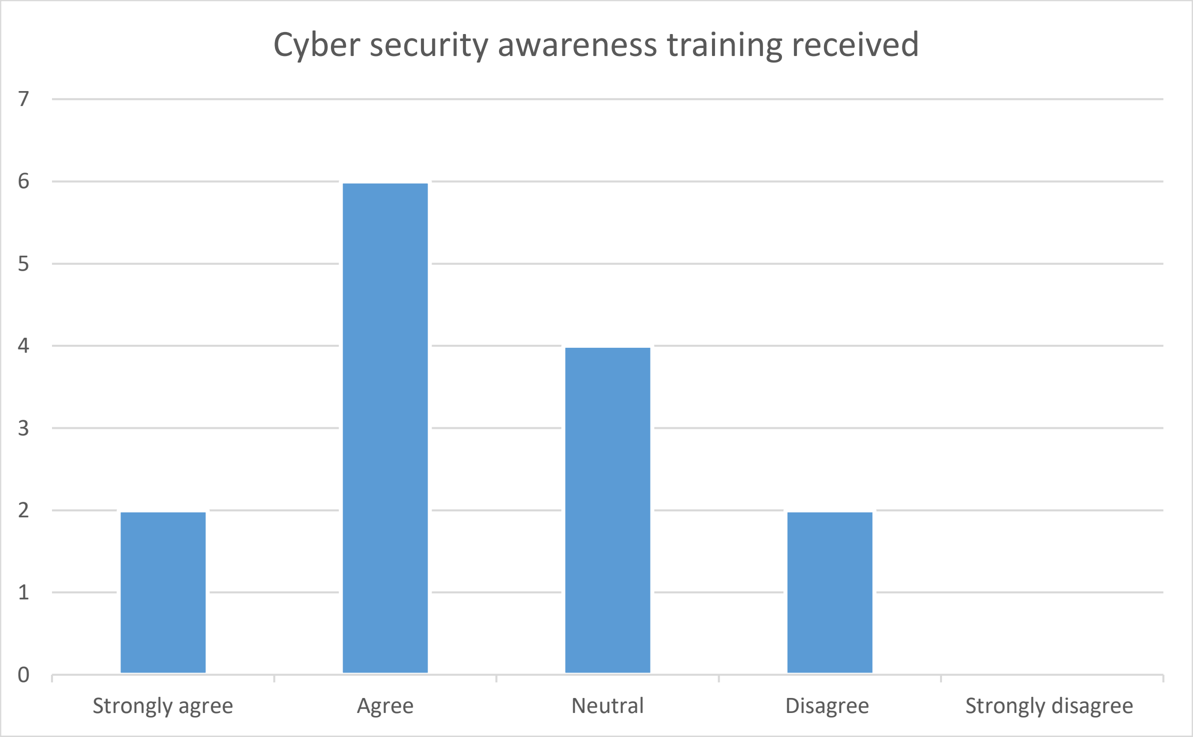


Figure D.198: Cyber security awareness training received (Less than a year)

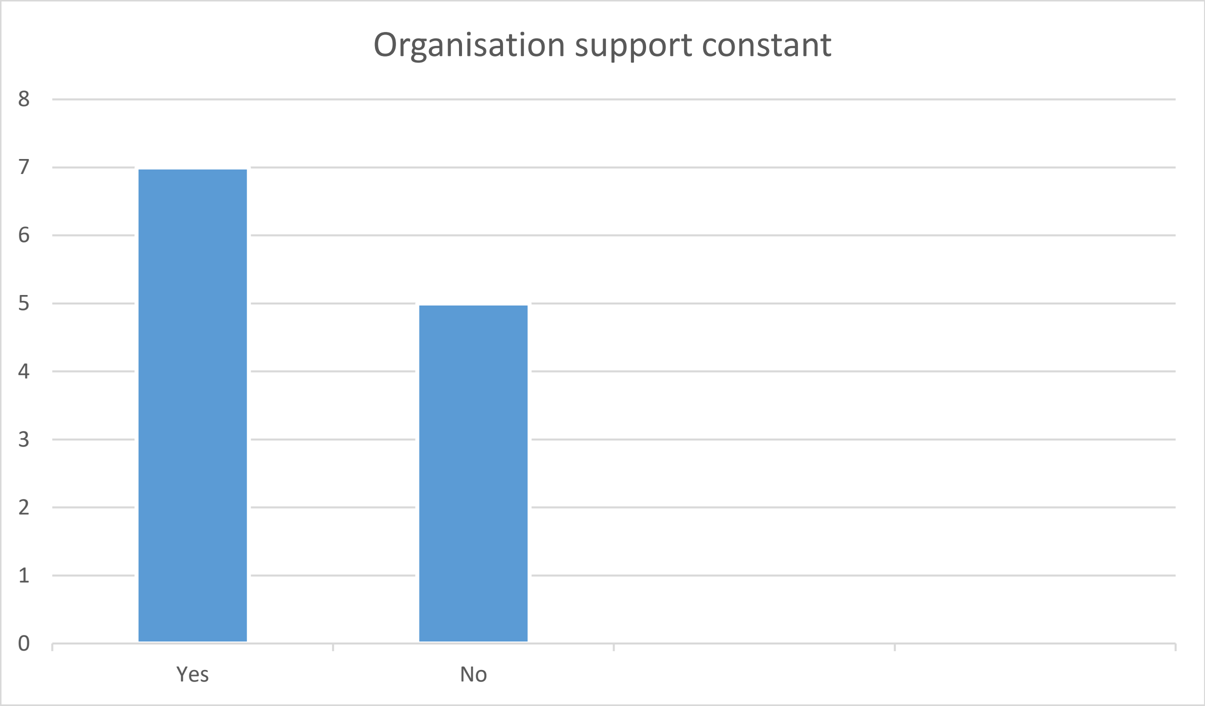


Figure D.199: Organisation support constant (Less than a year)

Responses received from 16 participants. According to 10, their organisations had an allocated budget allocation for information security; 5 non-comital (See figure D.197). Also, according to some participants, the funds allocated for information security was satisfactory but the security awareness training they received was inadequate. Only 8 participants received cybersecurity awareness training regularly; 2 did not receive any, 4 neither agreed nor disagreed (See figure D.198). Also, 7 received organisational support to protect personal information, and 5 did not (See figure D.199). This category has so many variable factors. Firstly, making a meaningful analysis is complicated by 'less than one year' time duration in employment. The employees may not have had sufficient time to assess their training needs, resource allocation, policy development process, organisational level planning including the provision of staff training to meet the challenges in their working environment. However, the majority of the employees have an awareness of the work in an organisation with high reliance on ICT, therefore, their training needs may not have been considered a priority. Also, the majority taking up employment did not receive constant support from the organisation in terms of protecting personal information intended to minimise end-user error.

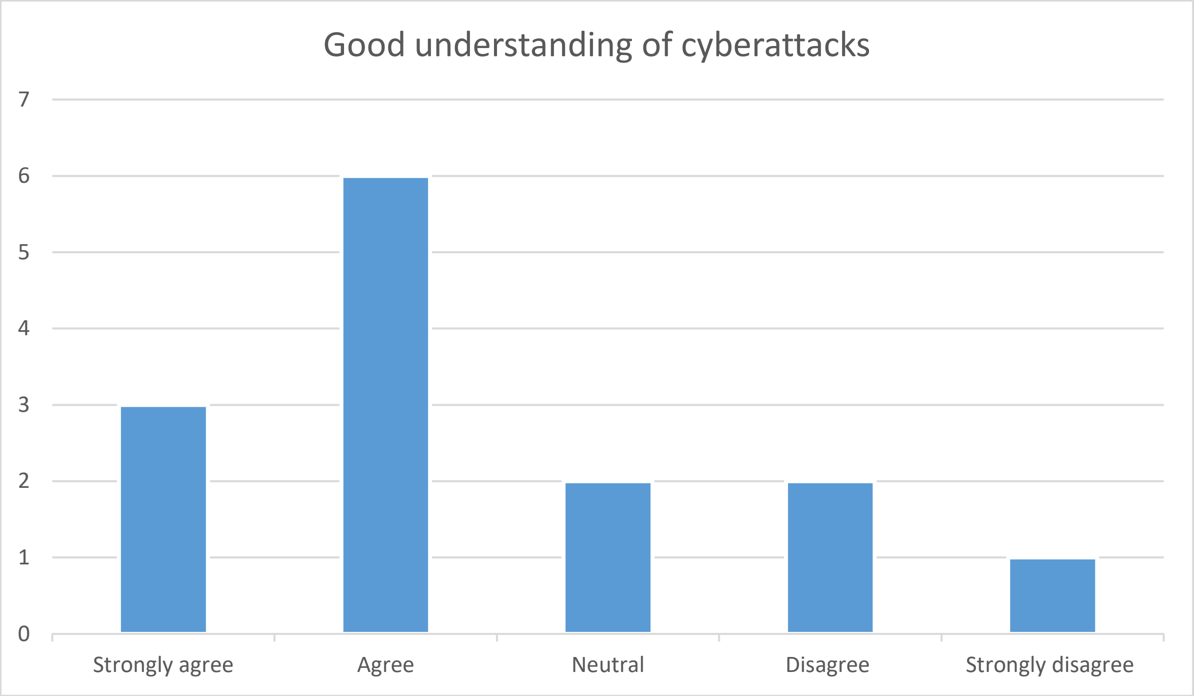


Figure D.200: Good understanding of cyberattacks (Less than a year)

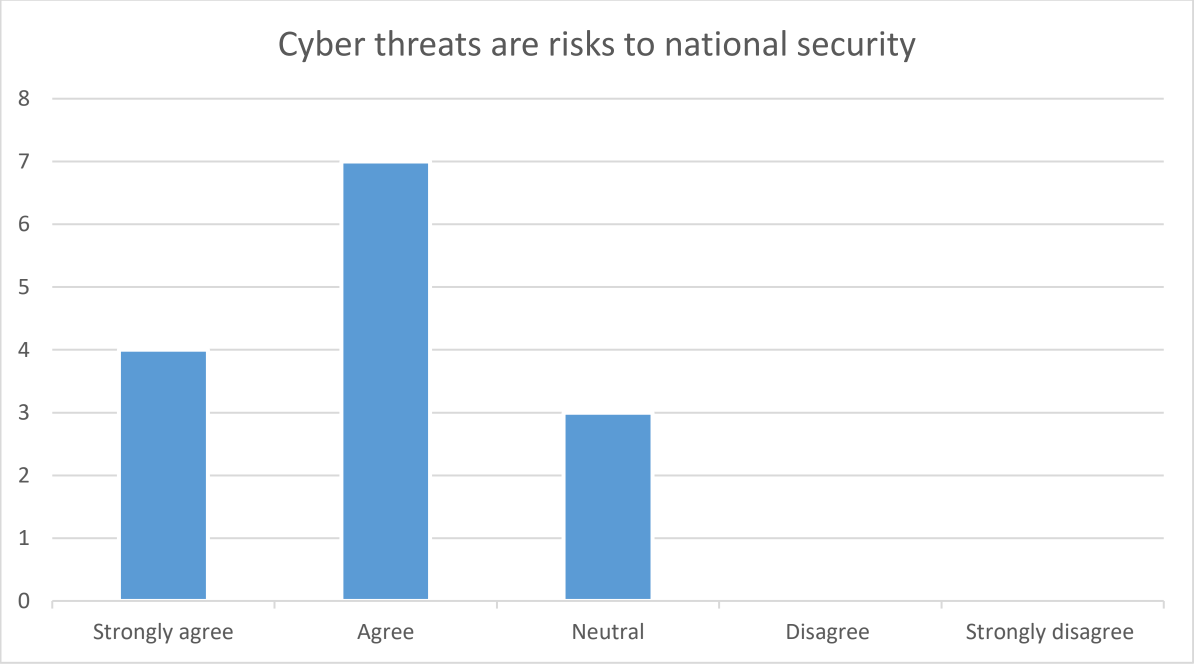


Figure D.201: Cyber threats are risks to national security (Less than a year)

9 participants have a high understanding of the impact of cyber-attacks on the public and the organisation despite the lack of security awareness training; only 3 do not, and 2 'not known' either way (See figure D.200). Furthermore, 68 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure D.201). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in time they will be in a strong position to influence and contribute to the process of accepting and implementing national, regional, and global level mechanisms.

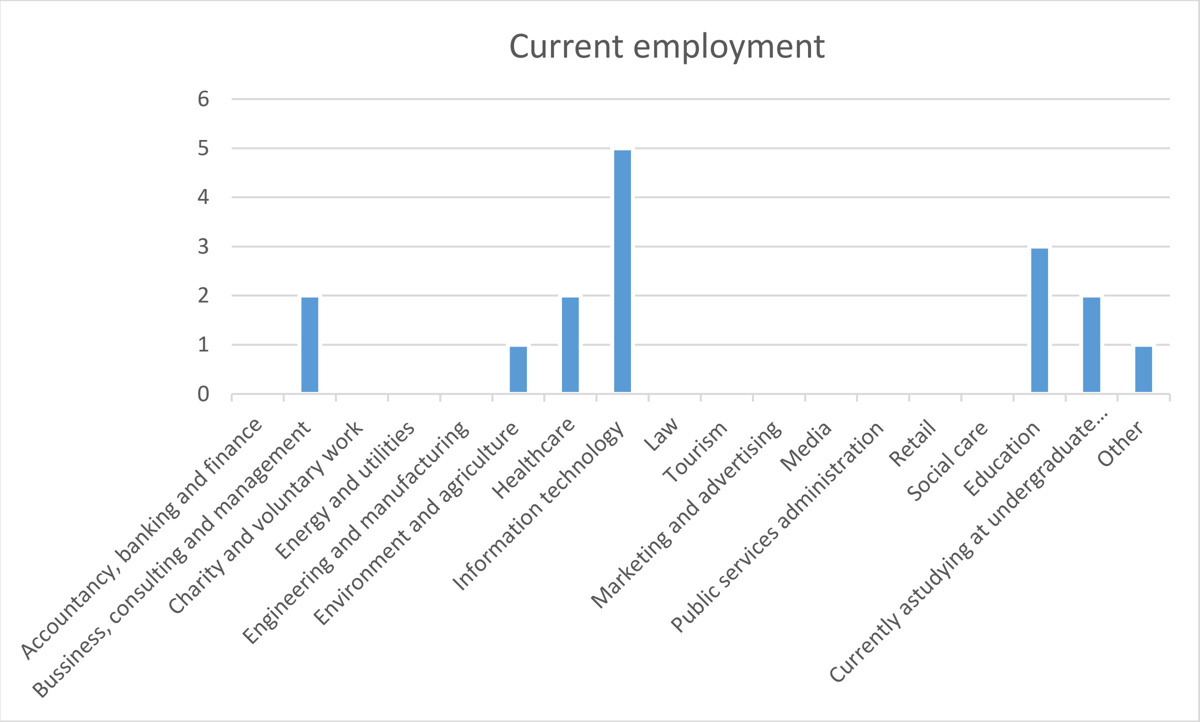


Figure D.202: Current employment (Less than a year)

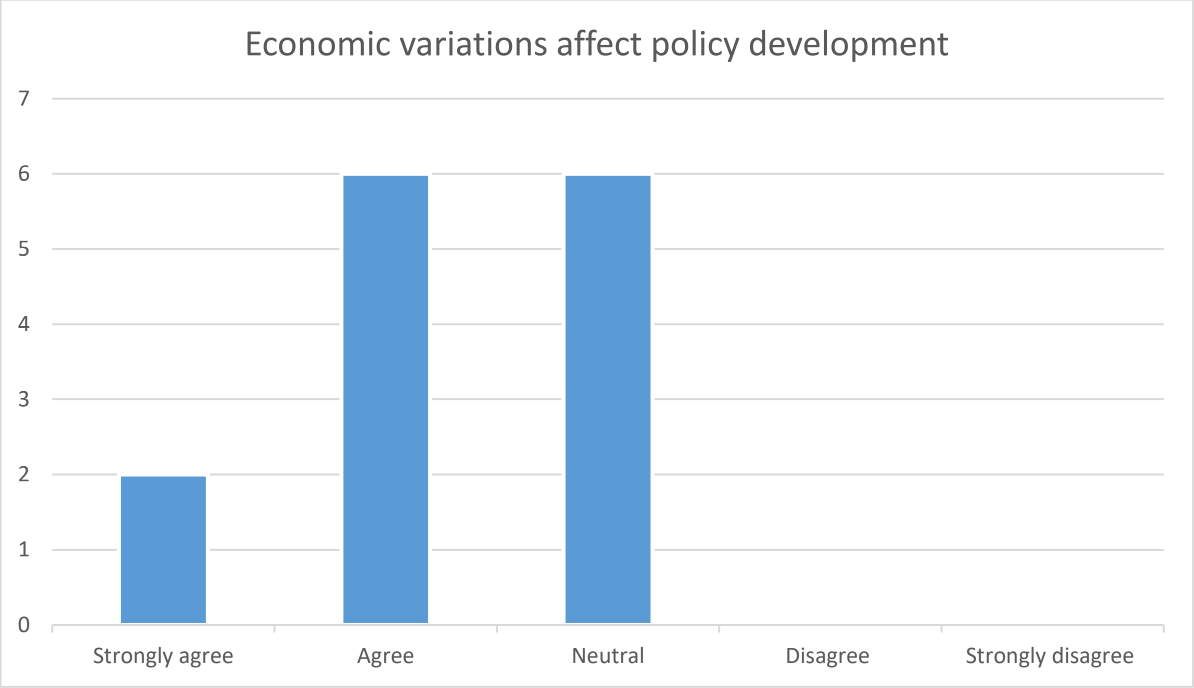


Figure D.203: Economic variations affect policy development (Less than a year)

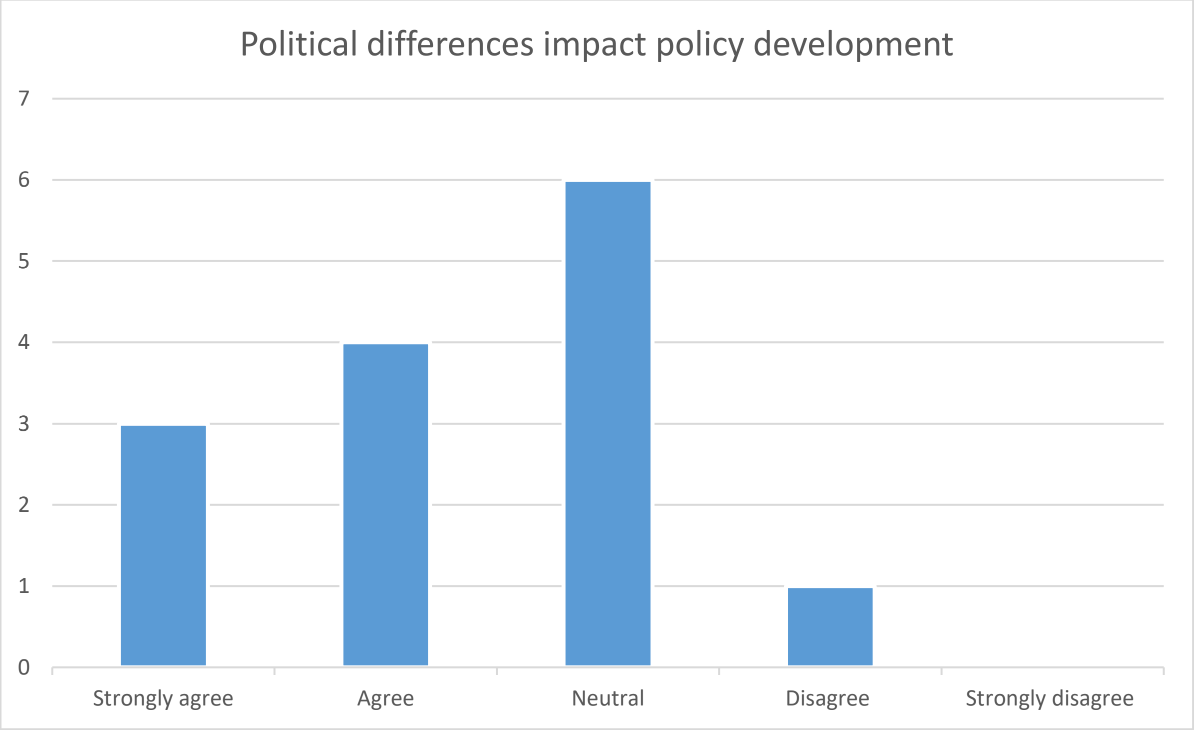


Figure D.204: Political differences impact policy development (Less than a year)

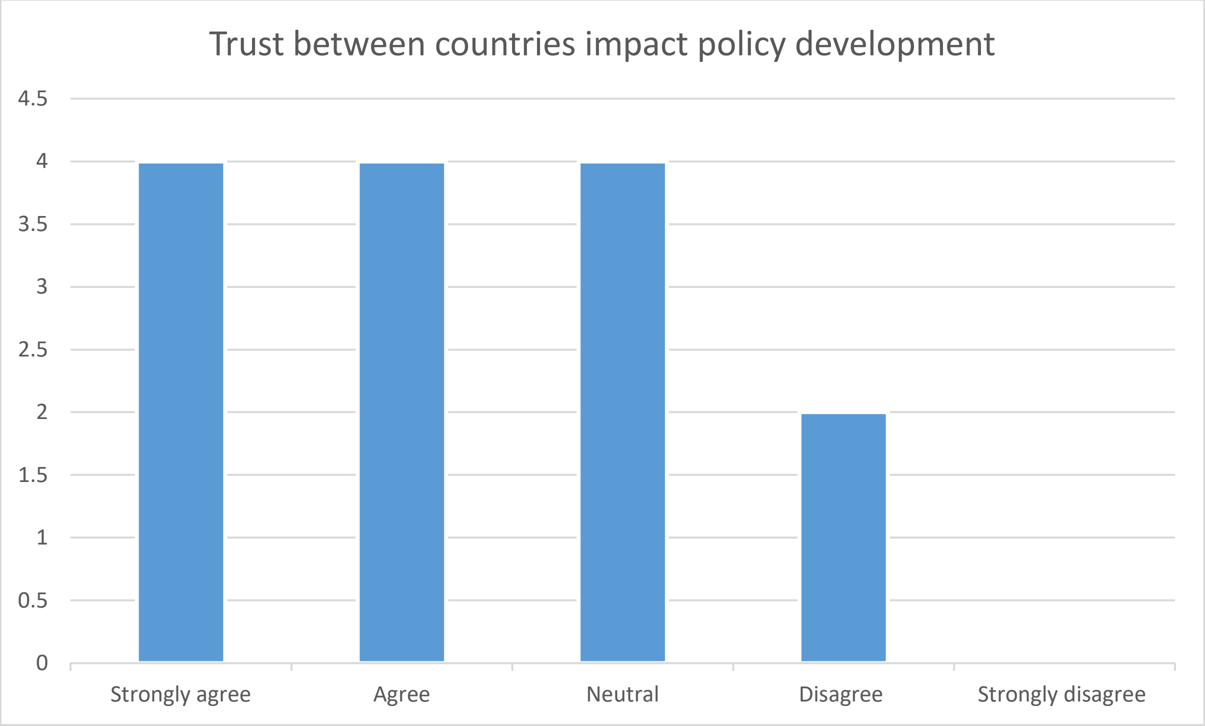


Figure D.205: Trust between countries impact policy development (Less than a year)

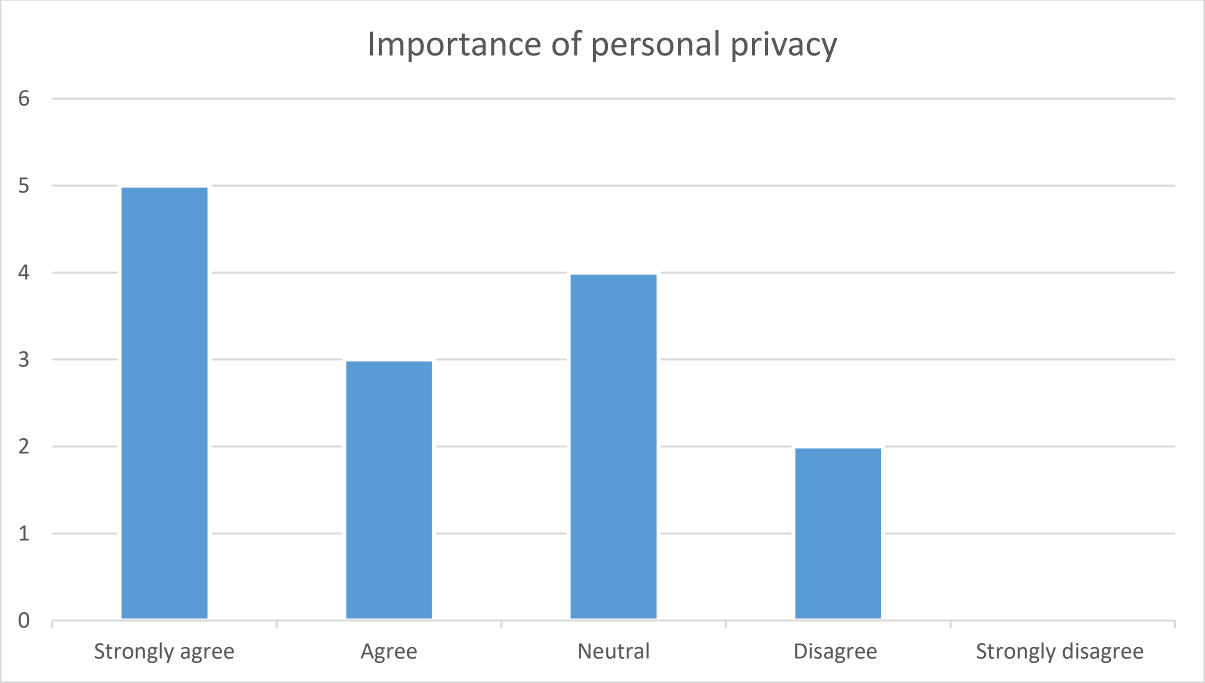


Figure D.206: Importance of personal privacy (Less than a year)

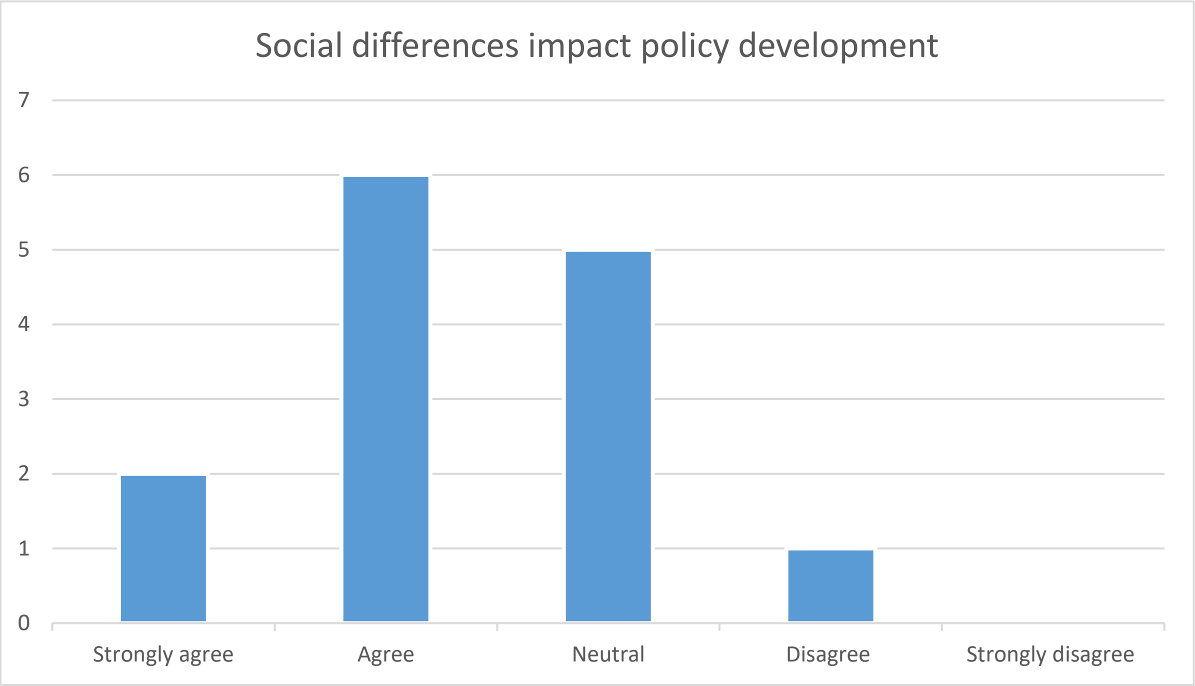


Figure D.207: Social differences impact policy development (Less than a year)

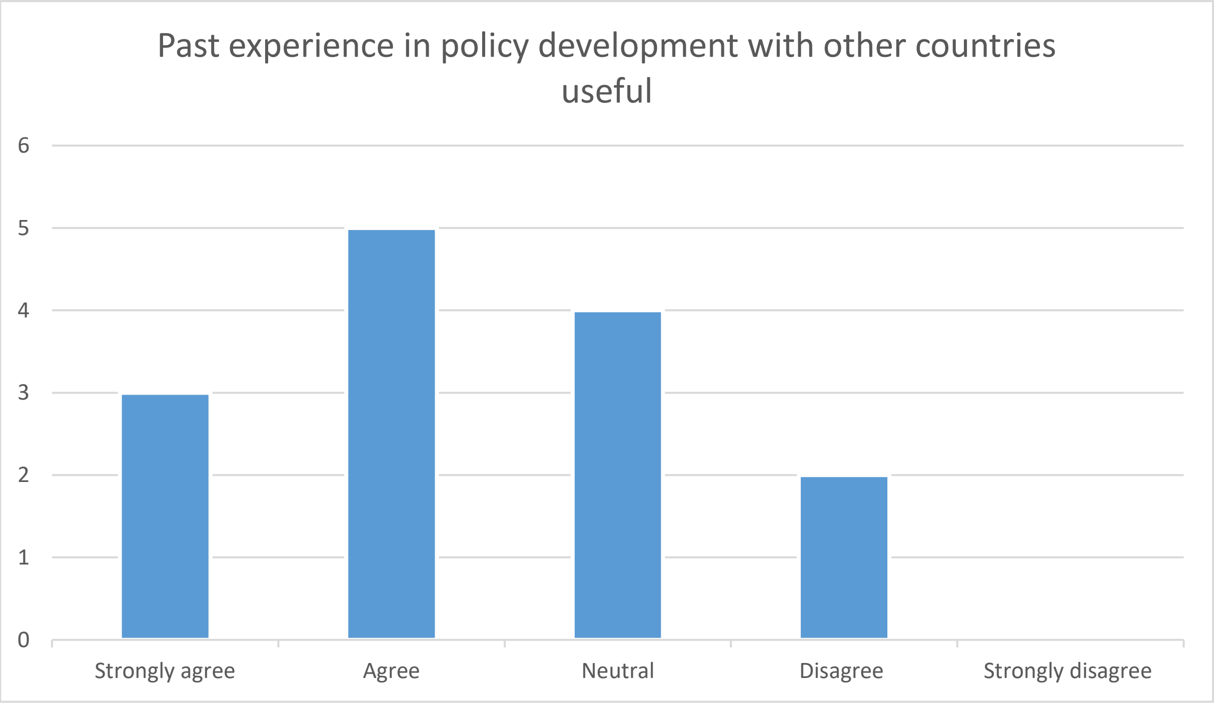


Figure D.208: Past experience in policy development with other countries useful (Less than a year)

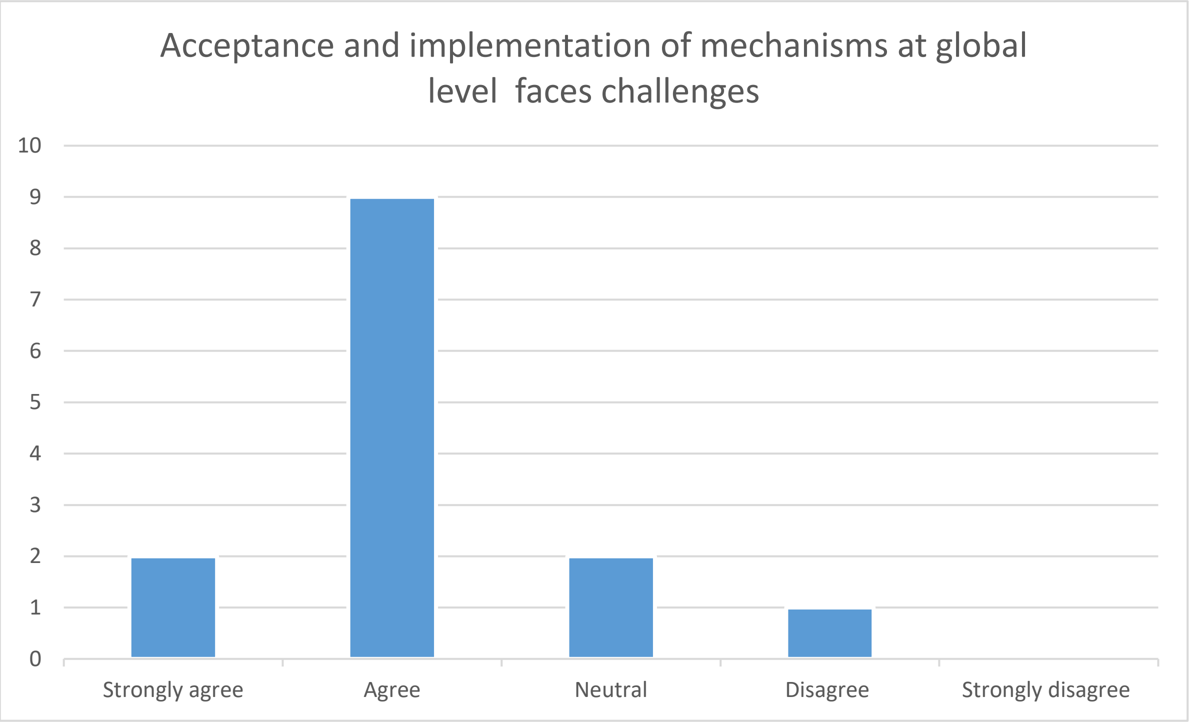


Figure D.209: Acceptance and implementation of mechanisms at global level face challenges (Less than a year)

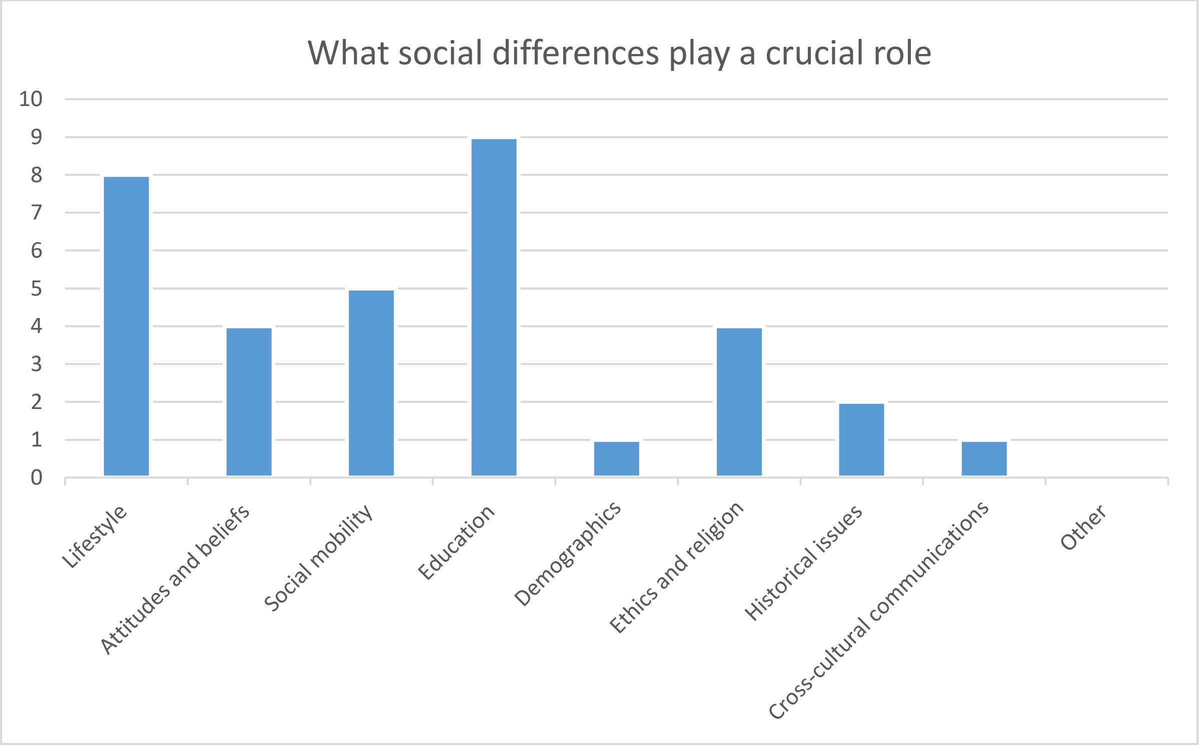


Figure D.210: What social differences play a crucial role (Less than a year)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and lifestyle (See figure D.210). The consensus coming out is a clear indication that educational training could be an effective way to make people understand the importance of privacy and the implications associated with privacy violations. High reliance on technology in handling or sharing personal information demands a high level of discipline and responsibility in accepting and implementing policies associated with data privacy and security. Equally important to have a high level of awareness of potential cyber threats, their impact on people and national security in accepting and implementing data privacy and security policies. Therefore, it is important to provide cybersecurity awareness training at the school and organisational level.

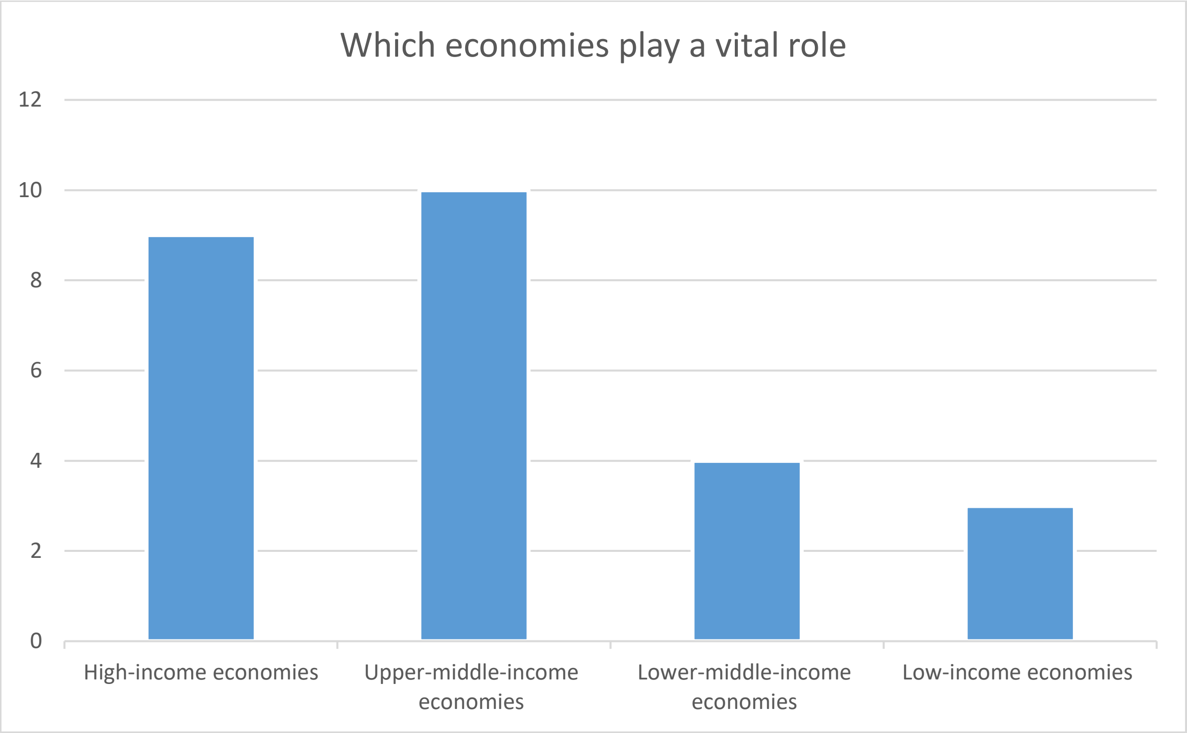


Figure D.211: Which economies play a vital role (Less than a year)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role in the policymaking process (See figure D.211). The key stages in the policymaking process aim to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the resources necessary, implement, and finally evaluate the policy. These stages are time-consuming and require sufficient funding and resources. Therefore, achieving success to a large extent depends on the economic stability of the country, which counts as a crucial factor in policymaking.

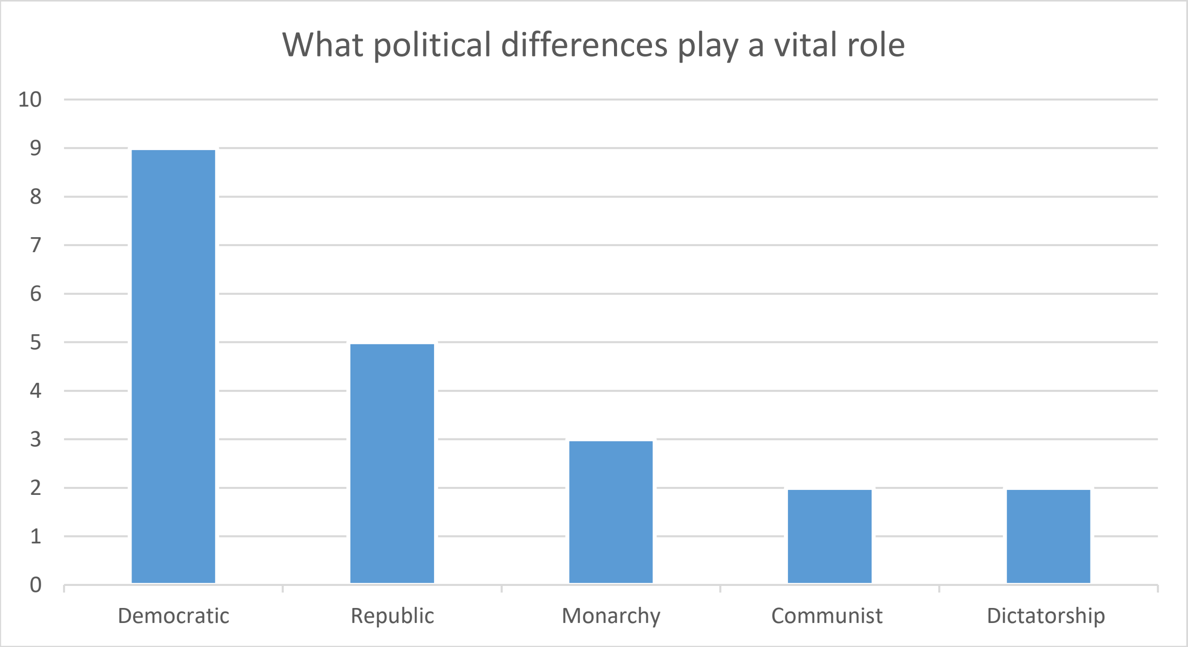


Figure D.212: What political differences play a vital role (Less than a year)

The majority have chosen a democratic political system (See figure D.212), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

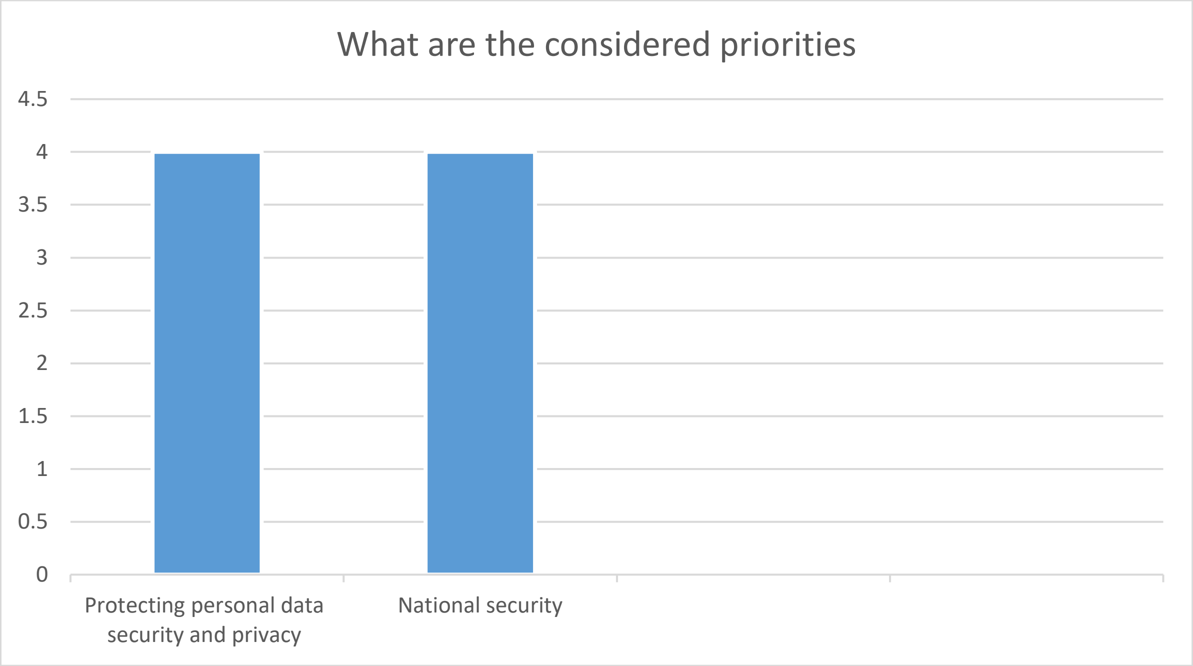


Figure D.213: What are the considered priorities (Less than a year)

The importance of both protecting personal data security and privacy counts in accepting and implementing a global data privacy and security policies but does not represent the majority view (See figure D.213).

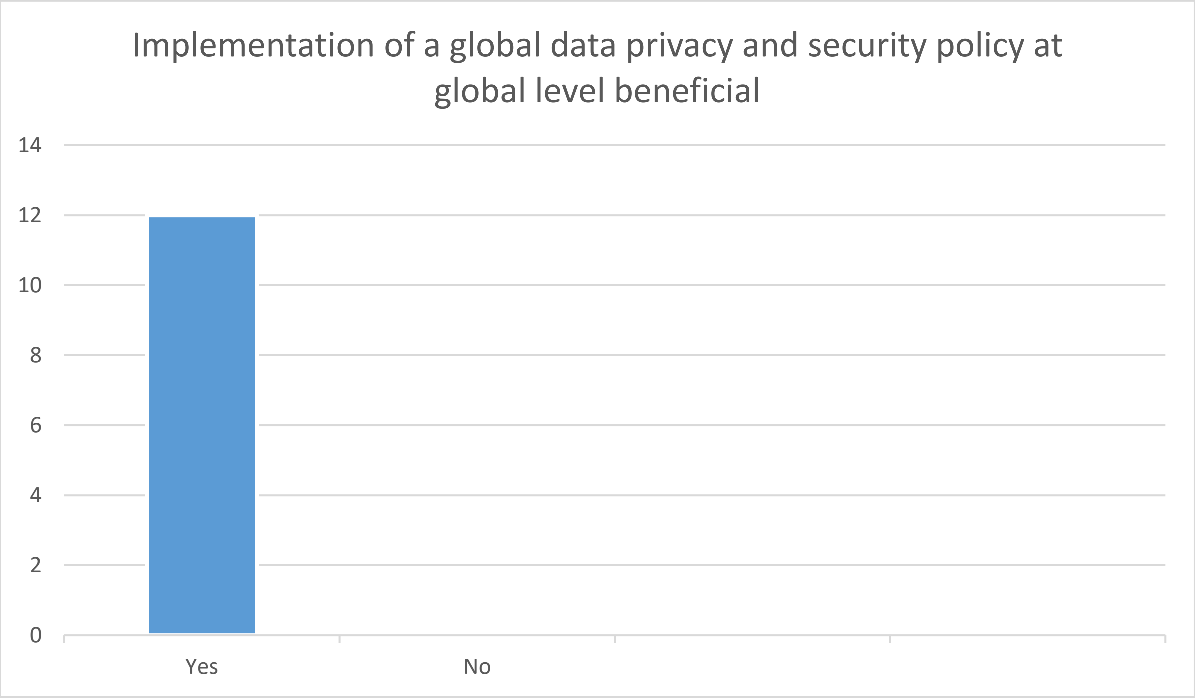


Figure D.214: Implementation of a data privacy and security policy at global level beneficial (Less than a year)

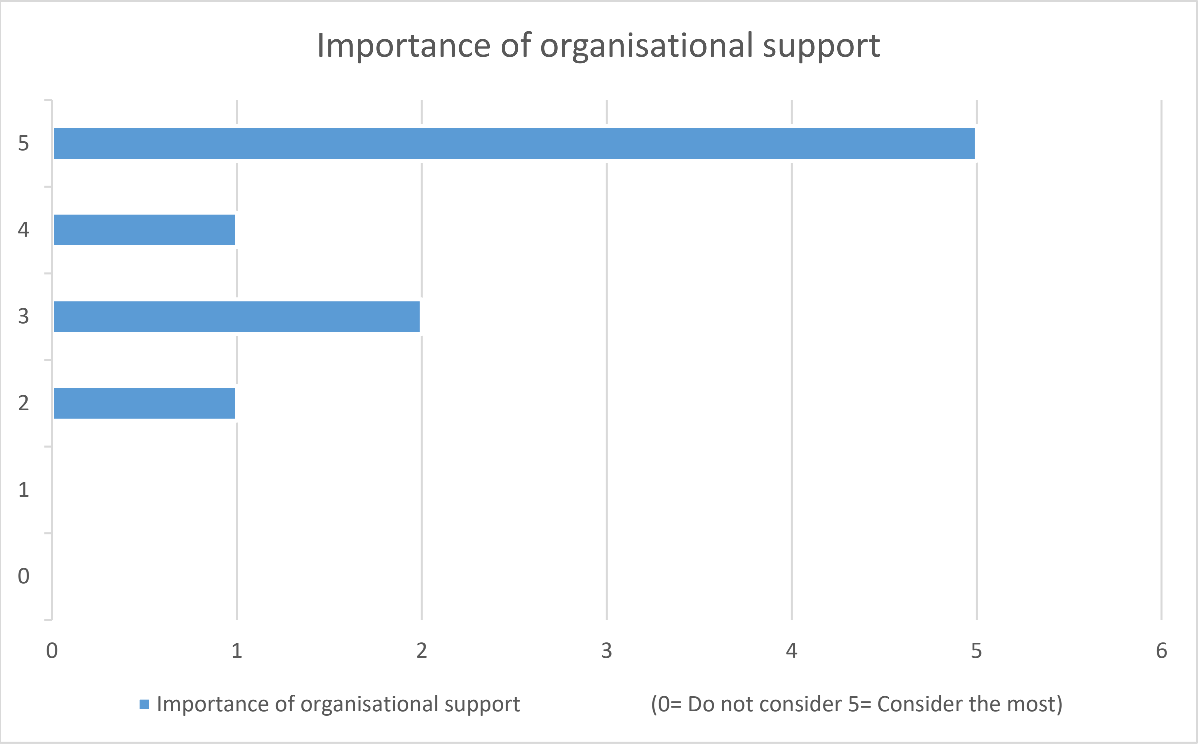


Figure D.215: Importance of organisational support (Less than a year)

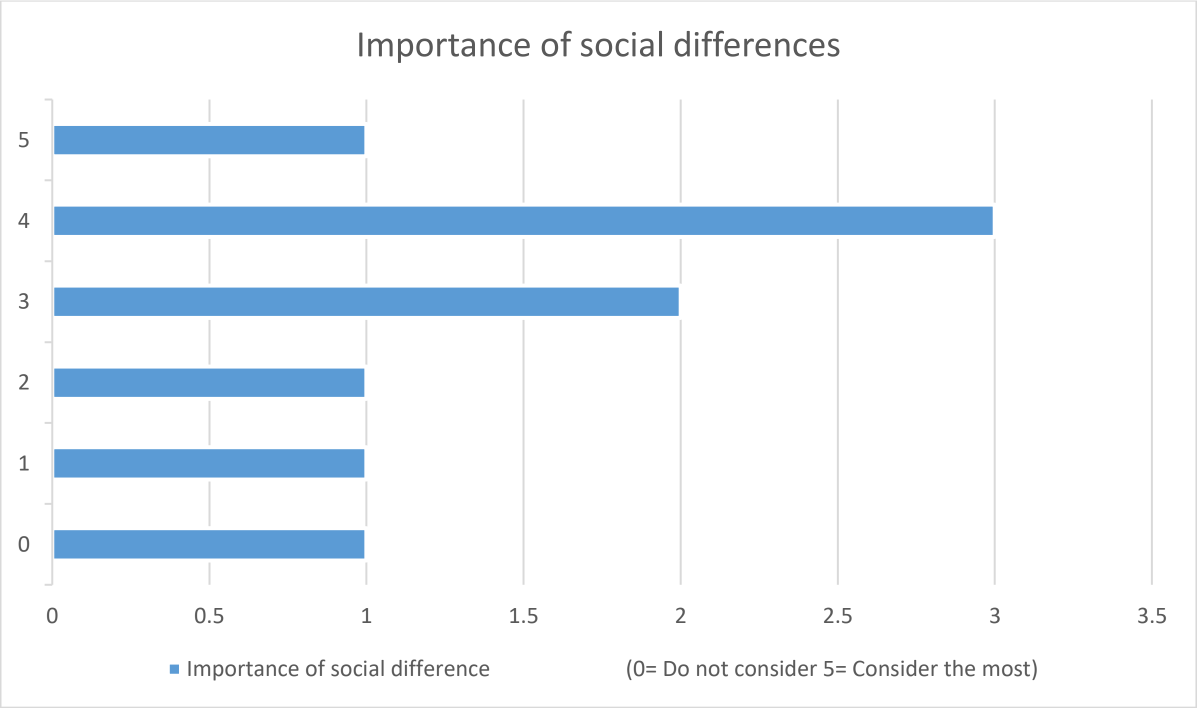


Figure D.216: Importance of social differences (Less than a year)

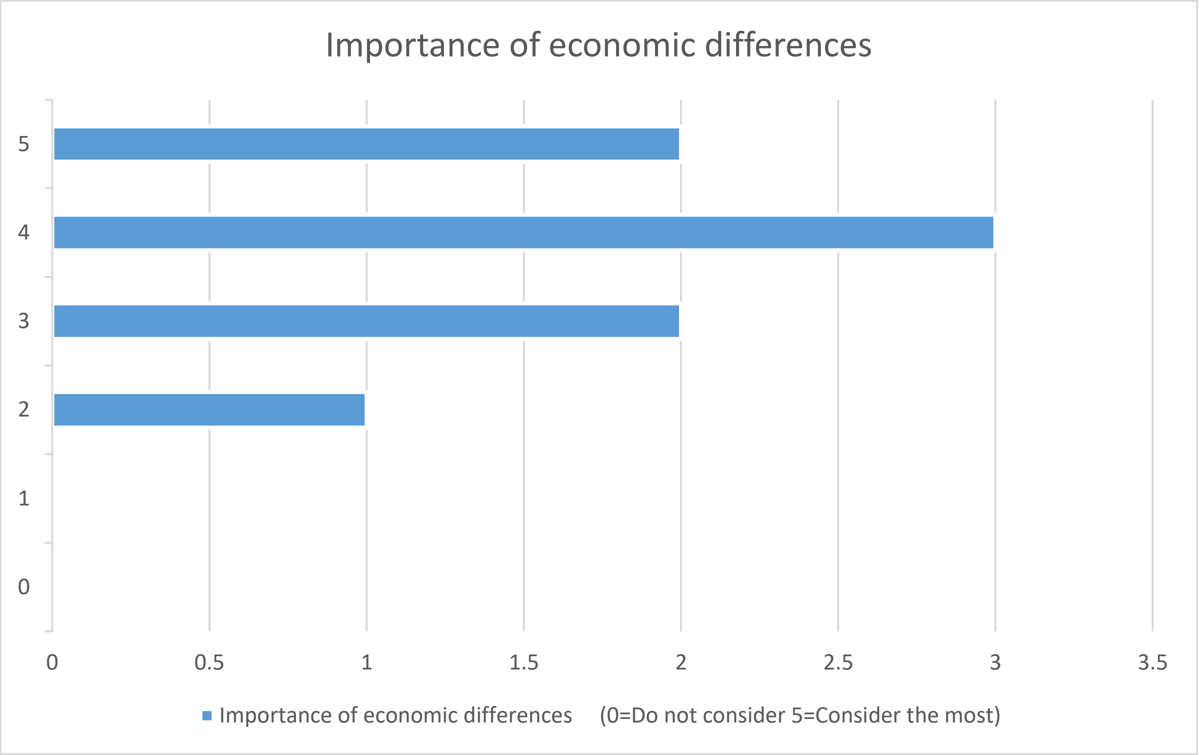


Figure D.217: Importance of economic differences (Less than a year)

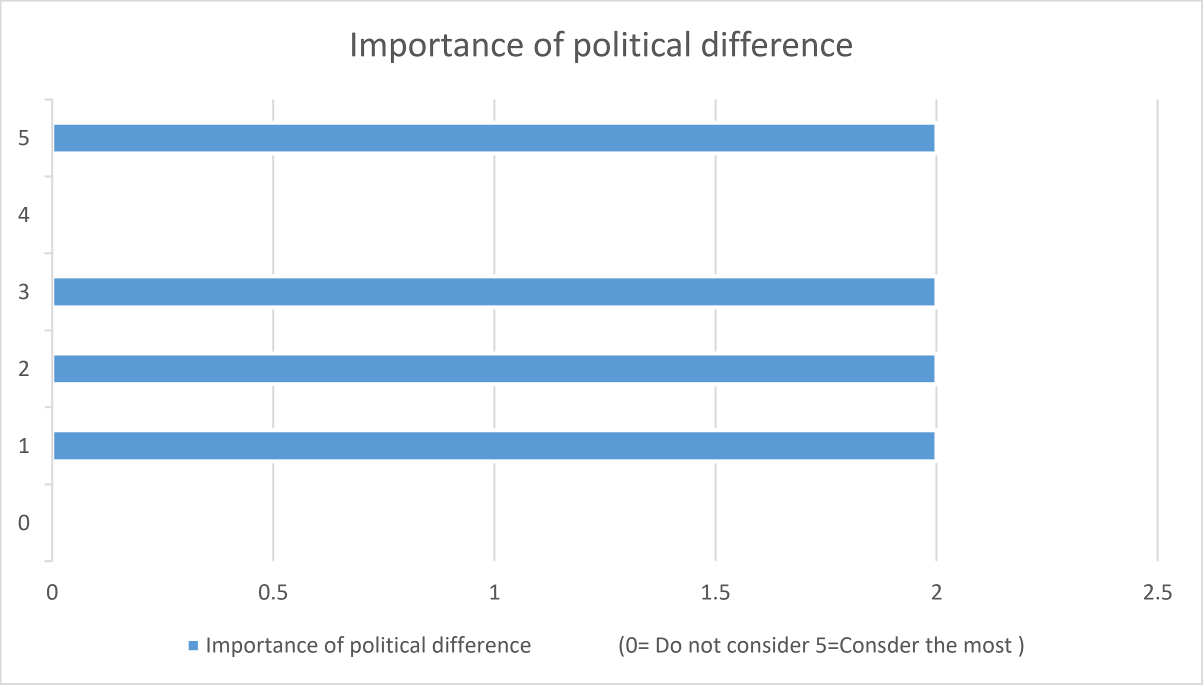


Figure D.218: Importance of political difference (Less than a year)

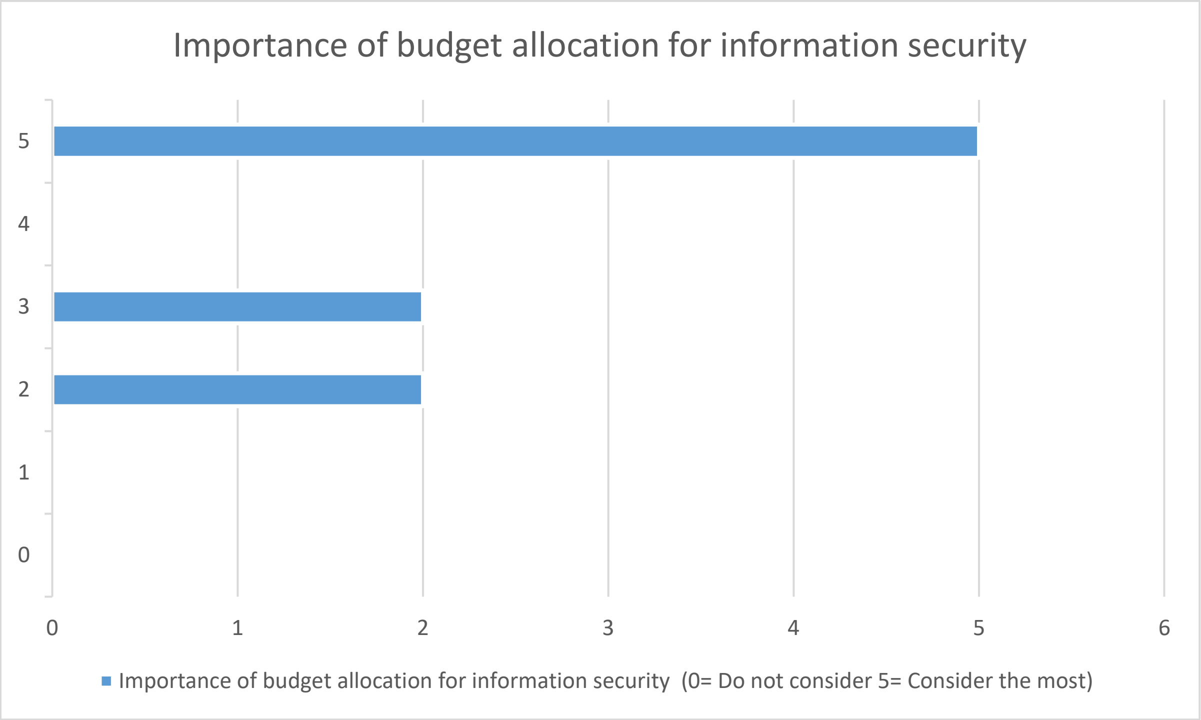


Figure D.219: Importance of budget allocation for information security (Less than a year)

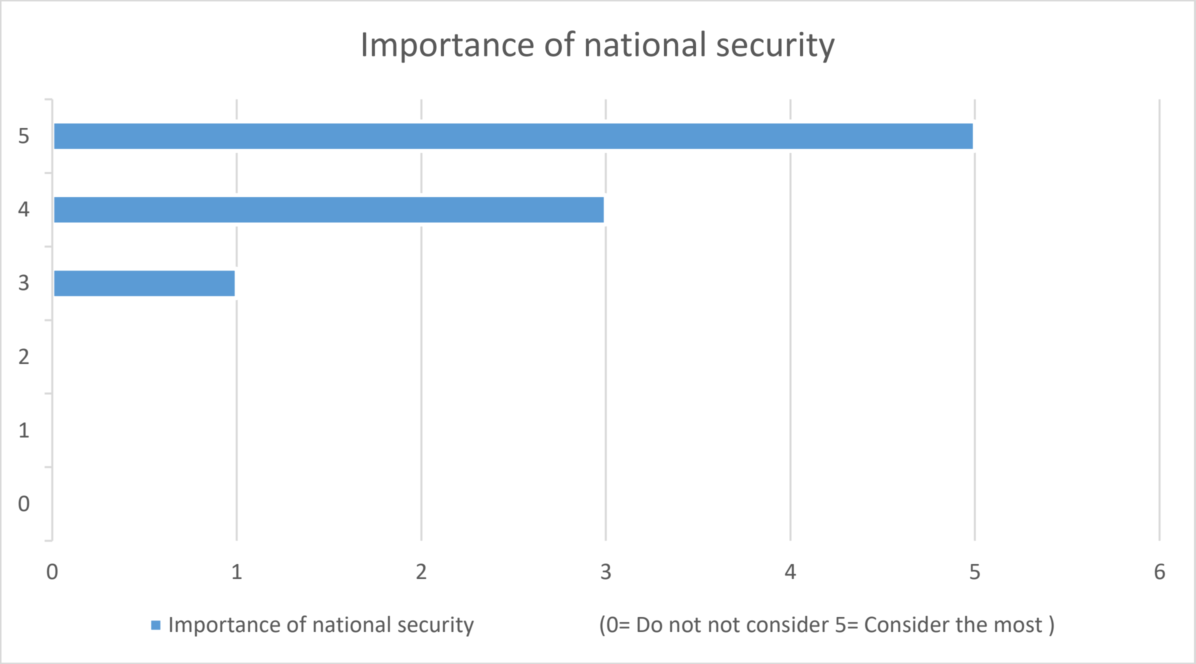


Figure D.220: Importance of national security (Less than a year)

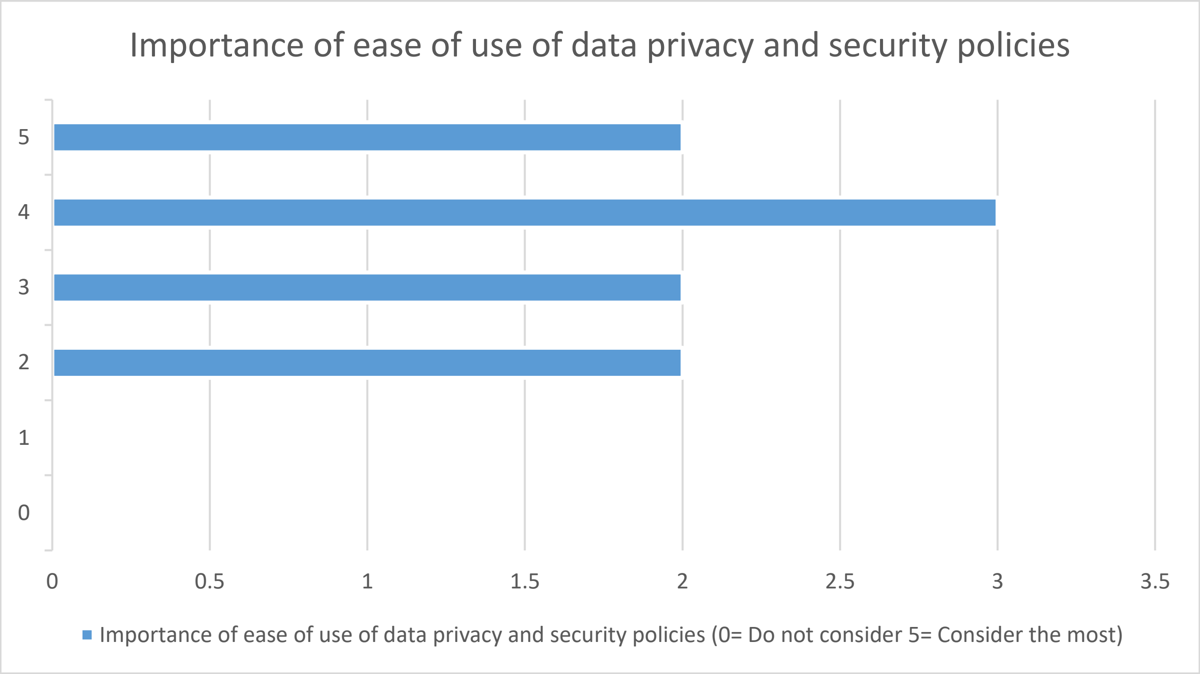


Figure D.221: Importance of ease of use of data privacy and security policies (Less than a year)

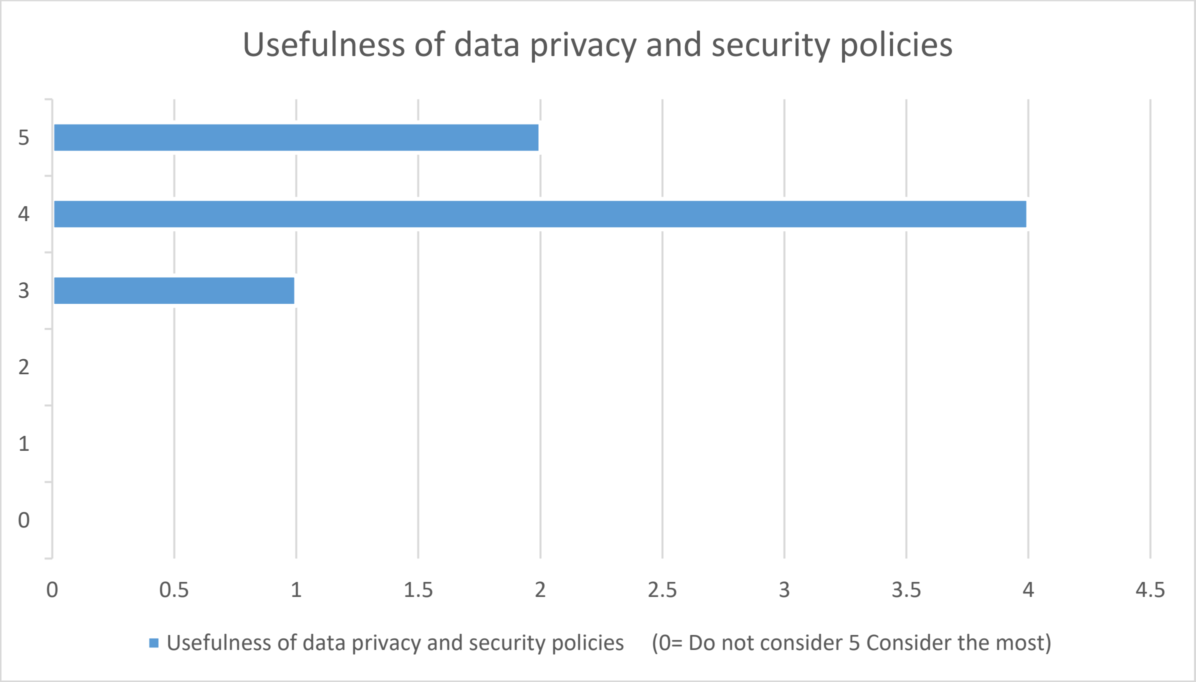


Figure D.222: Usefulness of data privacy and security policies (Less than a year)

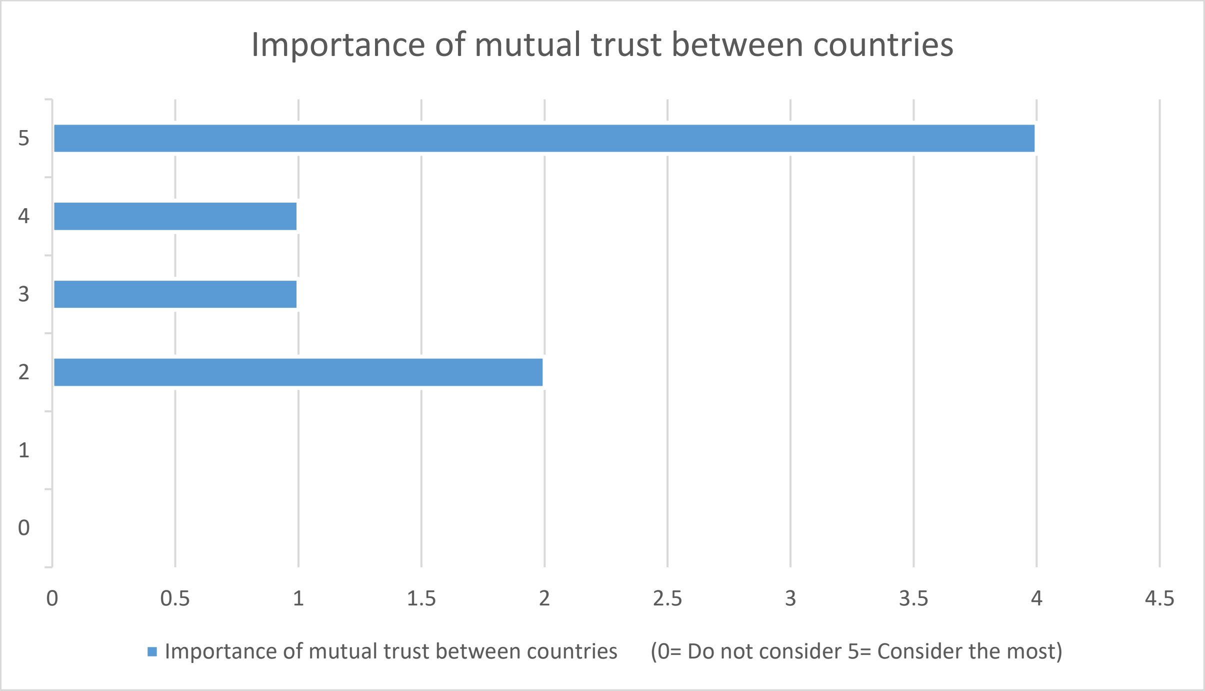


Figure D.223: Importance of mutual trust between countries (Less than a year)

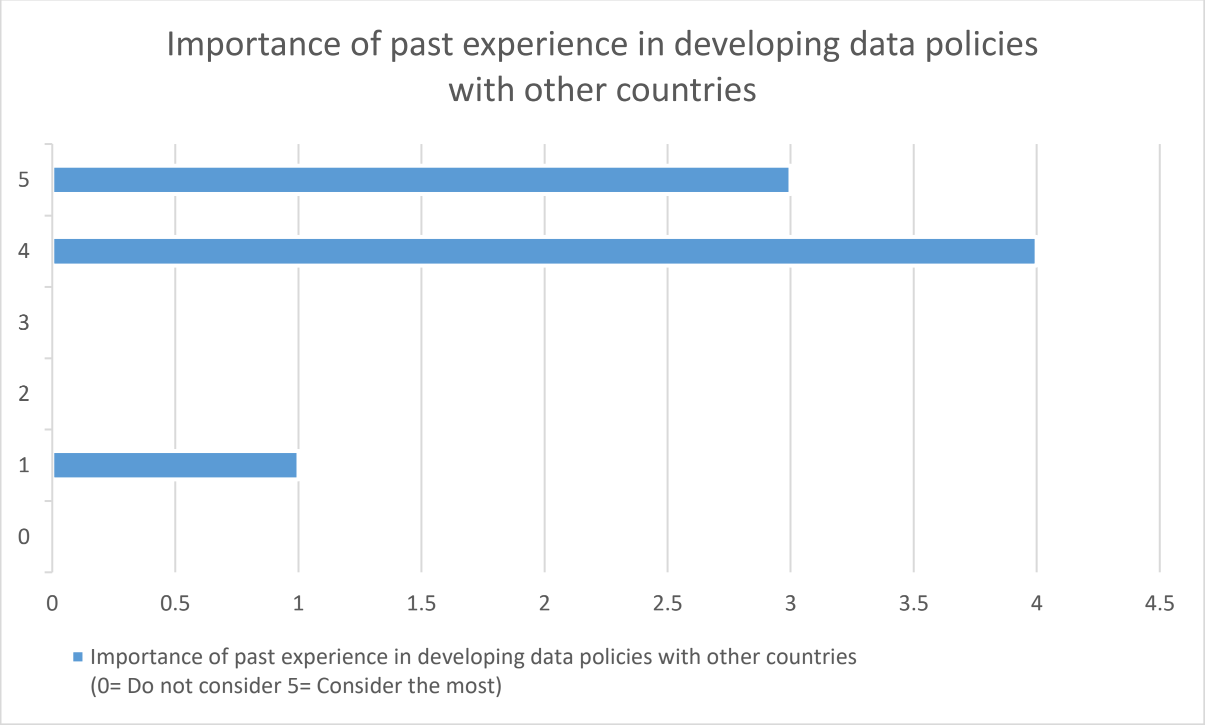


Figure D.224: Importance of past experience in developing data policies with other counties (Less than a year)

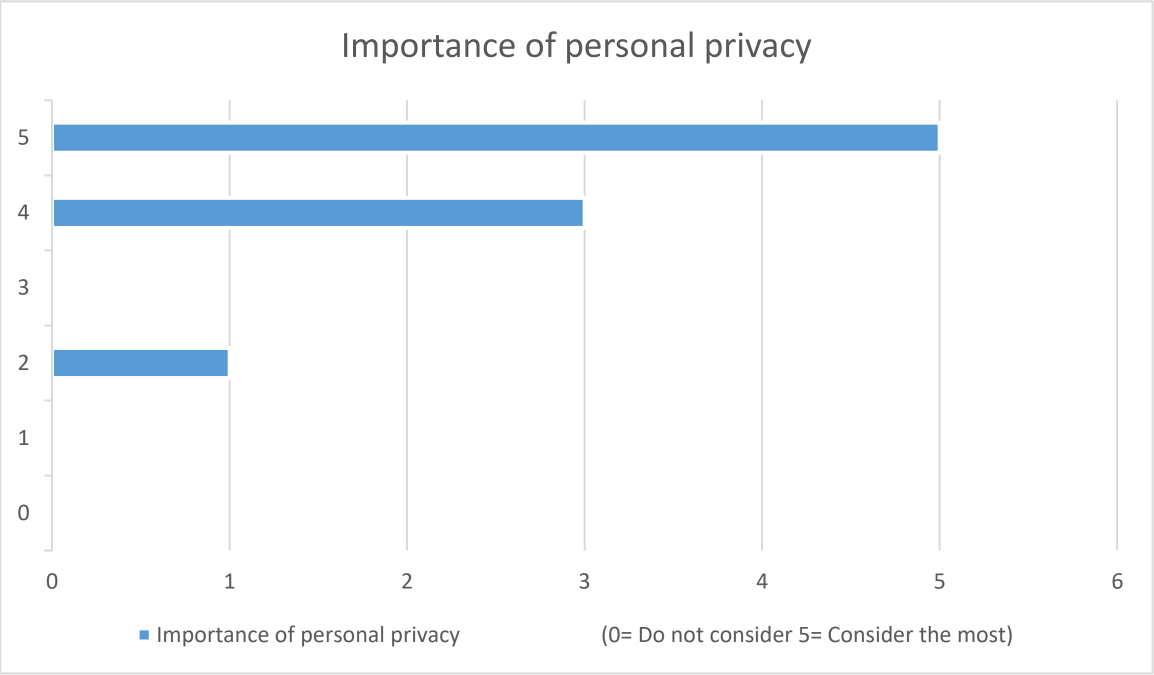


Figure D.225: Importance of personal privacy (Less than a year)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 69 percent of the respondents have endorsed (See figure D.214). The other notable factors that have come out of the survey aware organisational support, budget allocation for information security, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies and previous experience with other countries in developing policies (See figure D.203-213) (See figure D.215-225).

Sri Lanka – 1-5 years

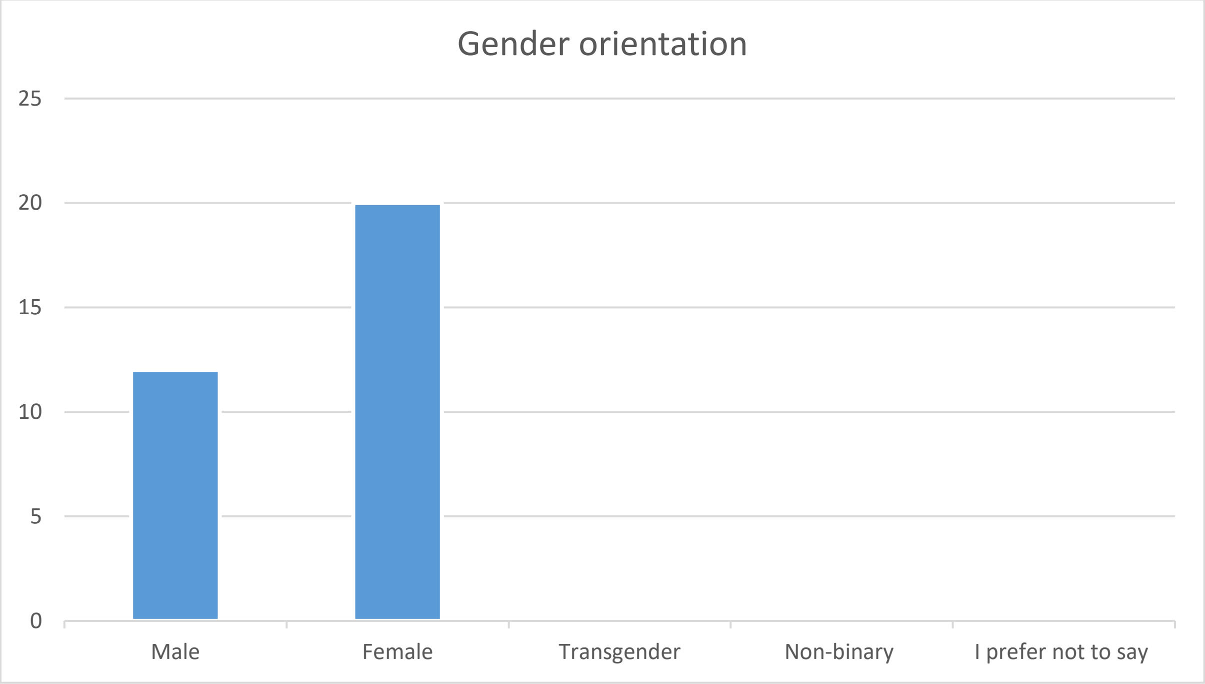


Figure D.226: Gender orientation (1-5 years)

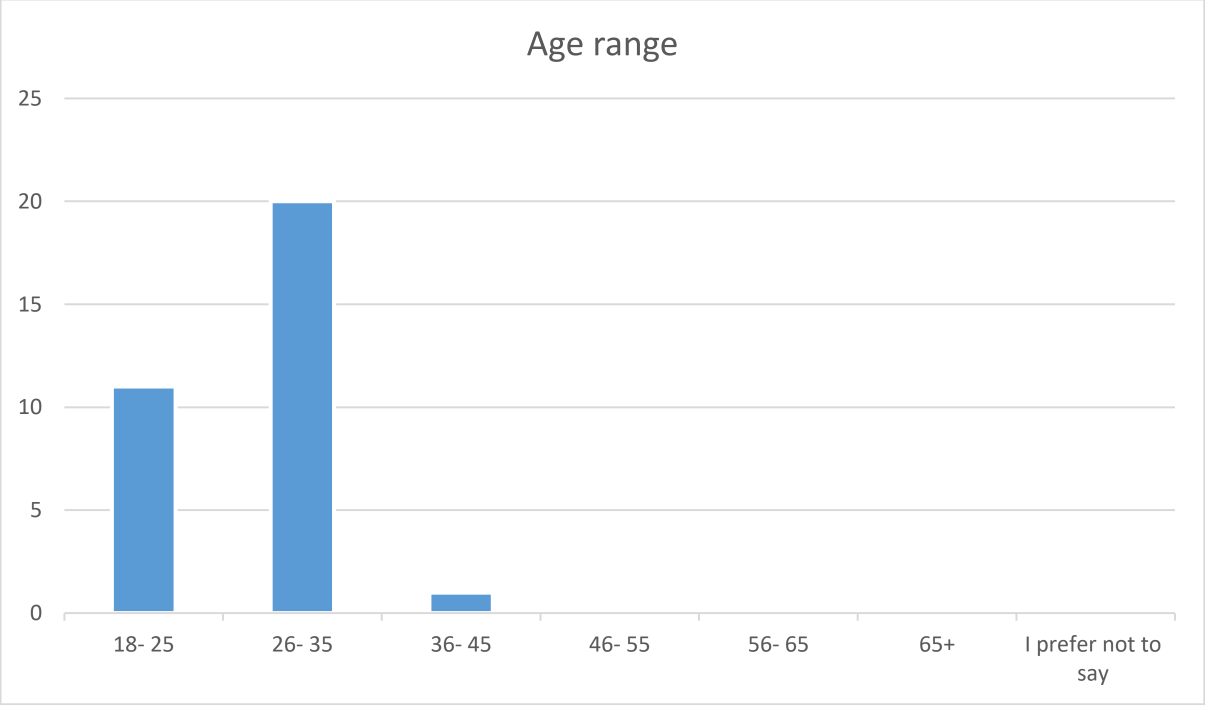


Figure D.227: Age range (1-5 years)

This analysis is based on the responses received from Sri Lankans with 1 to 5 years of employment in the industry. There were 32 participants and 12 out of them were males and 20 females (See figure D.226). They were within the 18-45 age range out of which 11 in the 18-25, 20 in the 26-35, and 1 in the 36-45 range (See figure D.227). This indicates that the age range of the majority of employees with 1-5 years of service is 45 years or less.

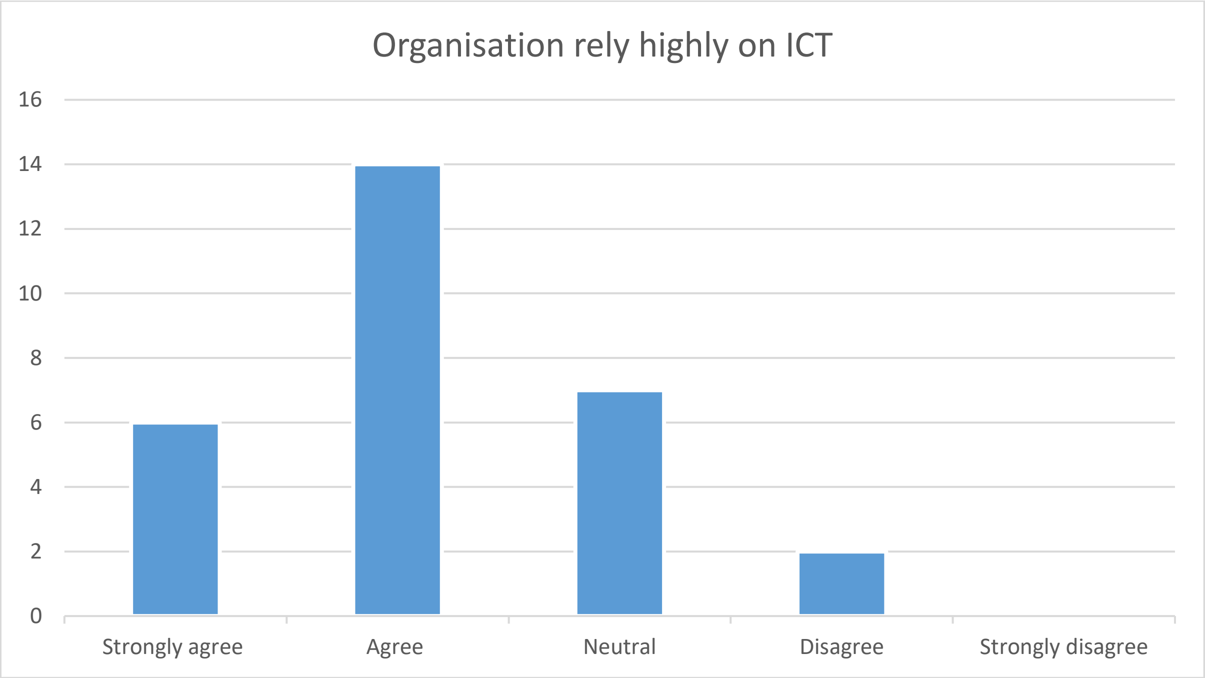


Figure D.228: Organisation rely highly on ICT (1-5 years)

Out of the 32 respondents, 20 have worked in a technology reliance working environment, 7 unaware of reliance on technology because of the nature of the work assigned to them, 2 have marked ‘disagree’ on ICT (See figure D.228). This indicates a majority of those who have been working in an organisation for 1-5 years do have high reliance on ICT.

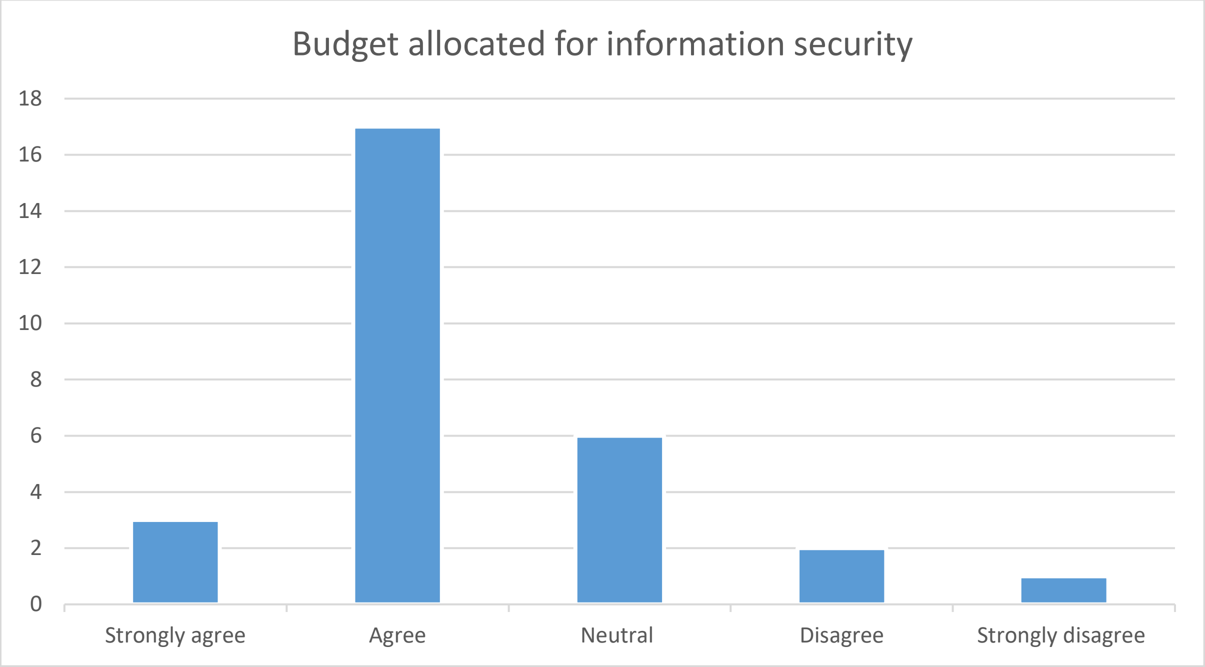


Figure D.229: Budget allocated for information security (1-5 years)

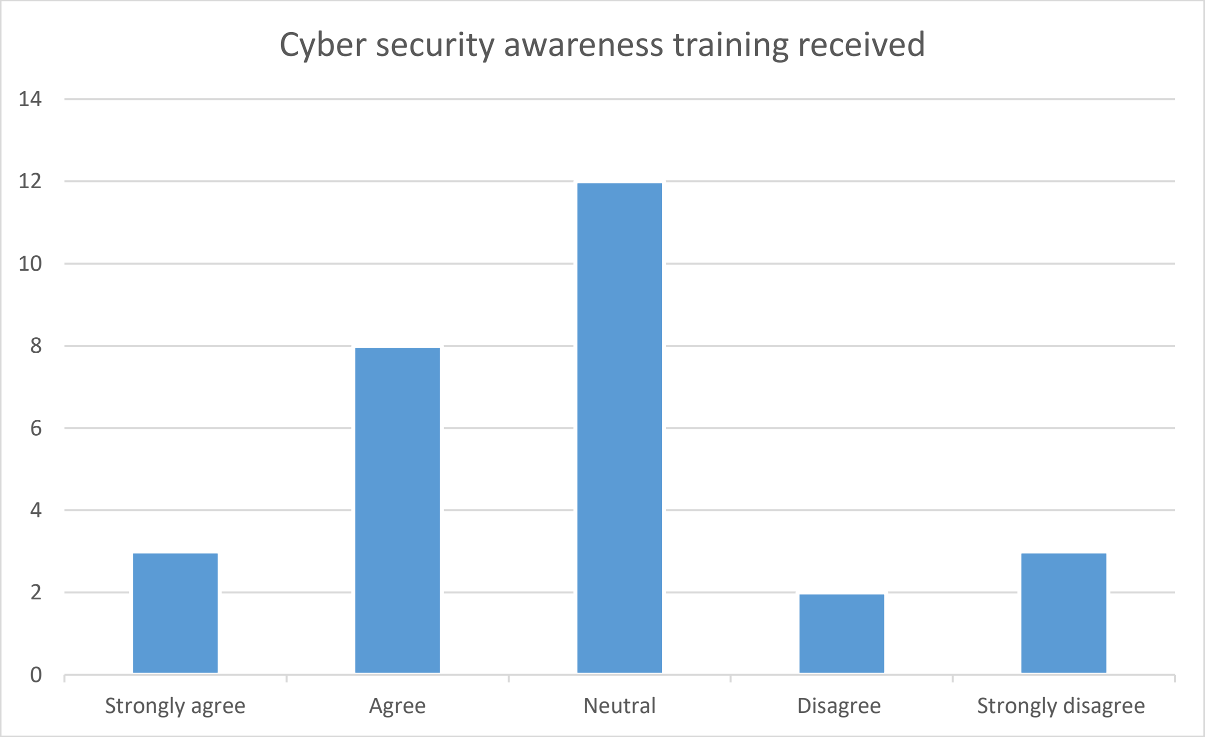


Figure D.230: Cyber security awareness training received (1-5 years)

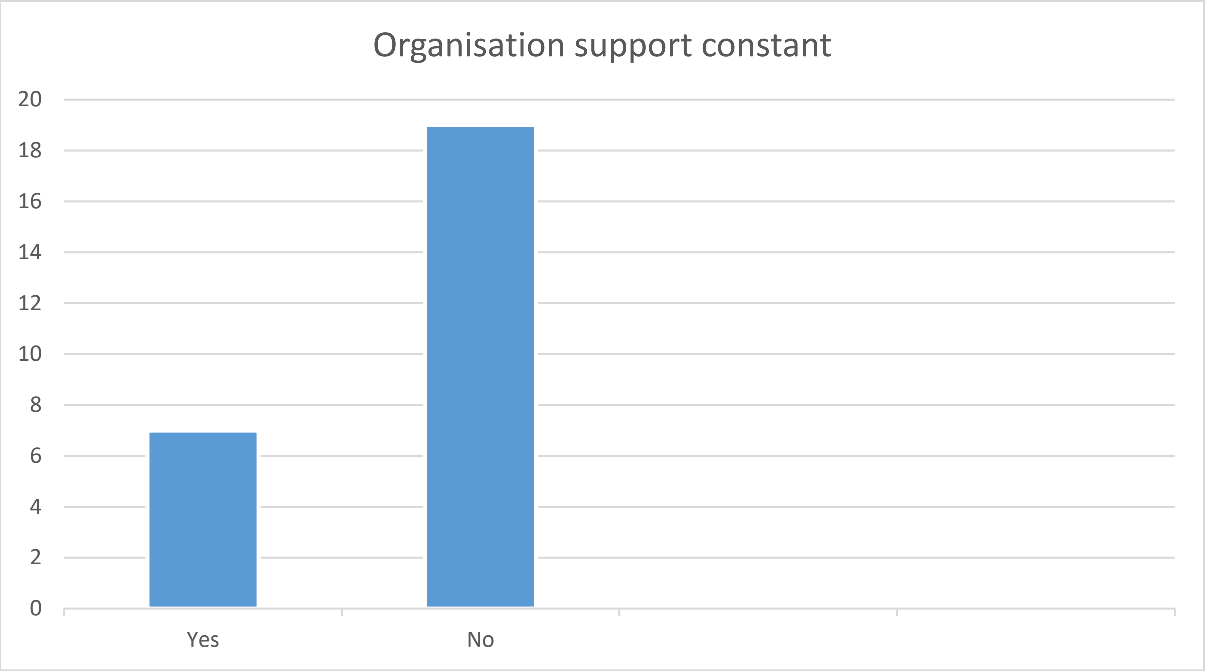


Figure D.231: Organisation support constant (1-5 years)

Funding has been sketchy. 20 out of the 32 have indicated that their organisations had an allocated budget for information security, whilst 6 had not expressed an opinion either way and notably according to the 3 disagreed, their organisations had no budget allocation for information security (See figure D.229). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 11 participants have received regular cybersecurity awareness training, whilst the majority neither agreed nor disagreed, except for 5 participants who had not regularly received security awareness training (See figure D.230). In addition, 19 participants had not received support from the organisation to protect personal information, whilst only 7 did (See figure D.231). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

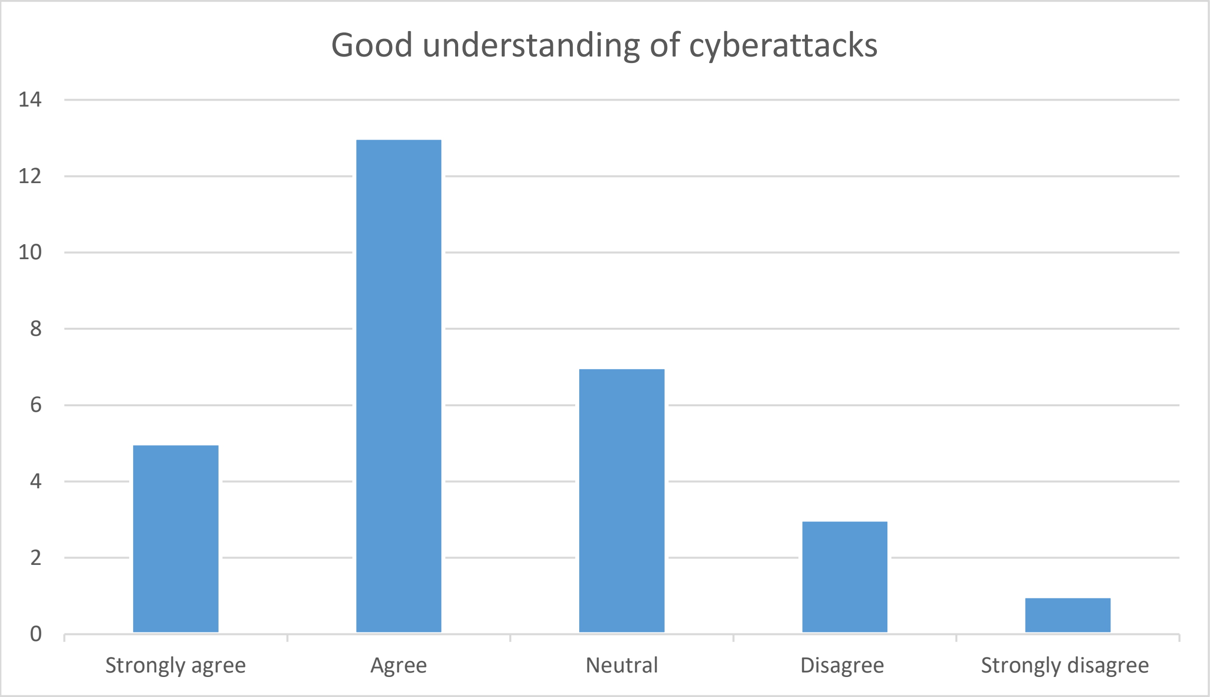


Figure D.232: Good understanding of cyberattacks (1-5 years)

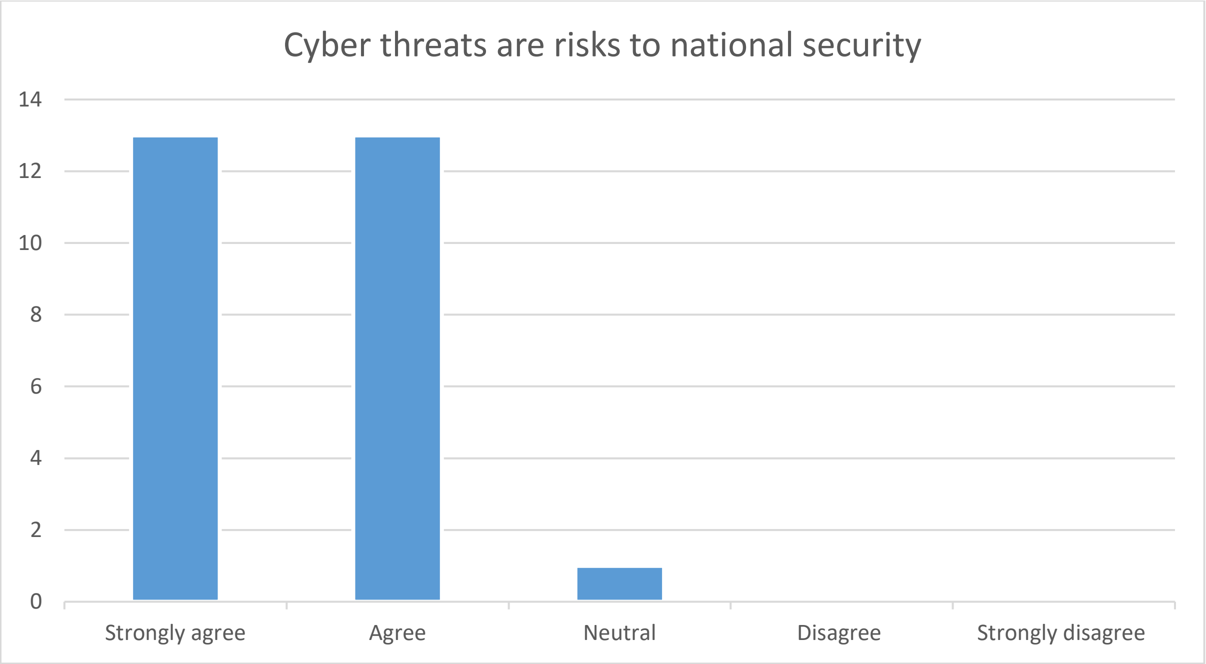


Figure D.233: Cyber threats are risks to national security (1-5 years)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 18 participants do have, 7 have not expressed opinion either way, and only 4 participants had no understanding (See figure D.232). Furthermore, majority of the participants also realises the potential threats to national security from cyber-attacks (See figure D.233). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

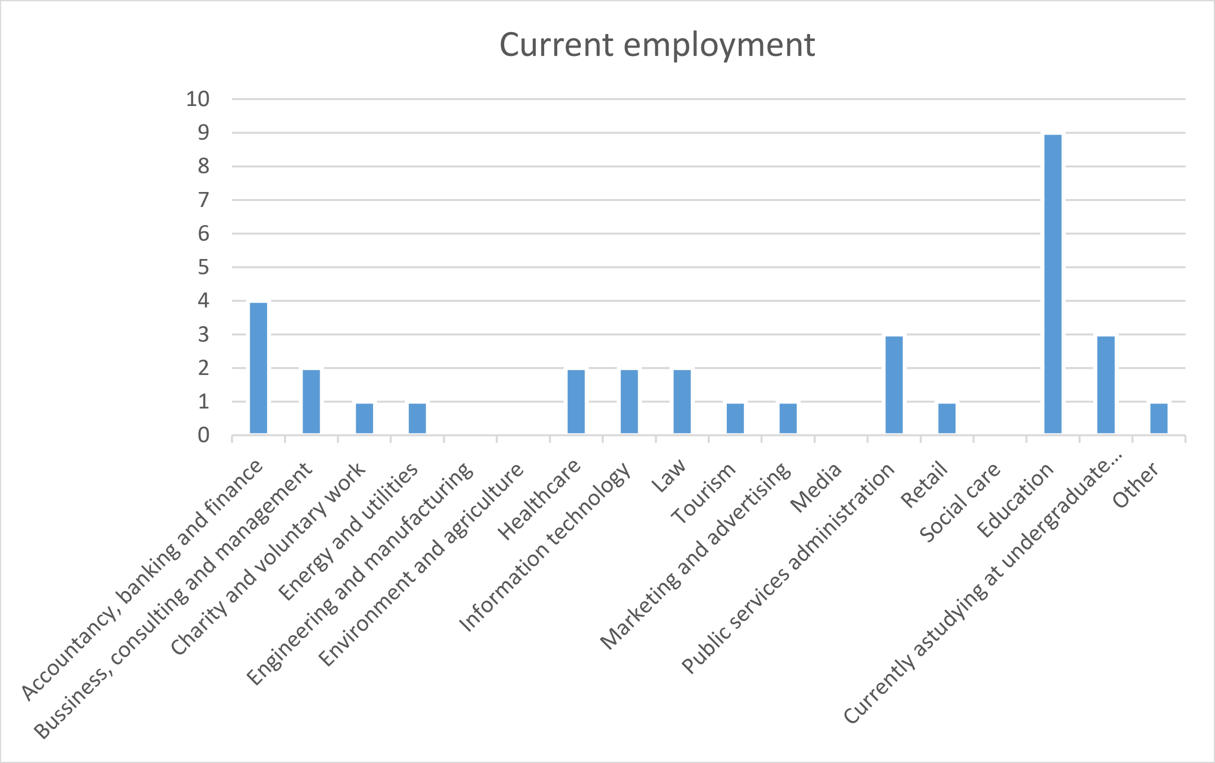


Figure D.234: Current employment (1-5 years)

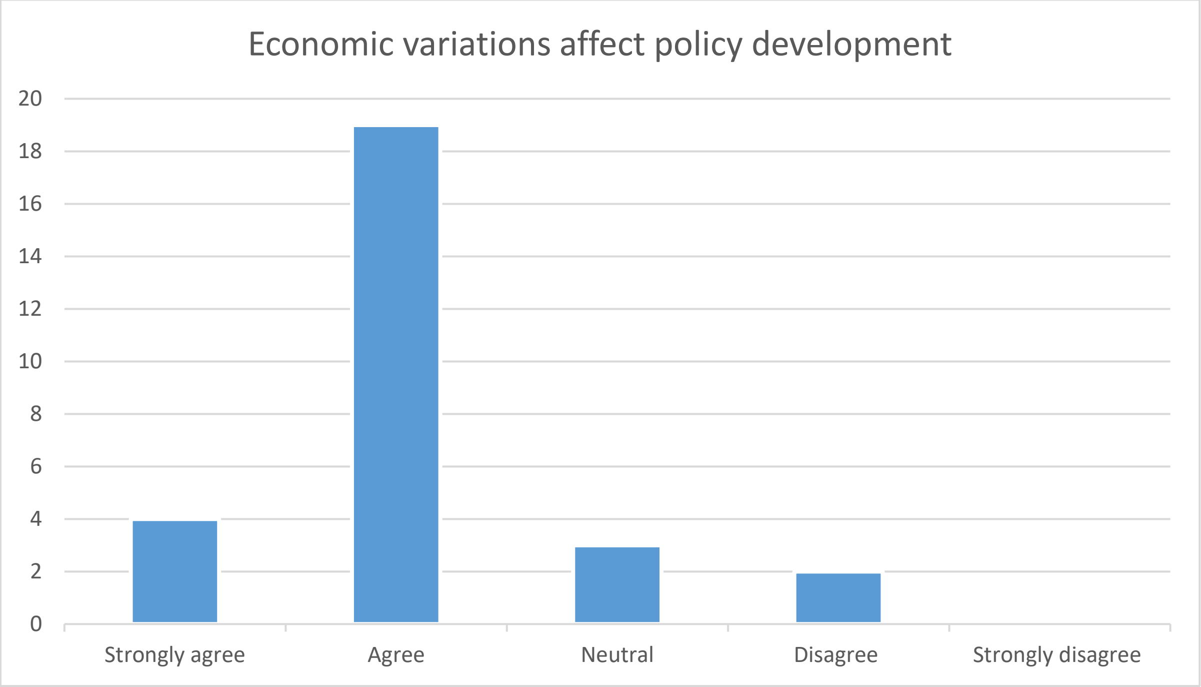


Figure D.235: Economic variations affect policy development (1-5 years)

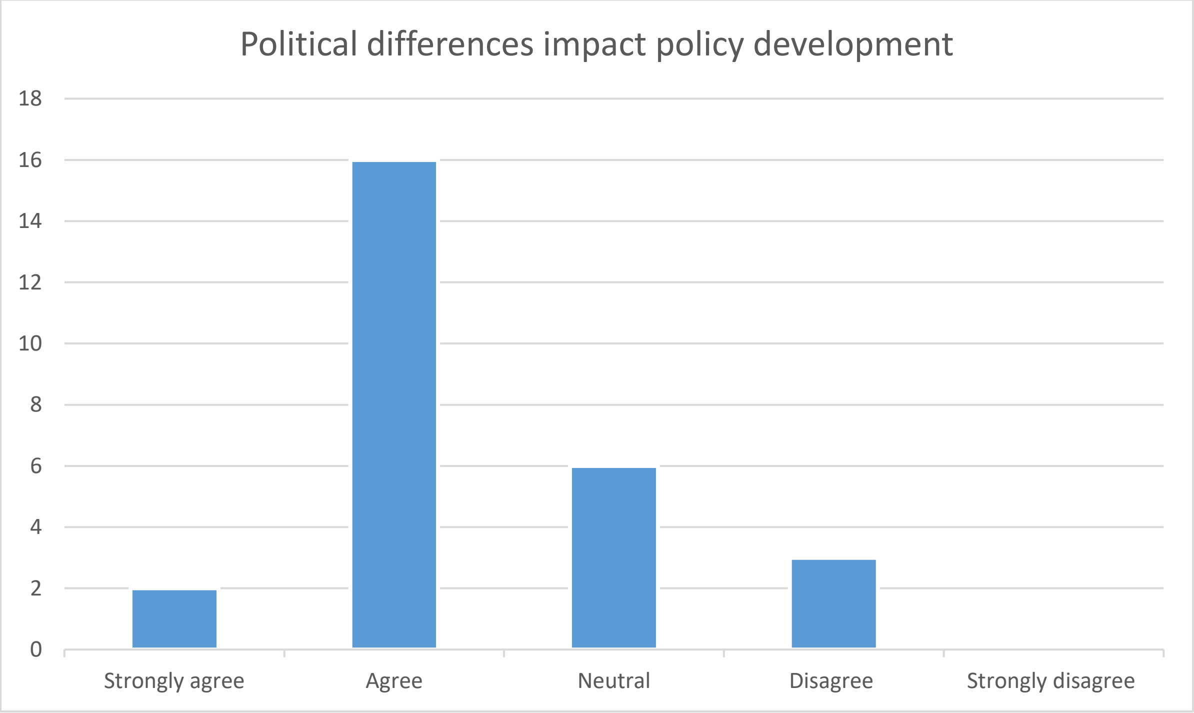


Figure D.236: Political differences impact policy development (1-5 years)

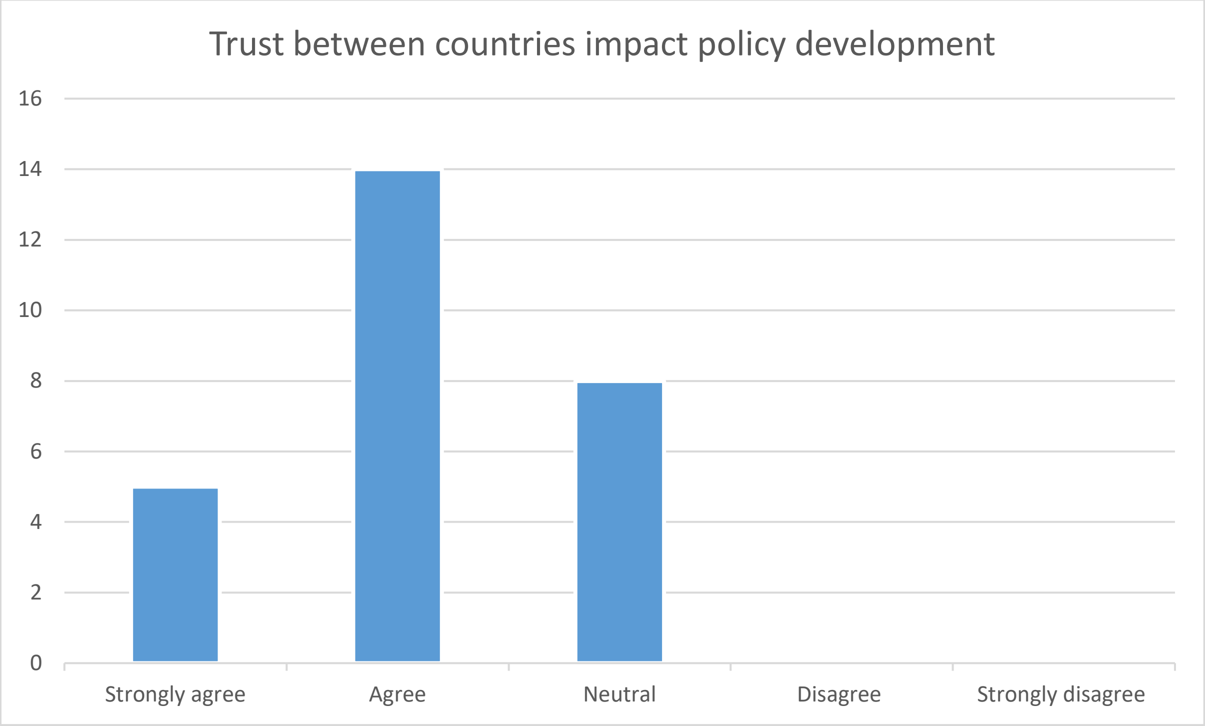


Figure D.237: Trust between countries impact policy development (1-5 years)

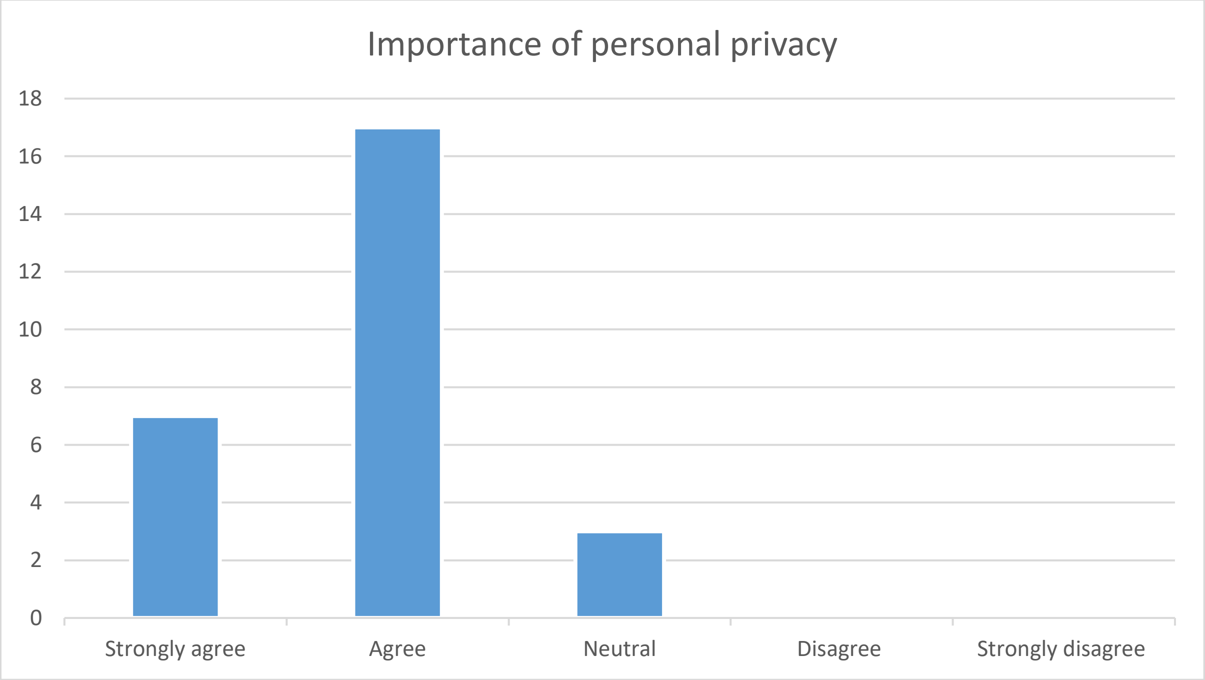


Figure D.238: Importance of personal privacy (1-5 years)

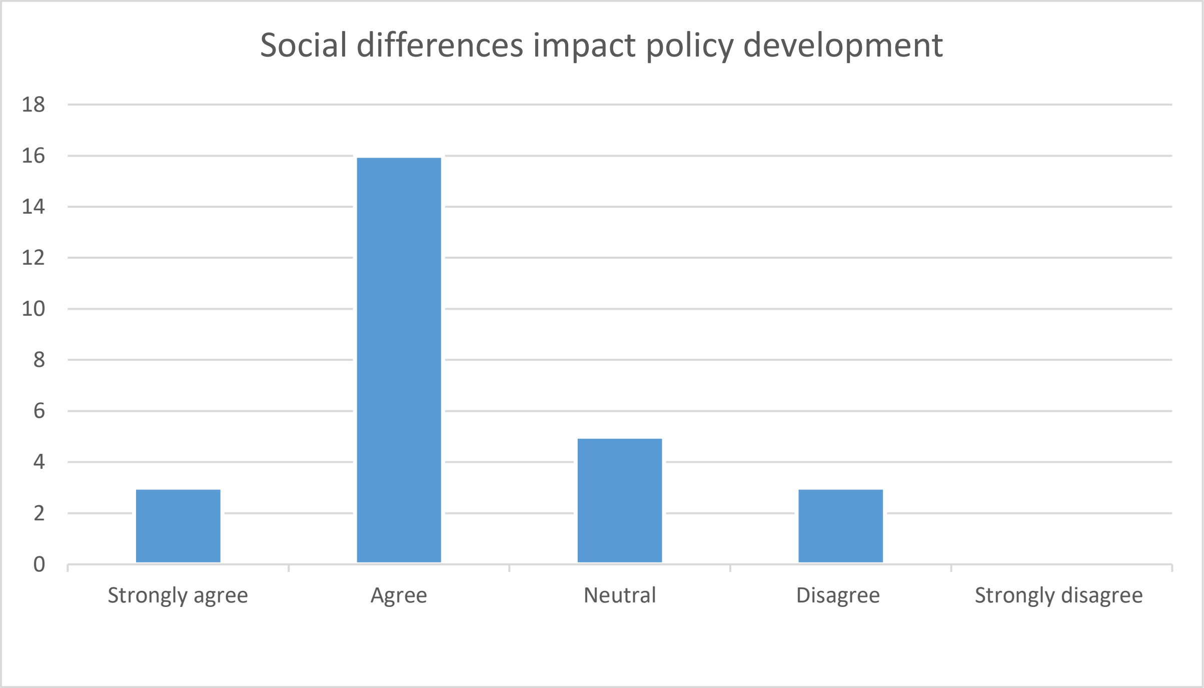


Figure D.239: Social differences impact policy development (1-5 years)

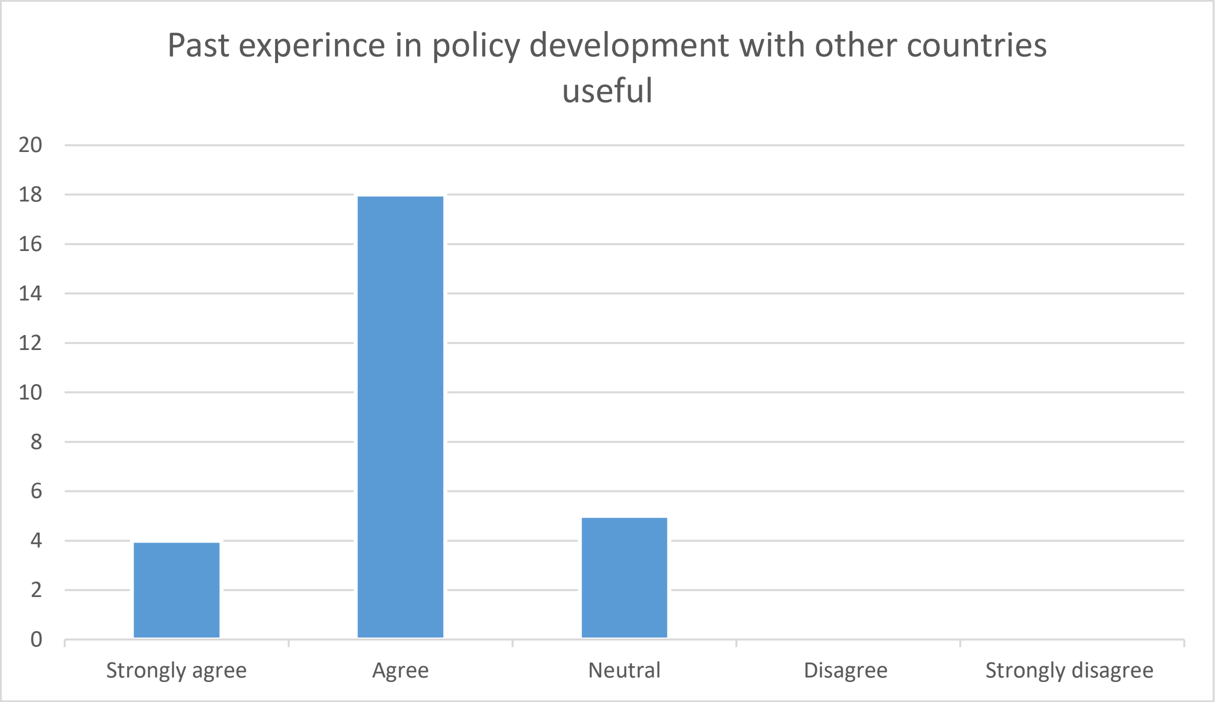


Figure D.240: Past experience in policy development with other countries useful (1-5 years)

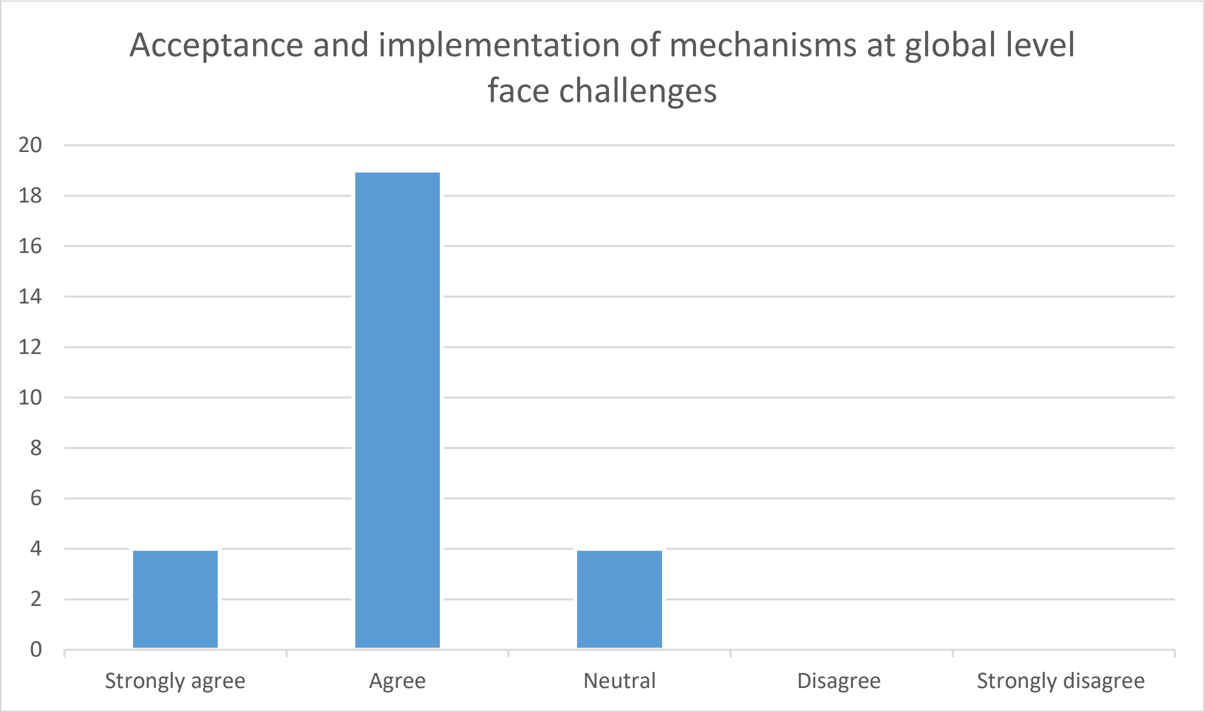


Figure D.241: Acceptance and implementation of mechanisms at global level face challenges (1-5 years)

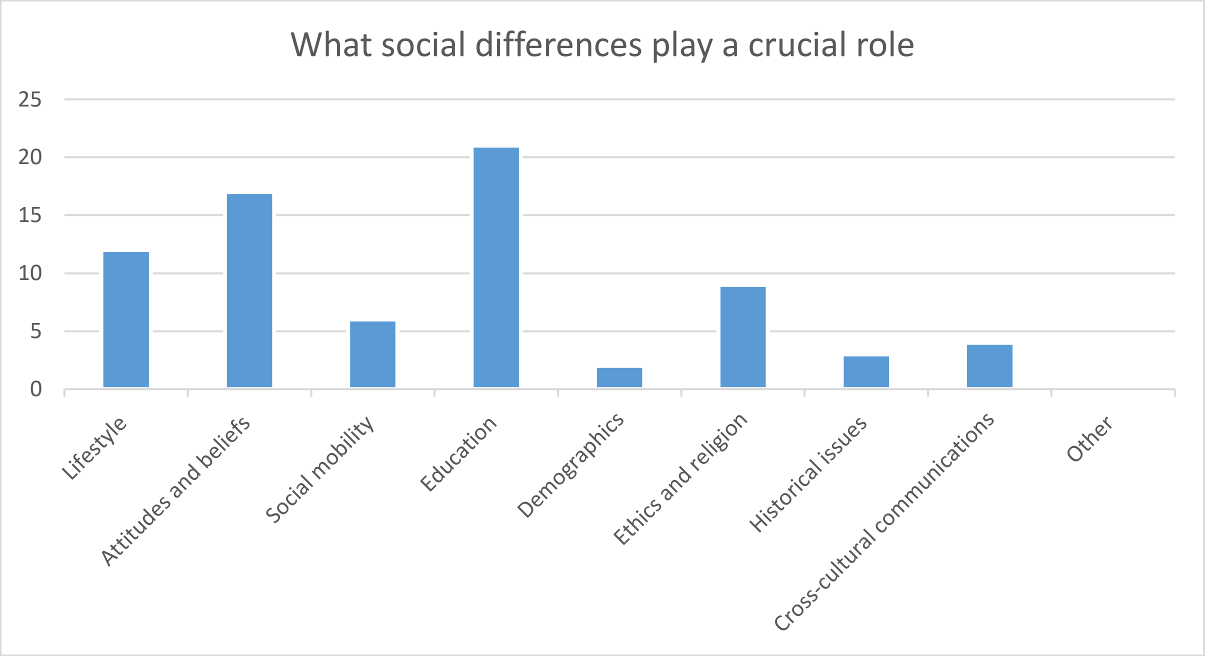


Figure D.242: What social differences play a crucial role (1-5 years)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure D.242). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at organisational level. Believing in privacy and respecting privacy of self and others are contributory factors that have been discussed under attitude and believes.

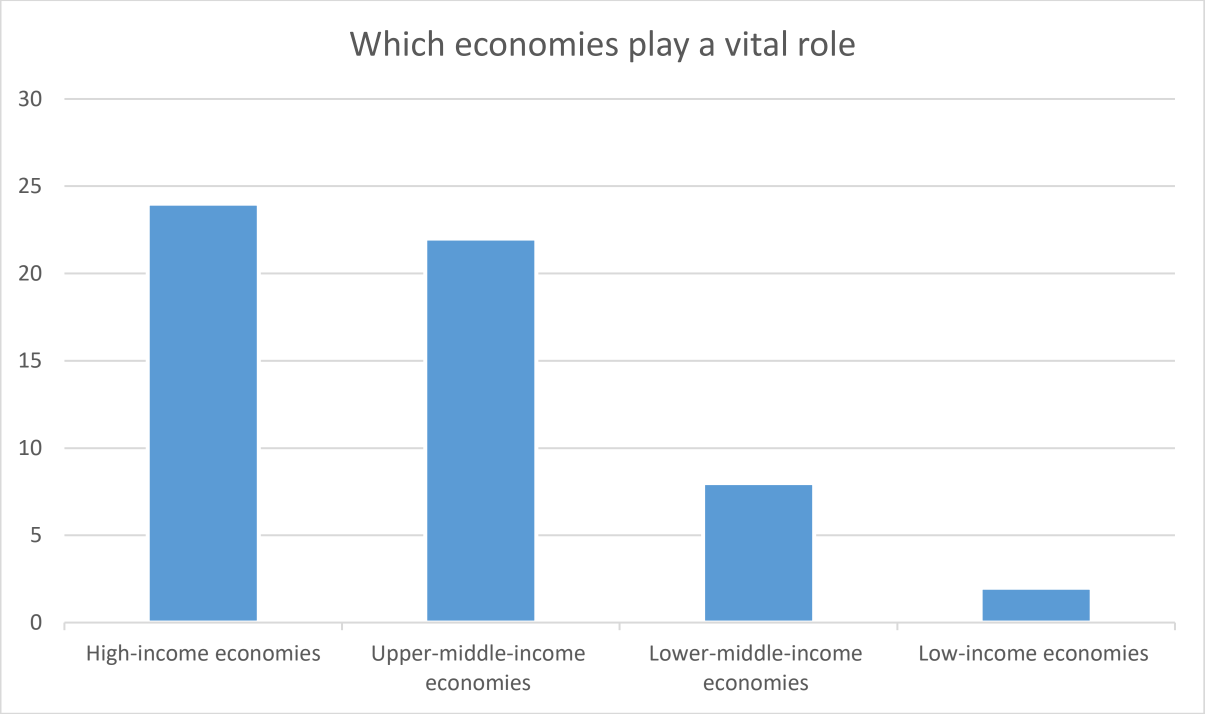


Figure D.243: Which economies play a vital role (1-5 years)

In the questionnaire, majority has stated that the high income and upper-middle-income countries play a vital role (See figure D.243). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

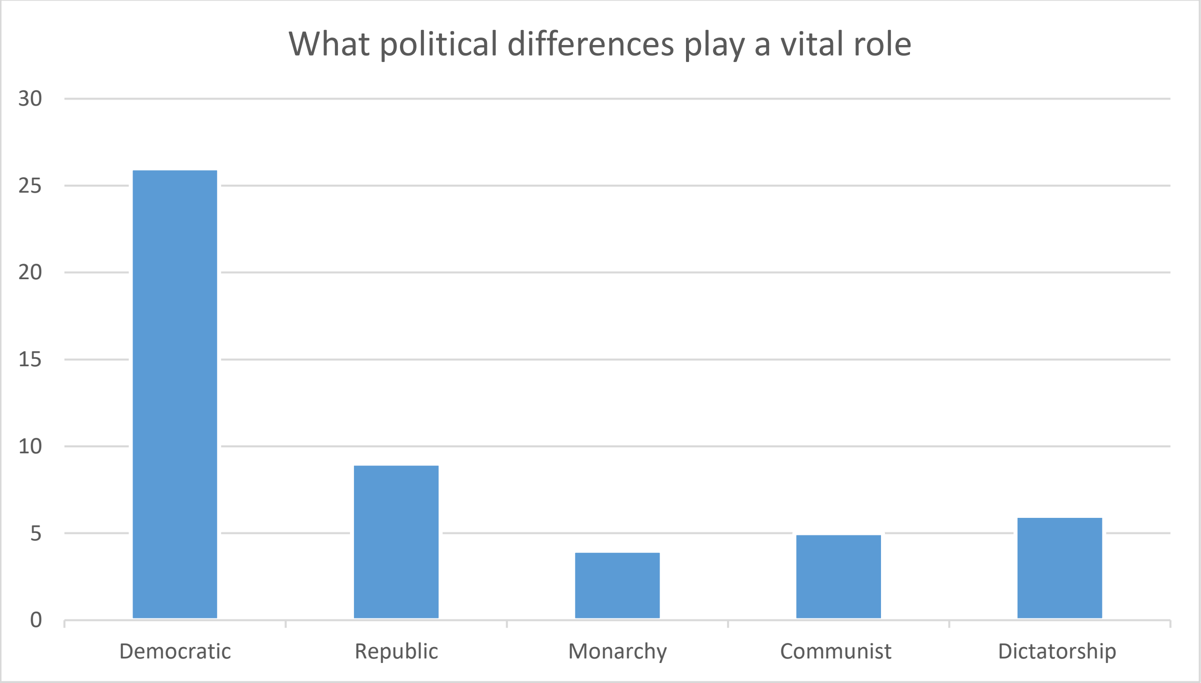


Figure D.244: What political differences play a vital role (1-5 years)

The majority have chosen democratic political system (See figure D.244), in preference to others because it allows a public voice to influence in the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

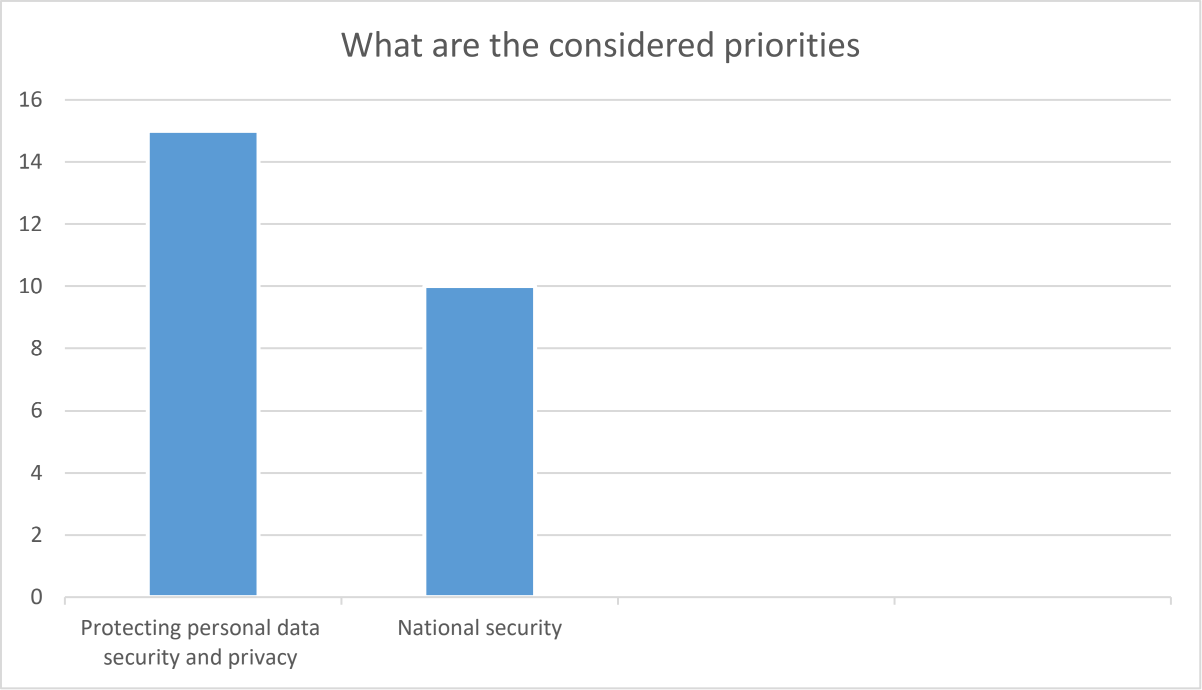


Figure D.245: What are the considered priorities (1-5 years)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security, which is a significant factor (See figure D.245). In an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

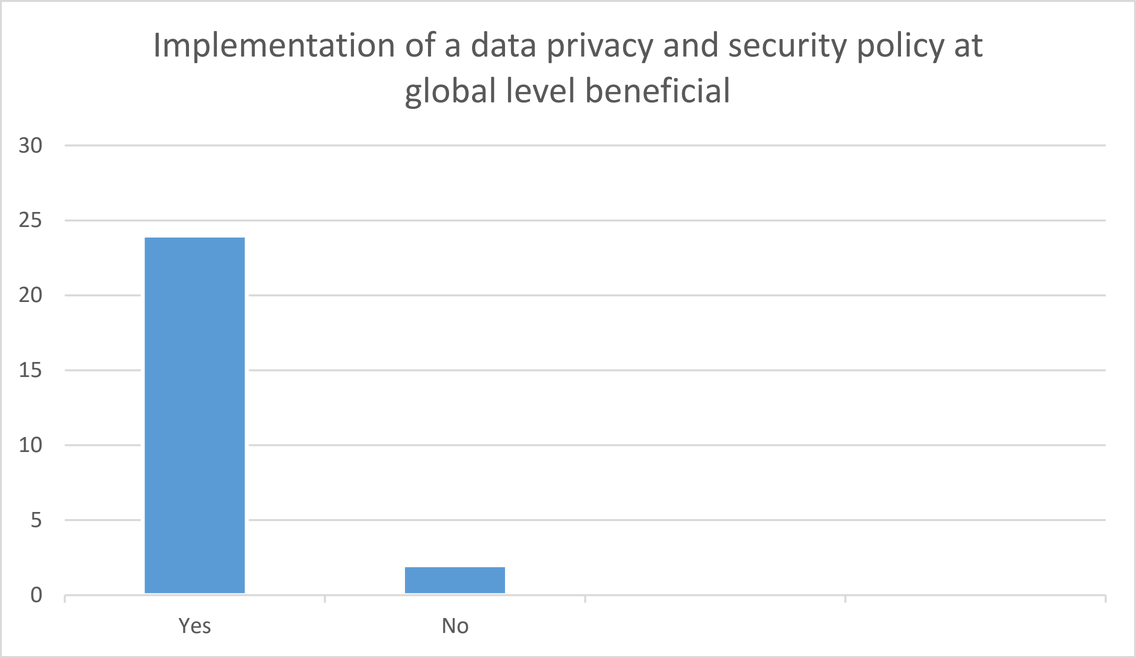


Figure D.246: Implementation of a data privacy and security policy at global level beneficial (1-5 years)

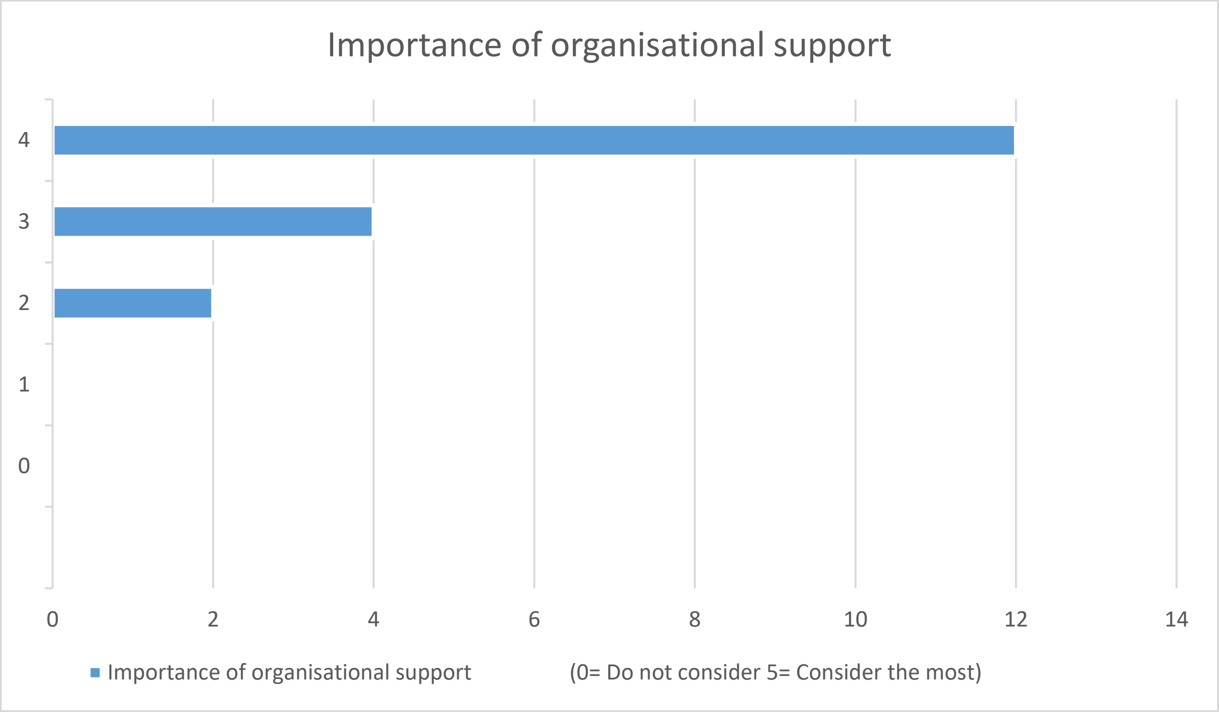


Figure D.247: Importance of organisational support (1-5 years)

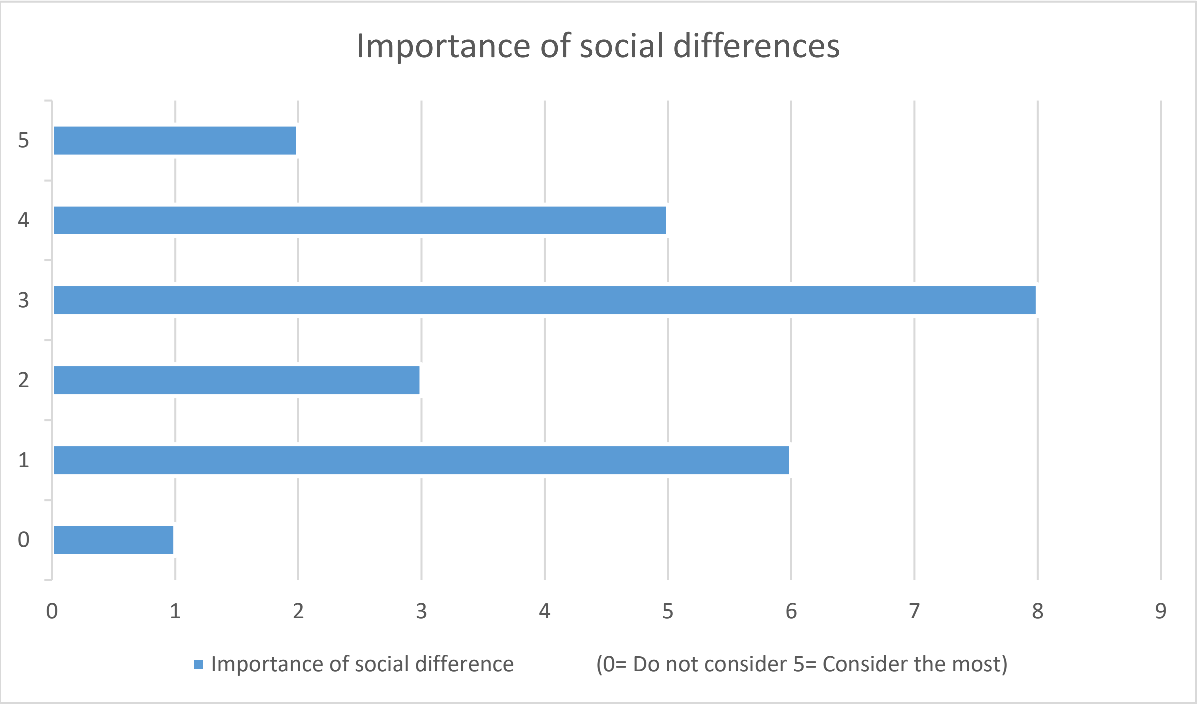


Figure D.248: Importance of social differences (1-5 years)

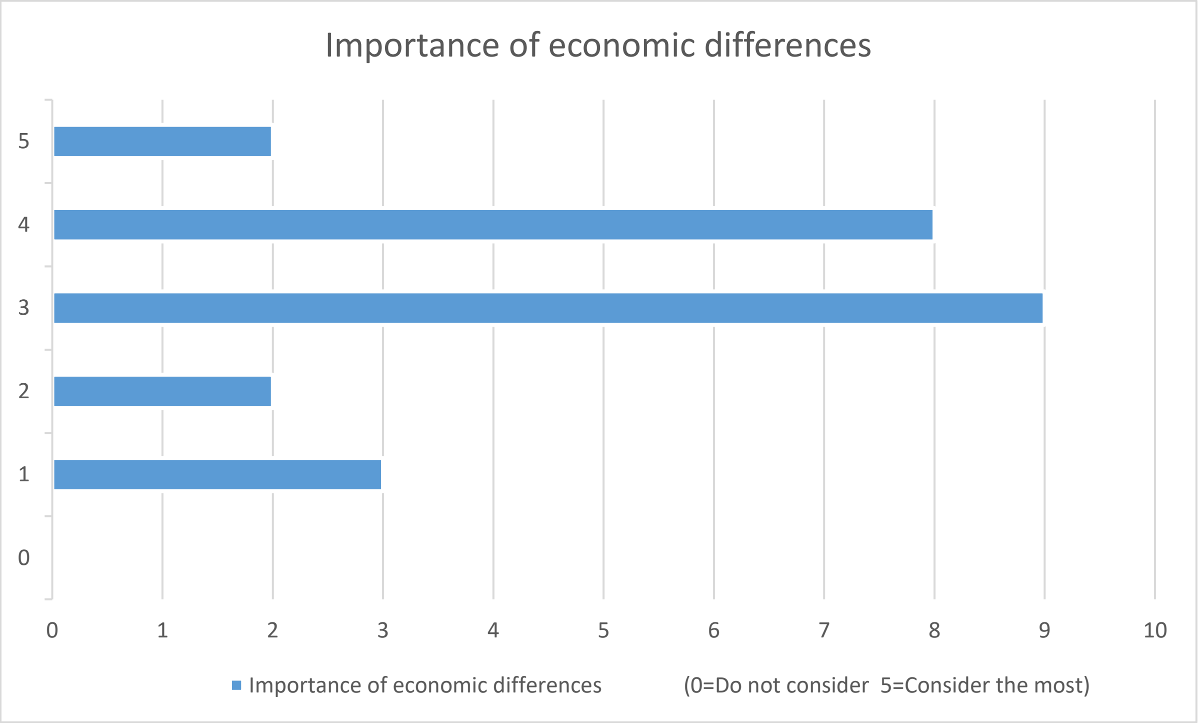


Figure D.249: Importance of economic differences (1-5 years)

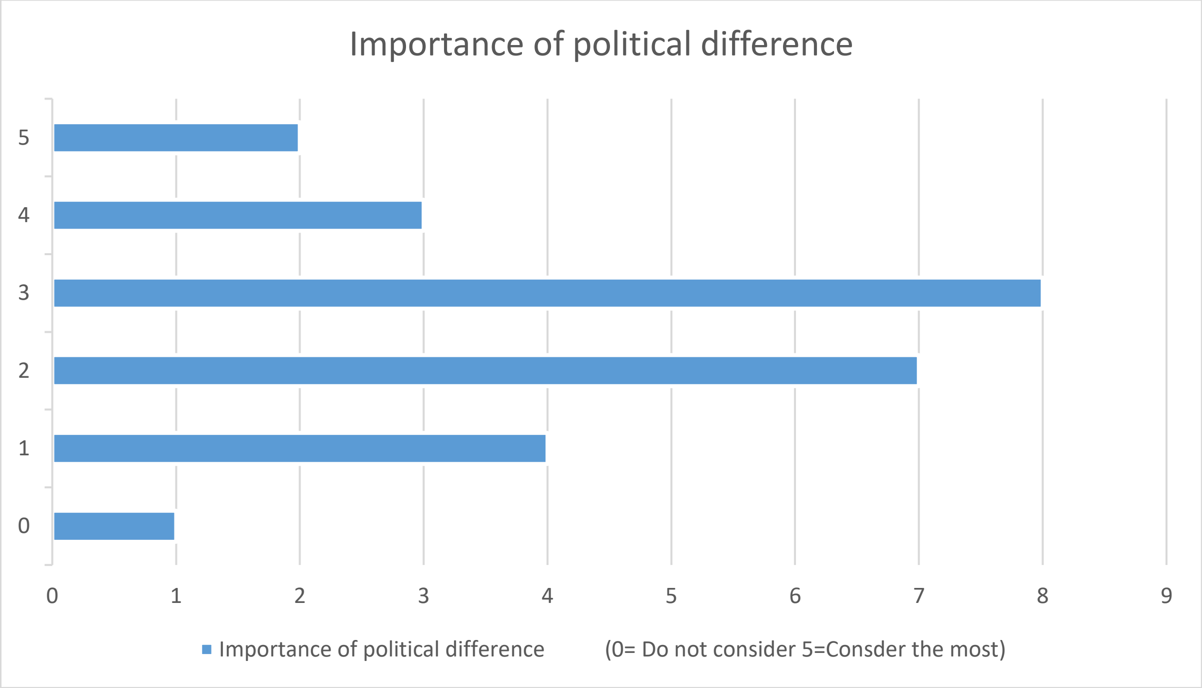


Figure D.250: Importance of political difference (1-5 years)

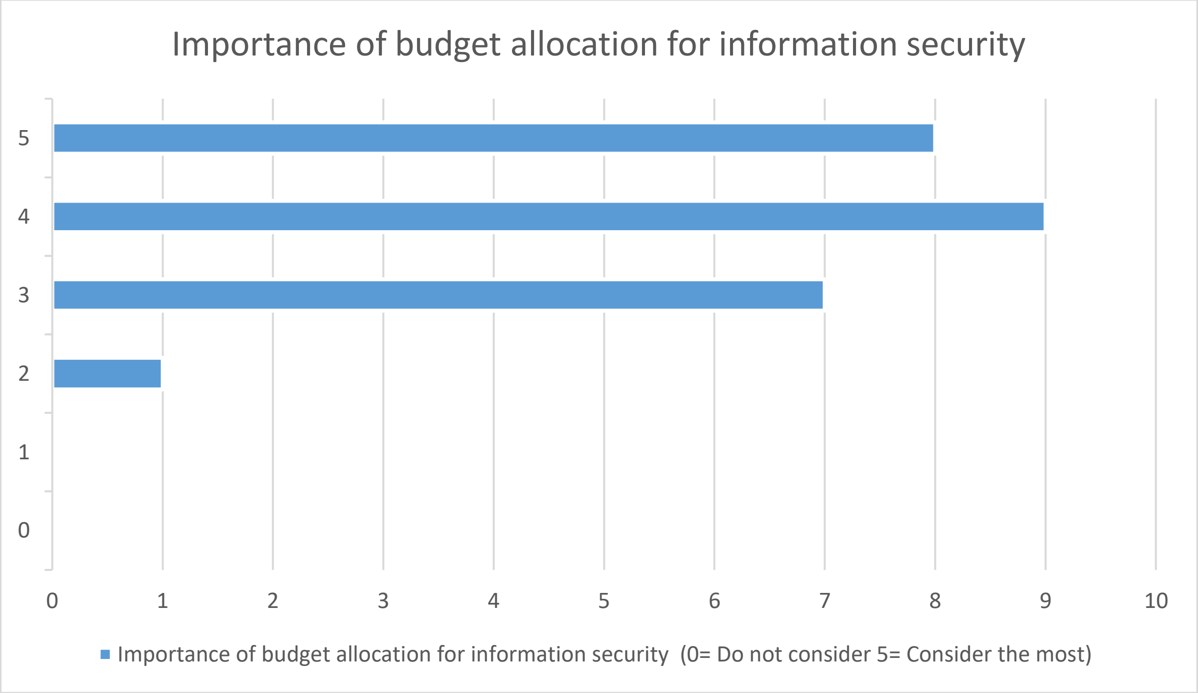


Figure D.251: Importance of budget allocation for information security (1-5 years)

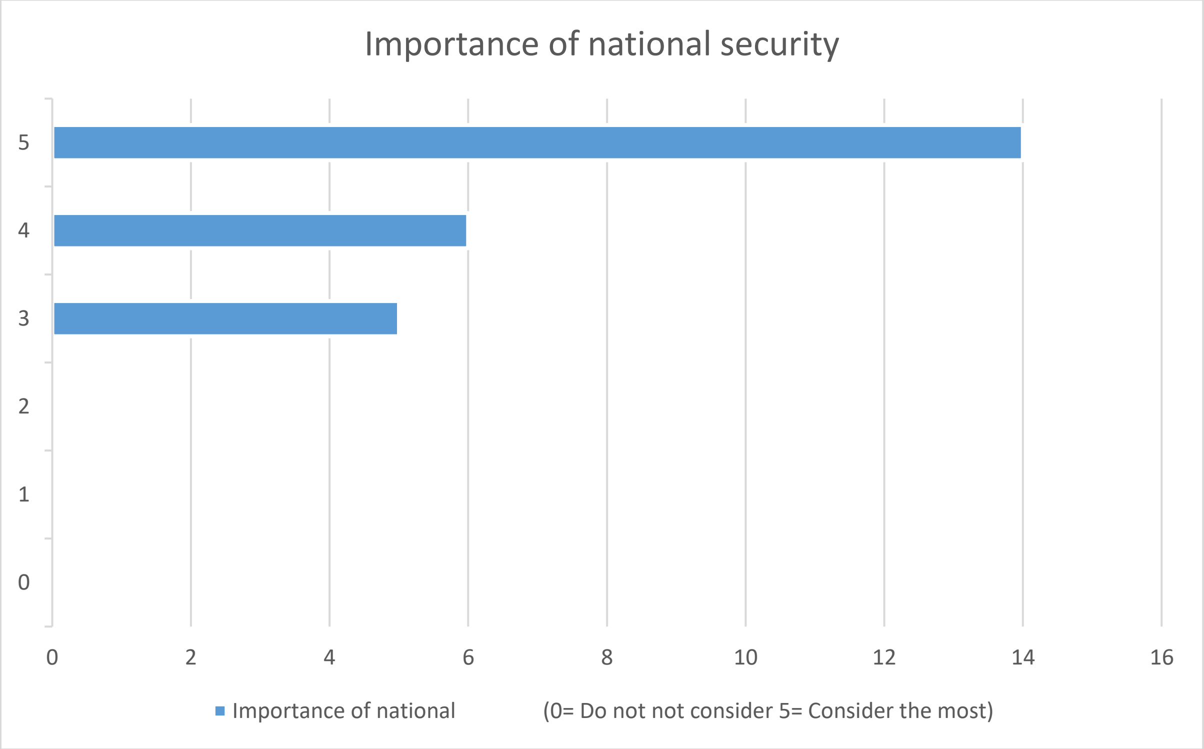


Figure D.252: Importance of national security (1-5 years)

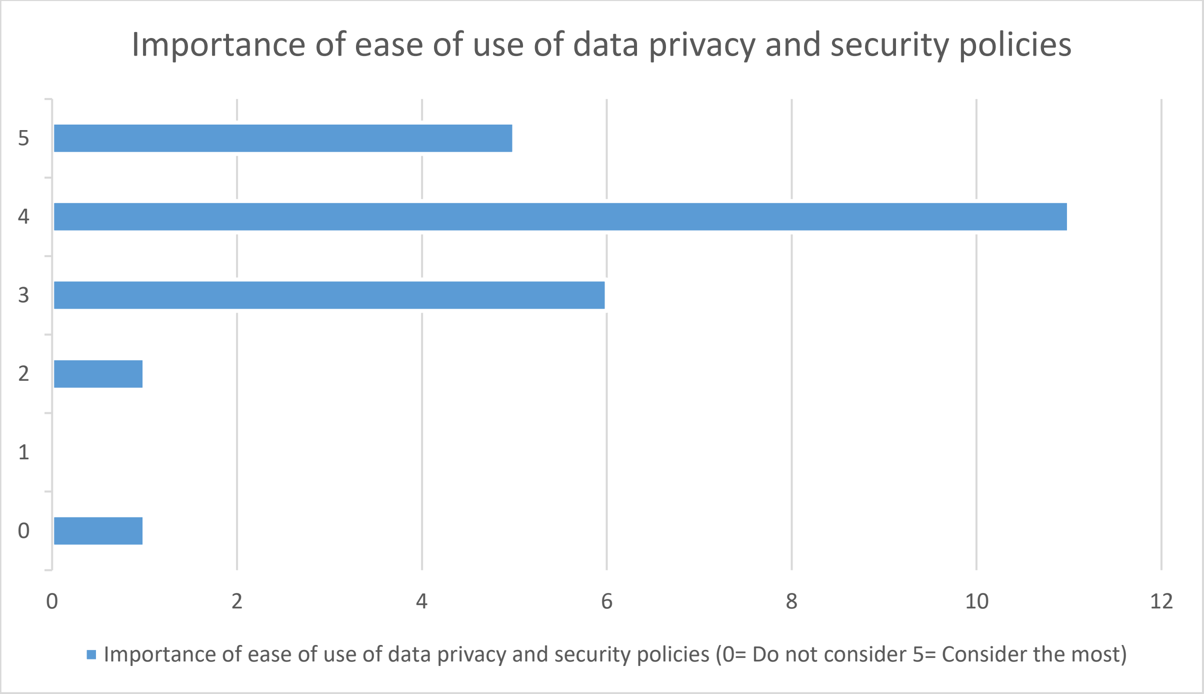


Figure D.253: Importance of ease of use of data privacy and security policies (1-5 years)

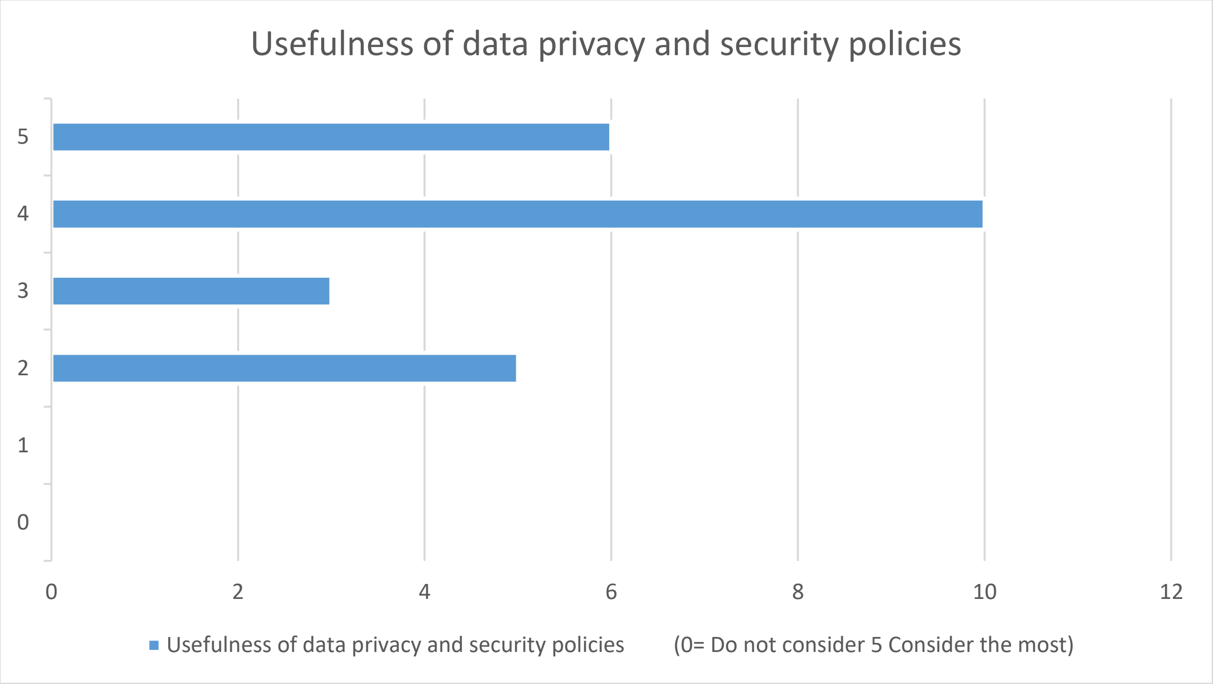


Figure D.254: Usefulness of data privacy and security policies (1-5 years)

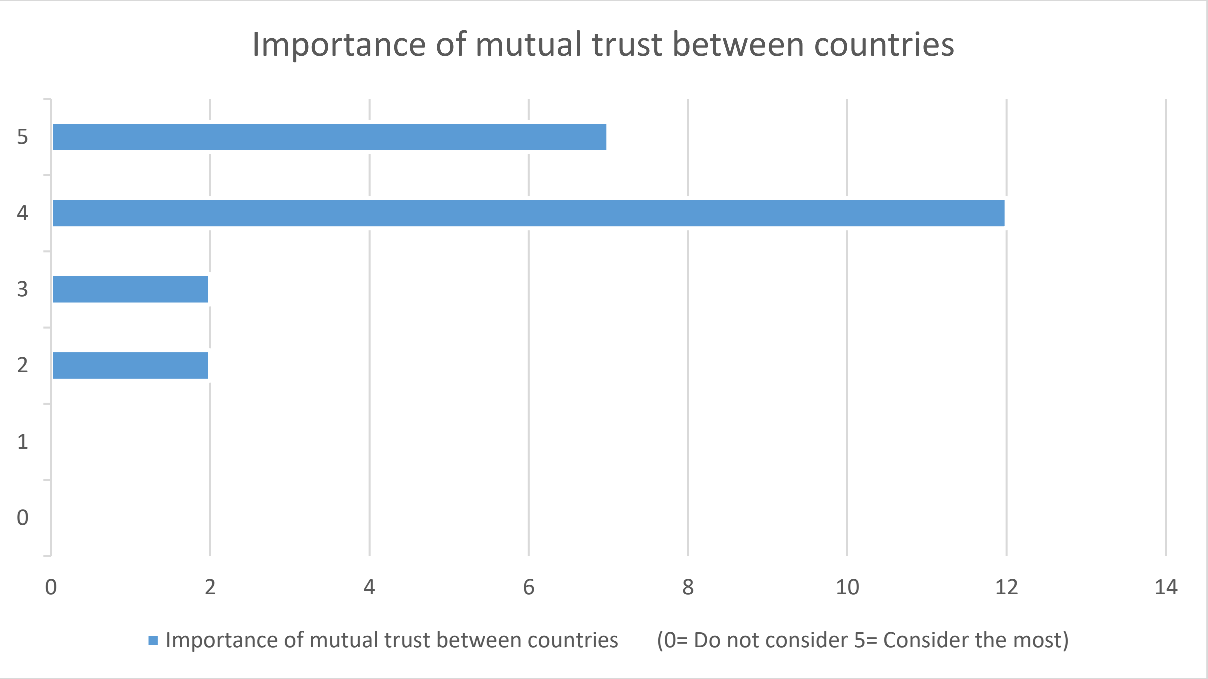


Figure D.255: Importance of mutual trust between countries (1-5 years)

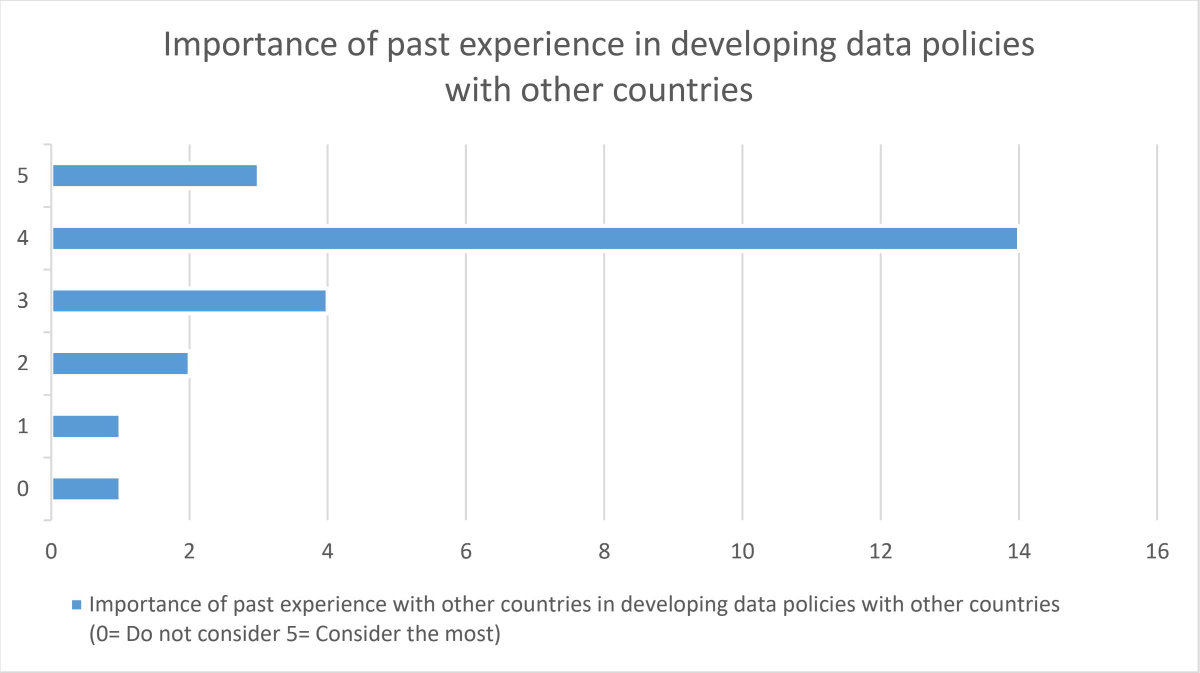


Figure D.256: Importance of past experience in developing data policies with other counties (1-5 years)

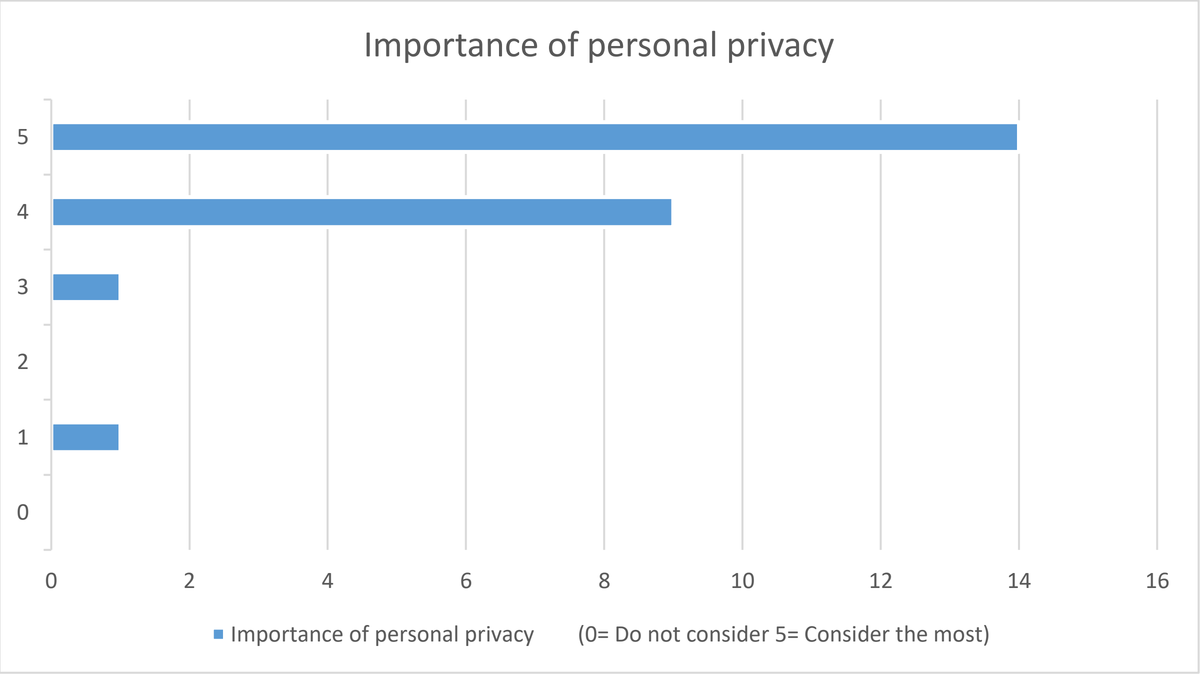


Figure D.257: Importance of personal privacy (1-5 years)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 75 percent of the respondents have endorsed (See figure D.246). The other notable factors that have come out of the survey are organisational support, budget allocation, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure D.235-245) (See figure D.247-257),

Sri Lanka – 6-10 years

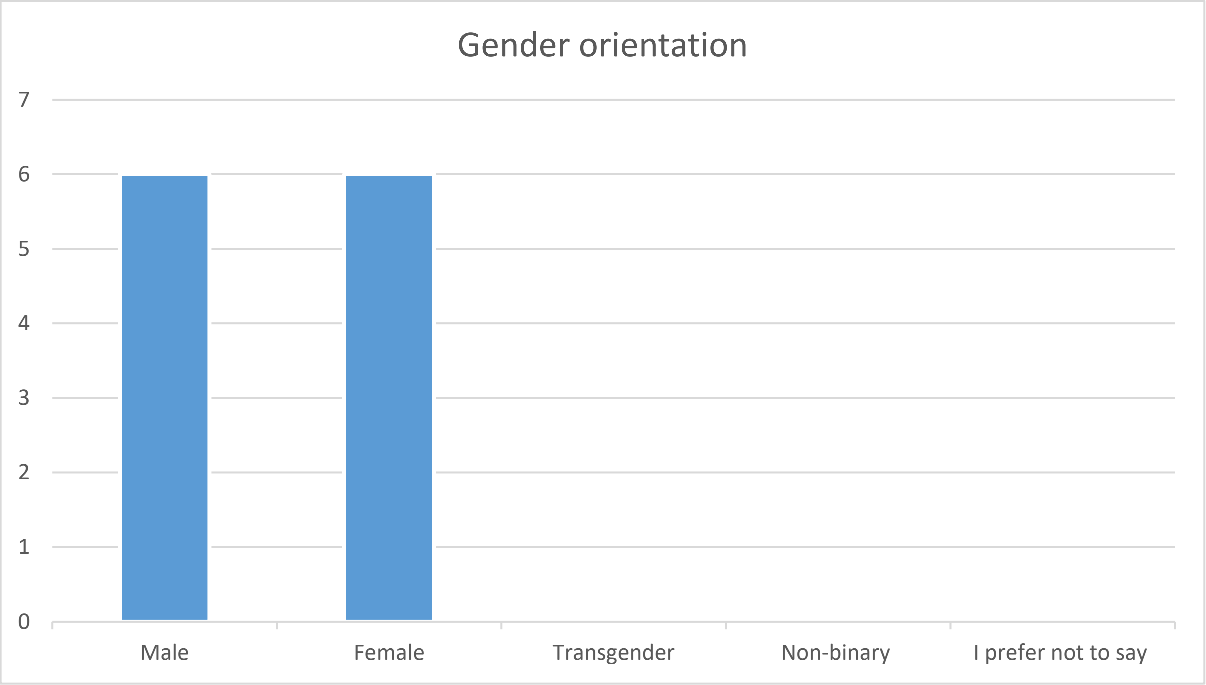


Figure D.258: Gender orientation (6-10)

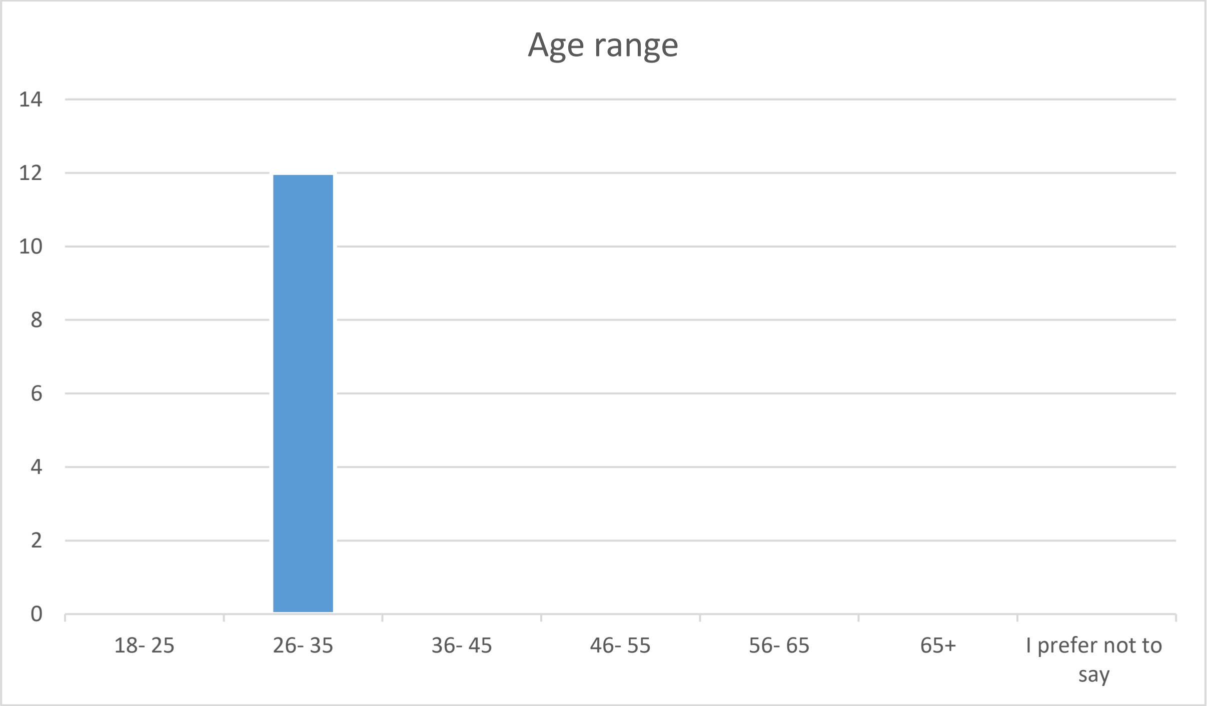


Figure D.259: Age range (6-10)

This analysis is based on the responses collected from Sri Lankan participants with 6 to 10 years of employment in the industry. There were 12 participants and 6 out of them were males and 6 females (See figure D.258). They were within 26-35 (See figure D.259).

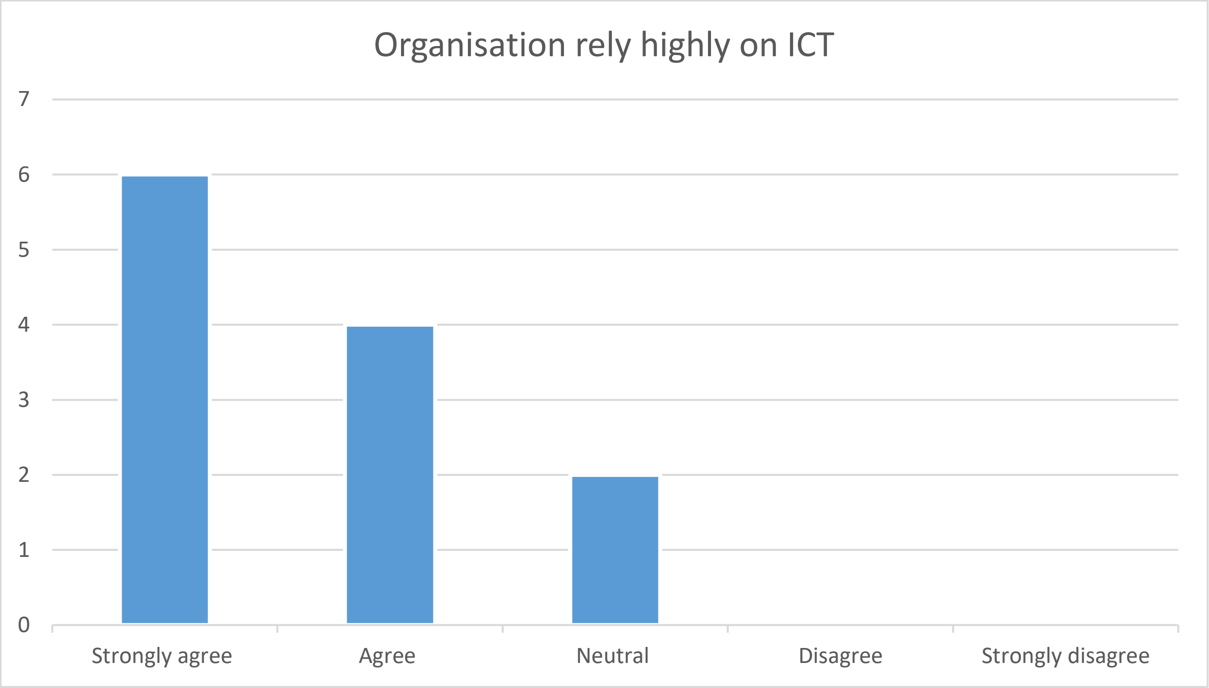


Figure D.260: Organisation rely highly on ICT (6-10)

Out of the 12 respondents, 10 have worked in a technology reliance working environment, 2 unaware of reliance on technology because of the nature of the work assigned to them (See figure D.260). This indicates a majority of those who have been working in an organisation for 6-10 years have had high reliance on ICT.

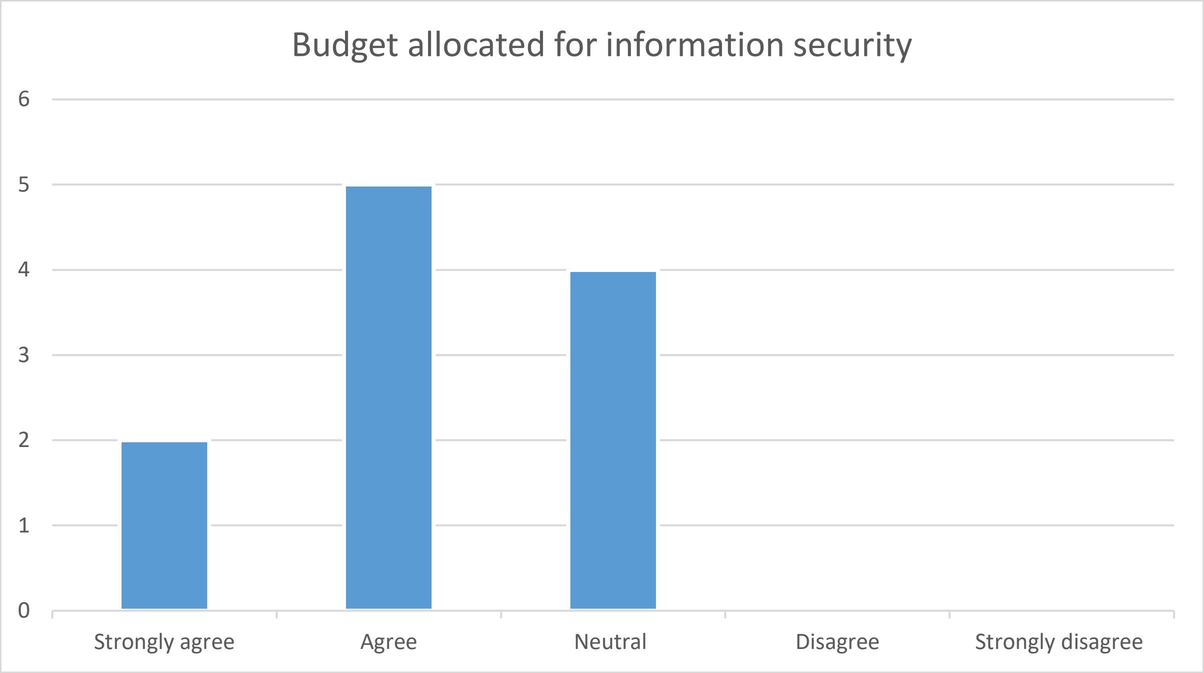


Figure D.261: Budget allocated for information security (6-10)

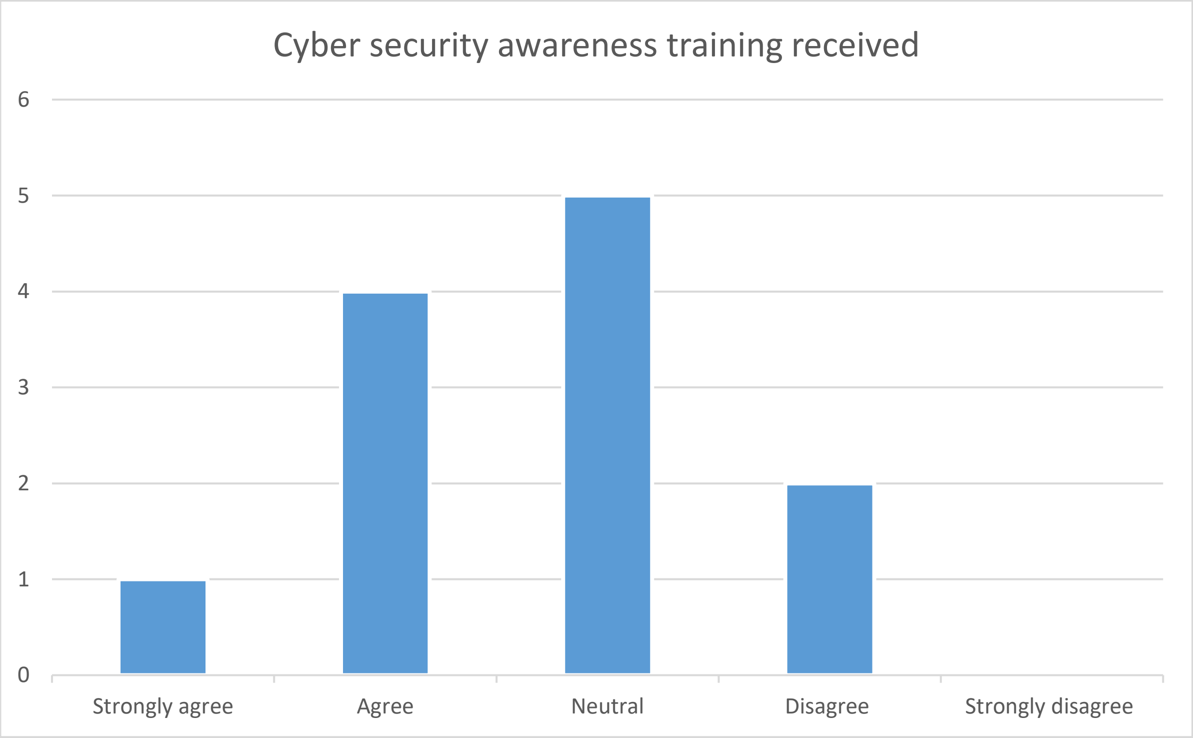


Figure D.262: Cyber security awareness training received (6-10)

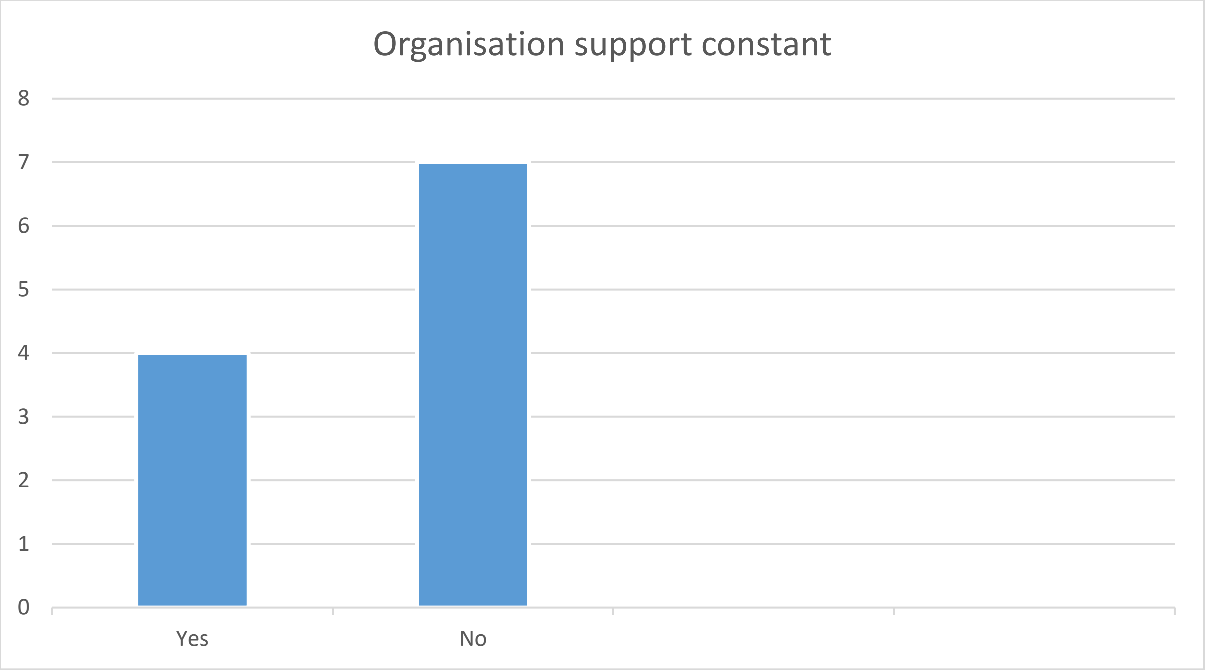


Figure D.263: Organisation support constant (6-10)

Funding has been sketchy. 7 out of the 12 have indicated that their organisations had an allocated budget for information security, whilst 4 had not expressed an opinion either way (See figure D.261). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 5 participants have received regular cybersecurity awareness training, whilst a similar number of participants neither agreed nor disagreed, except for 2 participants who had not regularly received security awareness training (See figure D.262). In addition, 7 participants had not received support from the organisation to protect personal information, whilst only 4 did (See figure D.263). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

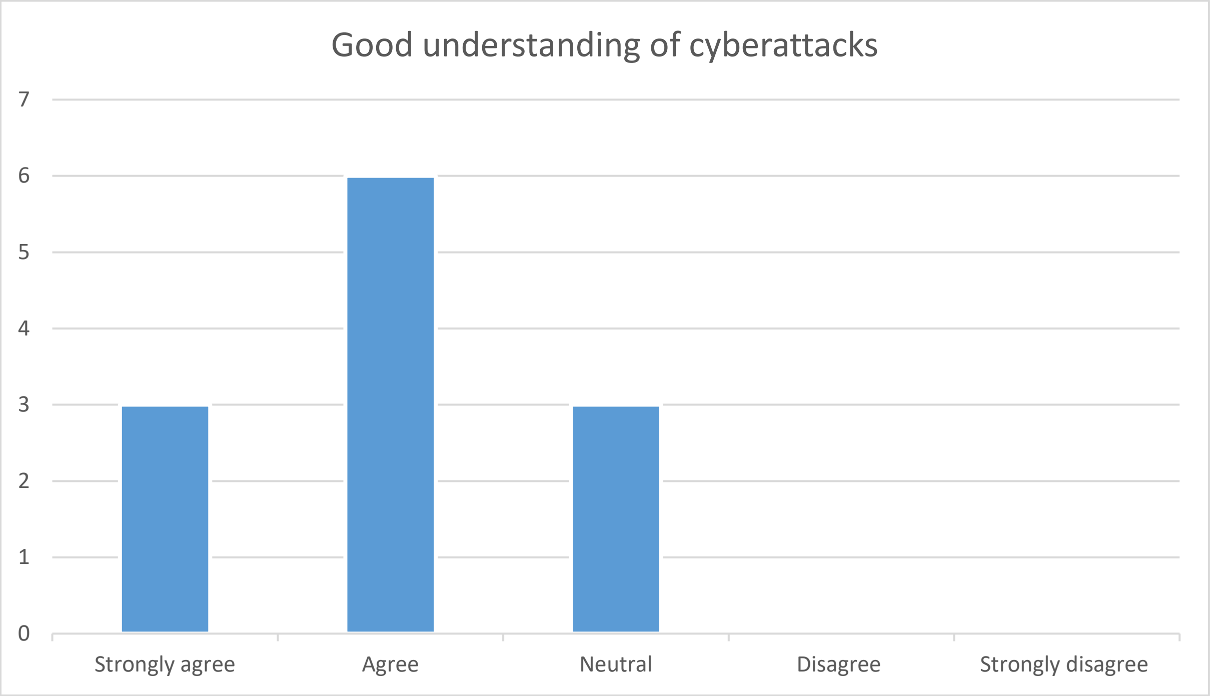


Figure D.264: Good understanding of cyberattacks (6-10)

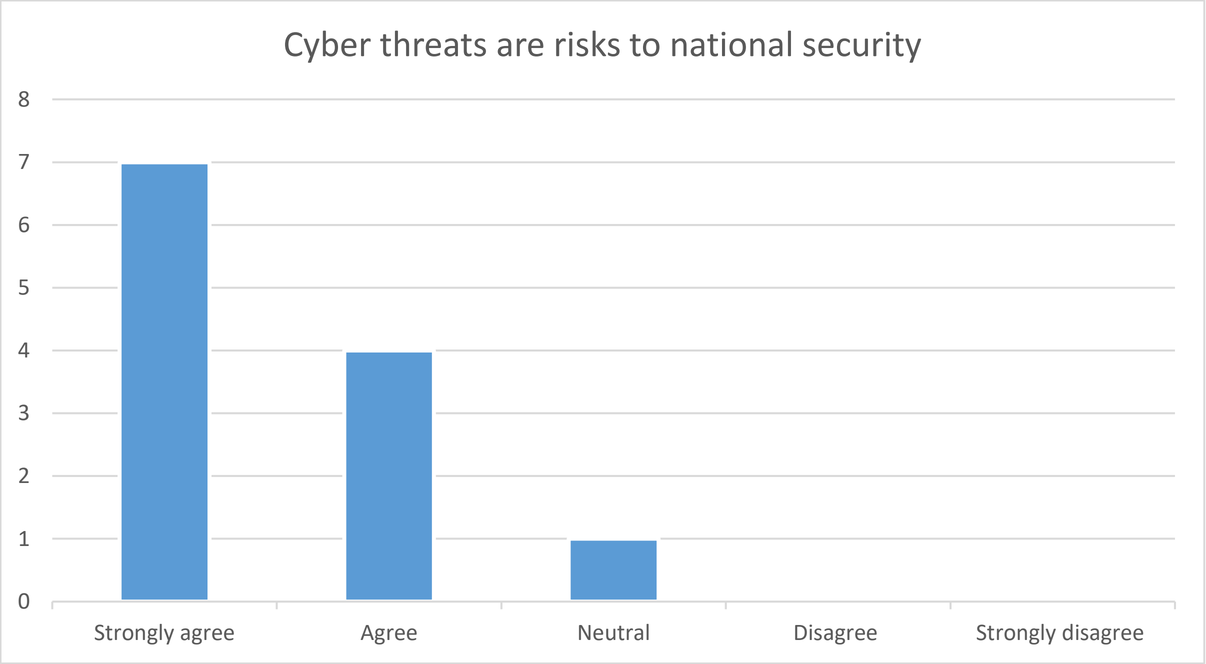


Figure D.265: Cyber threats are risks to national security (6-10)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 9 participants do have, 3 have not expressed opinion either way (See figure D.264). Furthermore, 91 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure D.265). In general, understanding of cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

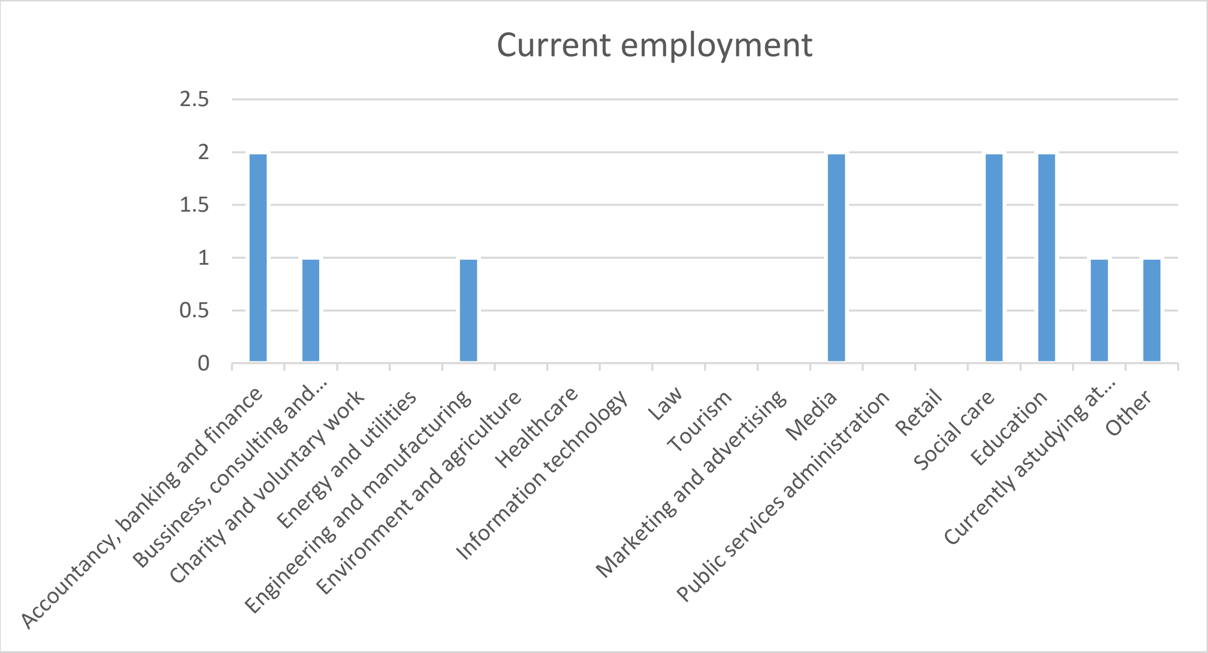


Figure D.266: Current employment (6-10)

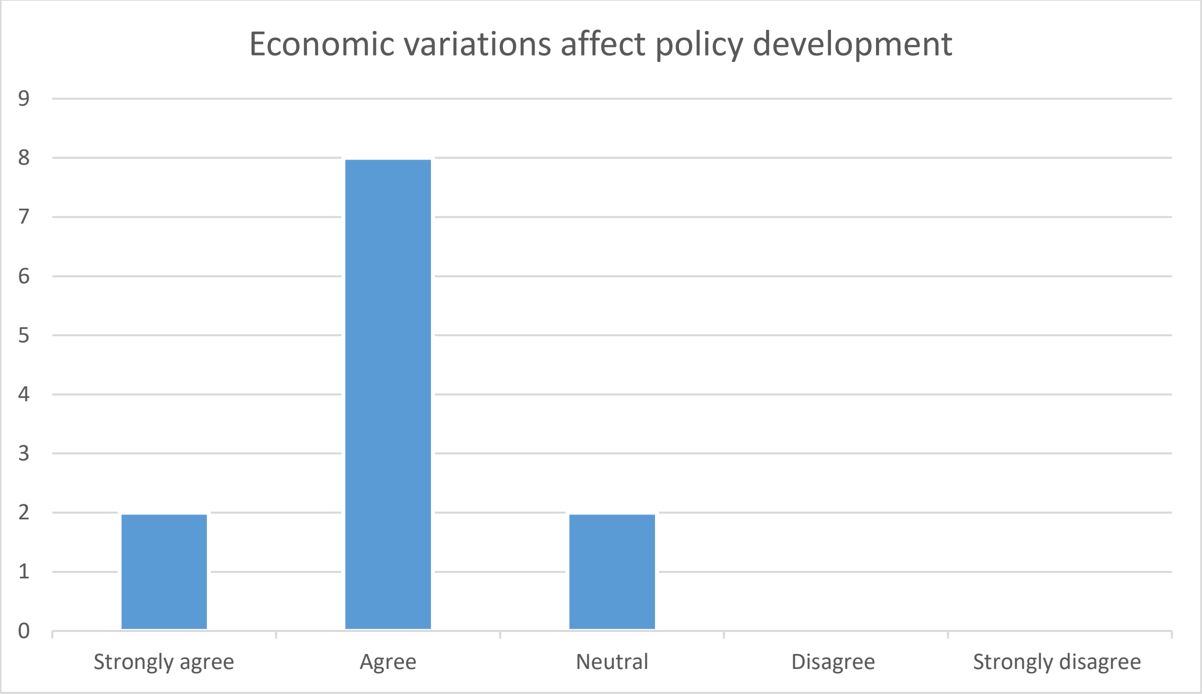


Figure D.267: Economic variations affect policy development (6-10)

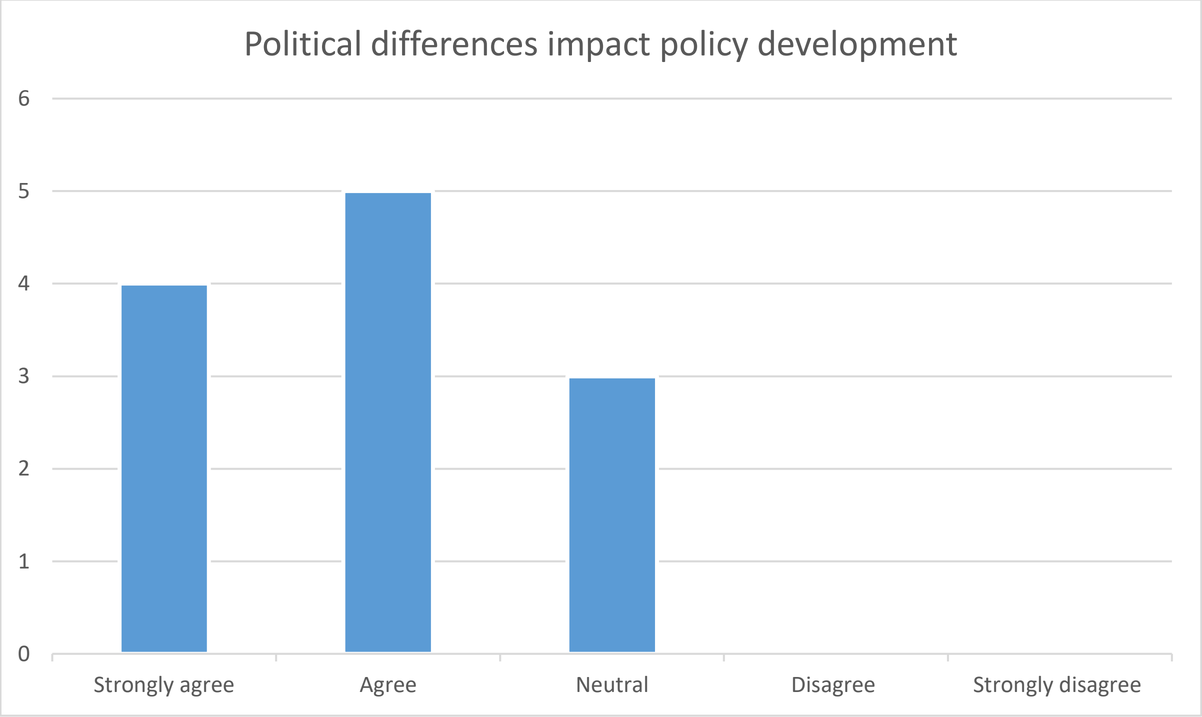


Figure D.268: Political differences impact policy development (6-10)

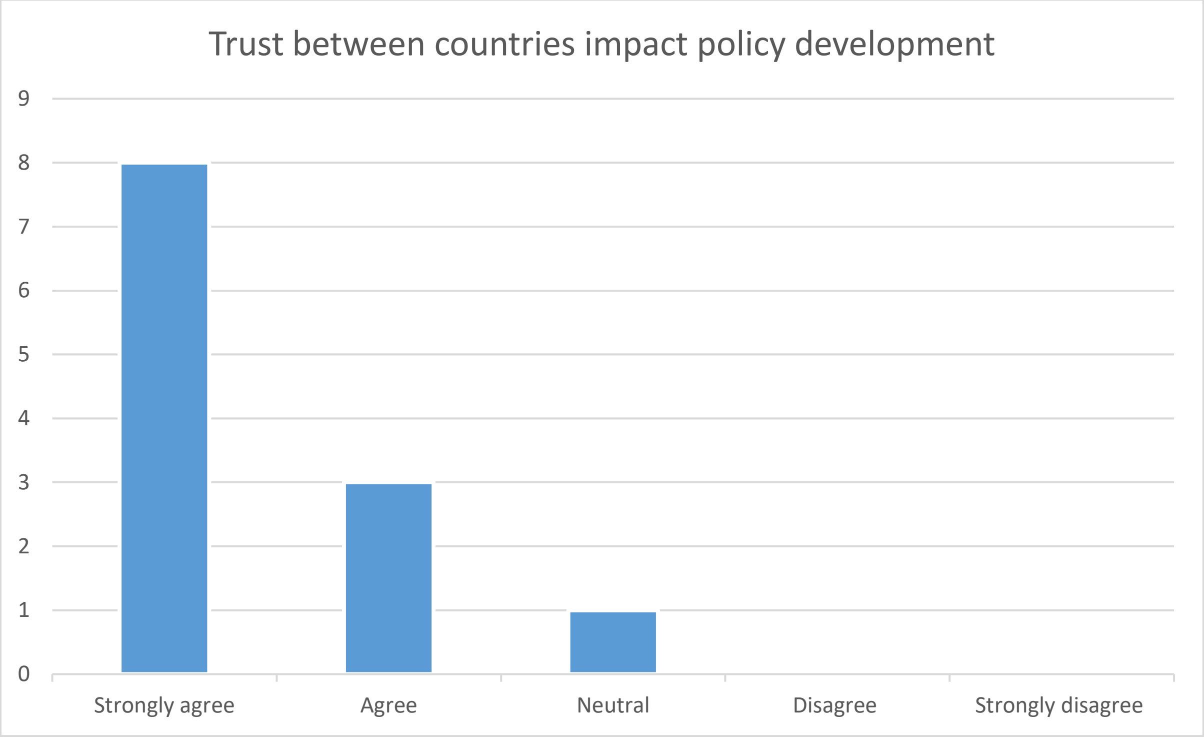


Figure D.269: Trust between countries impact policy development (6-10)

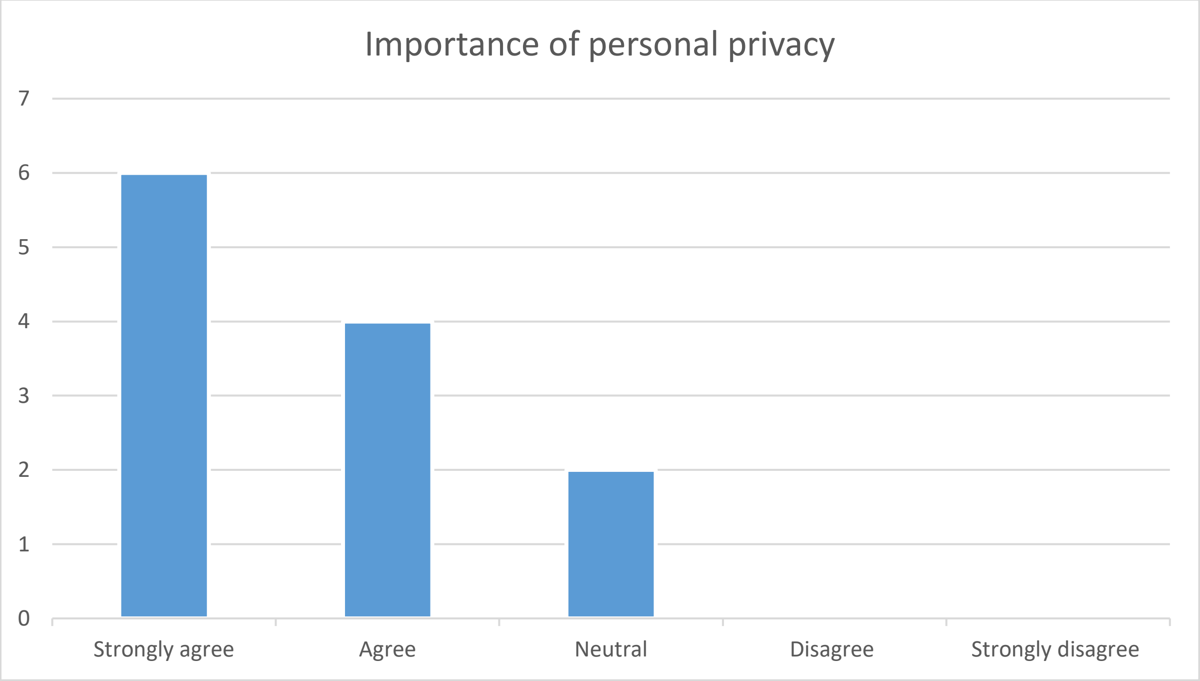


Figure D.270: Importance of personal privacy (6-10)

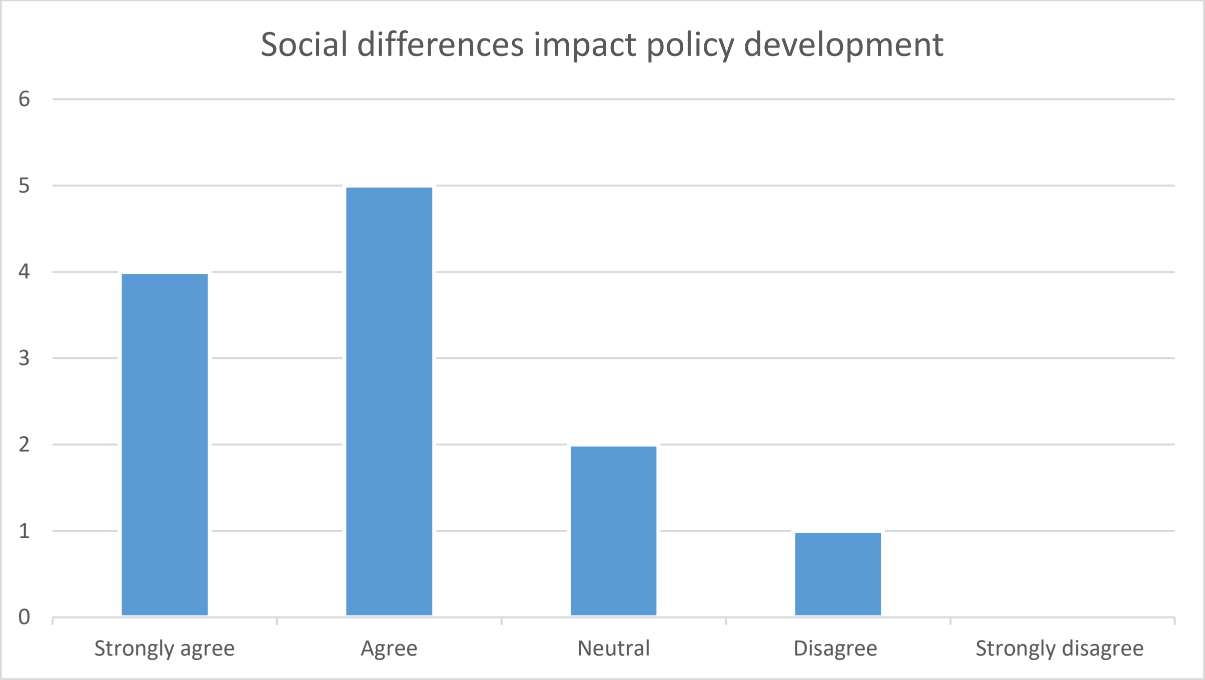


Figure D.271: Social differences impact policy development (6-10)

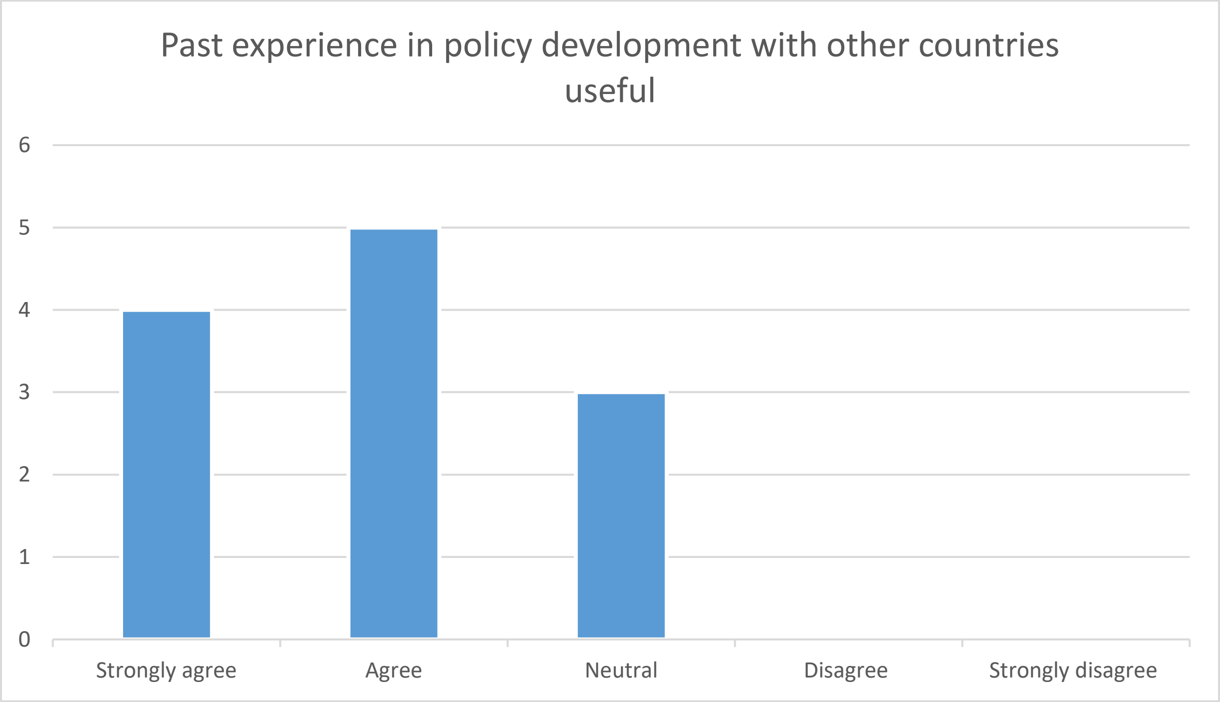


Figure D.272: Past experience in policy development with other countries useful (6-10)

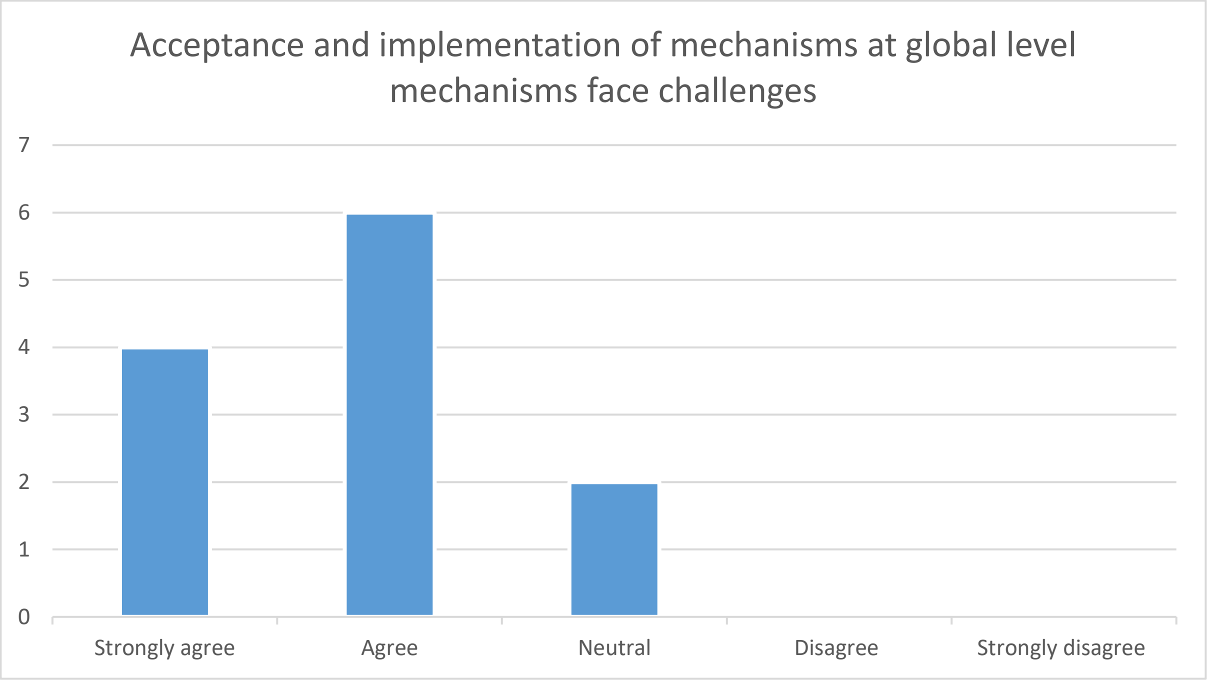


Figure D.273: Acceptance and implementation of mechanisms at global level face challenges (6-10)

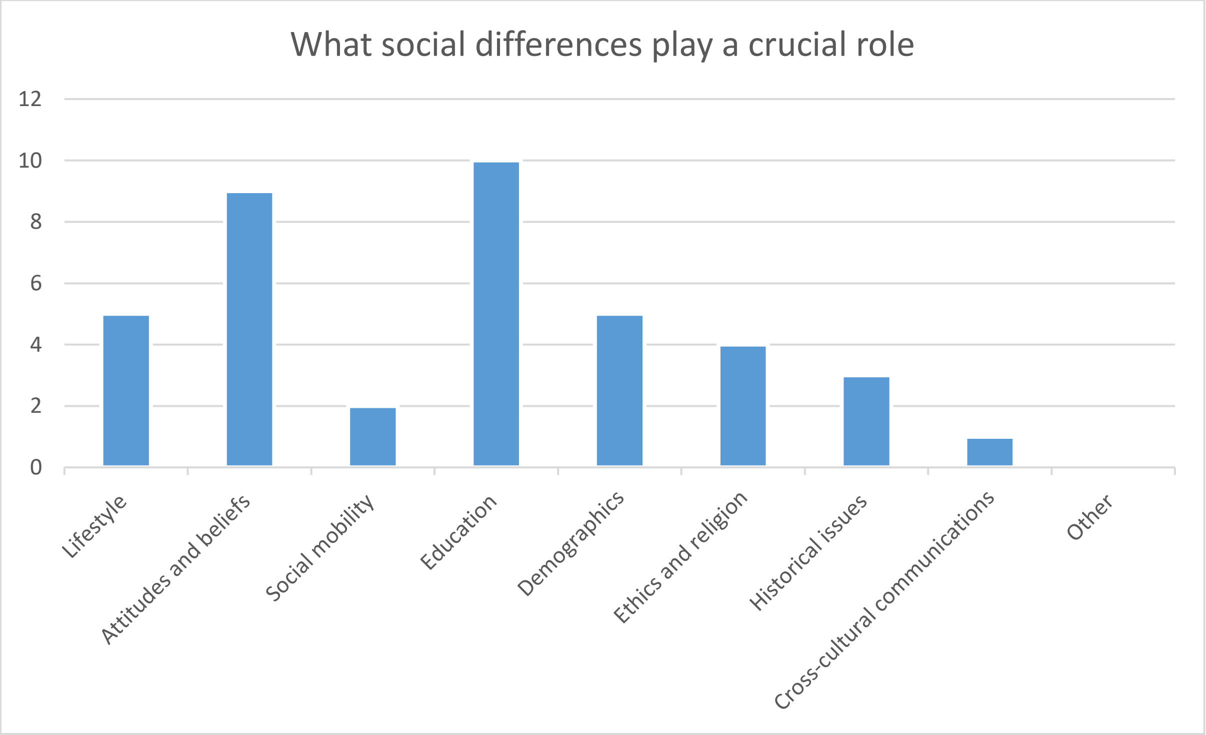


Figure D.274: What social differences play a crucial role (6-10)

Out of the listed social differences in the questionnaire, majority has highlighted the importance of education and the importance of attitude and beliefs (See figure D.274. In accepting and implementing data privacy and security policies, education about potential cyber threats, their impact on human and national security is crucial. To that end, it is important to conduct cybersecurity awareness training at schools and at organisational level. Believing in privacy and respecting privacy of yours and others is also a contributing factor that discusses under attitude and believes. Again the educational training can play a vital role for people to get an understanding of the importance of privacy and implications associated with privacy violations. The participants have put less weight on the factors like lifestyle, social mobility, demography, ethnicity and religion, historical issues and cross-cultural communication.

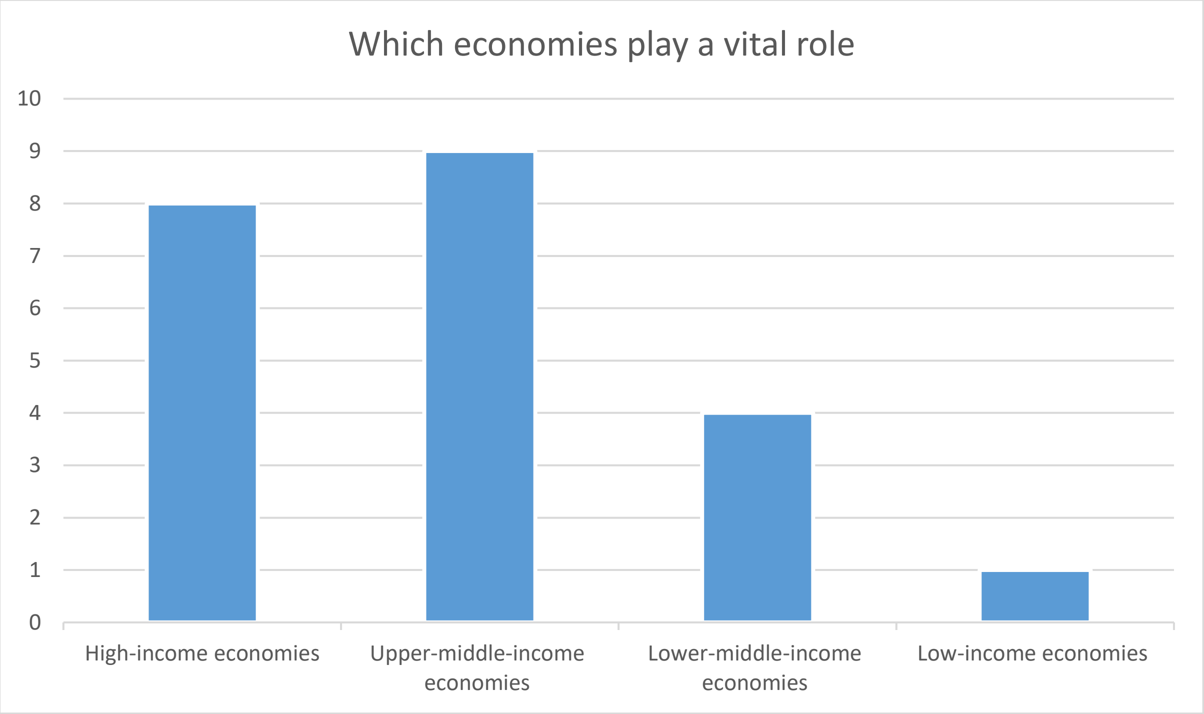


Figure D.275: Which economies play a vital role (6-10)

In the questionnaire, majority has stated that the high income and upper-middle-income countries play a vital role (See figure D.275). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

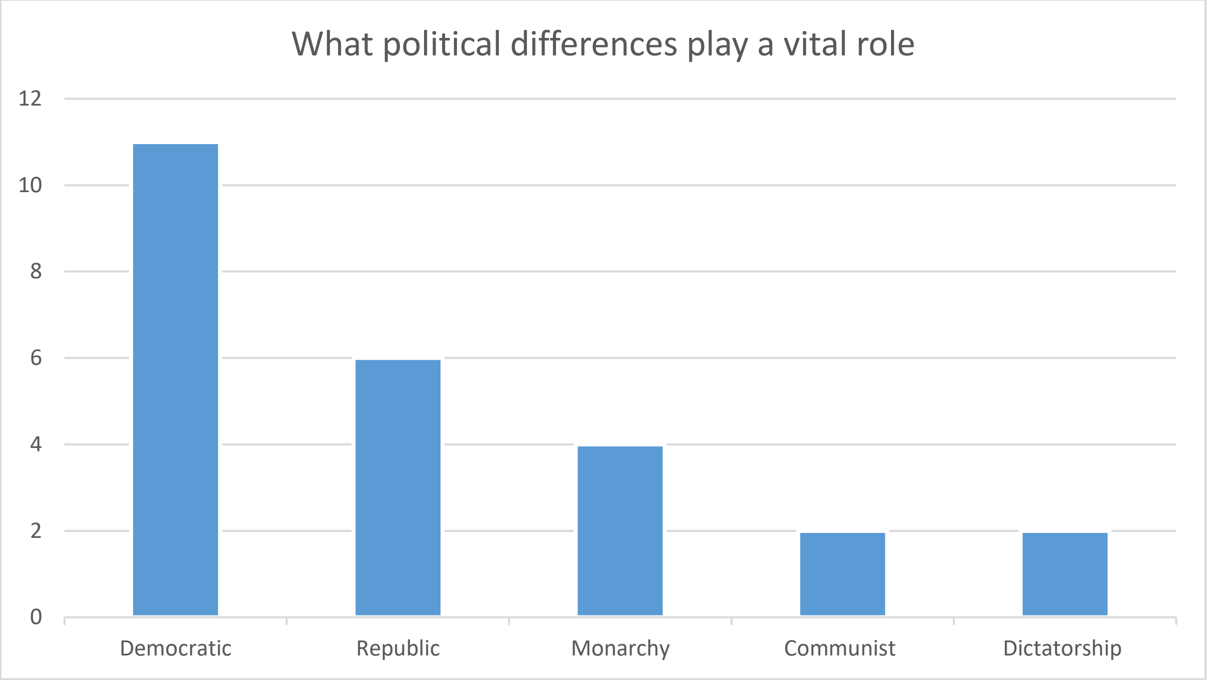


Figure D.276: What political differences play a vital role (6-10)

The majority have chosen democratic political system (See figure D.276), in preference to others because it allows a public voice to influence in the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

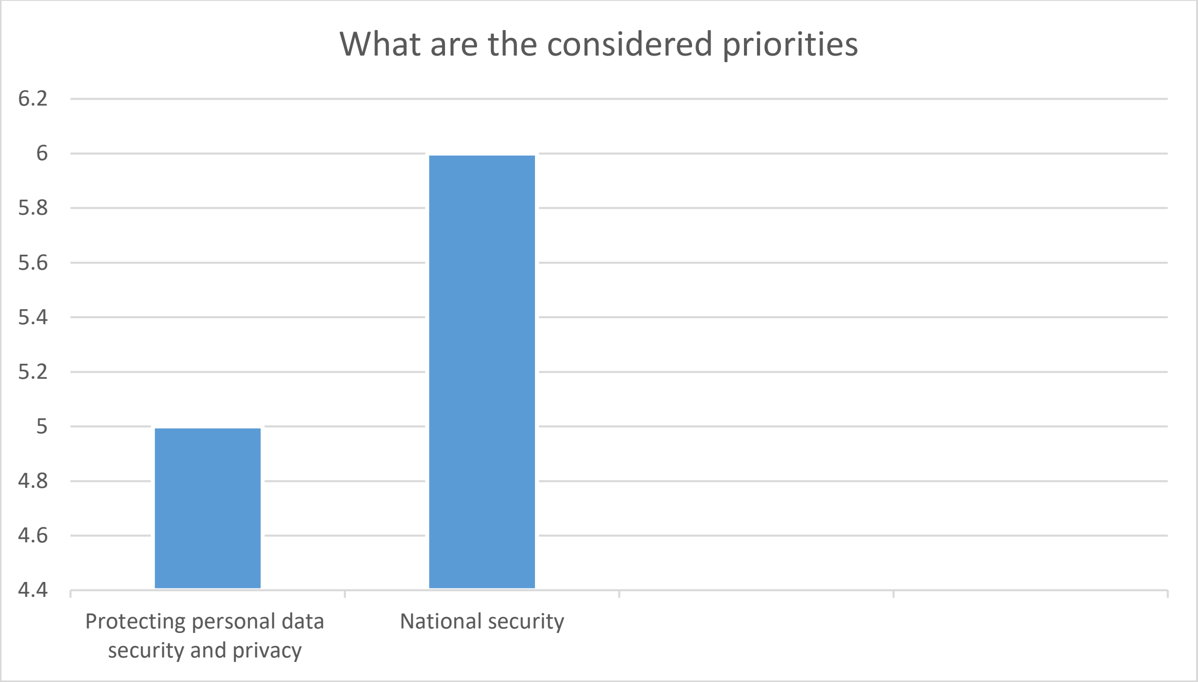


Figure D.277: What are the considered priorities (6-10)

In accepting and implementing a global data privacy and security policies, the importance of national security counts above the protection of personal data security and privacy, which is a significant factor (See figure D.277). In an incident of a personal data breach, there will potentially be a knock-on effect personal data security and privacy as well, and it will also be felt right across the groups as well as the community alike.

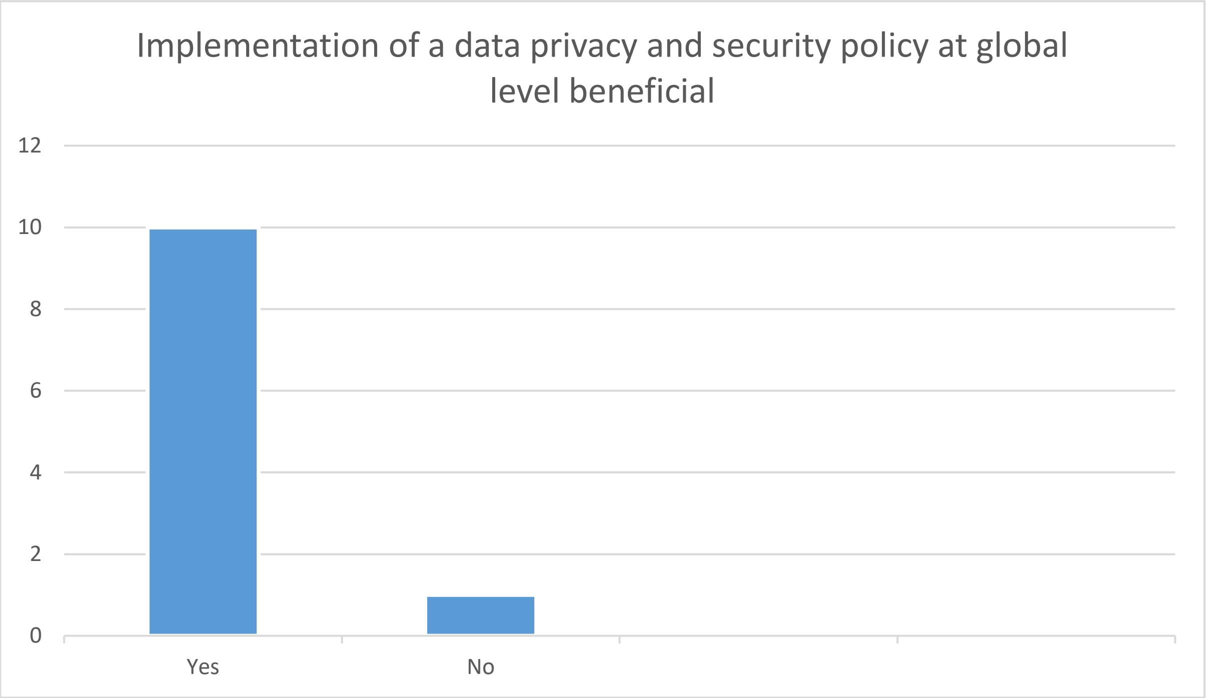


Figure D.278: Implementation of a data privacy and security policy at global level beneficial (6-10)

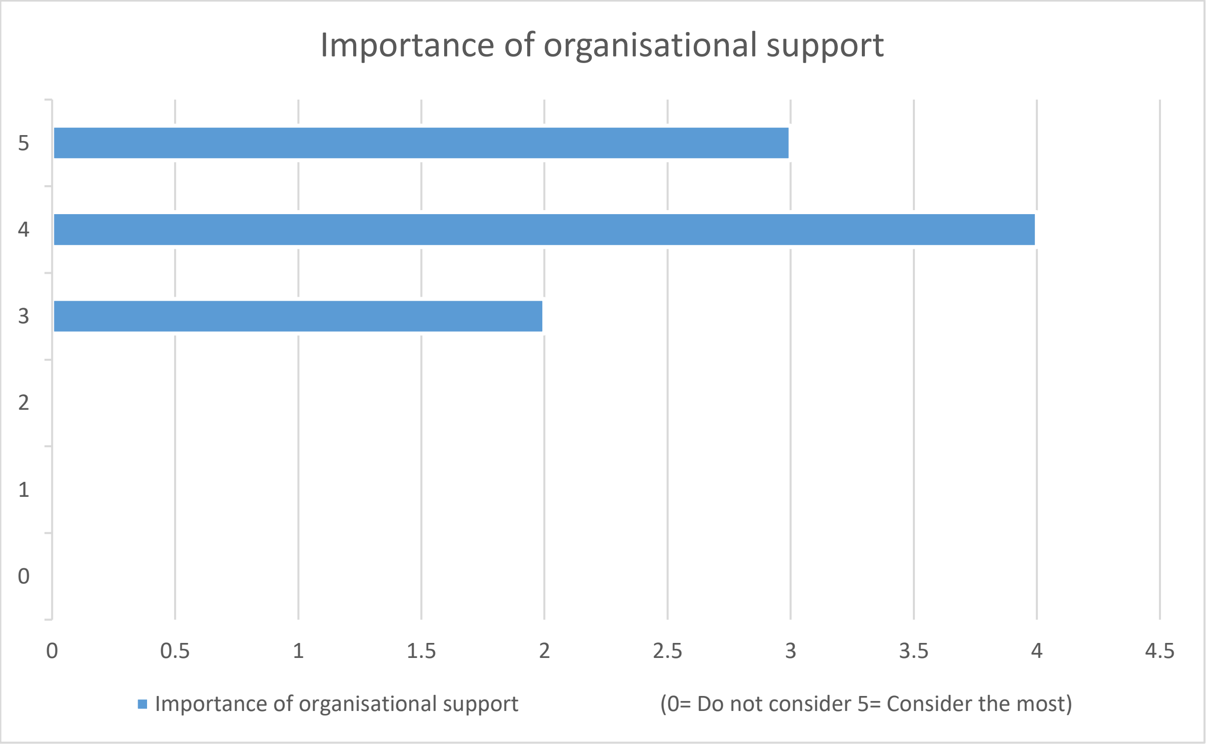


Figure D.279: Importance of organisational support (6-10)

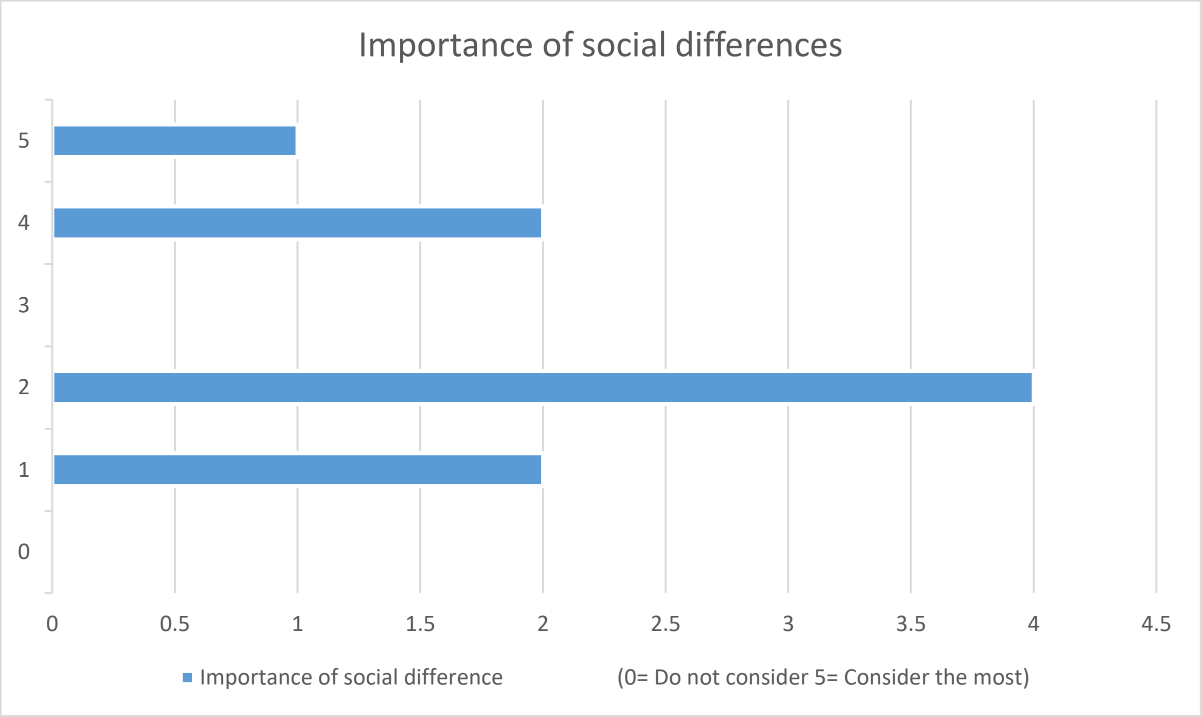


Figure D.280: Importance of social differences (6-10)

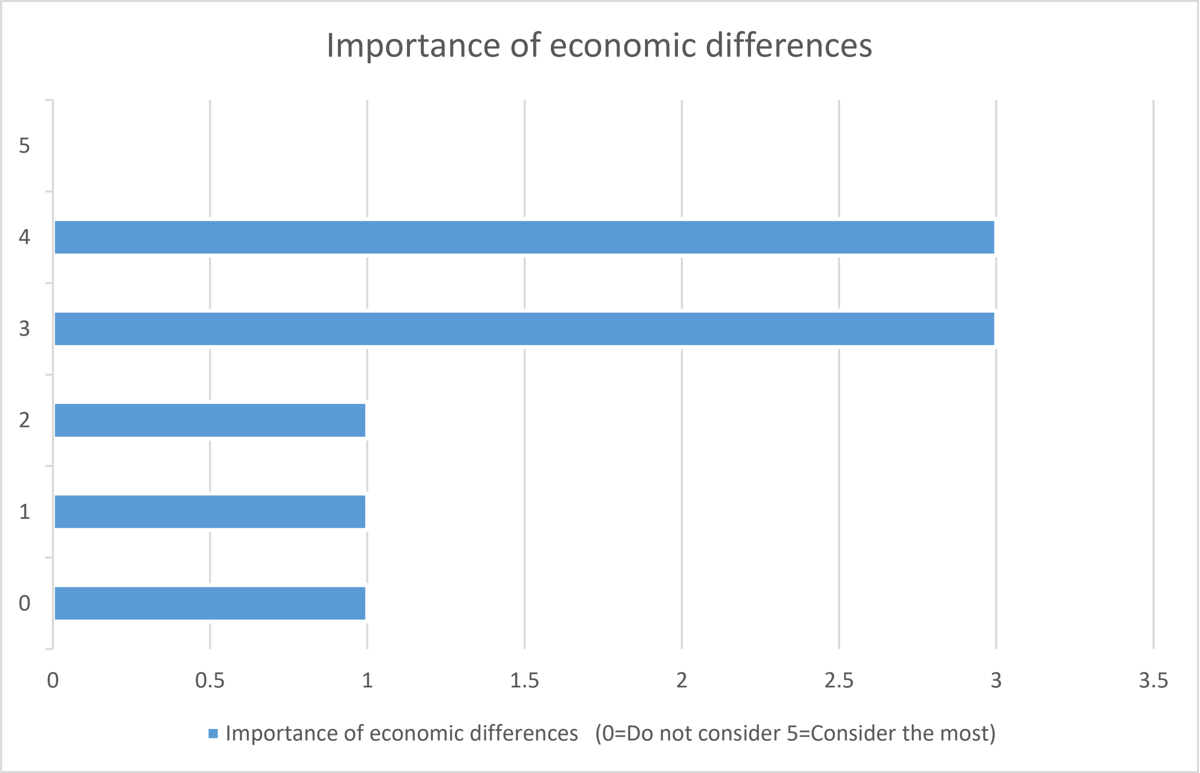


Figure D.281: Importance of economic differences (6-10)

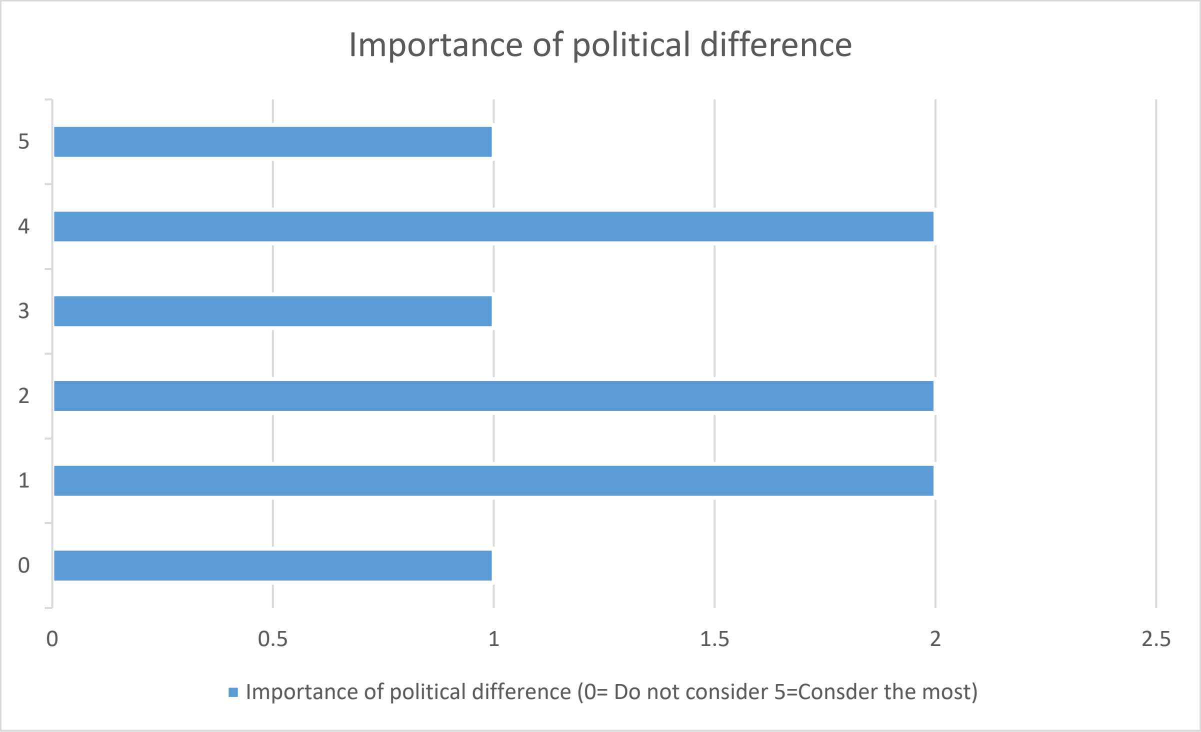


Figure D.282: Importance of political difference (6-10)

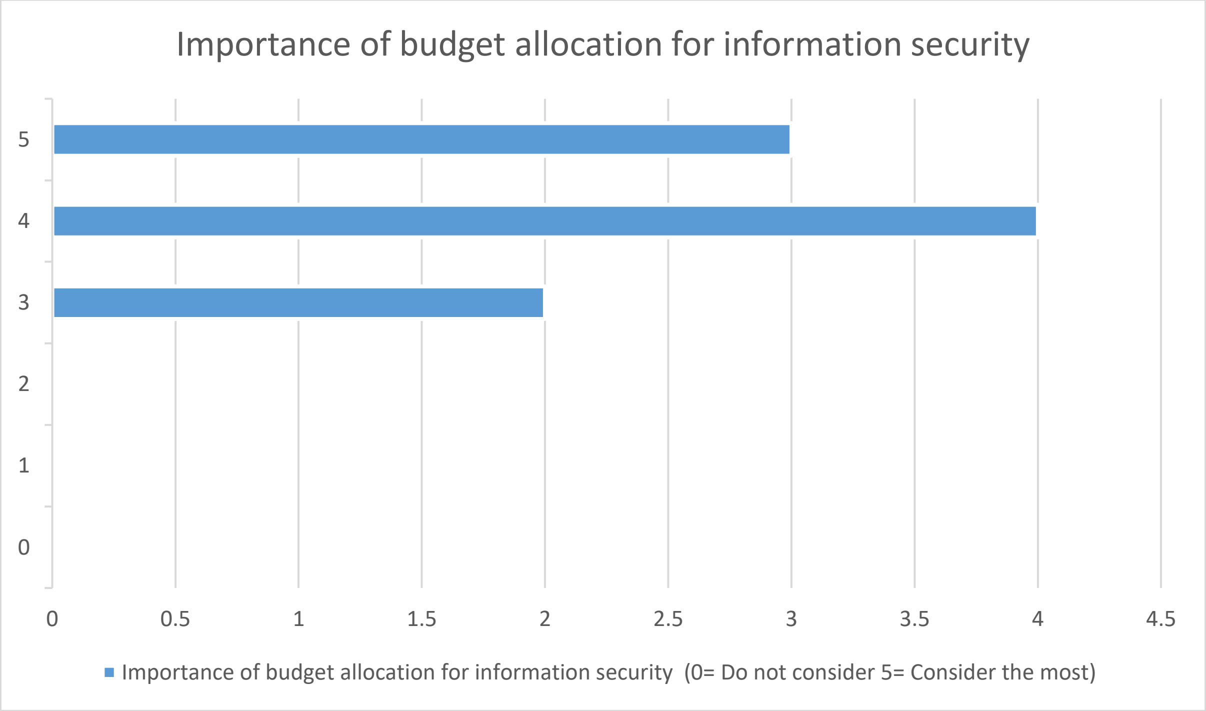


Figure D.283: Importance of budget allocation for information security (6-10)

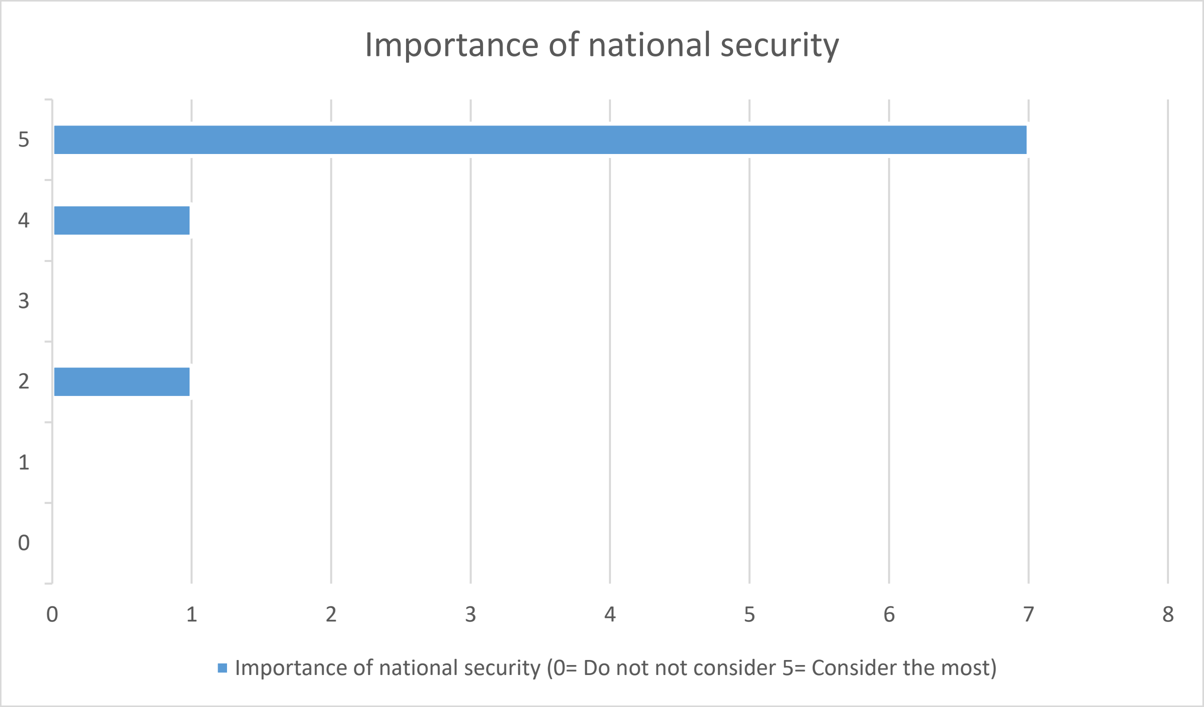


Figure D.284: Importance of national security (6-10)

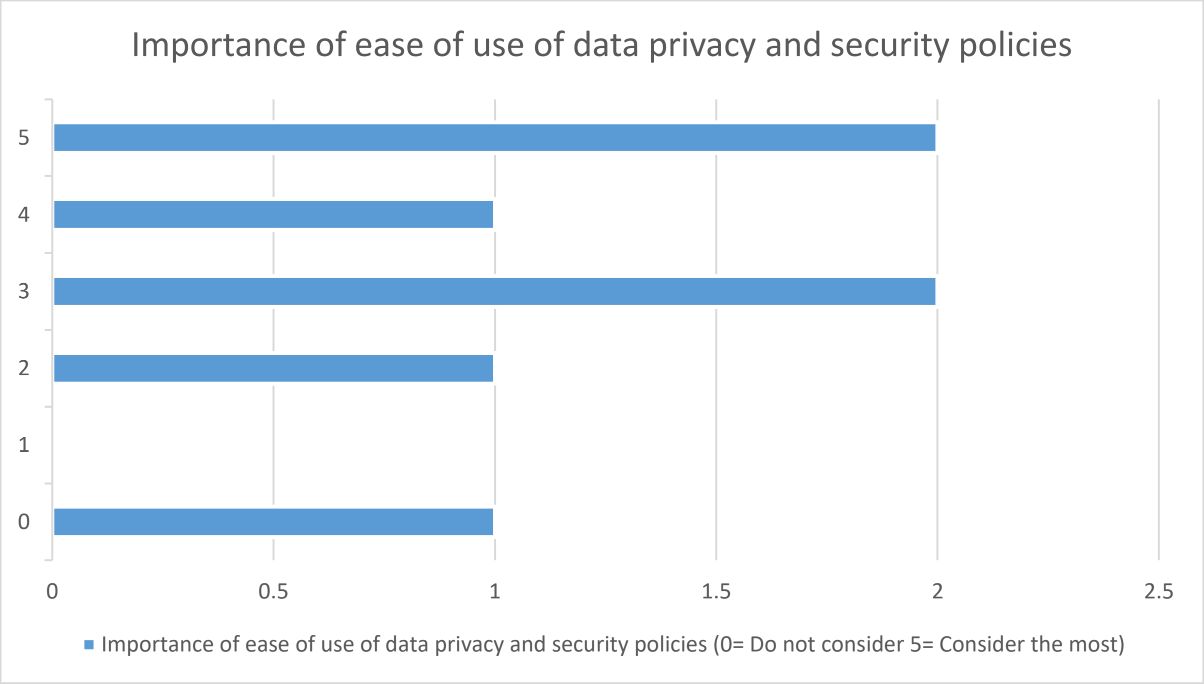


Figure D.285: Importance of ease of use of data privacy and security policies (6-10)

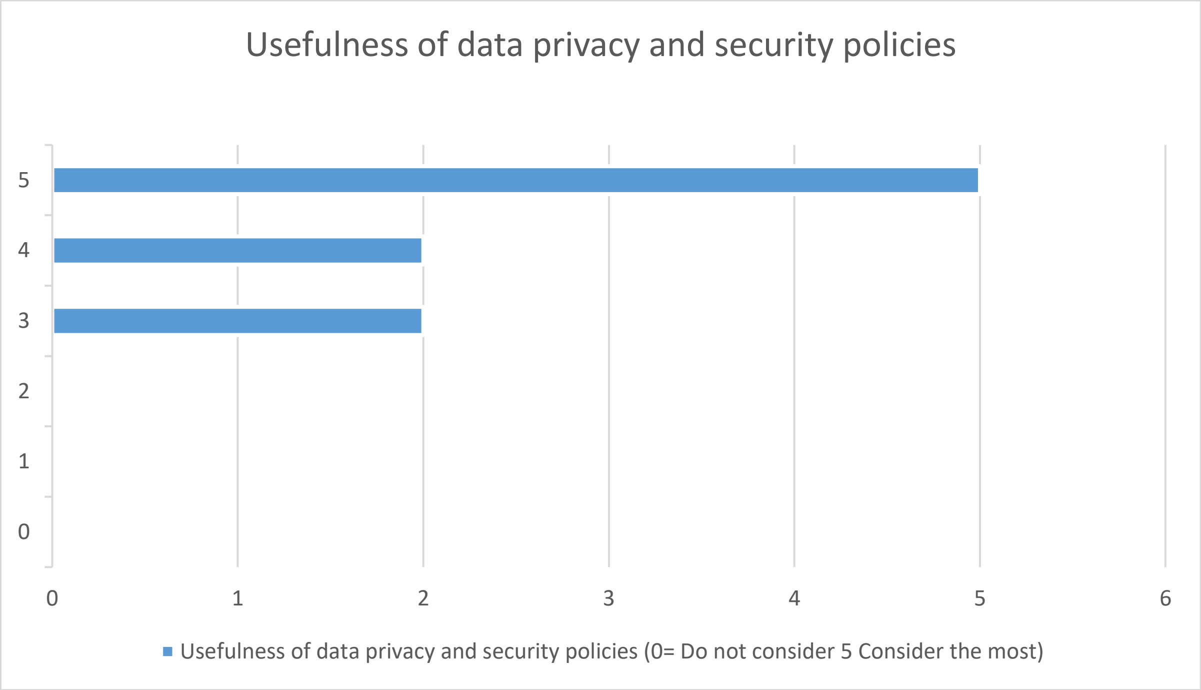


Figure D.286: Usefulness of data privacy and security policies (6-10)

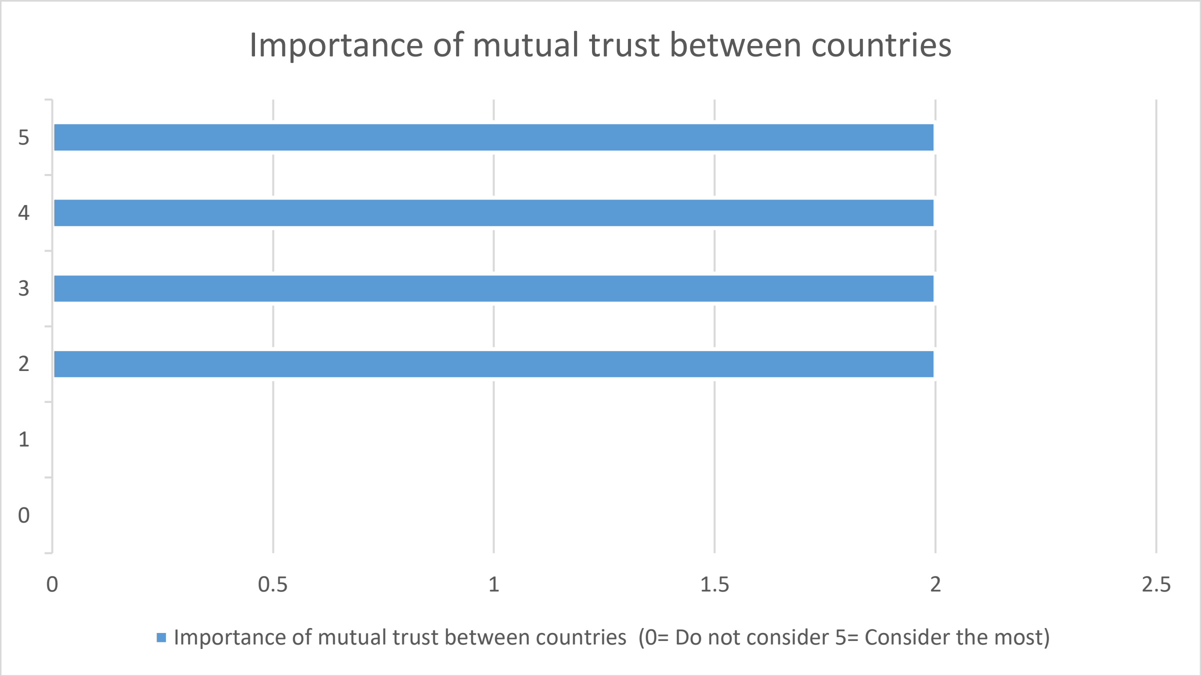


Figure D.287 Importance of mutual trust between countries (6-10)

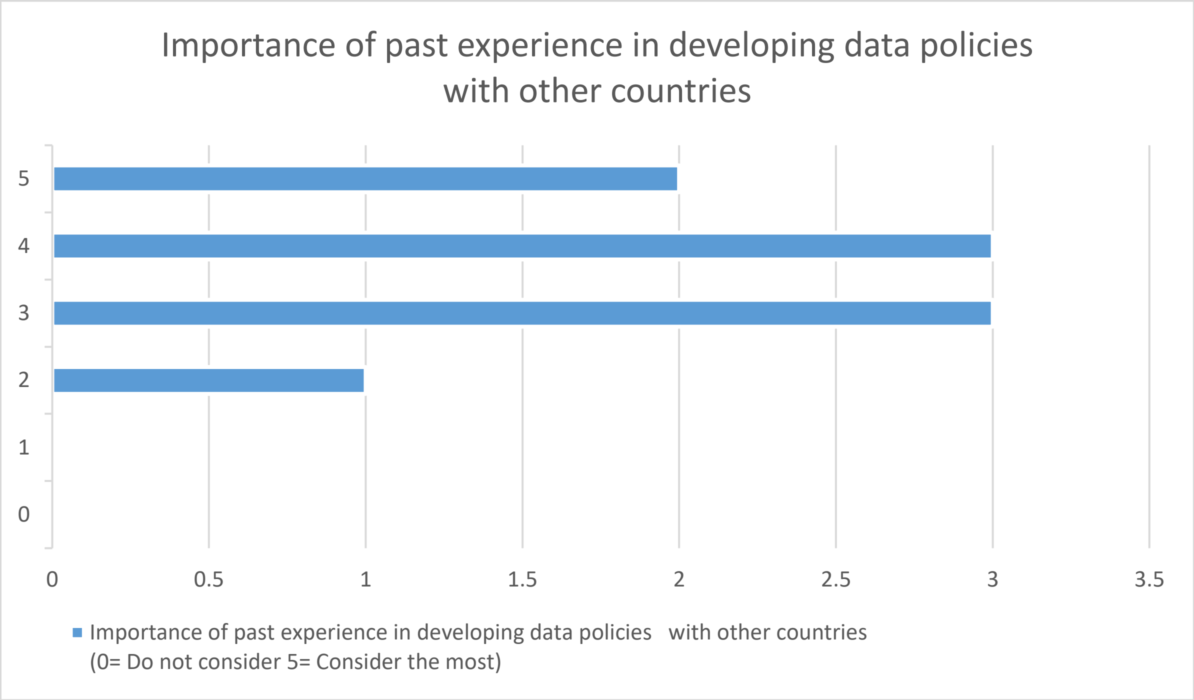


Figure D.288: Importance of past experience in developing data policies with other counties (6-10)

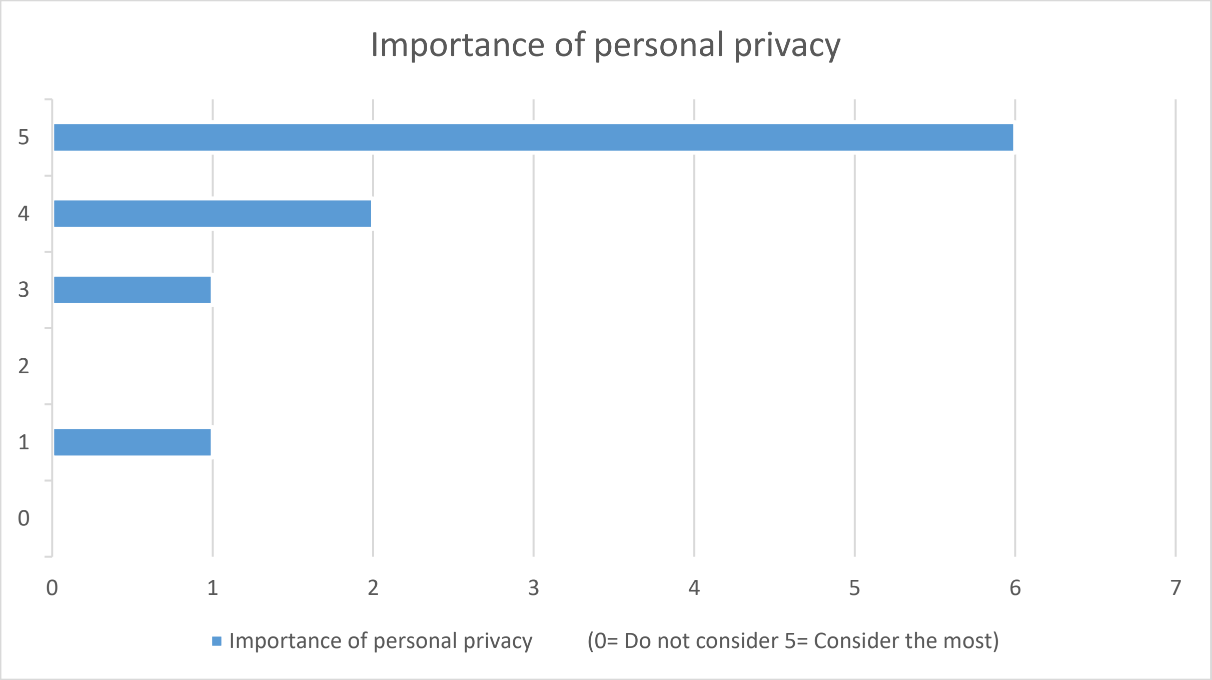


Figure D.289: Importance of personal privacy (**5-10**)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 83 percent of the respondents have endorsed (See figure D.278). The other notable factors that have come out of the survey are organisational support, budget allocation for information security, personal privacy, national security, the usefulness of data privacy and security policies and mutual trust between countries (See figure D.267-277) (See figure D.279-289). However, maturity of the participants in the industry, have not prioritised ease of use (See figure D.285) and previous experience with other countries (See figure D.288) in developing a global level data protection mechanism.

Sri Lanka – Over 10 years

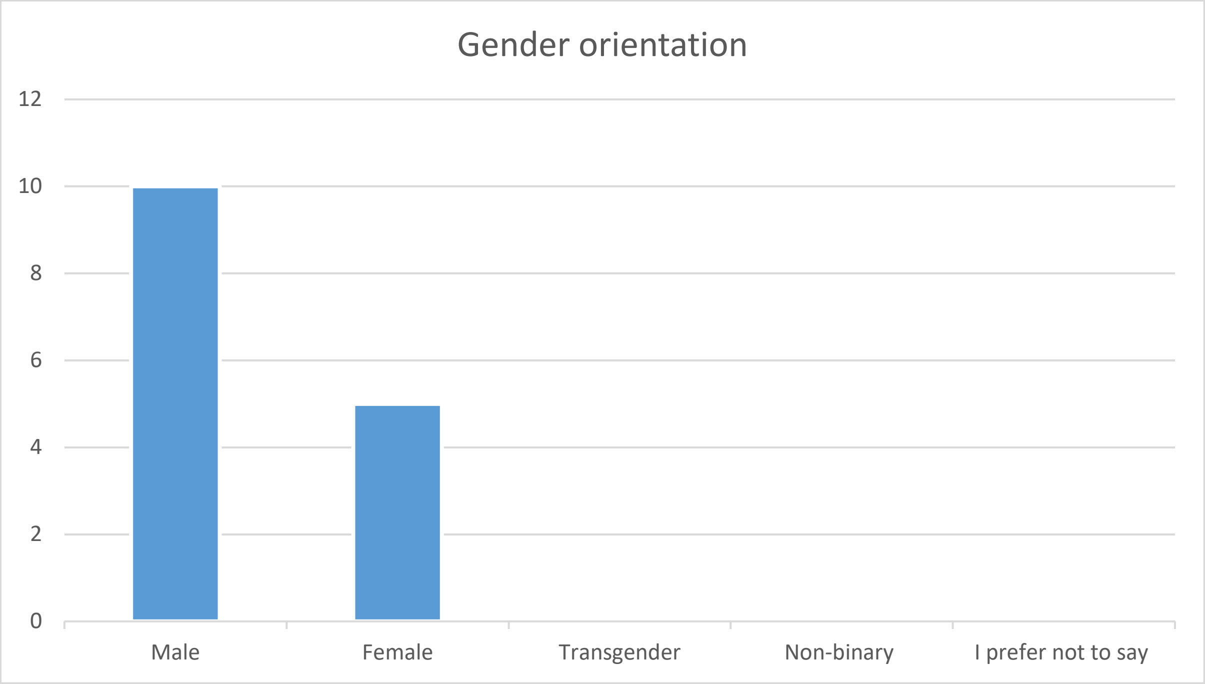


Figure D.290: Gender orientation (Over 10)

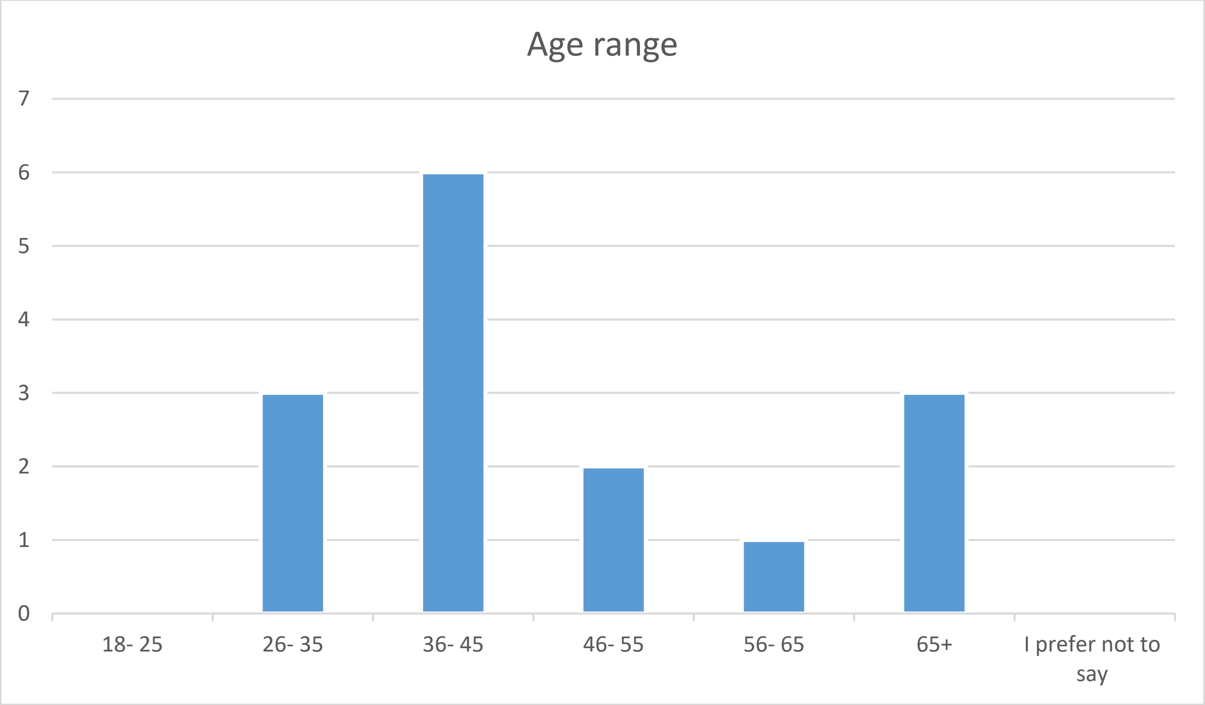


Figure D.291: Age range (Over 10)

This analysis is based on the responses received from Sri Lankans participant in employment in the industry for over 10 years. A total of the 15 participants responded, 10 are males and 5 are females (See figure D.290), all within the 26-65 plus age range. Each age range group consists of 3 in the 26-35; 6 in the 36-45; 2 in the 46-55; 1 in the 56-65; 3 in the 65 plus range (See figure D.291).

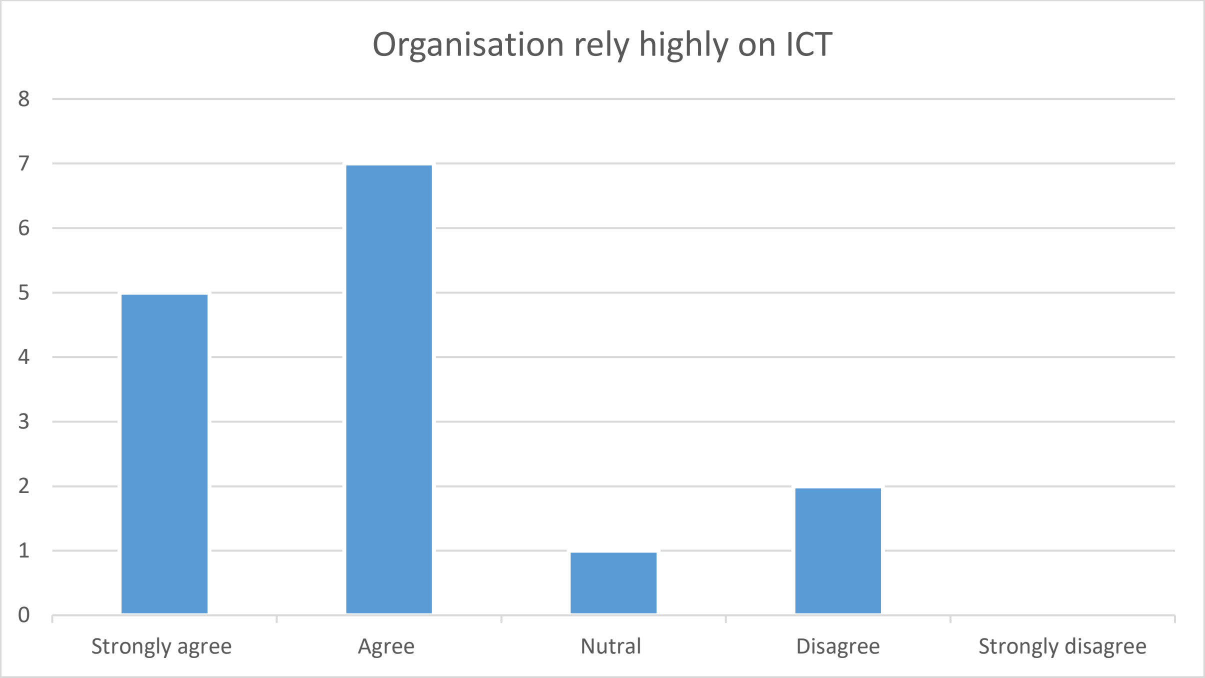


Figure D.292: Organisation rely highly on ICT (Over 10)

Out of the 15 respondents, 12 have worked in a technology reliance working environment, 1 unaware of reliance on technology because of the nature of the work assigned to them, 2 have marked ‘disagree’ on ICT (See figure D.292). This indicates a majority of those who have been working in an organisation for over 10 years have had a high reliance on ICT.

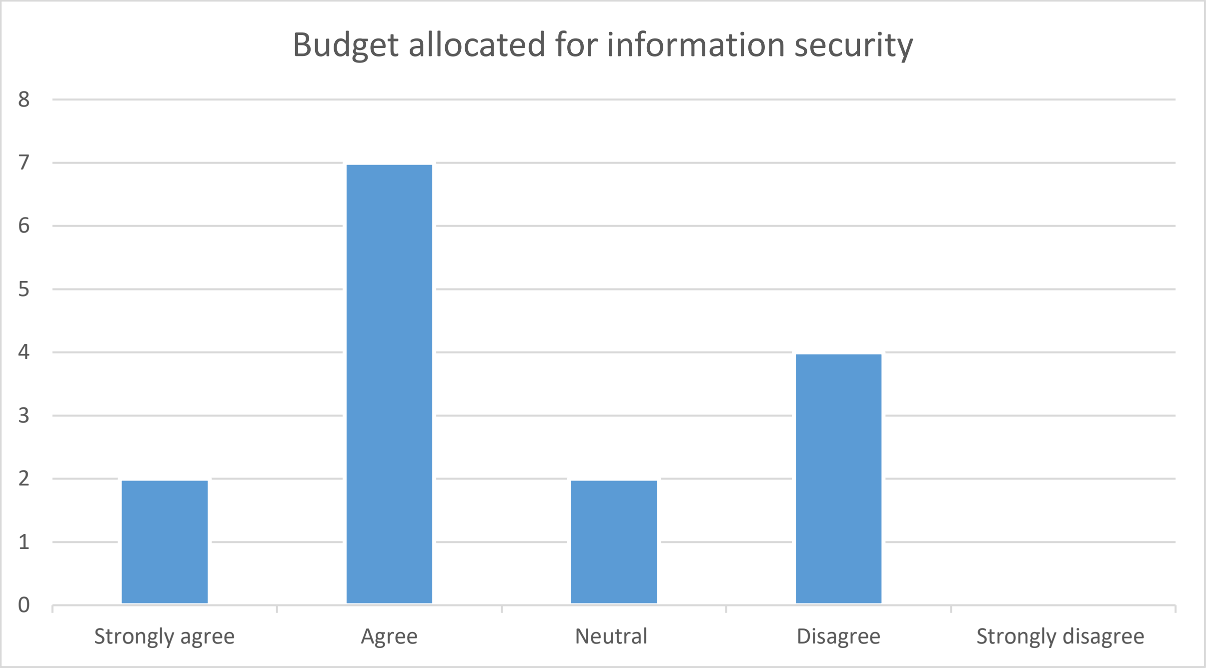


Figure D.293: Budget allocated for information security (Over 10)

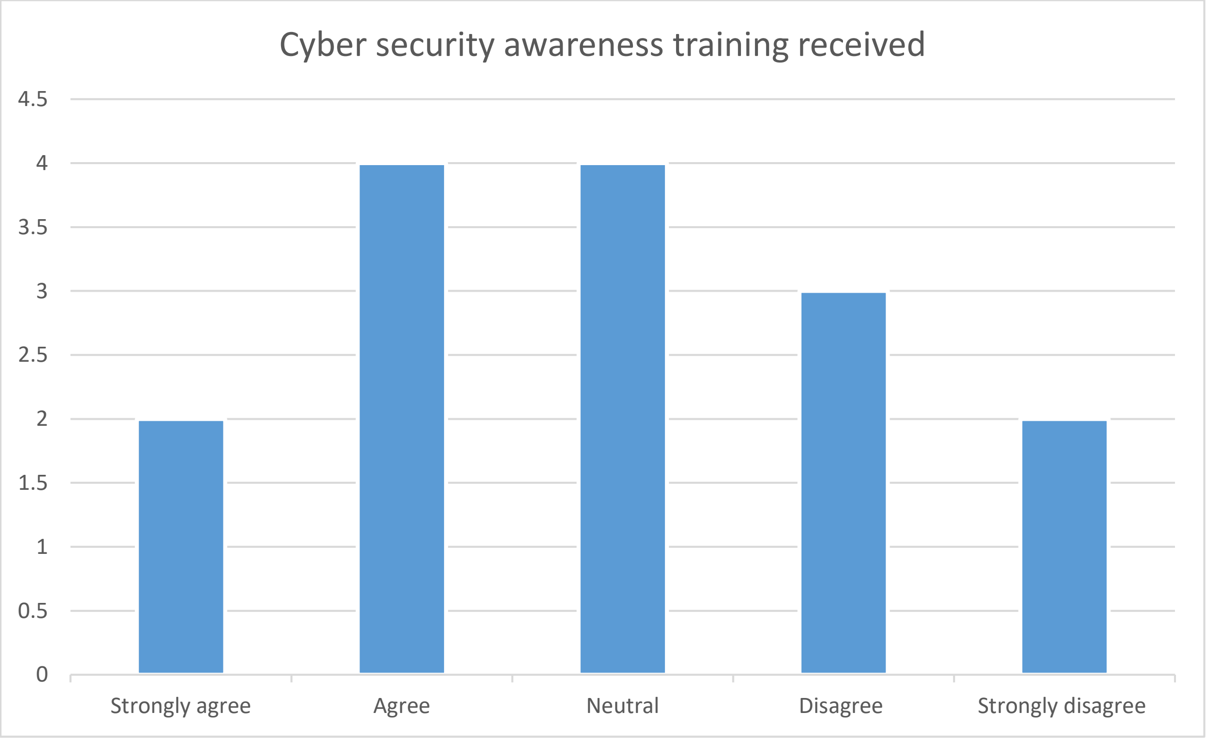


Figure D.294: Cyber security awareness training received (Over 10)

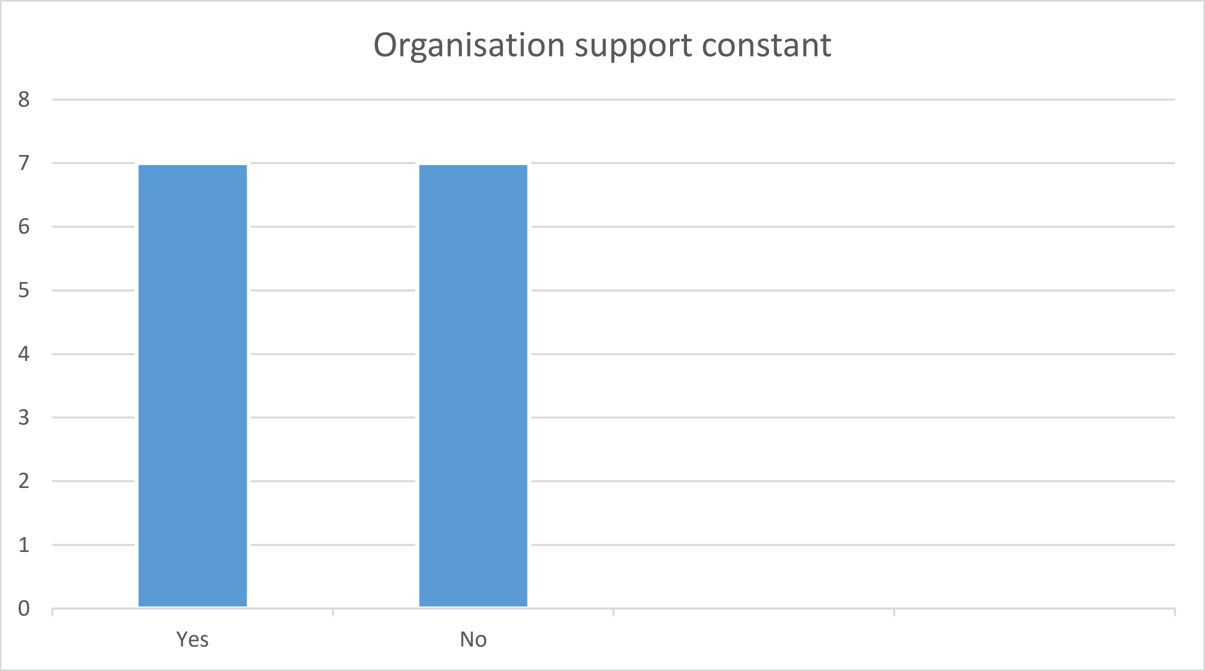


Figure D.295: Organisation support constant (Over 10)

According to 9 out of the 15 participants, their organisations have a budget allocated for information security, 2 unable to comment either way; according to the 4 who disagreed, their organisations had no budget allocation for information security (See figure D.293). According to some of the participants, they find the level of resources allocated for information security satisfactory but regular security awareness training they received was inadequate. Only 6 participants received regular cyber security awareness training; 5 had not: 4 neither agreed nor disagreed (See figure D.294). In addition, 7 participants did receive support from the organisation to protect personal information, another 7 did not (See figure D.295). The members of the organisation did not receive training despite the funding allocated. 50/50 participants have expressed a contrasting opinion about the level of organisational support.

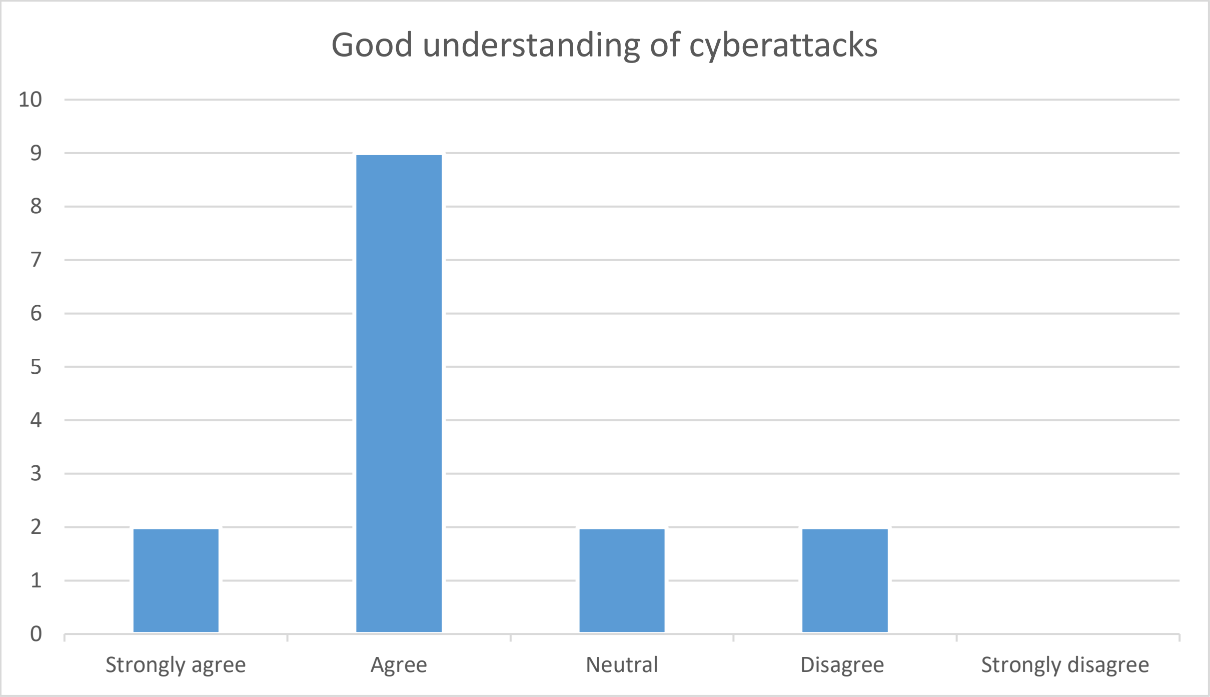


Figure D.296: Good understanding of cyberattacks (Over 10)

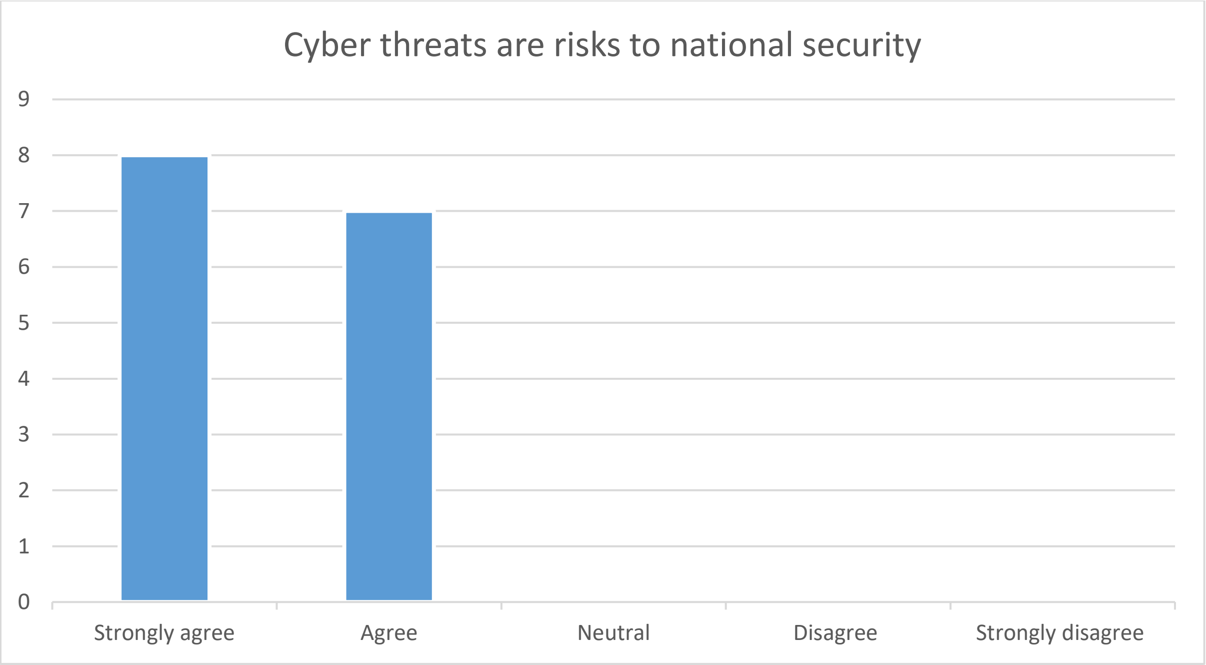


Figure D.297: Cyber threats are risks to national security (Over 10)

The feedback suggests that despite the lack of security awareness training, 11 participants do have a high understanding of the impact of cyber-attacks on the public and the organisation; 2 have no understanding; 2 did not score either way (See figure D.296). Furthermore, 100 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure D.297). This shows that those employed in industry for a long time, through experience and awareness, have a good understanding of potential cyber threats and the devastating impact of breaches to national security. In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

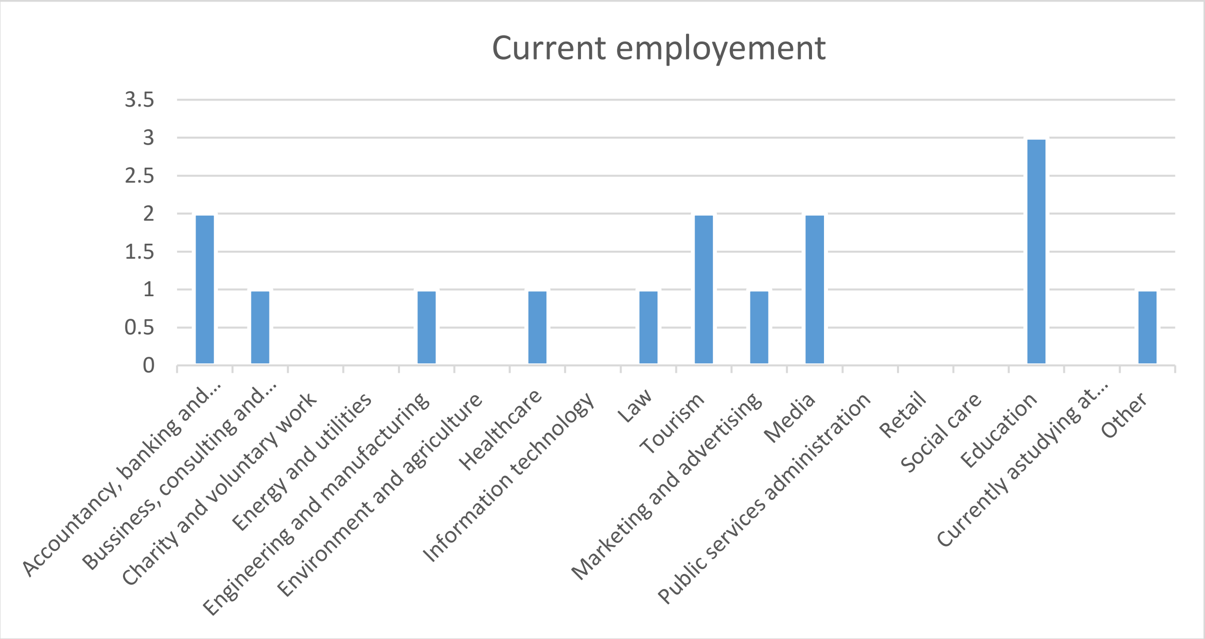


Figure D.298: Current employment (Over 10)

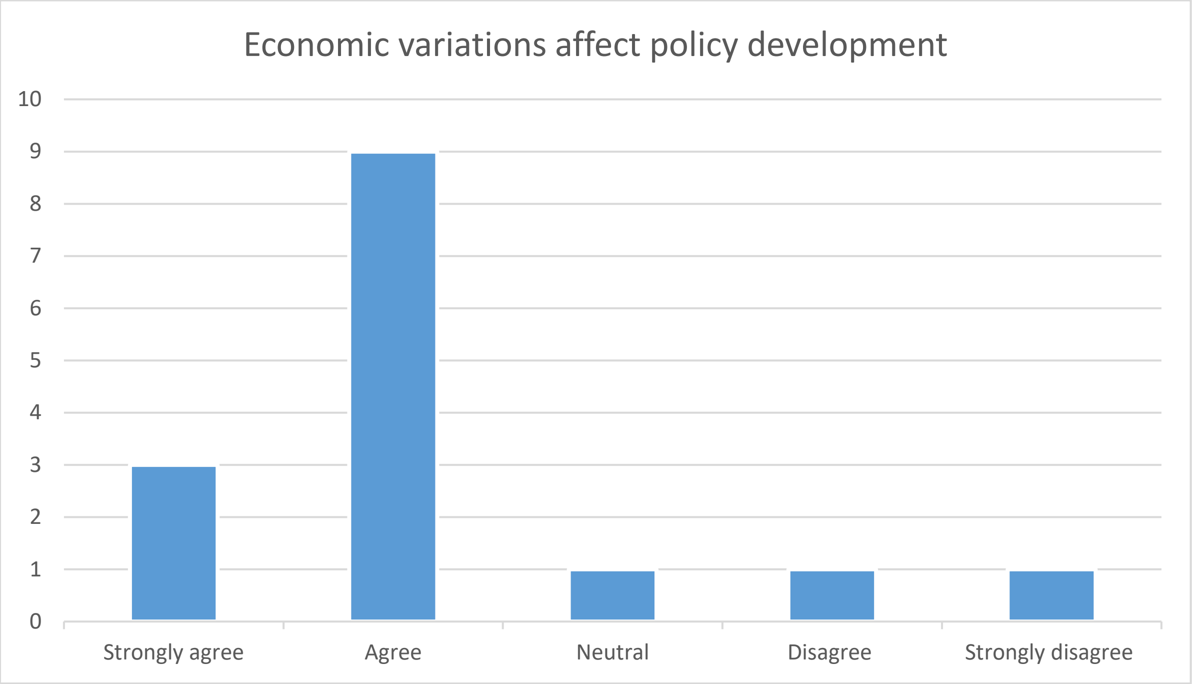


Figure D.299: Economic variations affect policy development (Over 10)

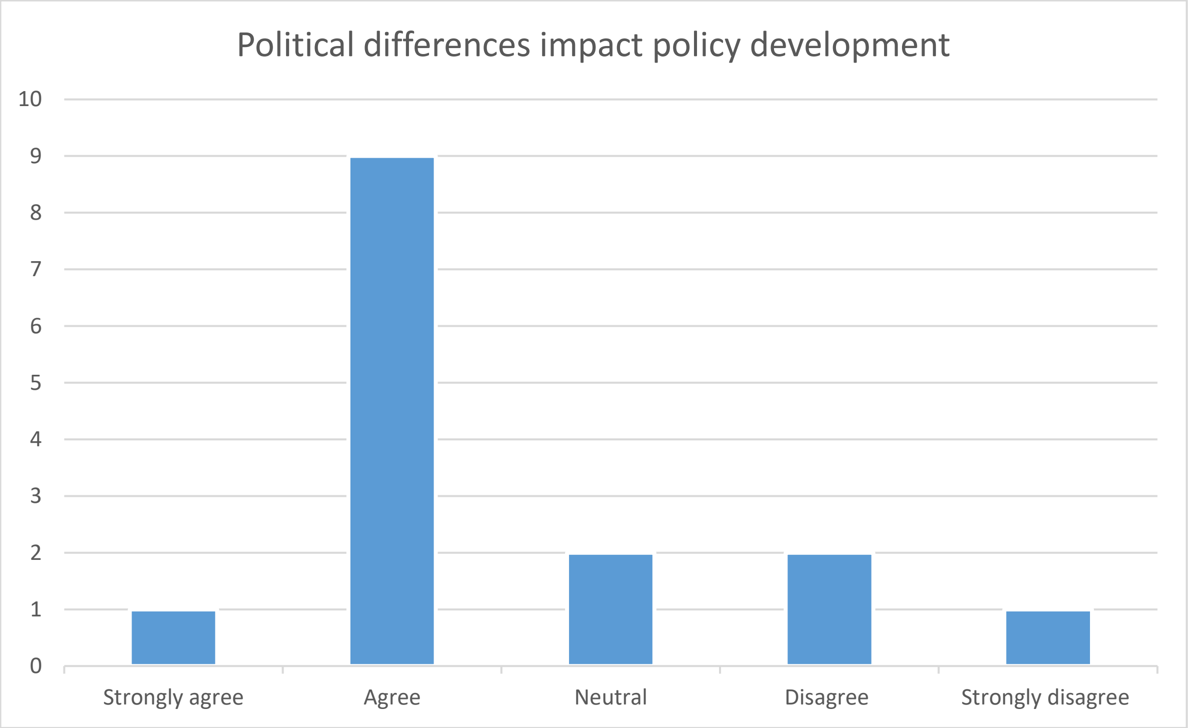


Figure D.300: Political differences impact policy development (Over 10)

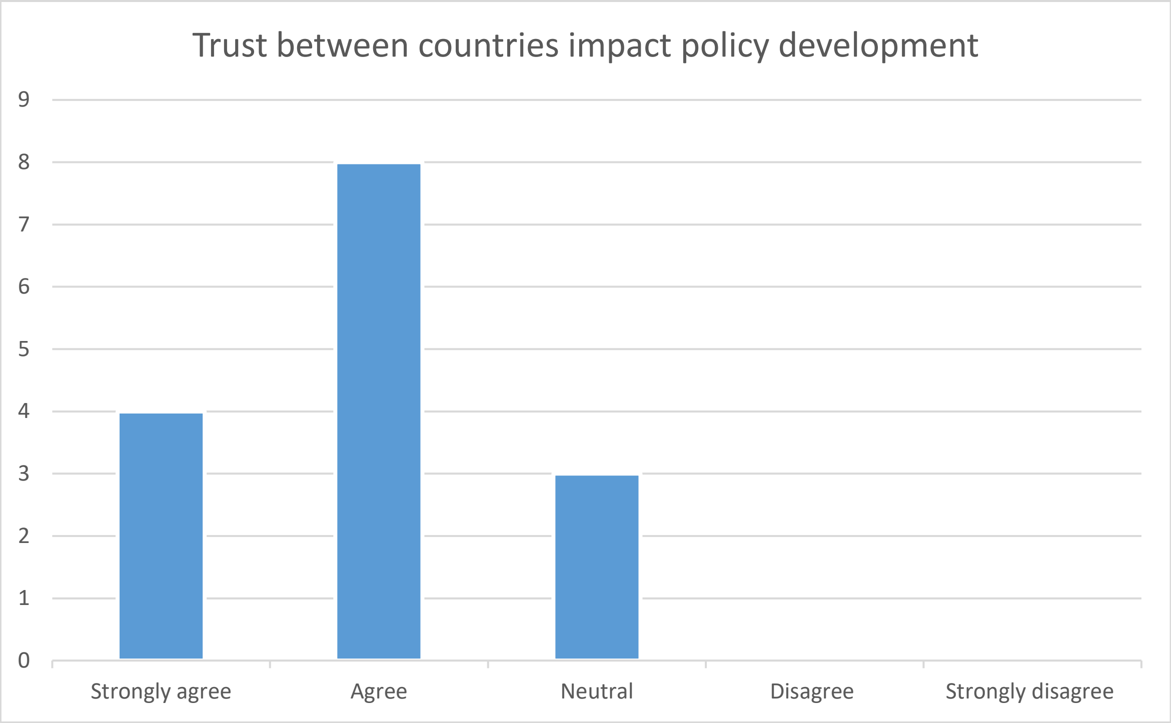


Figure D.301: Trust between countries impact policy development (Over 10)

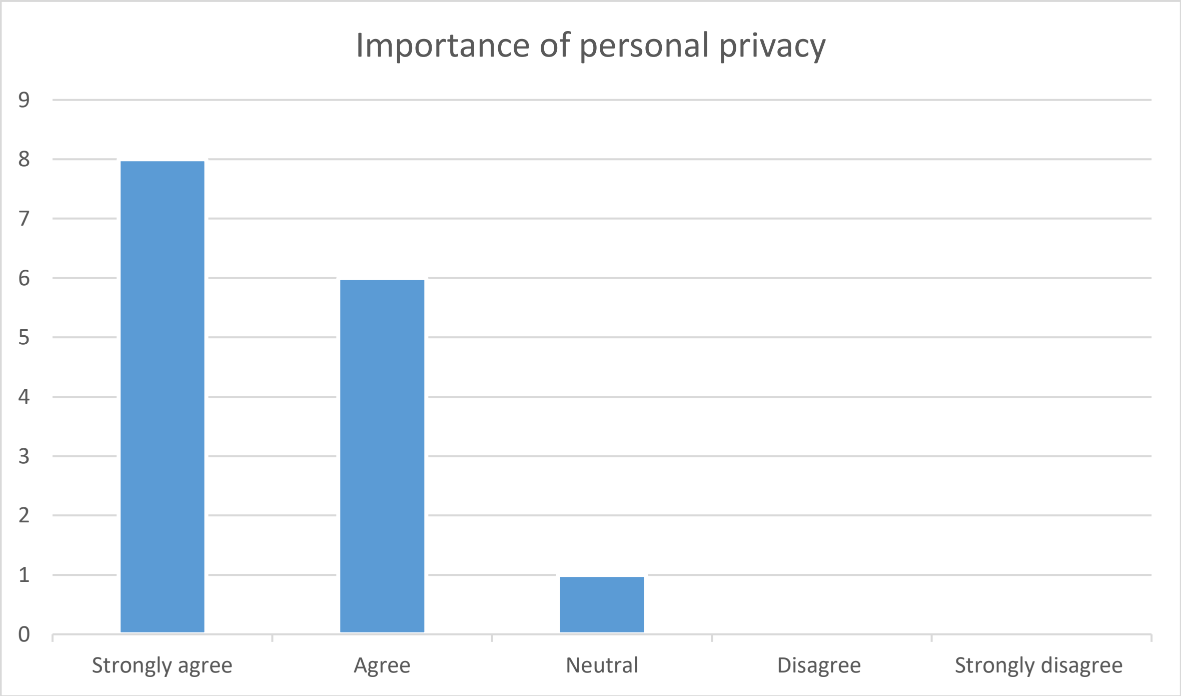


Figure D.302: Importance of personal privacy (Over 10)

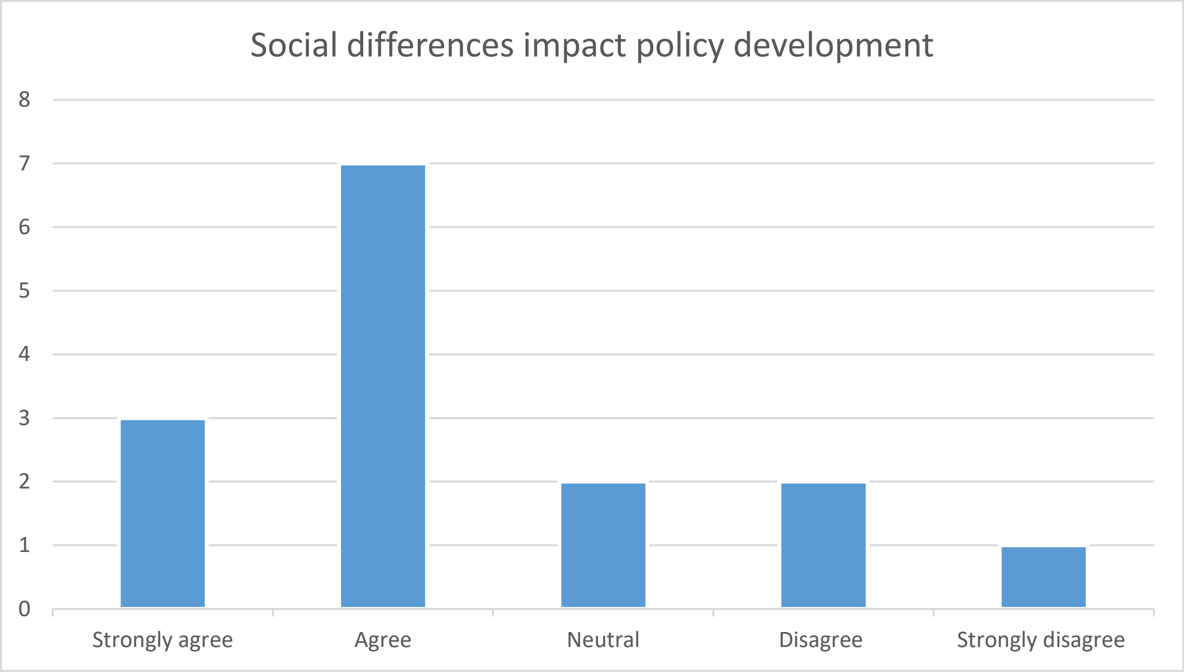


Figure D.303: Social differences impact policy development (Over 10)

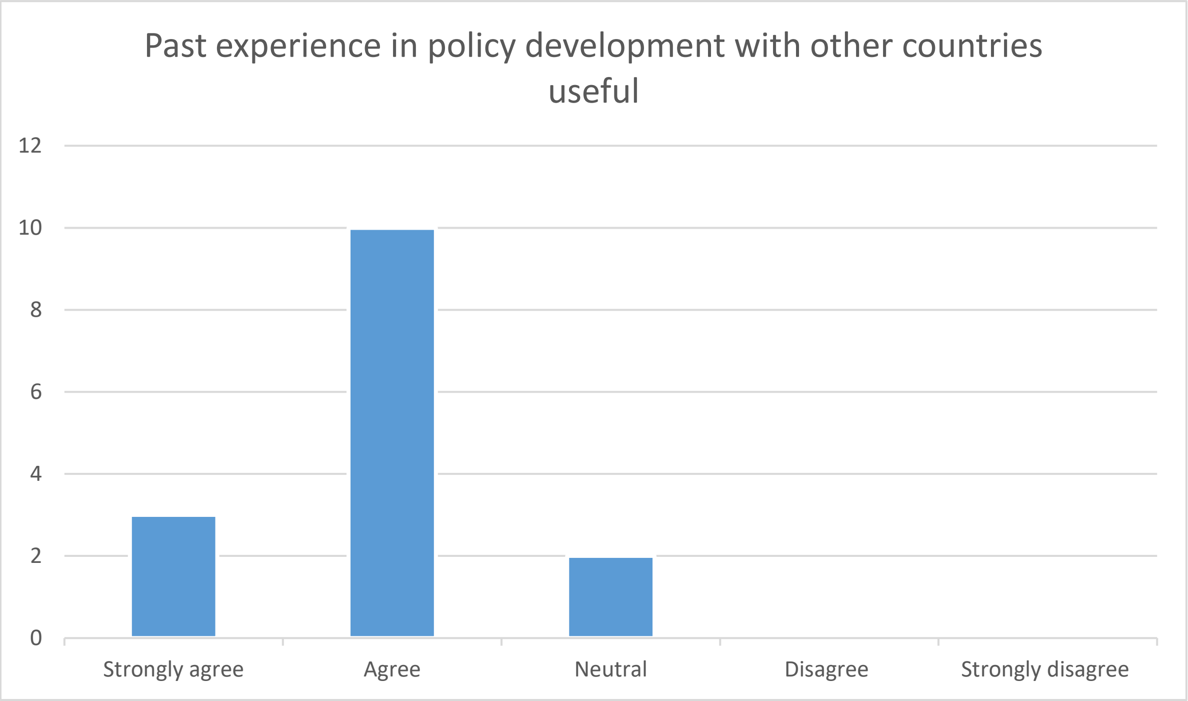


Figure D.304: Past experience in policy development with other countries useful (Over 10)

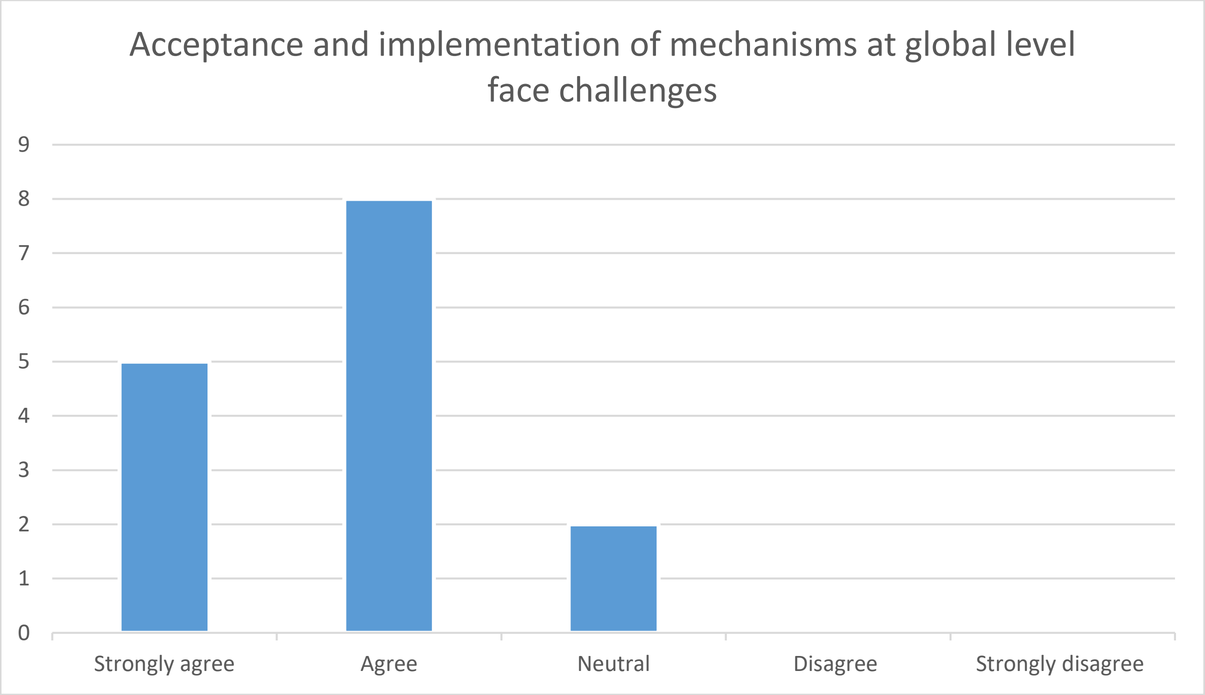


Figure D.305: Acceptance and implementation of mechanisms at global level face challenges (Over 10)

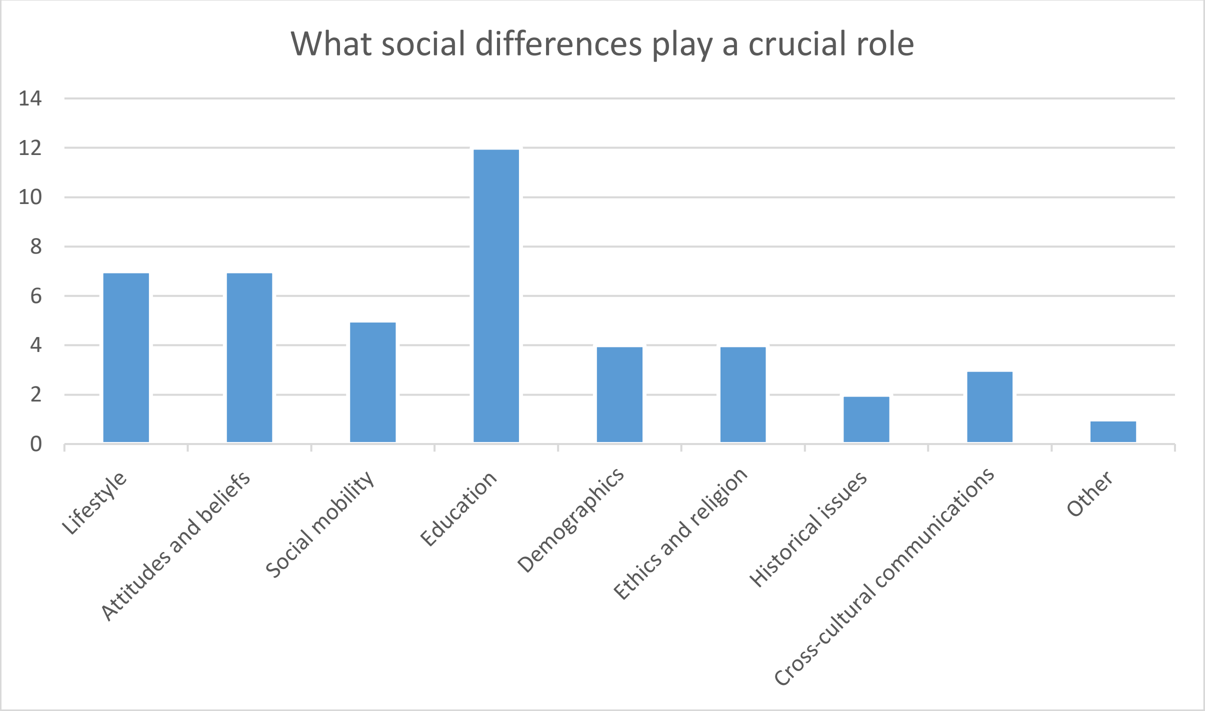


Figure D.306: What social differences play a crucial role (Over 10)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education, attitude and beliefs and lifestyle (See figure D.306). It becomes clear that educational training can be an effective way to make people understand the importance of privacy and the implications associated with privacy violations. People will have to make crucial choices in their lifestyles when considering reliance on technology at the workplace. If there is a high reliance on technology in sharing or handling personal information, the demand for accepting and implementing policies associated with data privacy and security also should be high. Having knowledge and being familiar with potential cyber threats, their impact on people and national security is of utmost importance in accepting and implementing data privacy and security policies. Therefore, it is beneficial to conduct cybersecurity awareness training at schools and at the organisational level. Putting trust in the privacy and respecting the privacy of self and others are further discussed under attitude and believes

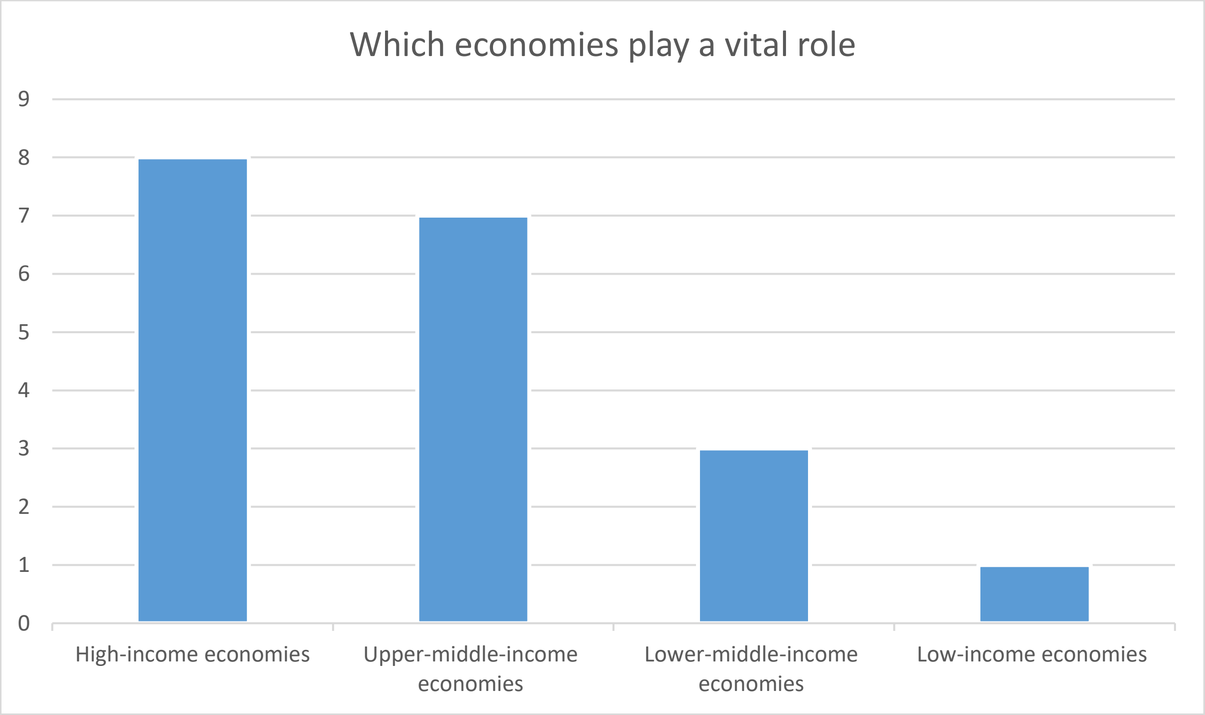


Figure D.307: Which economies play a vital role (Over 10)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role in policymaking, according to feedback (See figure D.307). The key stages in the policymaking process aim to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the resources necessary, implement, and finally evaluate the policy. These stages are time-consuming and require sufficient funding and resources. Therefore, achieving success to a large extent depends on the economic stability of the country, which counts as a crucial factor in policymaking.

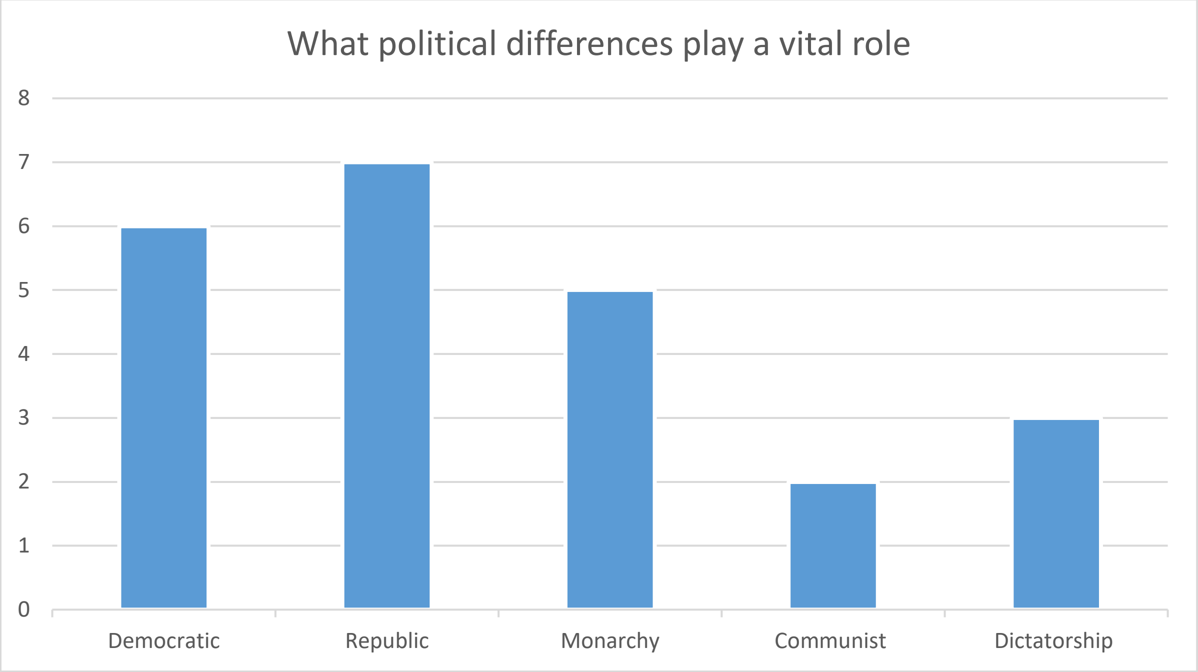


Figure D.308: What political differences play a vital role (Over 10)

Interestingly those who have been in the industry for less than 10 years have not voted for a democratic political system. In a democratic system, public voice counts, in contrast to in any other forms of political systems. However, it is an interesting point to note that majority of those who have been in the industry for more than 10 years prefers a republican political system over a democratic system (See figure D.308). In a Republican system of governance, people and their elected representatives hold power and take decisions in accordance with the constitution. It is fair to assume that people look for the constitution of the state and the personal data collection organisations to protect personal information and assurances not to compromise by sharing.

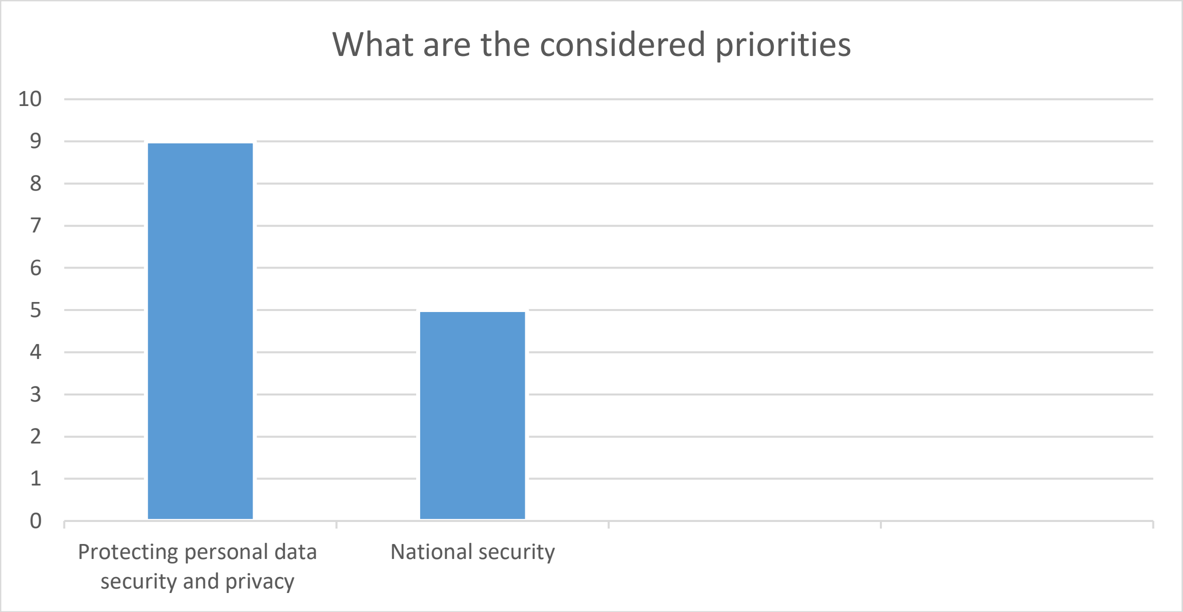


Figure D.309: What are the considered priorities (Over 10)

In accepting and implementing a global data privacy and security policies, the participant focuses more on the importance of protecting personal data security and privacy, and less on protecting national security without completely losing focus on the importance of national security (See figure D.309). It is likely that their instinct and personal experience over time may have contributed to their preference. The people in this category do not come from the young generation (teenagers). Their careers and family life would have been built up over a considerable life span, and cared more about the privacy of the family, family connections, and concerned about the impact that may have on their wellbeing.

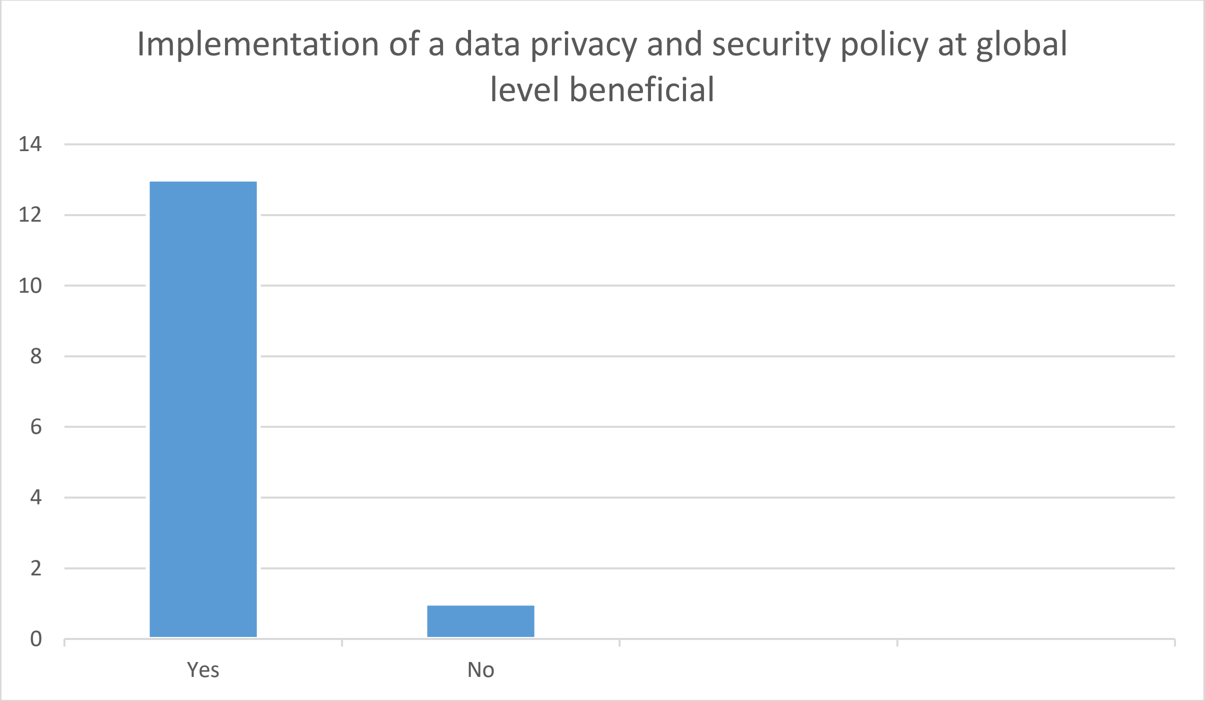


Figure D.310: Implementation of a data privacy and security policy at global level beneficial (Over 10)

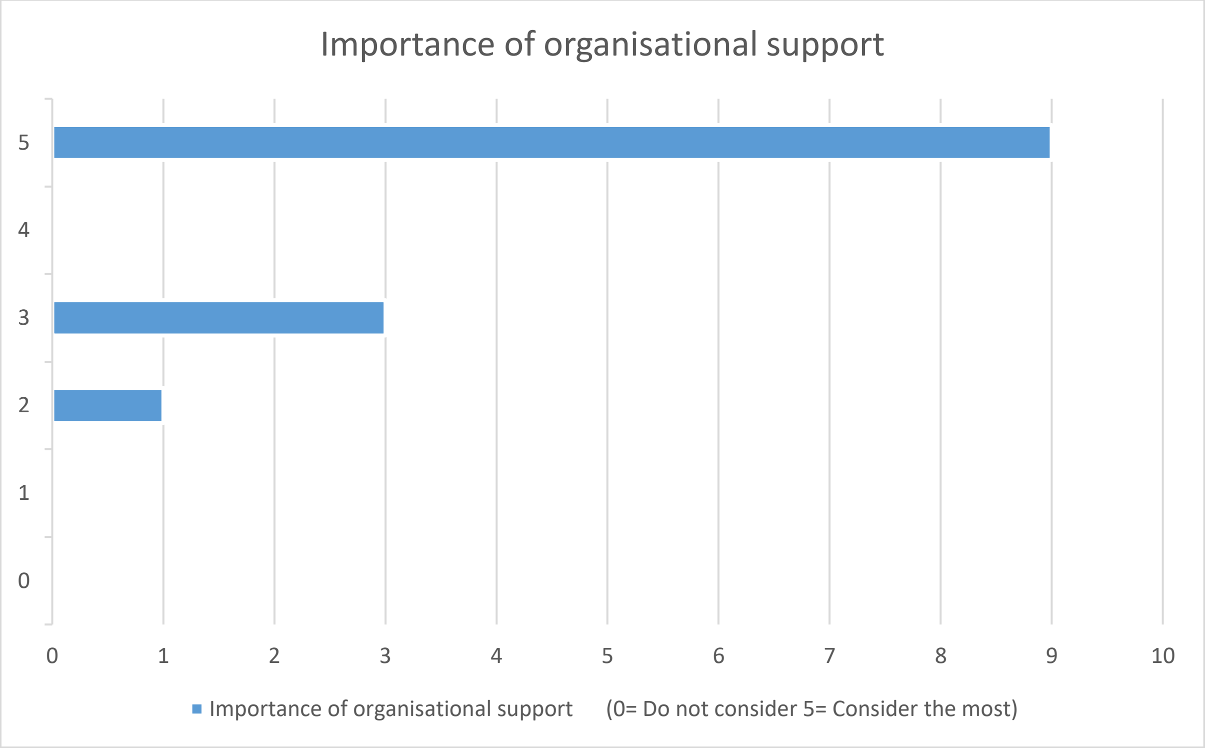


Figure D.311: Importance of organisational support (Over 10)

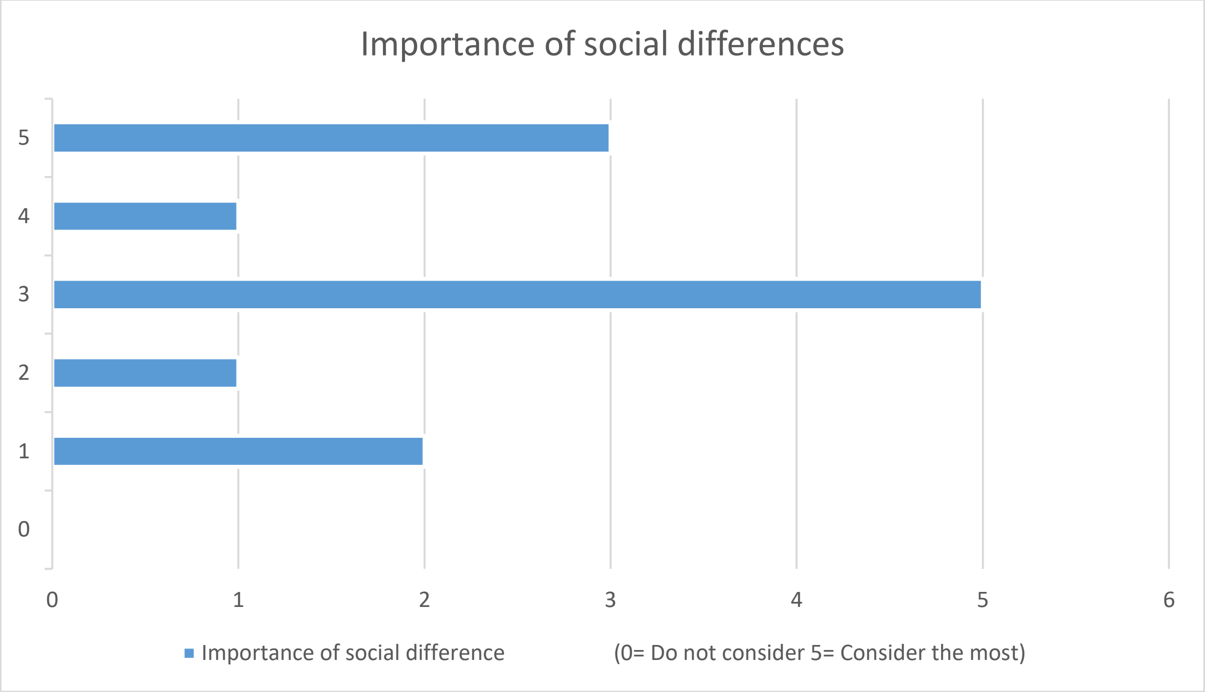


Figure D.312: Importance of social differences (Over 10)

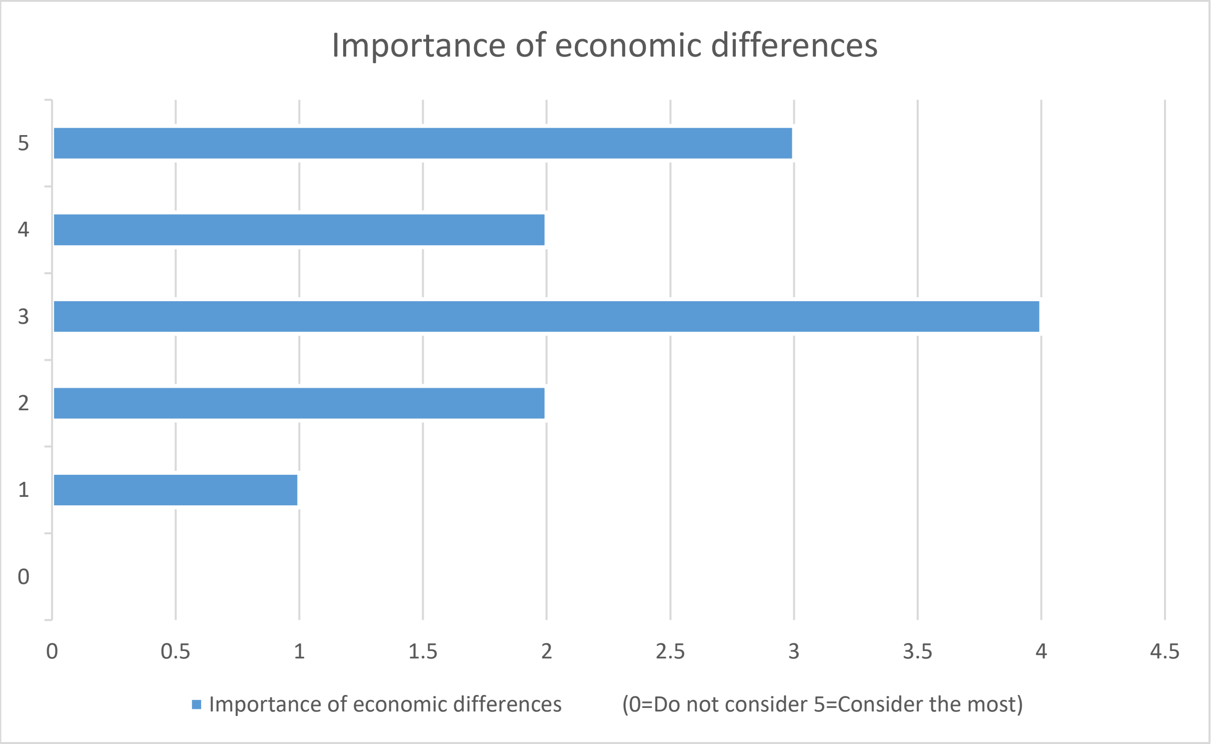


Figure D.313: Importance of economic differences (Over 10)

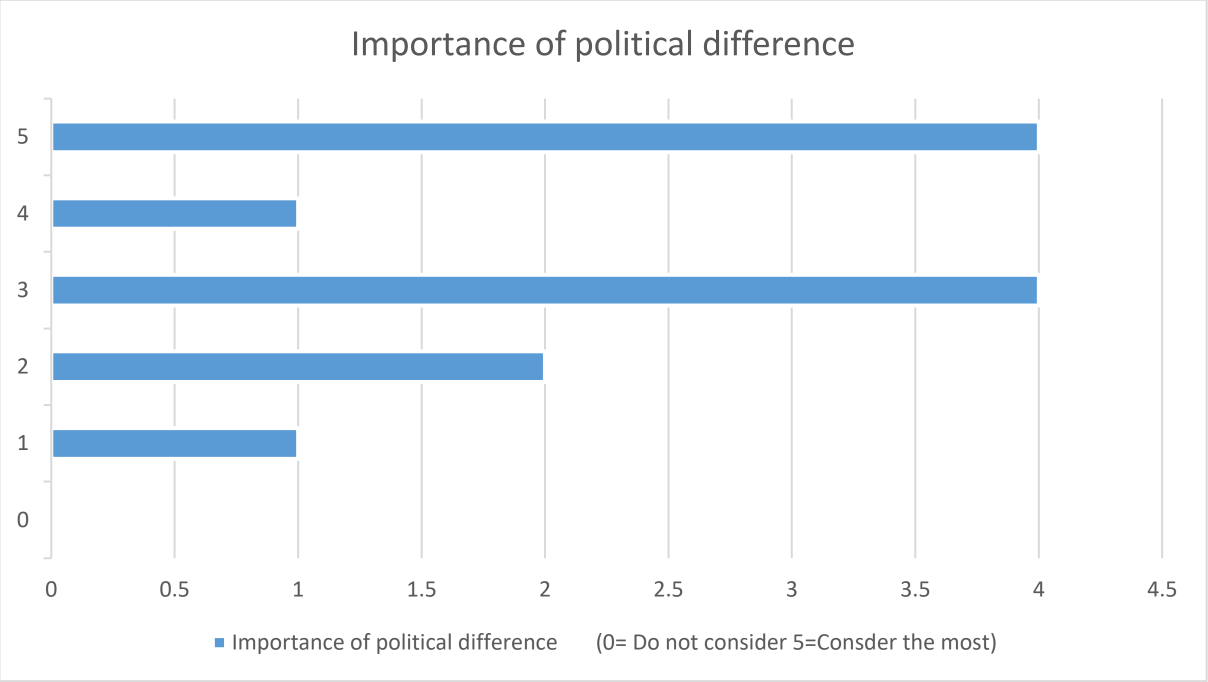


Figure D.314: Importance of political difference (Over 10)

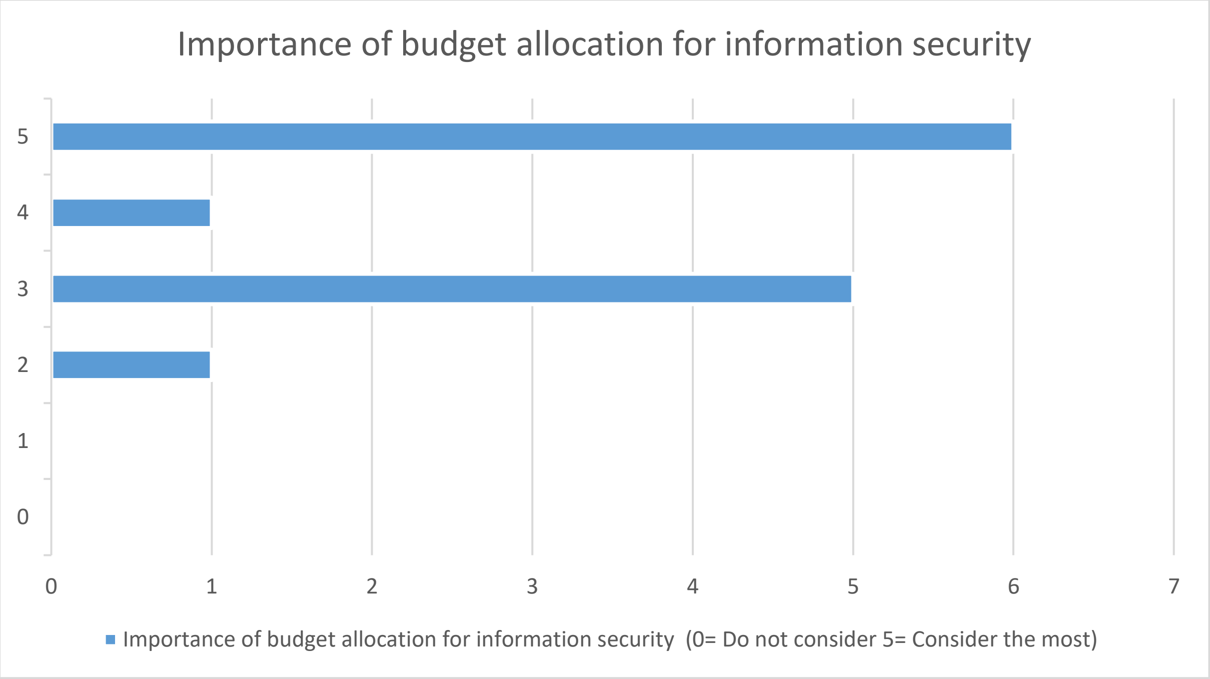


Figure D.315: Importance of budget allocation for information security (Over 10)

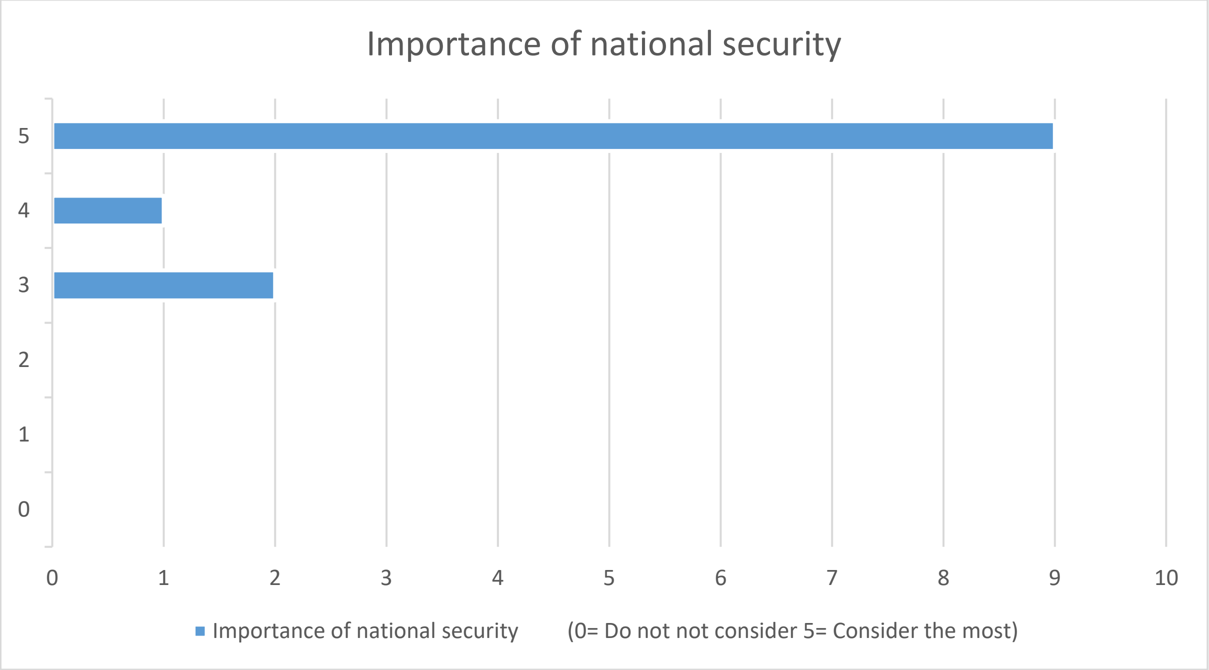


Figure D.316: Importance of national security (Over 10)

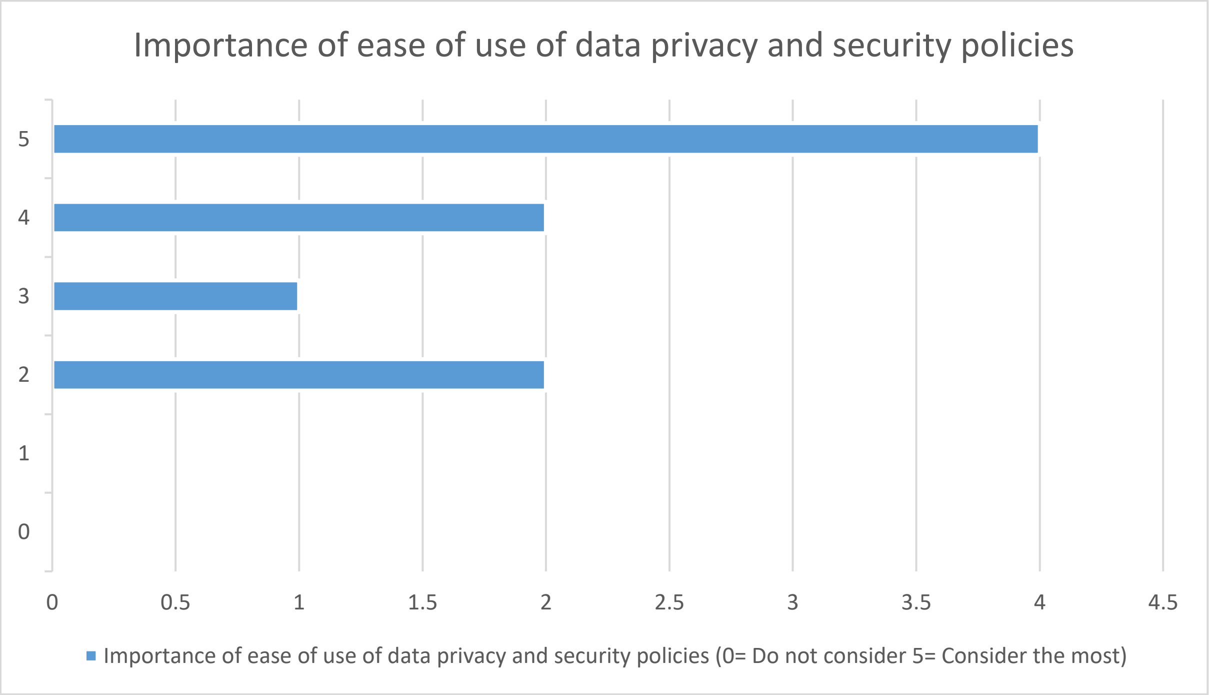


Figure D.317: Importance of ease of use of data privacy and security policies (Over 10)

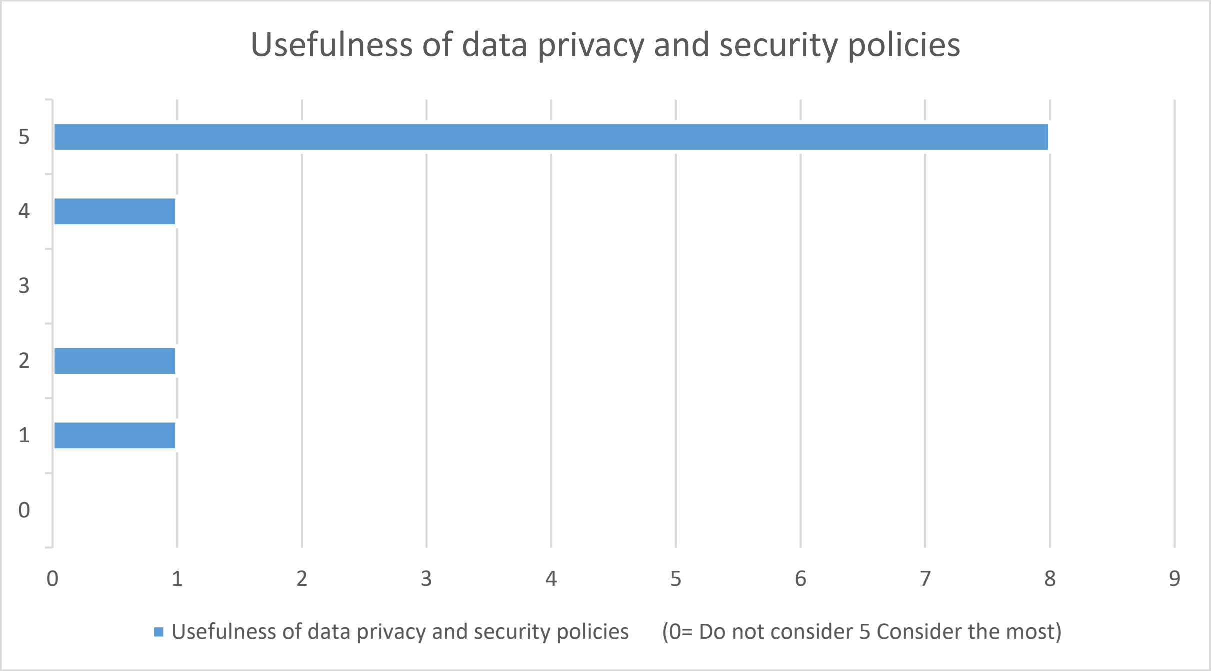


Figure D.318: Usefulness of data privacy and security policies (Over 10)

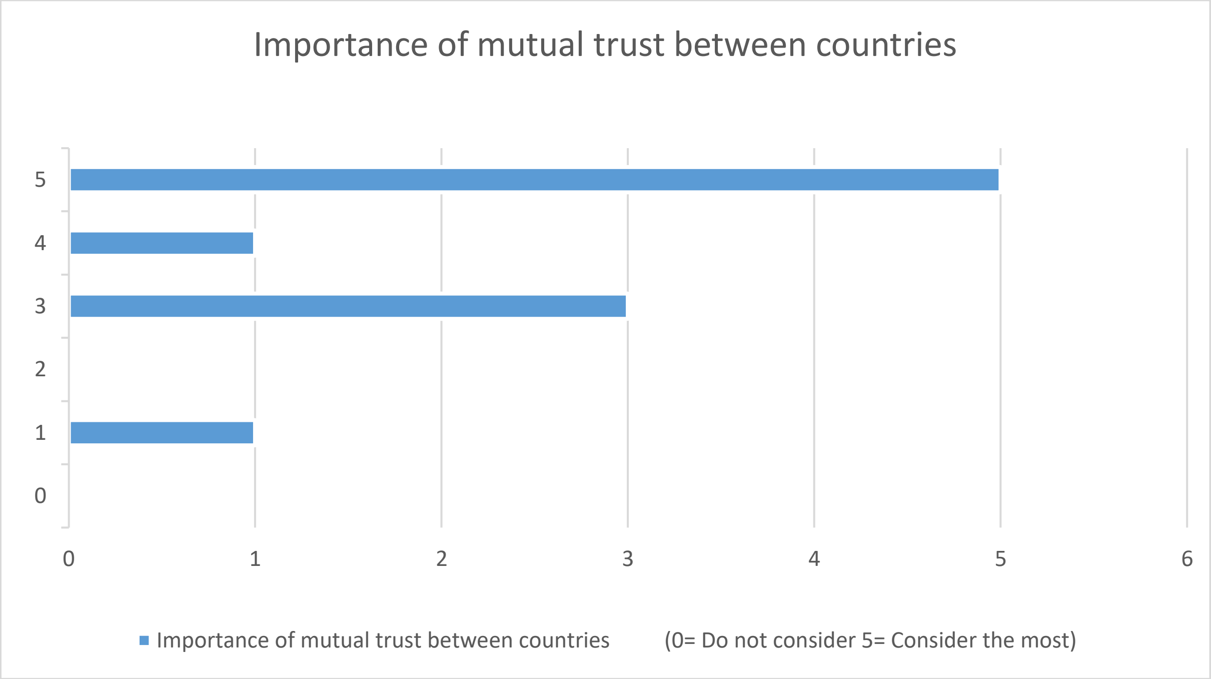


Figure D.319: Importance of mutual trust between countries (Over 10)

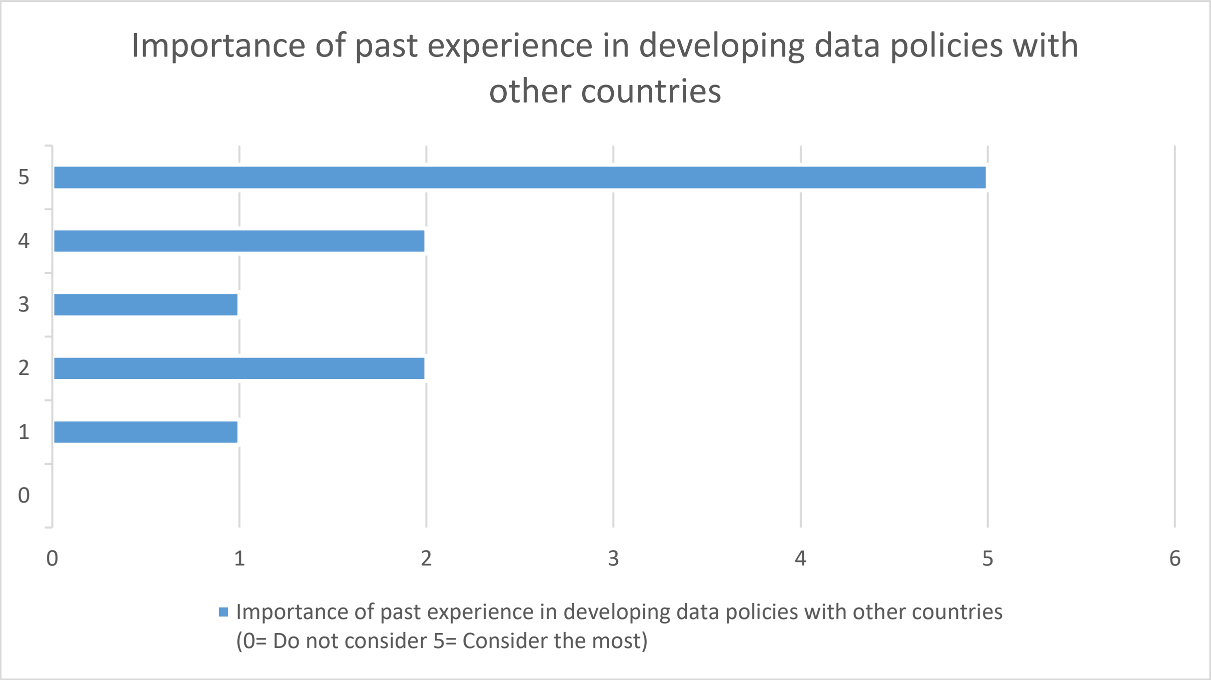


Figure D.320: Importance of past experience in developing data policies with other counties (Over 10)

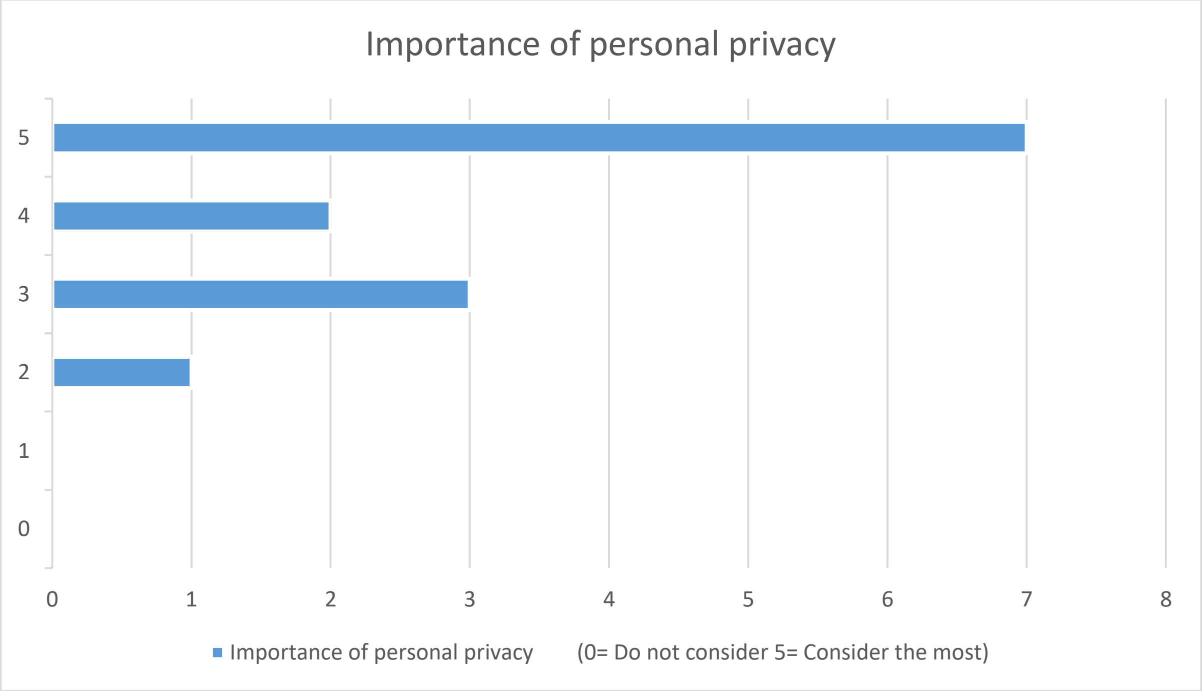


Figure D.321: Importance of personal privacy (Over 10)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 100 percent of the respondents have endorsed (See figure D.310). The other notable factors that have come out of the survey are organisational support, budget allocation for information security, social differences, economic differences, political differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure D.299-309) (See figure D.311-321). The respondents with less than 10 years in employment tend to agree that social (See figure D.312) and political difference (See figure D.314), also plays a key role in accepting and implementing policies. The interesting message coming out of this group is that those over the 26 years age range have gone through social and political changes, in comparison to those under 26 years age range. This observation emphasises the importance of social and political changes play in the policy development process.

Sri Lanka – Accountancy, Banking, Finance

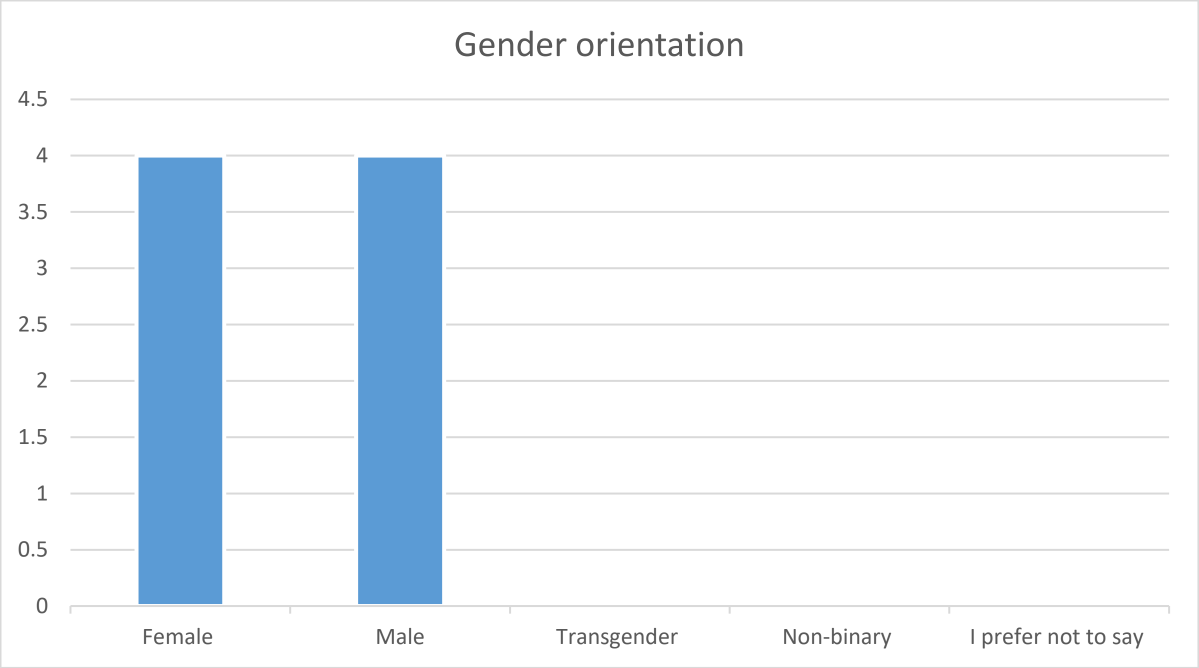


Figure D.322: Gender orientation (Accountancy, Banking, Finance)

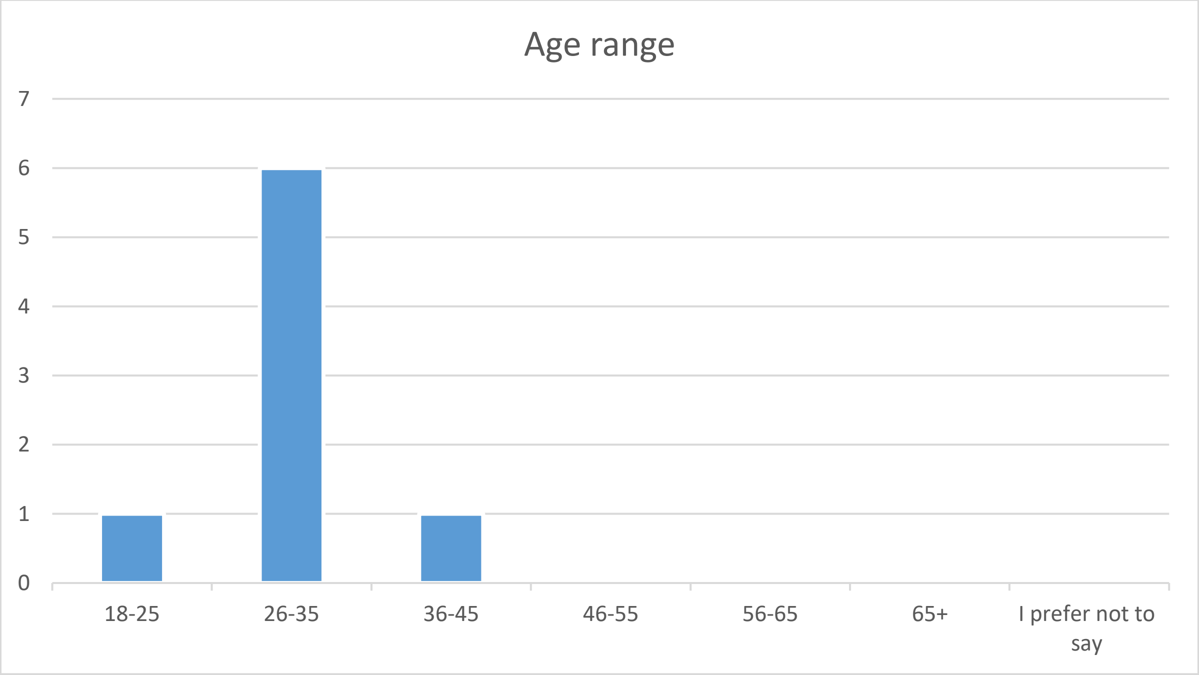


Figure D.323: Age range (Accountancy, Banking, Finance)

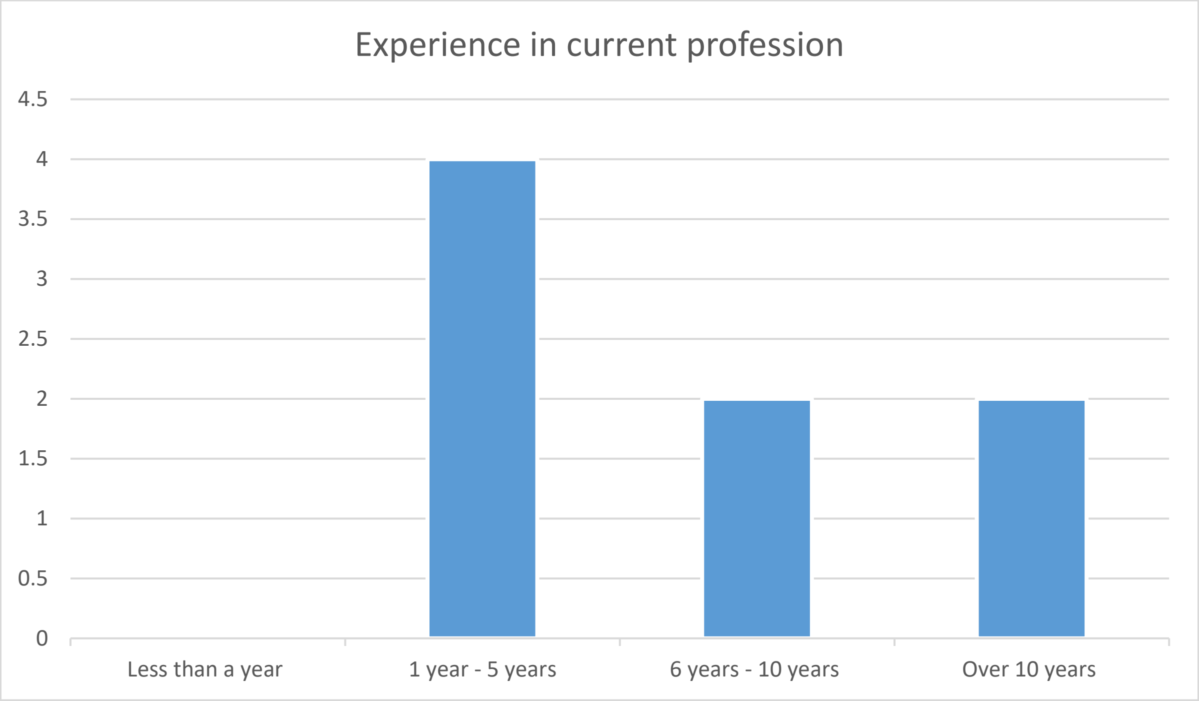


Figure D.324: Experience in current profession (Accountancy, Banking, Finance)

This analysis is based on the responses received from Sri Lankan participants employed in Accountancy, banking and finance industry. There were 8 participants and 4 out of them were males and 4 females (See figure D.322). They were within the 18-45 age range out of which 1 in the 18-25, 6 in the 26-35, and 1 in the 36-45 range (See figure D.323). The participants employed in industry between 1 and over 10 years (See figure D.324).

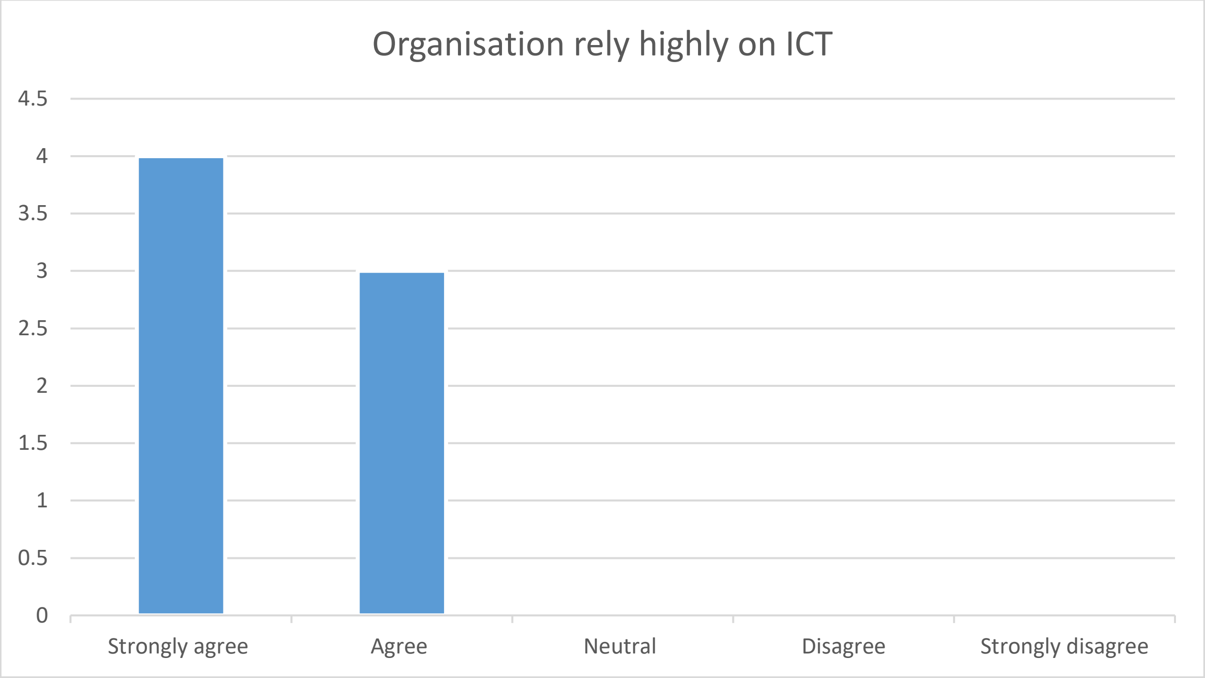


Figure D.325: Organisation rely highly on ICT (Accountancy, Banking, Finance)

Out of the 8 respondents, most importantly nobody has neither unaware of reliance on technology because of the nature of the work assigned to them, nor have marked 'disagree' on ICT (See figure D.325). This indicates a majority of those who have been working in this industry has had a high reliance on ICT.

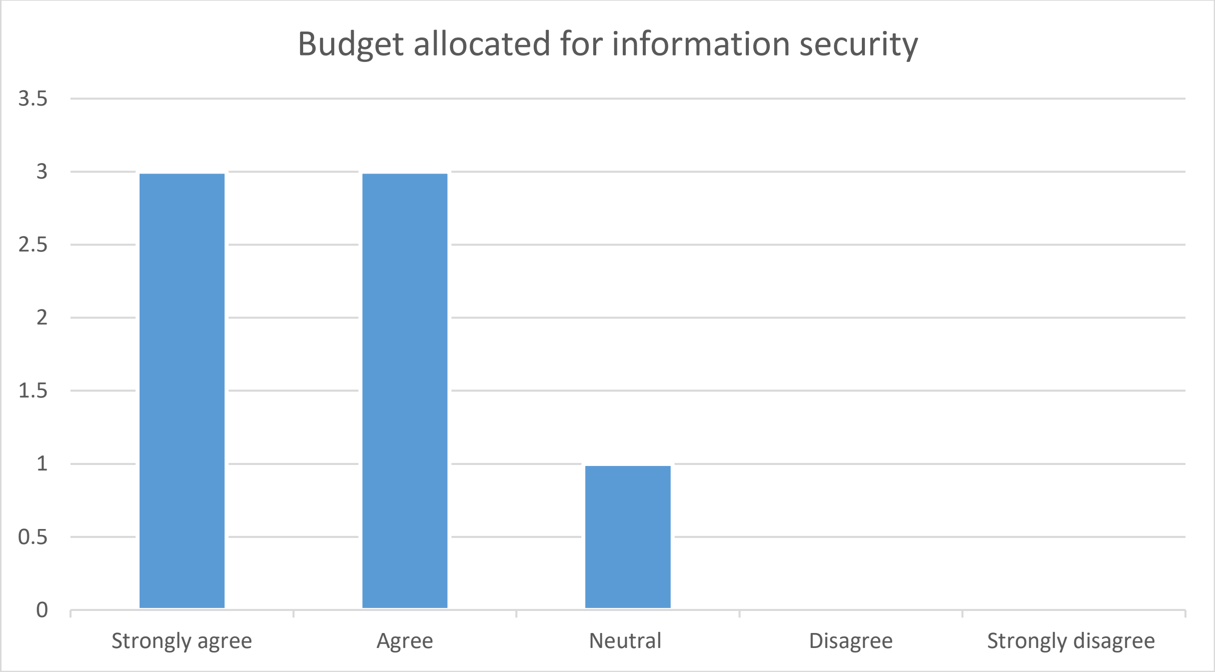


Figure D.326: Budget allocated for information security (Accountancy, Banking, Finance)

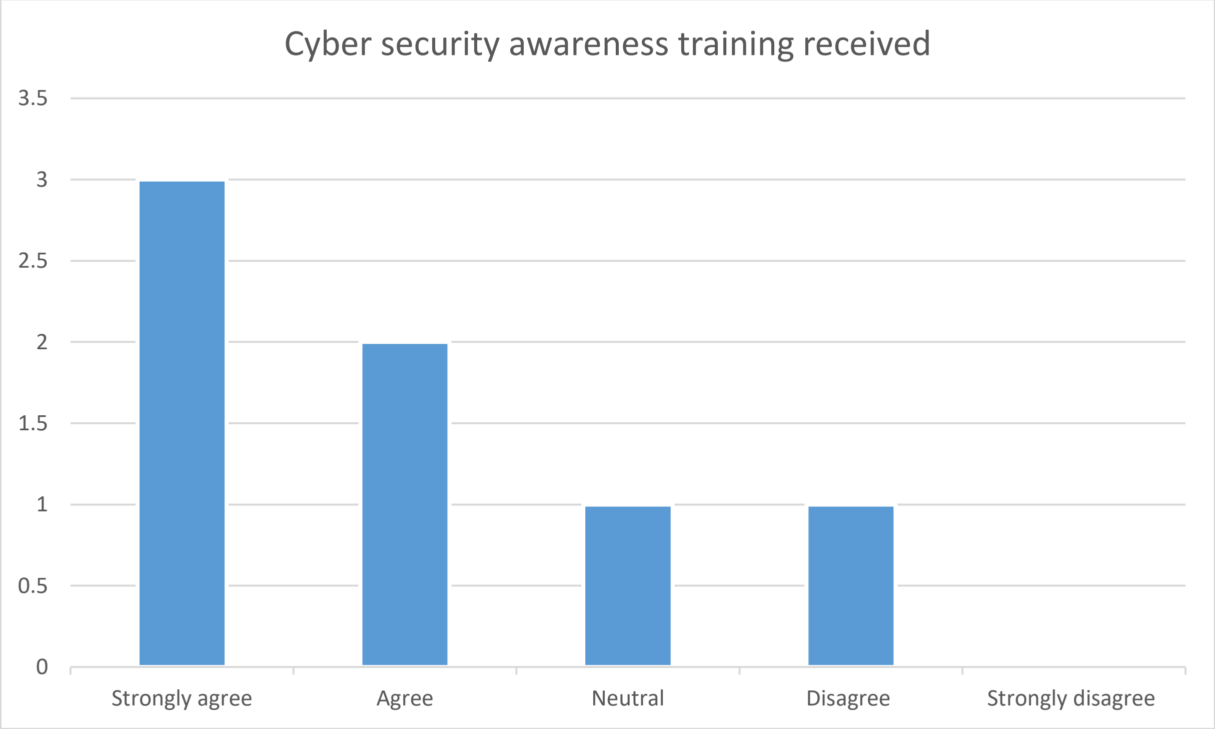


Figure D.327: Cyber security awareness training received (Accountancy, Banking, Finance)

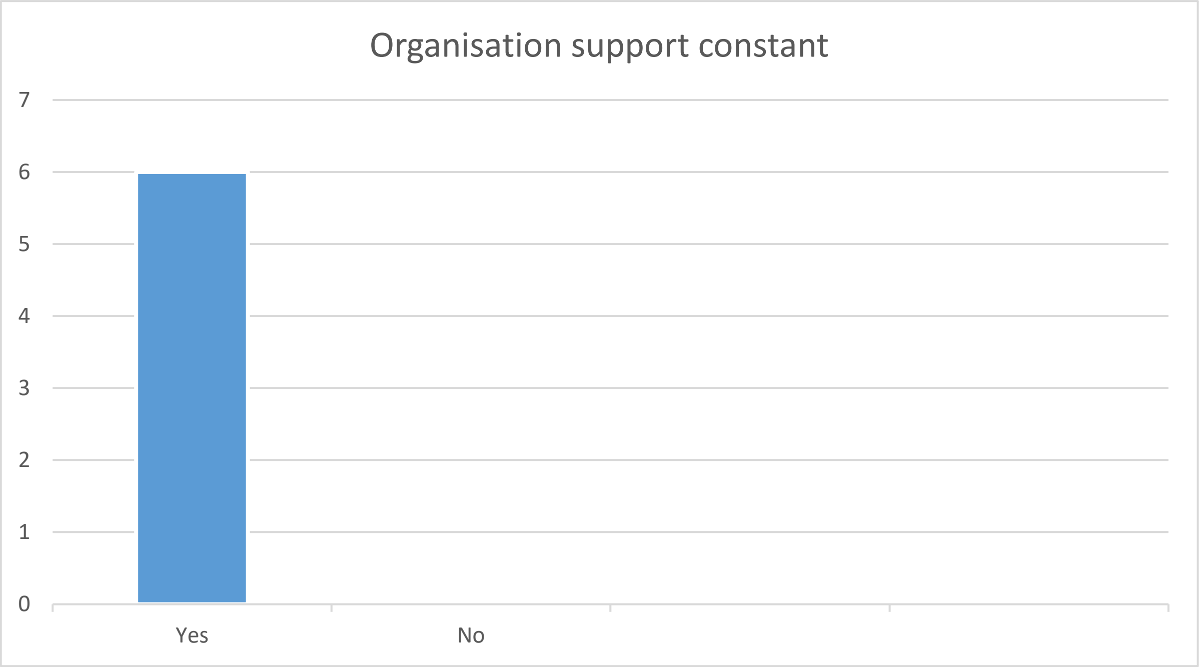


Figure D.328: Organisation support constant (Accountancy, Banking, Finance)

According to the 6 participants, their organisations had an allocated budget for information security (See figure D.326), and the regular security awareness training they received was adequate. 5 of them received regular cybersecurity awareness training, whilst 1 had not expressed an opinion either way and notably according to the 1 disagreed (See figure D.327). Also, 6 participants received support from the organisation to protect personal information (See figure D.328). This represents funding commitments of the accountancy, banking, and finance industry towards information security, provision of resources for regular security awareness training, and protection of personal information of the employees. These are organisations with high reliance on ICT, and clearly, they have invested in all essential areas involving technology to protect personal information and avoid potential privacy breaches.

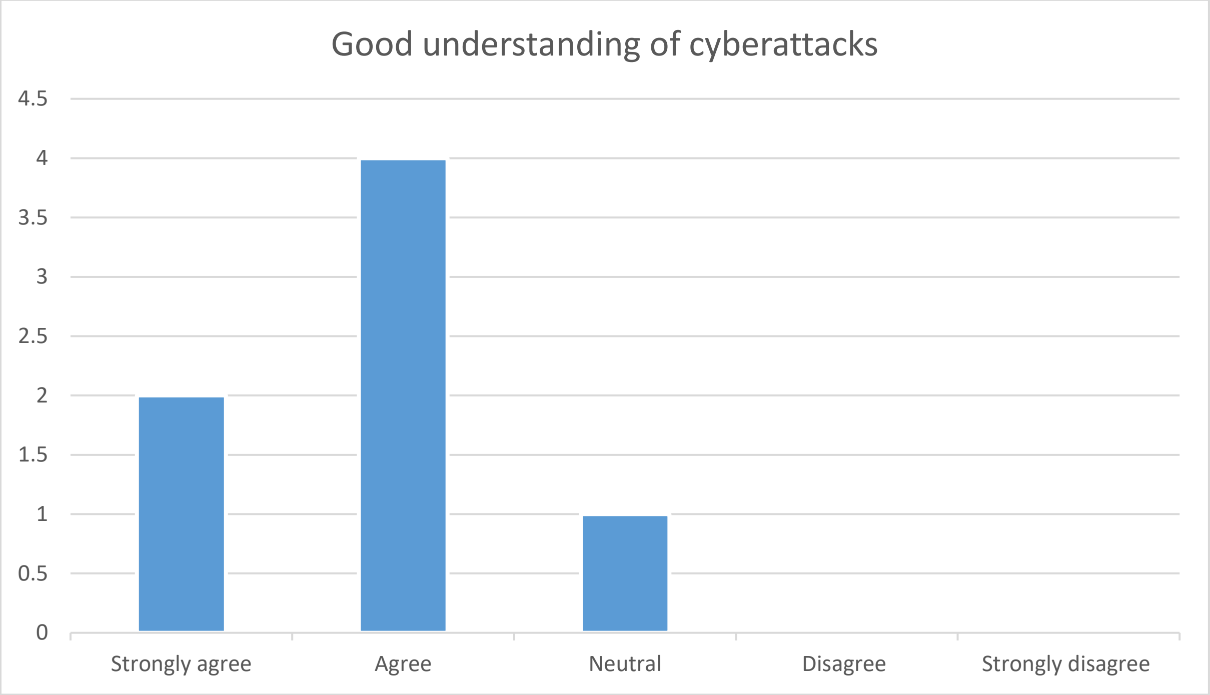


Figure D.329: Good understanding of cyberattacks (Accountancy, Banking, Finance)

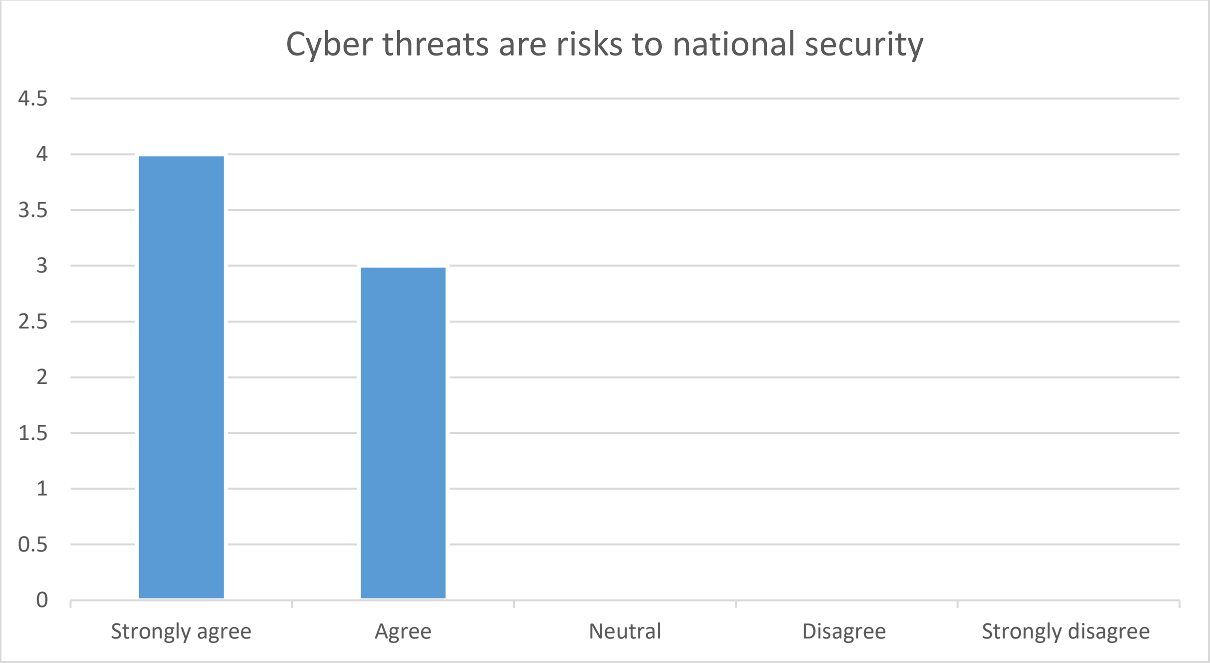


Figure D.330: Cyber threats are risks to national security (Accountancy, Banking, Finance)

Also, the figures show that 6 of the participants have a high understanding of the impact of cyber-attacks on the public and the organisation, with 1 remained not committing either away (See figure D.329). 7 of the participants also realises the potential threats to national security from cyber-attacks (See figure D.330). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and they will be in a strong position to influence the acceptance and implementation of a national, regional, and global level mechanism.

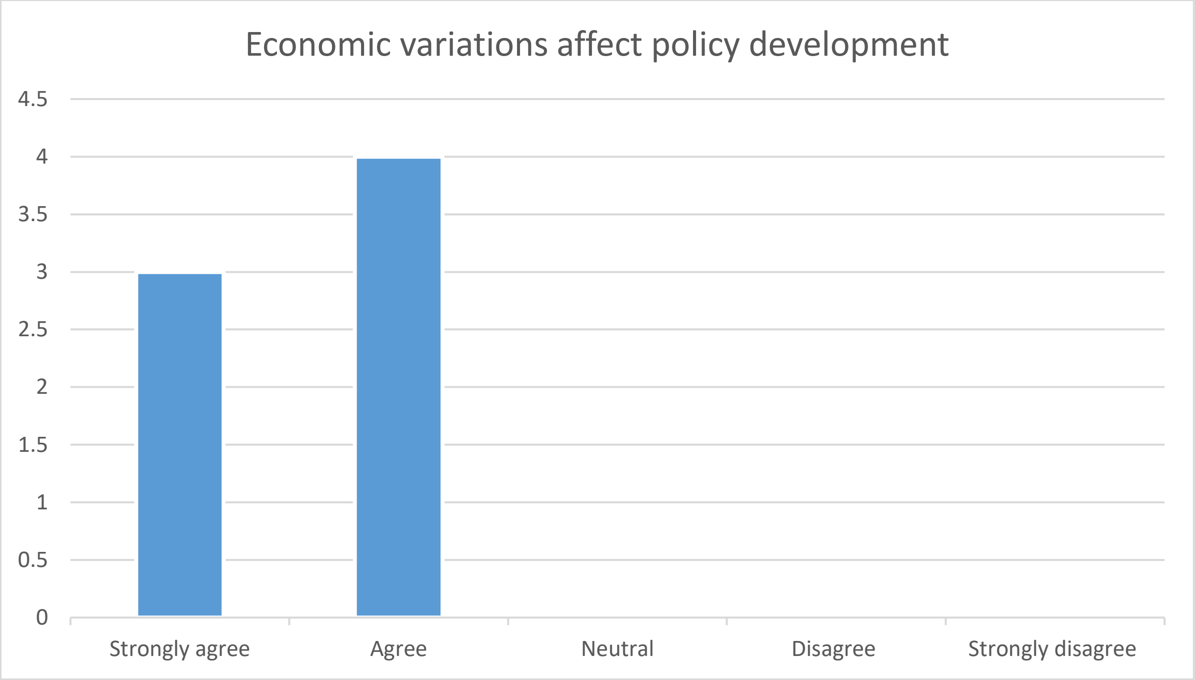


Figure D.331: Economic variations affect policy development (Accountancy, Banking, Finance)

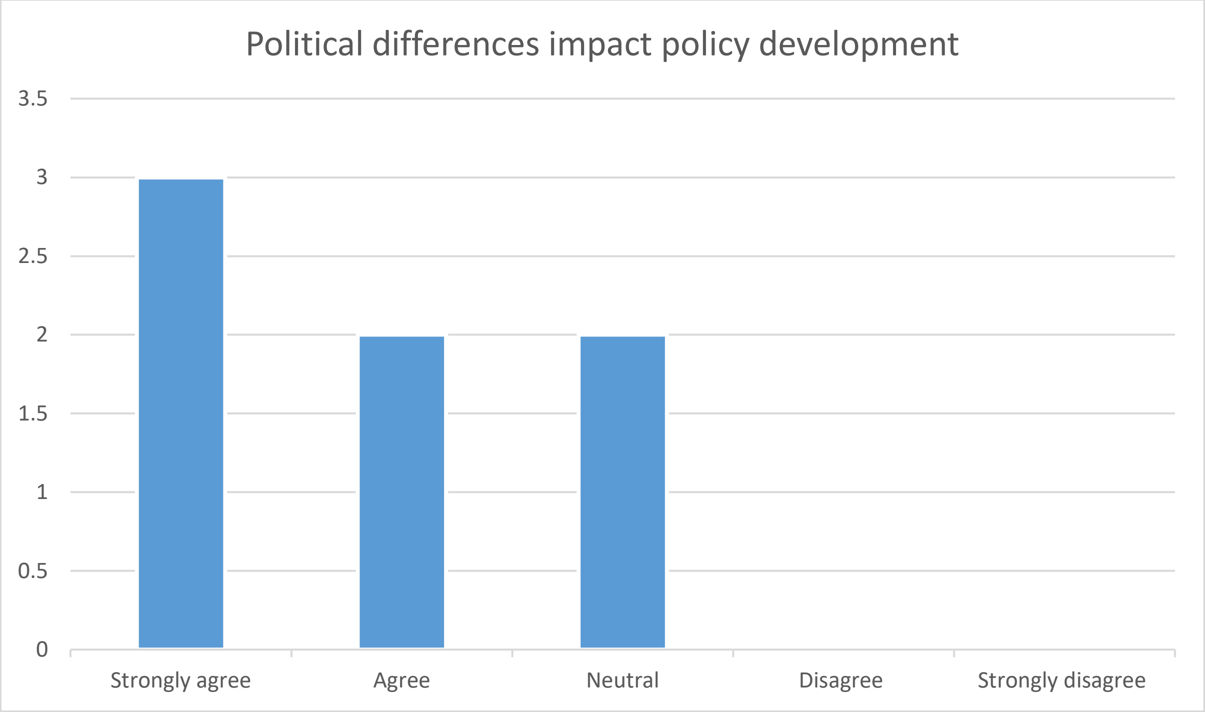


Figure D.332: Political differences impact policy development (Accountancy, Banking, Finance)

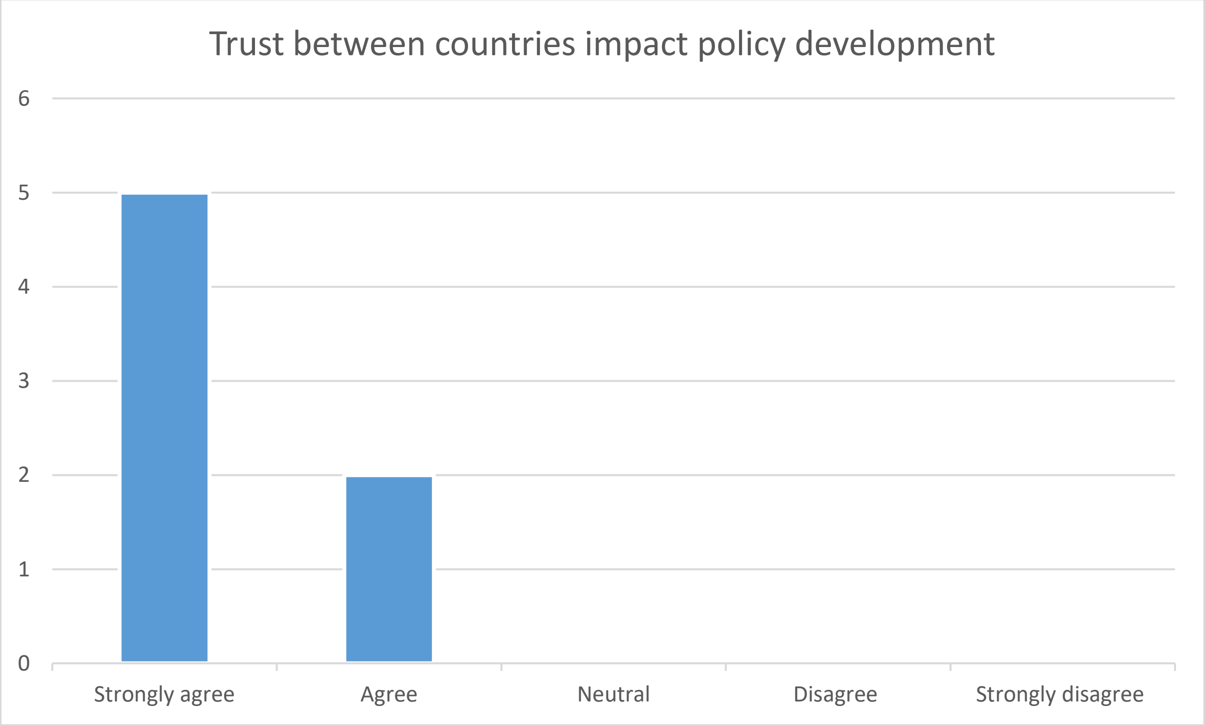


Figure D.333: Trust between countries impact policy development (Accountancy, Banking, Finance)

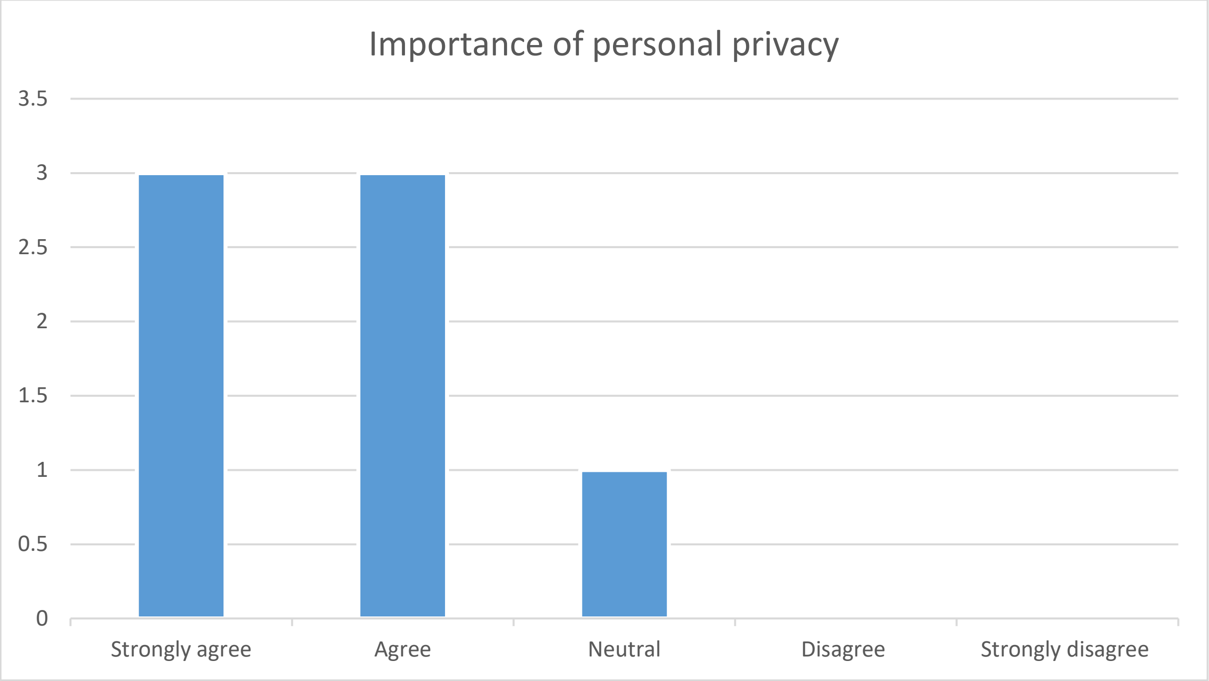


Figure D.334: Importance of personal privacy (Accountancy, Banking, Finance)

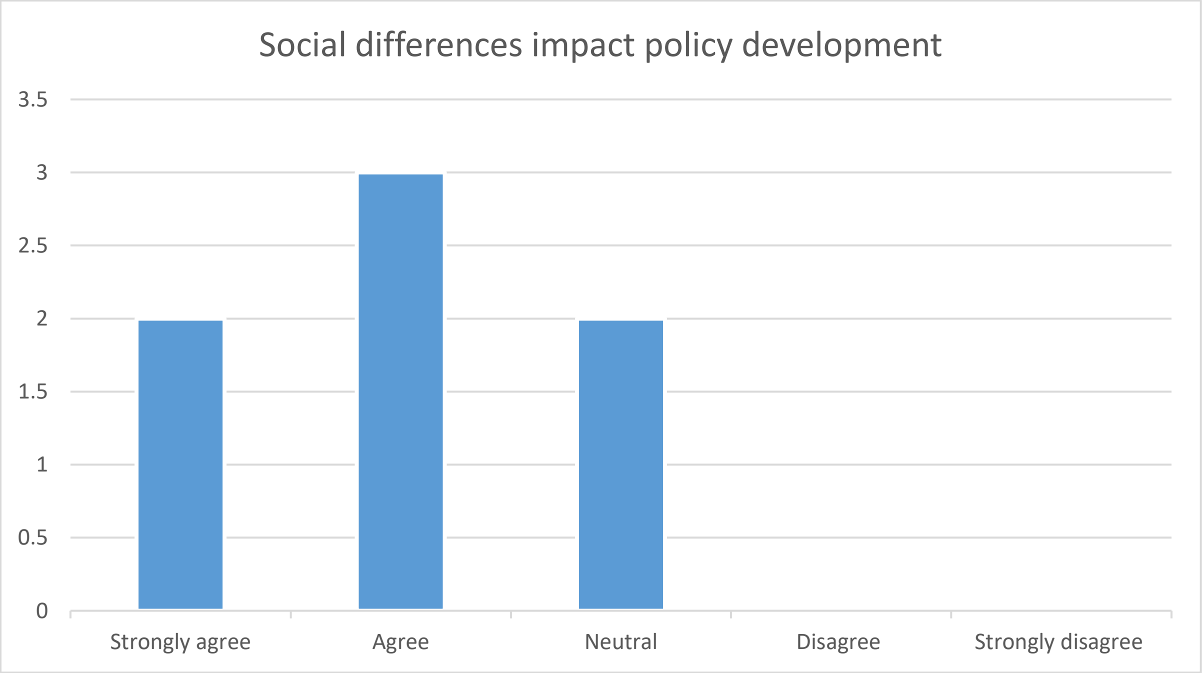


Figure D.335: Social differences impact policy development (Accountancy, Banking, Finance)

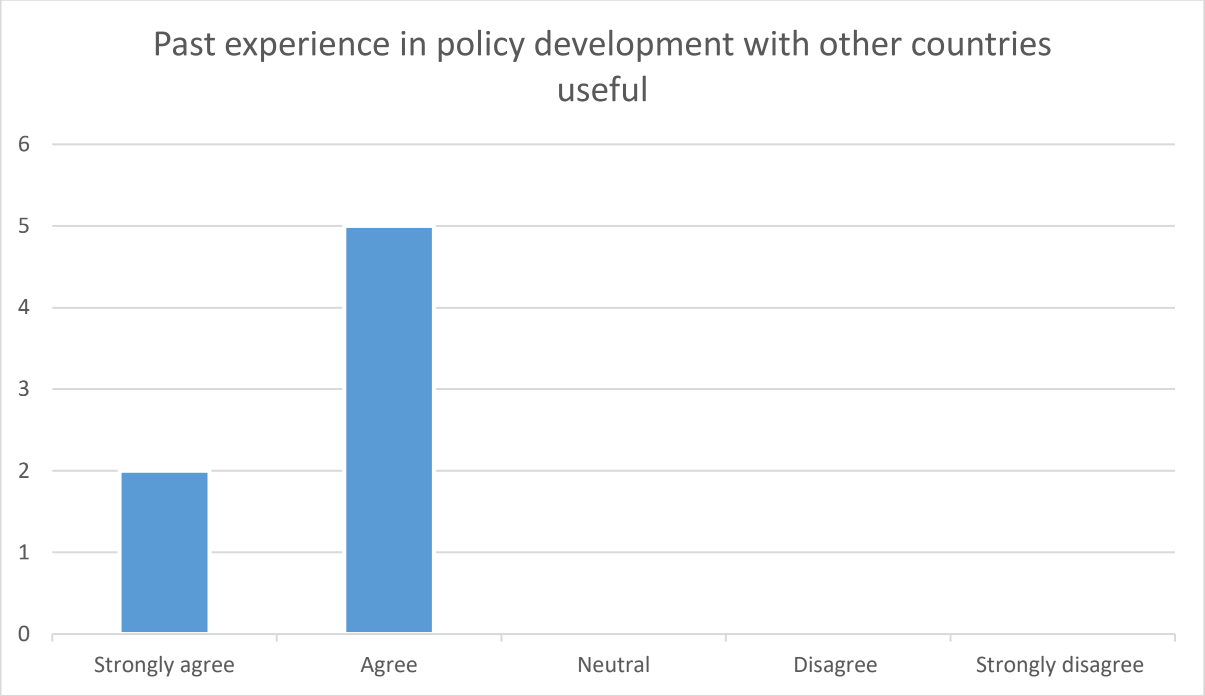


Figure D.336: Past experience in policy development with other countries useful (Accountancy, Banking, Finance)

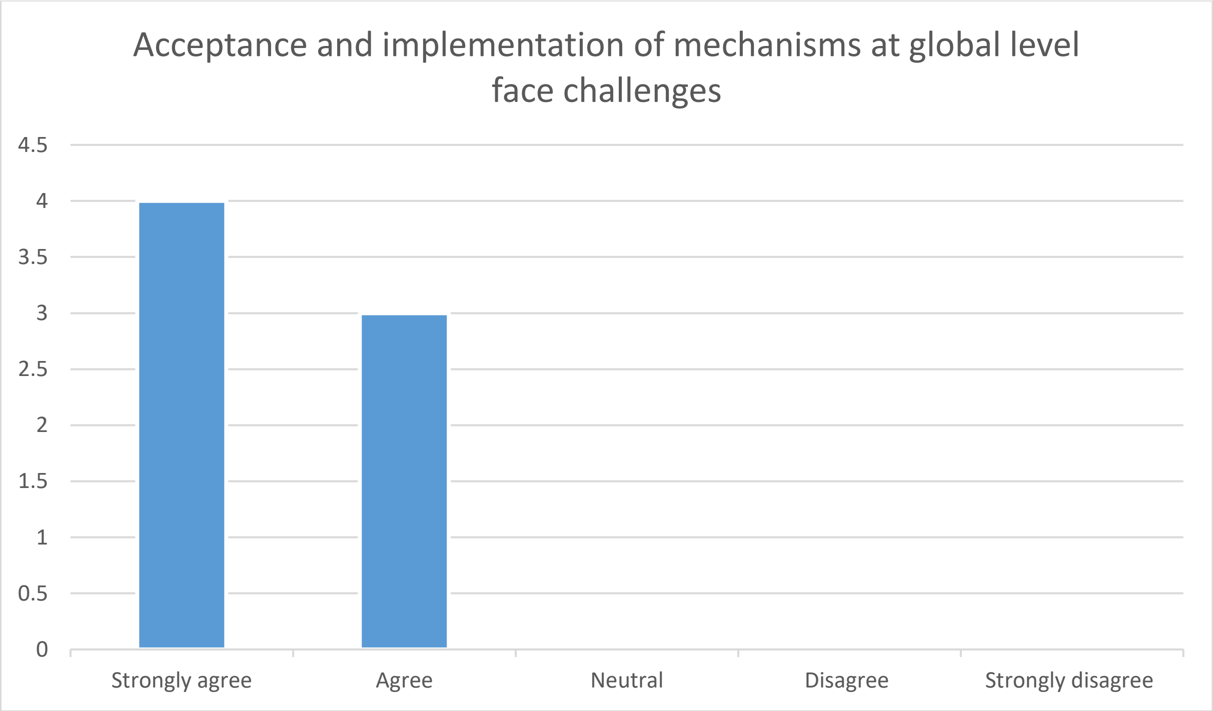


Figure D.337: Acceptance and implementation of mechanisms at global level face challenges (Accountancy, Banking, Finance)

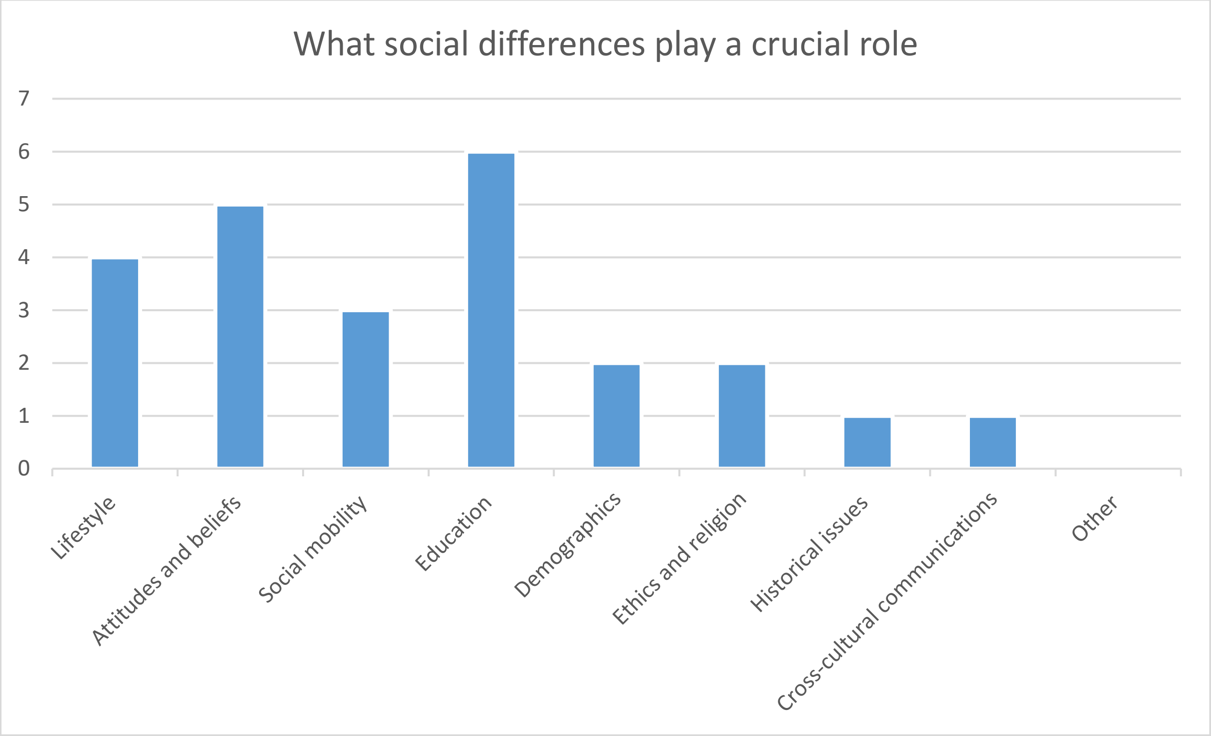


Figure D.338: What social differences play a crucial role (Accountancy, Banking, Finance)

On the question of social differences, the majority flag up the importance of education, lifestyle and attitude and beliefs (See figure D.338). This implies that through educational training, people can be made to understand the importance of privacy and the consequences of privacy violations. In a high reliance technology environment, the sharing or handling of personal information, data privacy and security, are normal occurrences, and it is of utmost importance that employees in such a workplace, have a responsibility to become conversant with risks and threats to them and the organisations. The survey feedback emphasises the importance of knowledge and awareness of potential cyber threats, and their impact on people and national security when accepting and implementing data privacy and security policies. Therefore, the delivery of cybersecurity awareness training at schools and at the organisational level is of utmost importance. In that context, familiarity with potential cyber threats, their impact on people and national security will be crucial in accepting and implementing data privacy and security policies. Therefore, the case for providing cybersecurity awareness training to the employees, at schools and at the organisational level is of utmost importance. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

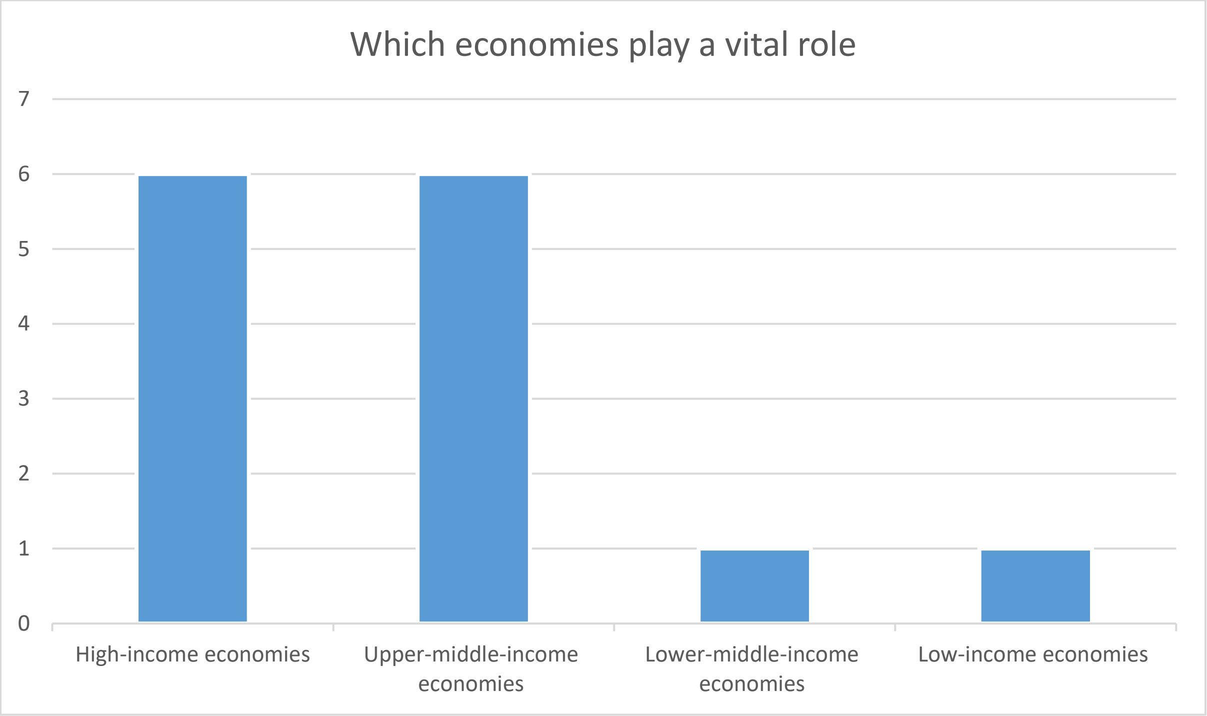


Figure D.339: Which economies play a vital role (Accountancy, Banking, Finance)

The respondents suggest that high income and upper-middle-income countries are well placed to influence the policymaking process (See figure D.339). The key stages in the policymaking process aim to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the resources necessary, implement, and finally evaluate the policy. These stages are time-consuming and require sufficient funding and resources. Therefore, achieving success to a large extent depends on the economic stability of the country, which counts as a crucial factor in policymaking.

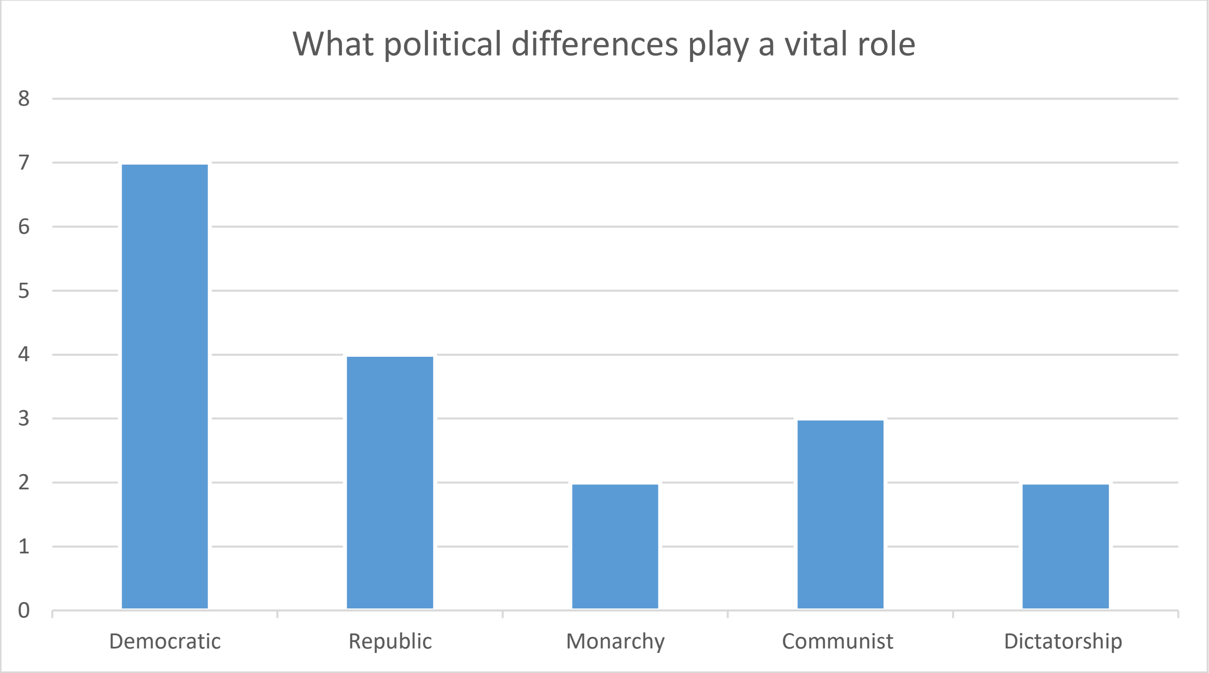


Figure D.340: What political differences play a vital role (Accountancy, Banking, Finance)

Interestingly, those who have been in industry favour both democratic and republic political system, in preference to others (See figure D.340). This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

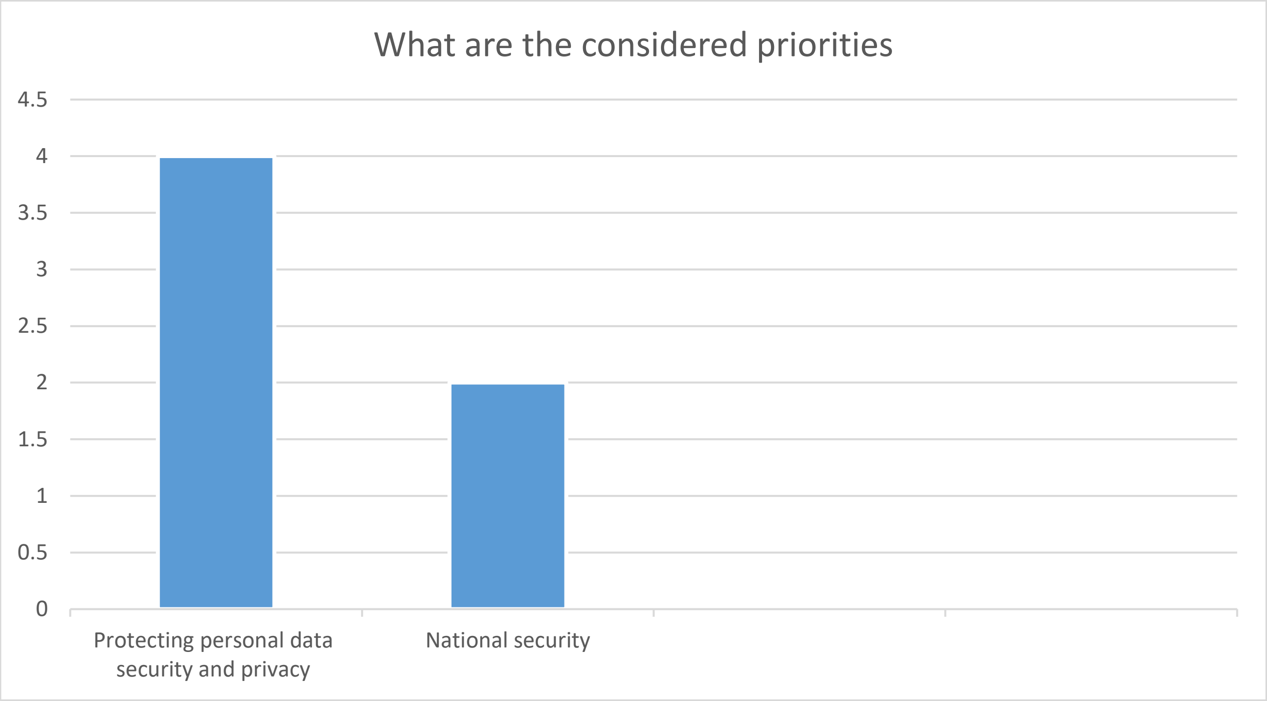


Figure D.341: What are the considered priorities (Accountancy, Banking, Finance)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security, which is a significant factor (See figure D.341). However, in an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

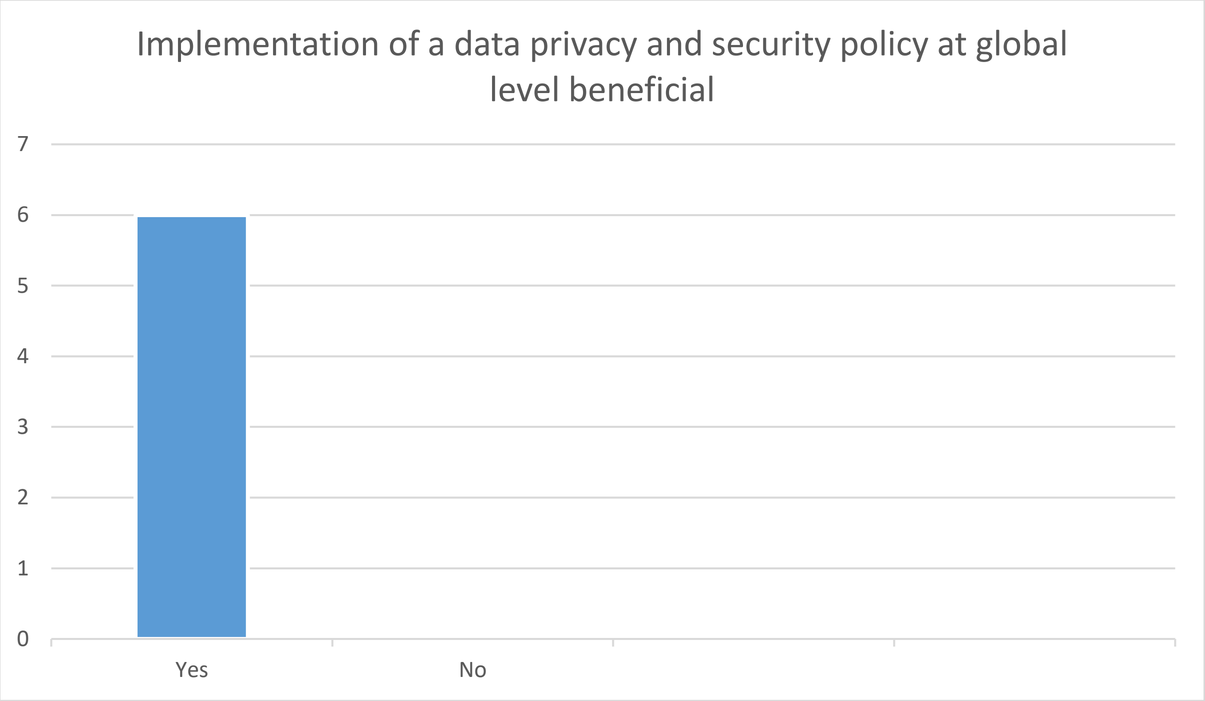


Figure D.342: Implementation of a data privacy and security policy at global level beneficial (Accountancy, Banking, Finance)

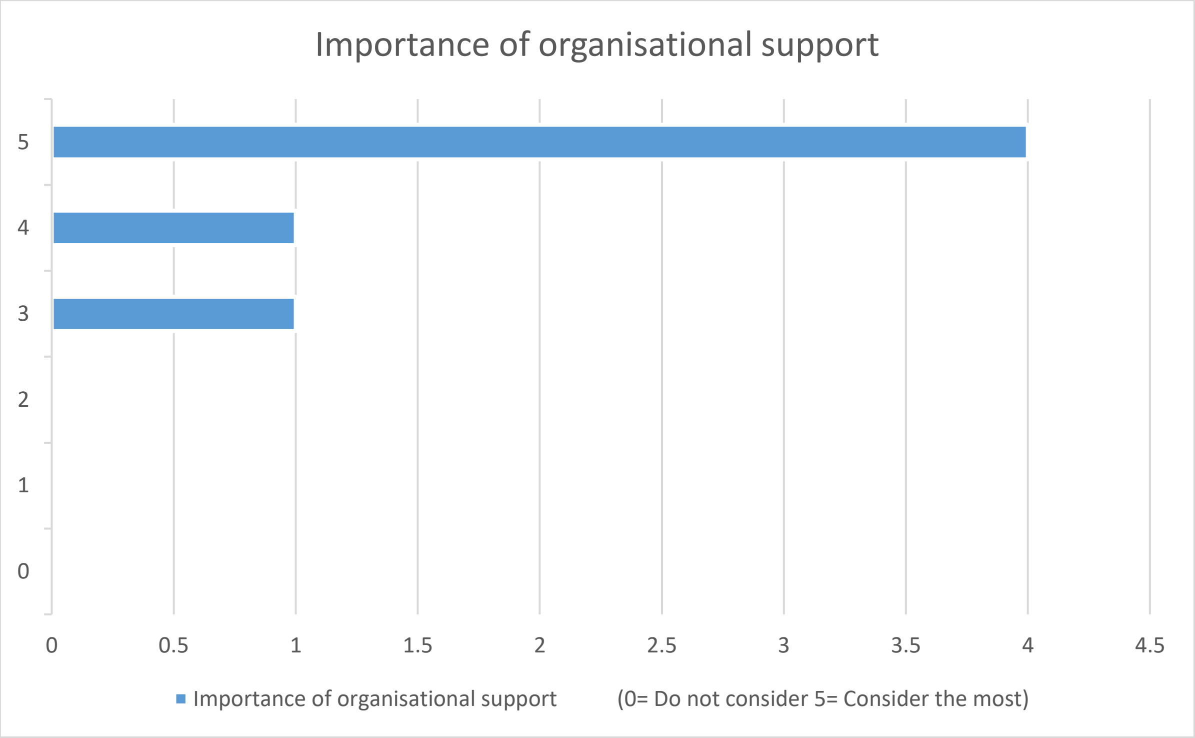


Figure D.343: Importance of organisational support (Accountancy, Banking, Finance)

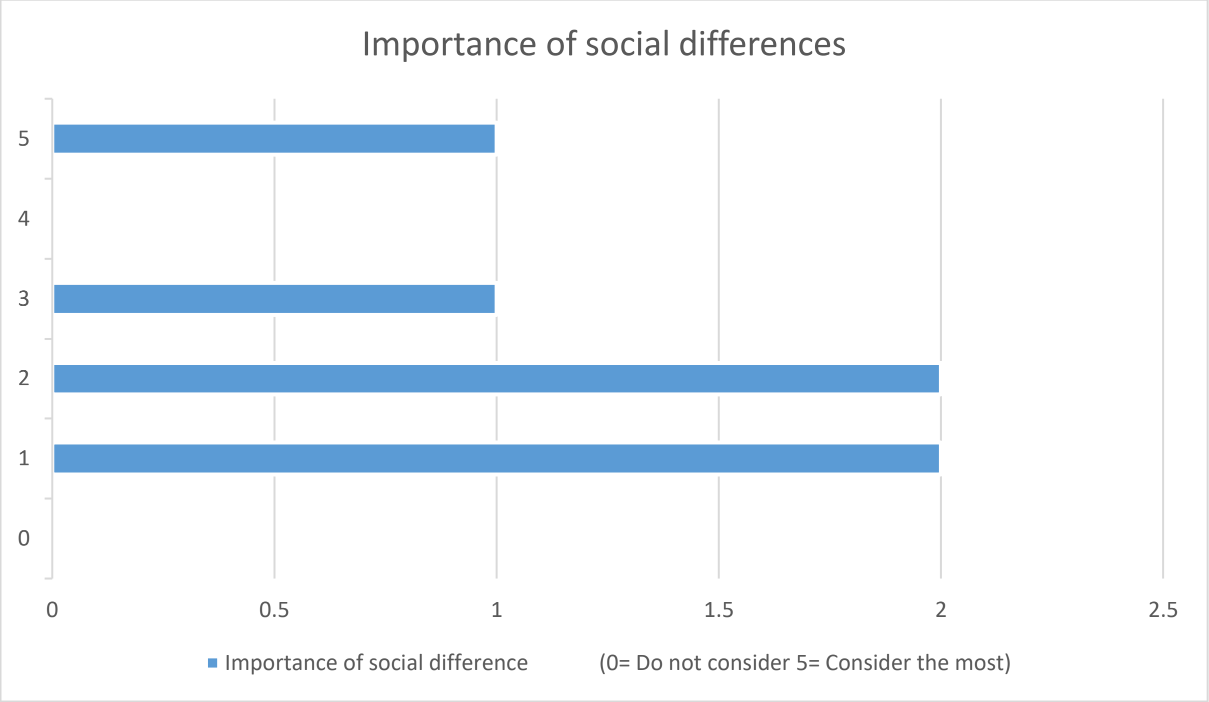


Figure D.344: Importance of social differences (Accountancy, Banking, Finance)

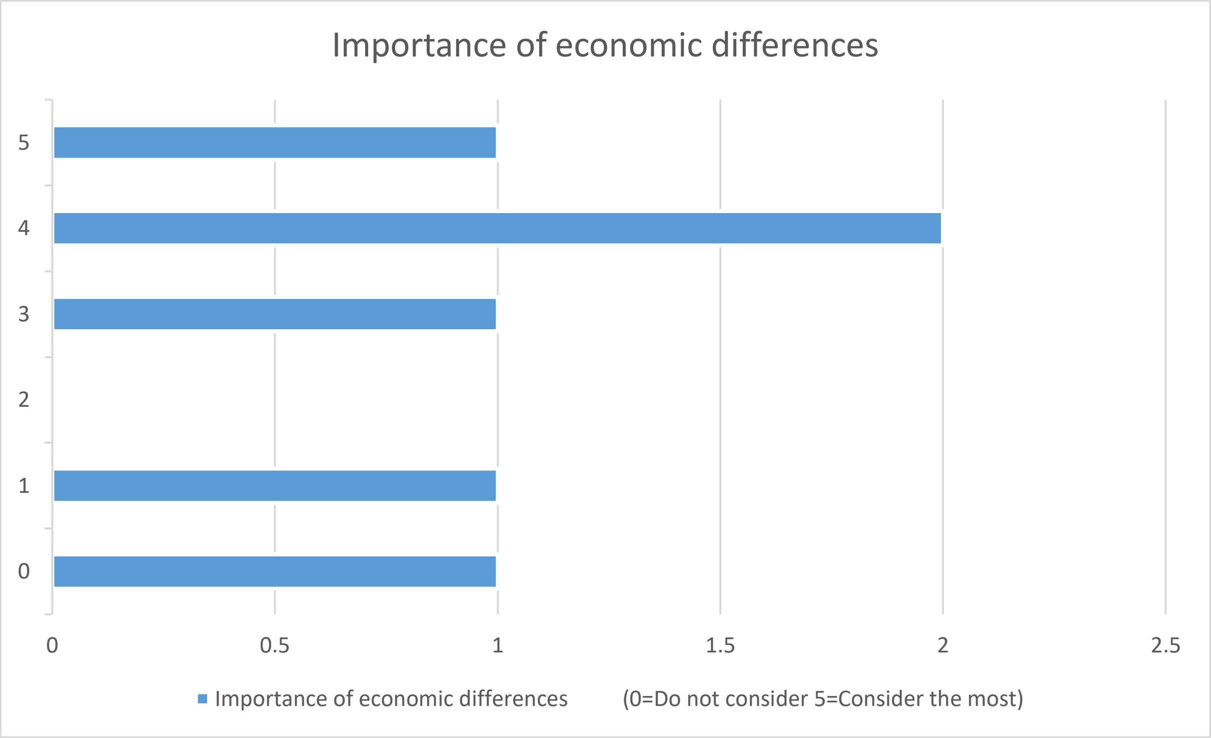


Figure D.345: Importance of economic differences (Accountancy, Banking, Finance)

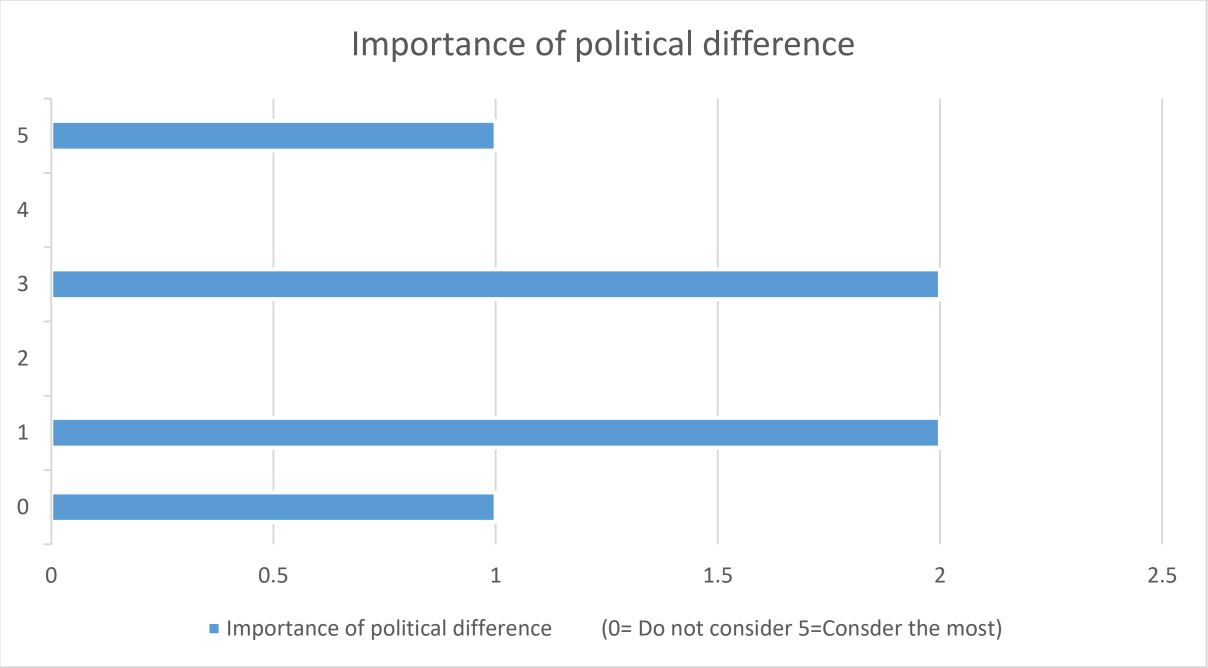


Figure D.346: Importance of political difference (Accountancy, Banking, Finance)

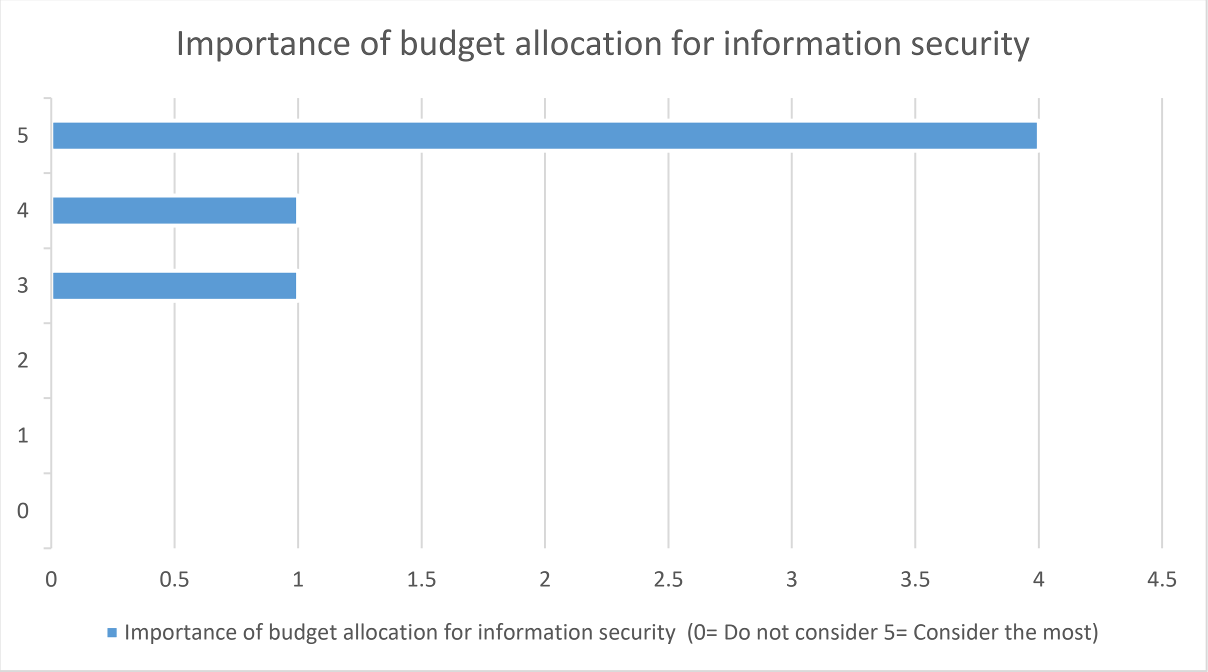


Figure D.347: Importance of budget allocation for information security (Accountancy, Banking, Finance)

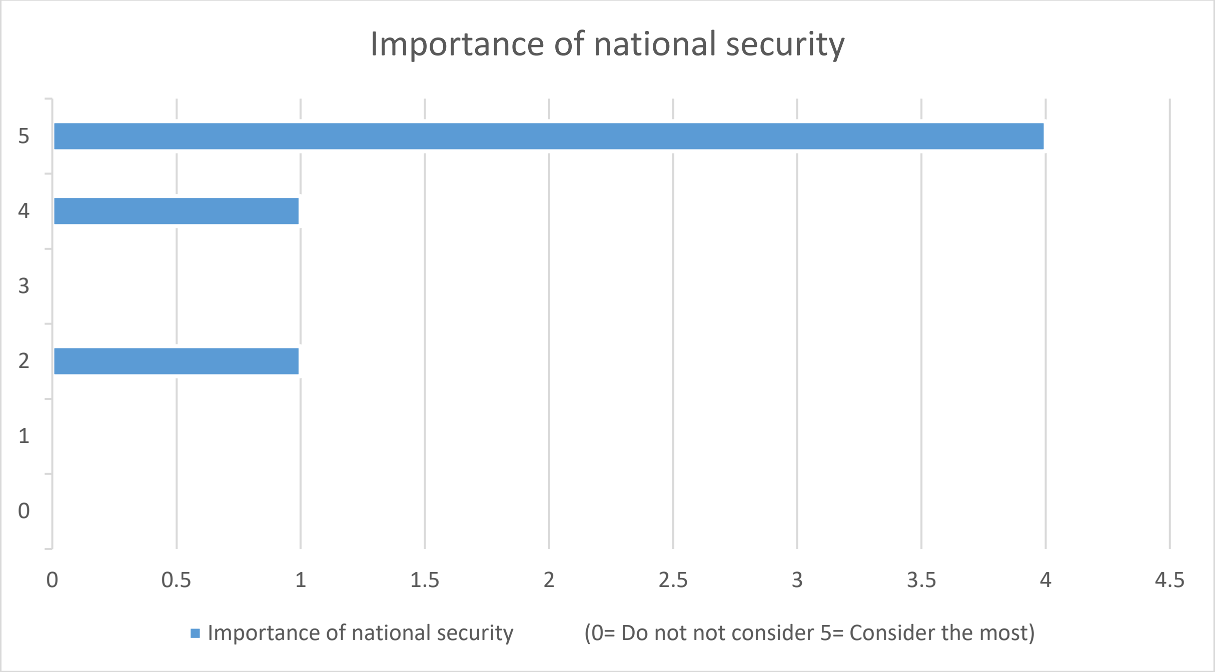


Figure D.348: Importance of national security (Accountancy, Banking, Finance)

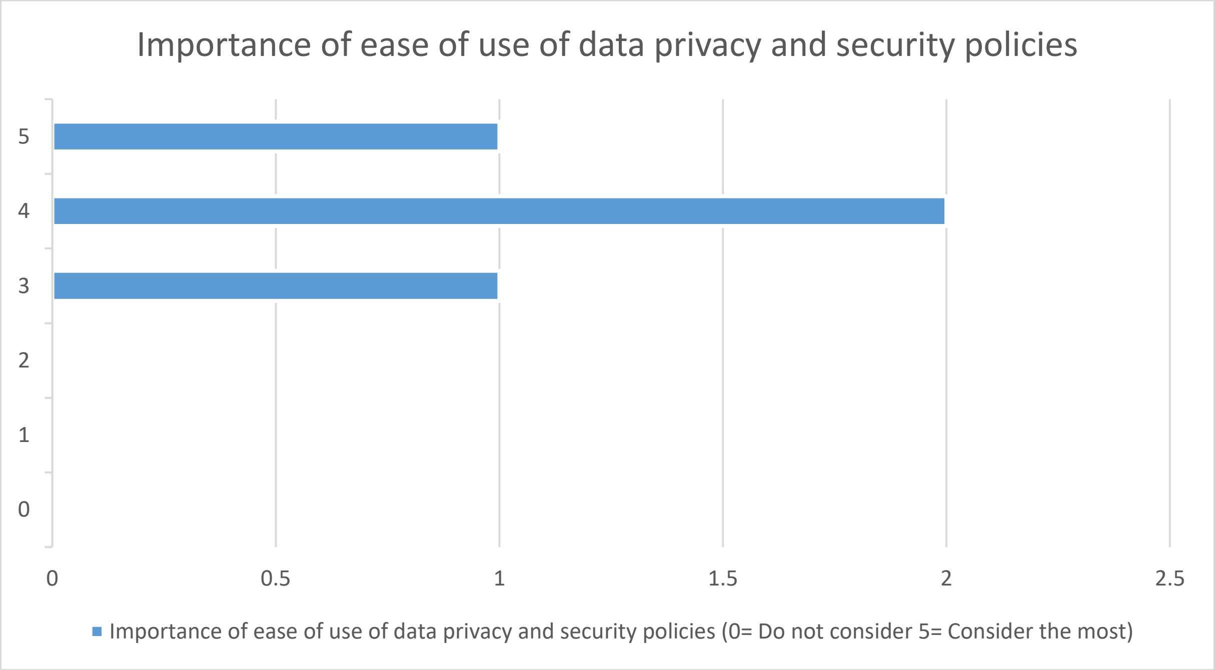


Figure D.349: Importance of ease of use of data privacy and security policies (Accountancy, Banking, Finance)

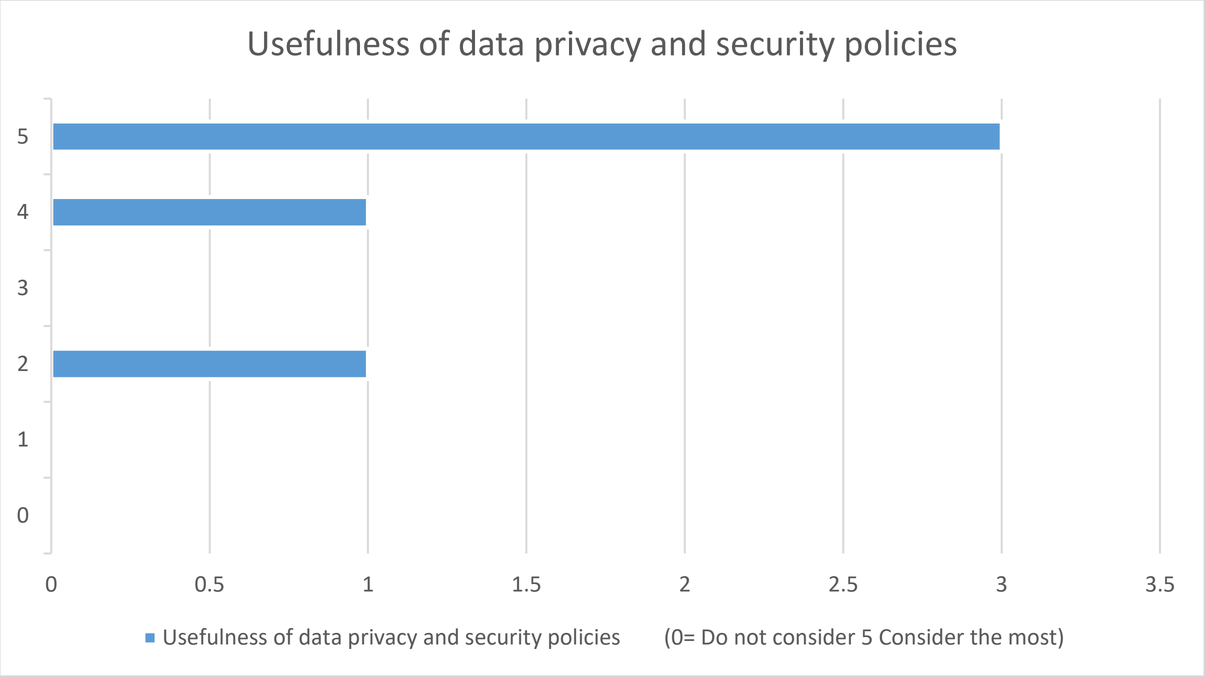


Figure D.350: Usefulness of data privacy and security policies (Accountancy, Banking, Finance)

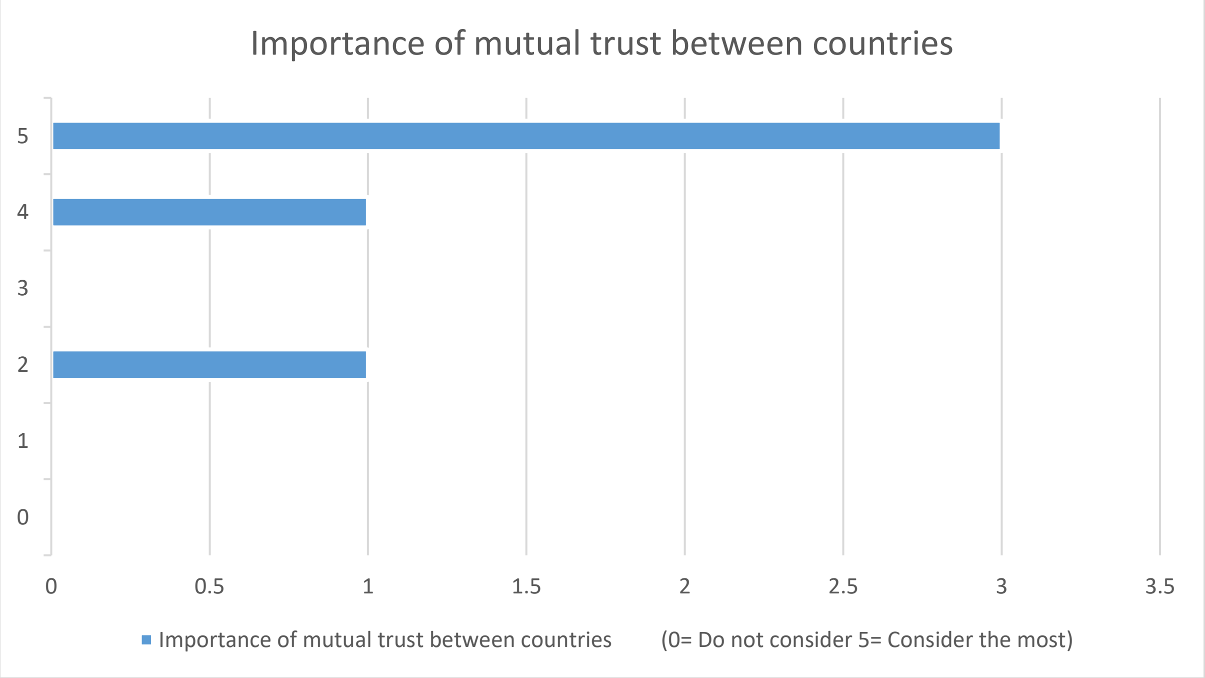


Figure D.351: Importance of mutual trust between countries (Accountancy, Banking, Finance)

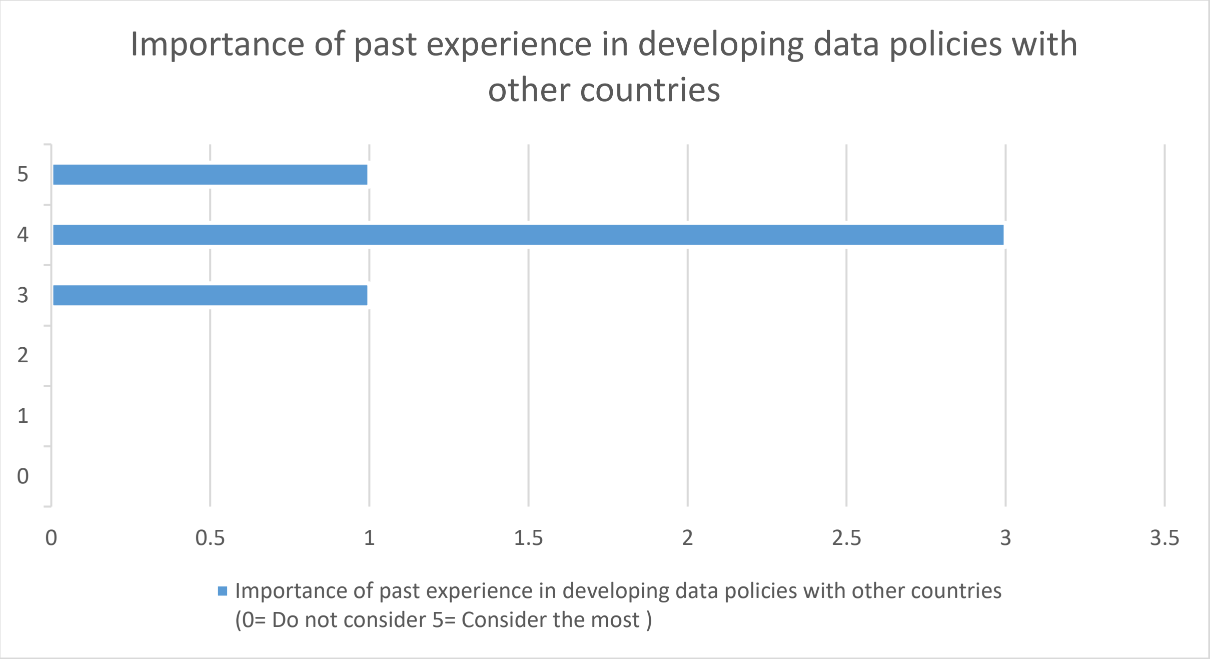


Figure D.352: Importance of past experience in developing data policies with other counties (Accountancy, Banking, Finance)

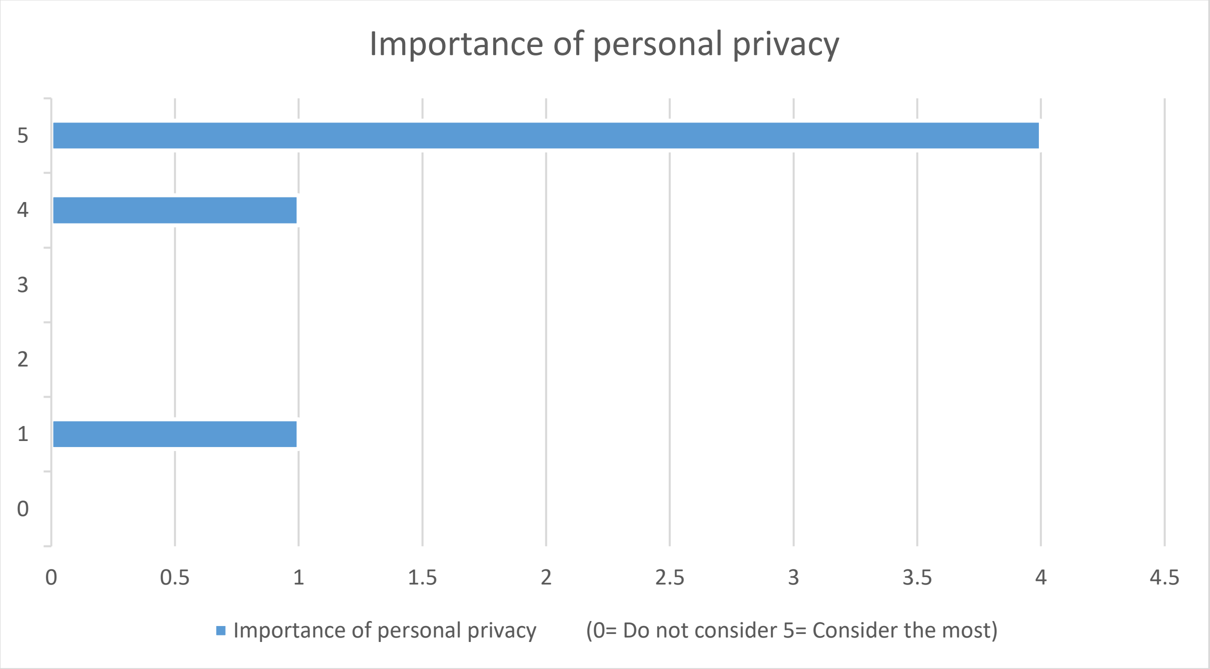


Figure D.353: Importance of personal privacy (Accountancy, Banking, Finance)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 75 percent of the respondents have endorsed (See figure D.342). The other notable factors that have come out of the survey are organisational support, budget allocation for information security, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between countries, previous experience with other countries in developing policies (See figure D.331-341) (See figure D.343-353). It is interesting to note that employees in commerce give less consideration to economical differences (See figure D.345).

Sri Lanka – Business, consultancy and management

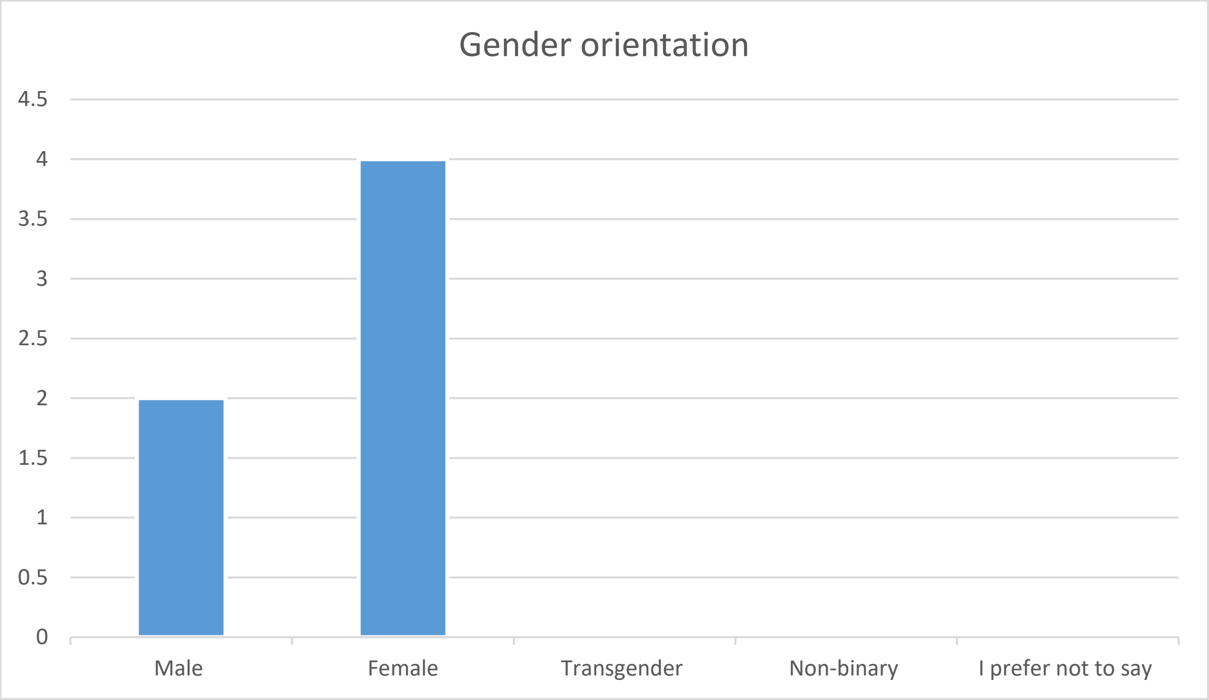


Figure D.354: Gender orientation (Business, consultancy and management)

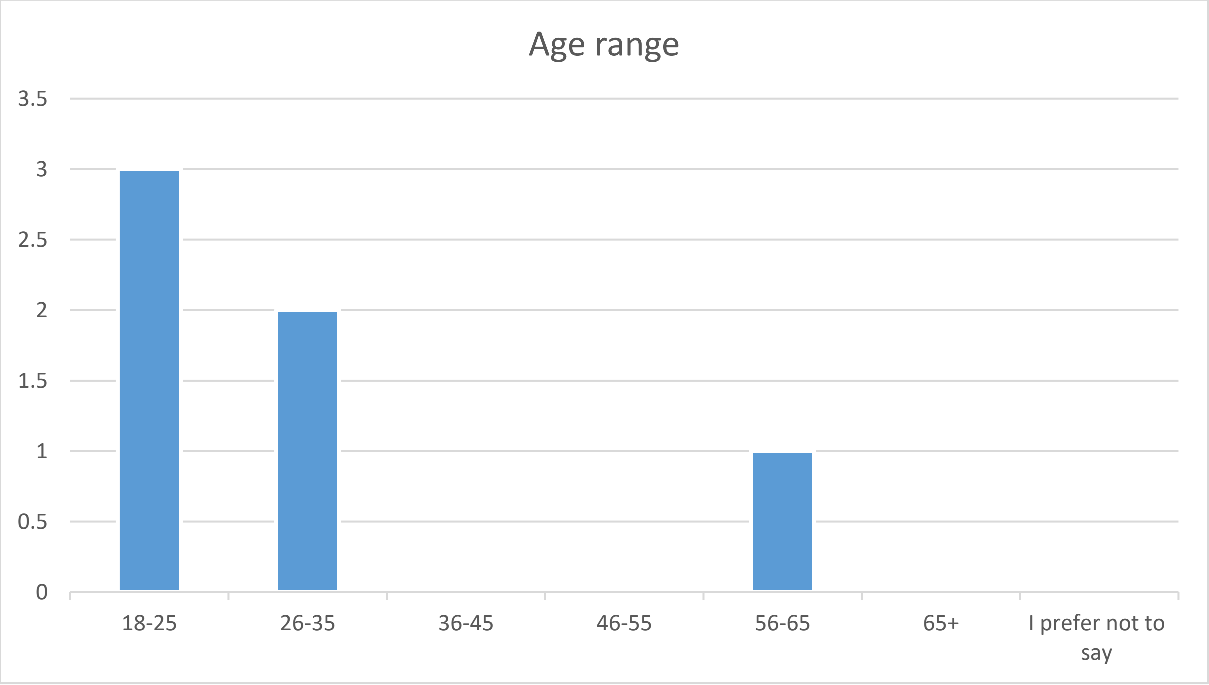


Figure D.355: Age range (Business, consultancy and management)

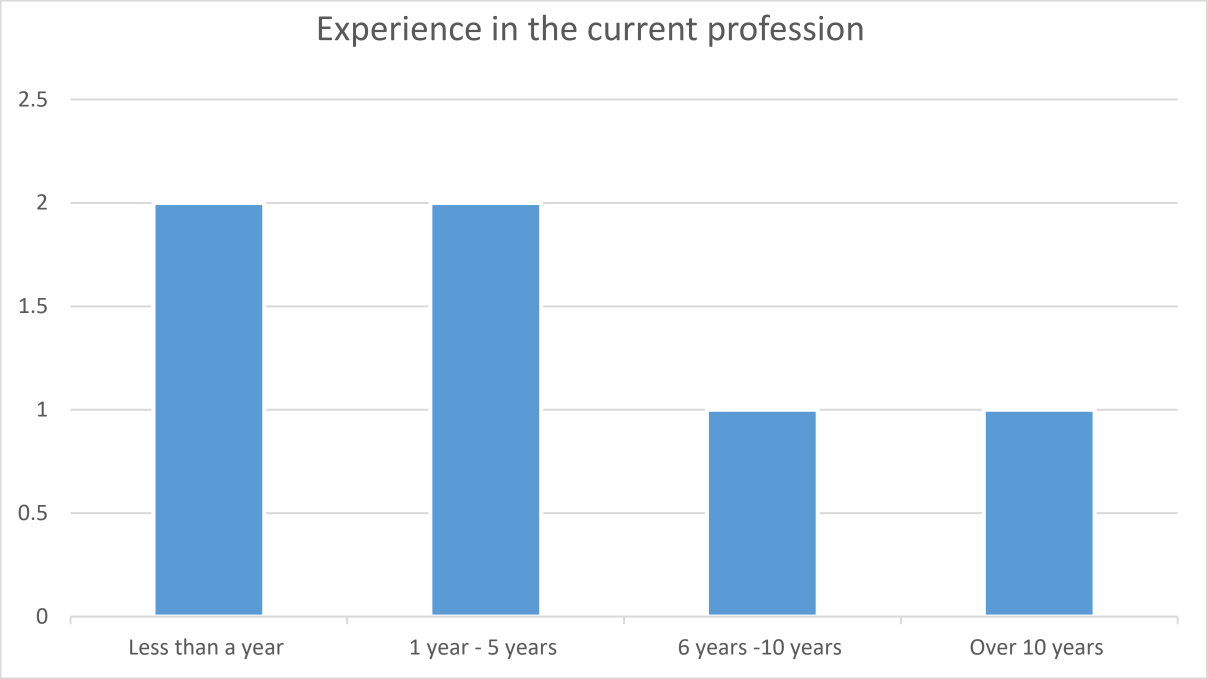


Figure D.356: Experience in current profession (Business, consultancy and management)

This analysis is based on the responses received from Sri Lankan participants employed in the business, consultancy, and management sector. 6 participants comprising 2 males and 4 females (See figure D.354), between 18-65 age range, in groups of 3 in 18-25, 2 in 26-35, and 1 in 56-65 age range (See figure D.355). The participants employed in industry between less than a year and over 10 years (See figure D.356).

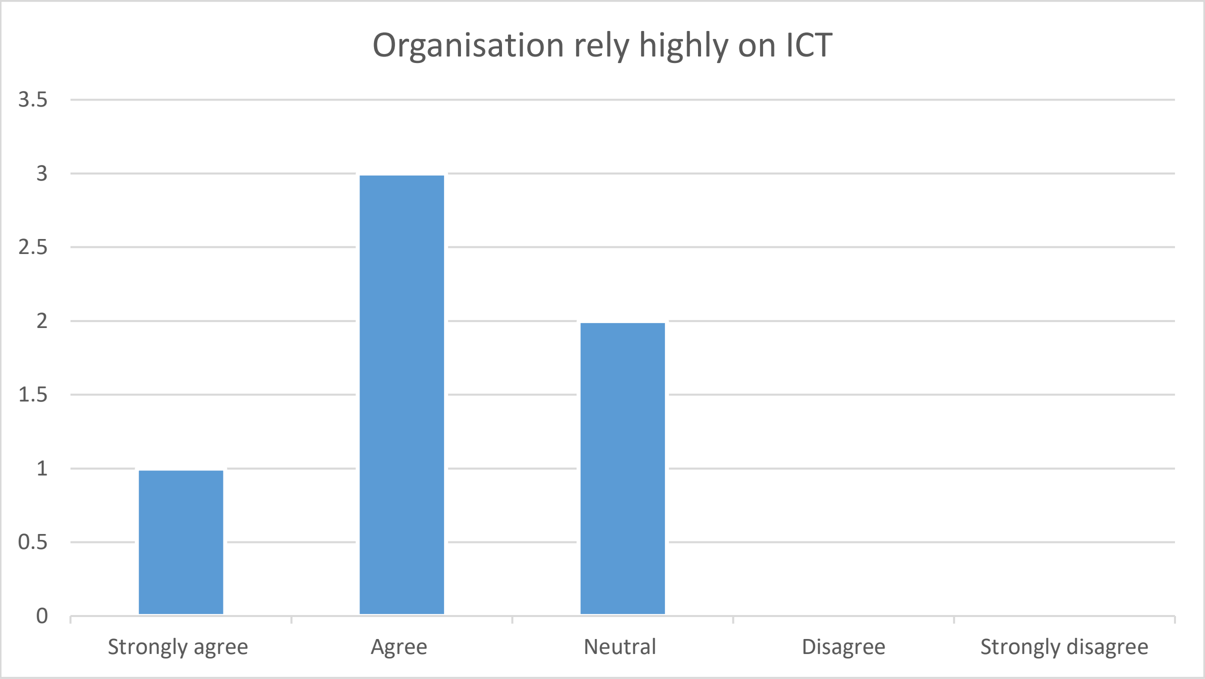


Figure D.357: Organisation rely highly on ICT (Business, consultancy and management)

Out of the 6 respondents, 4 employed in a technology reliance working environment; 2 unaware; none ‘disagreed’ (See figure D.357). This suggests that a higher number of employees are in heavily ICT dependent Business, consultancy, and management sector.

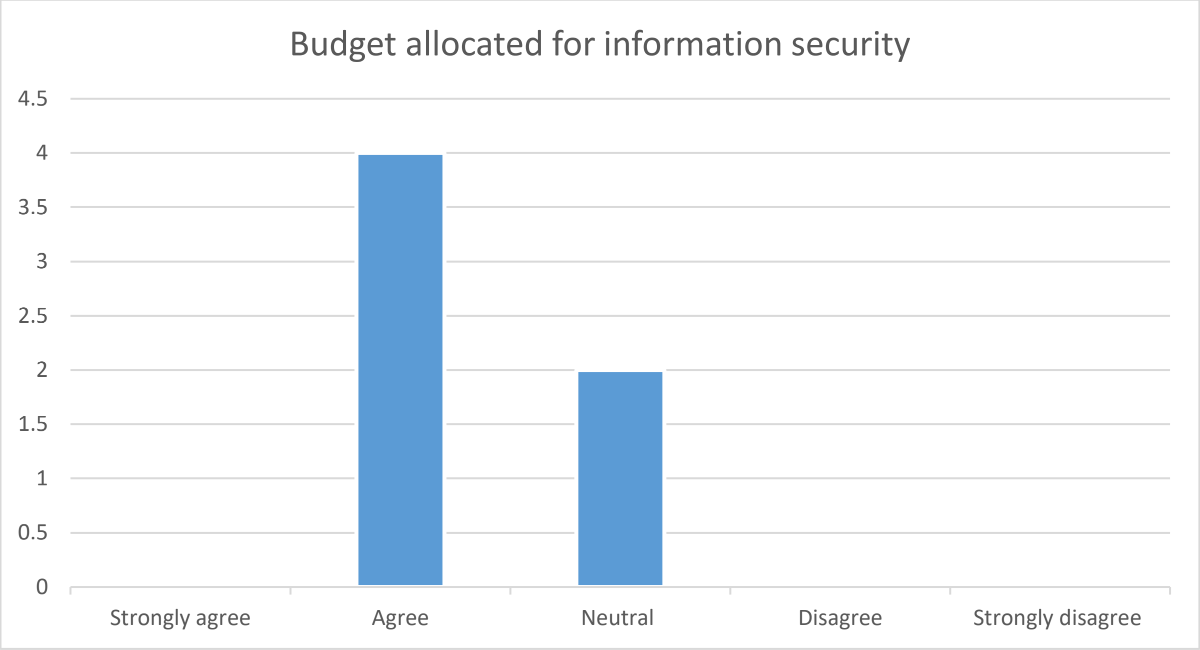


Figure D.358: Budget allocated for information security (Business, consultancy and management)

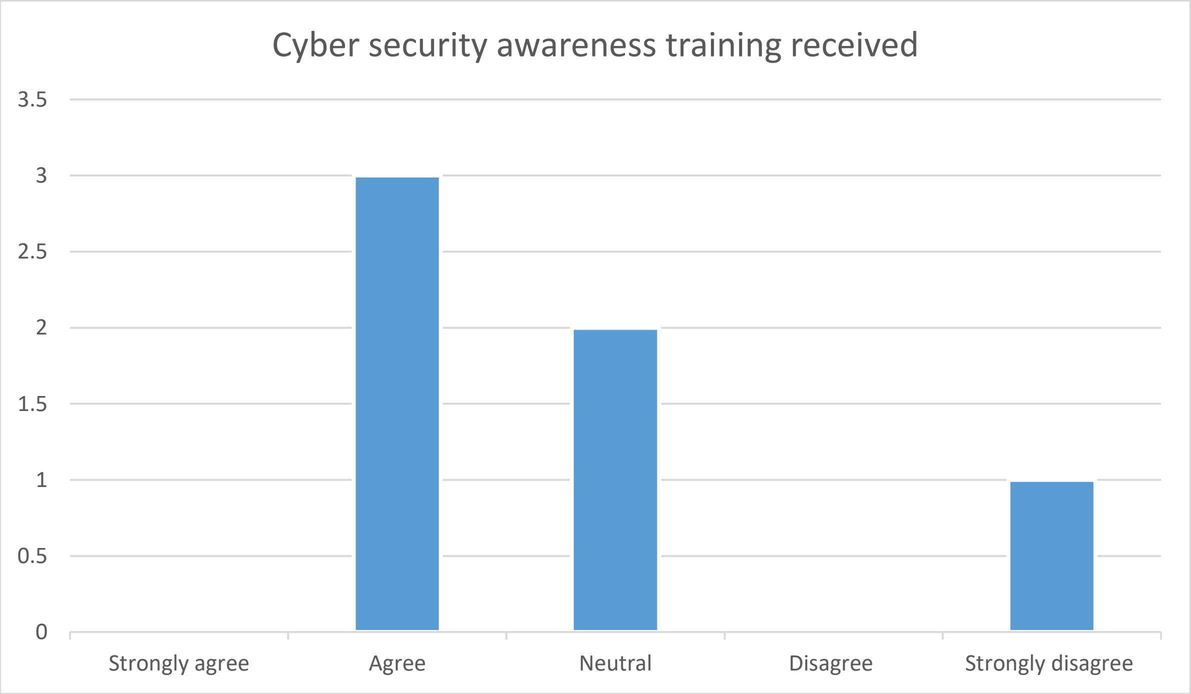


Figure D.359: Cyber security awareness training received (Business, consultancy and management)

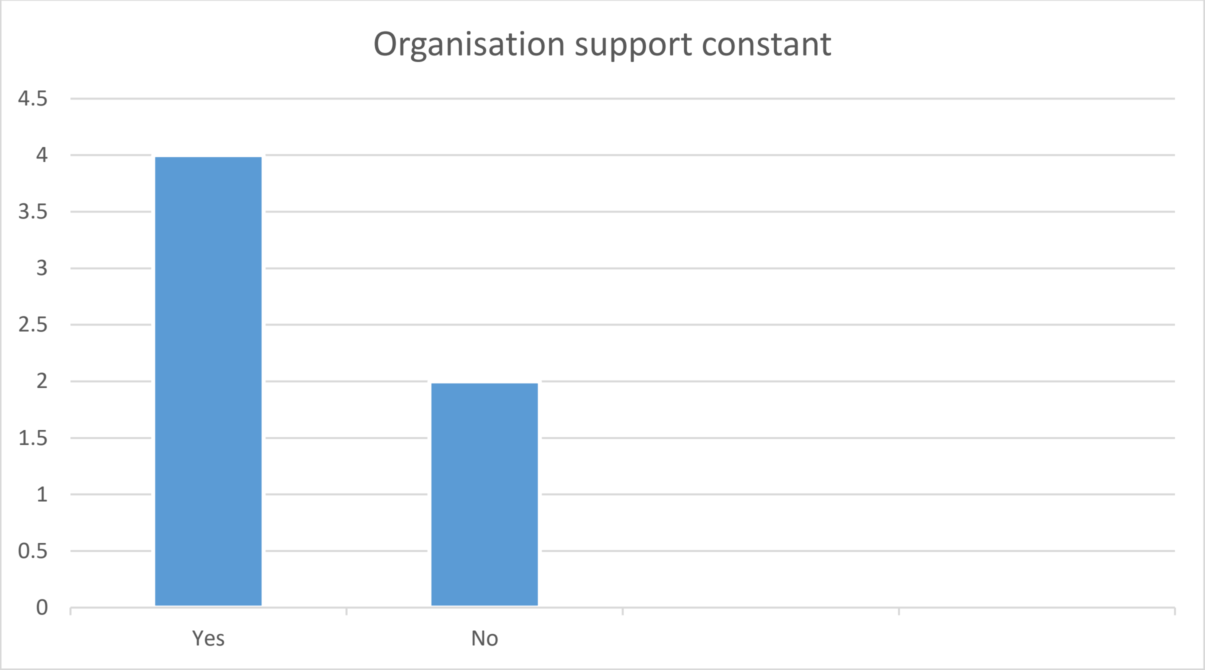


Figure D.360: Organisation support constant (Business, consultancy and management)

Funding has been sketchy. Only 4 out of the 6 respondents scored for budget allocation for information security, and 2 did not express an opinion either way (See figure D.358). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 3 participants have received regular cybersecurity awareness training, 1 had no training; 2 neither agreed nor disagreed (See figure D.359). In addition, 4 participants did receive support from the organisation to protect personal information; 2 did not (See figure D.360). This a limited organisational support despite the budget allocation for information security and high reliance on technology. The organisation provided a satisfactory level of security awareness training and provided support to protect personal information in light of the nature of the industry and high reliance on technology. The provision of training and support will limit the risks to the security of personal information, help maintain trust between the organisation and the clients, without affecting the reputation of the organisation, and avoid financial repercussion to the company.

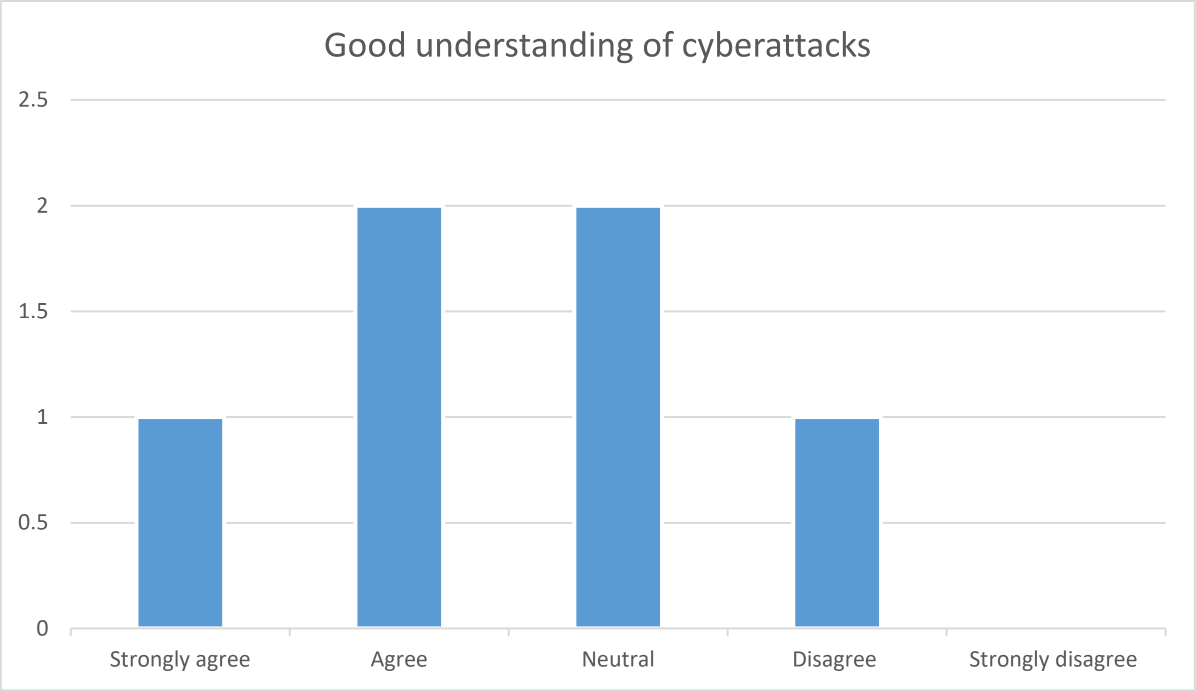


Figure D.361: Good understanding of cyberattacks (Business, consultancy and management)

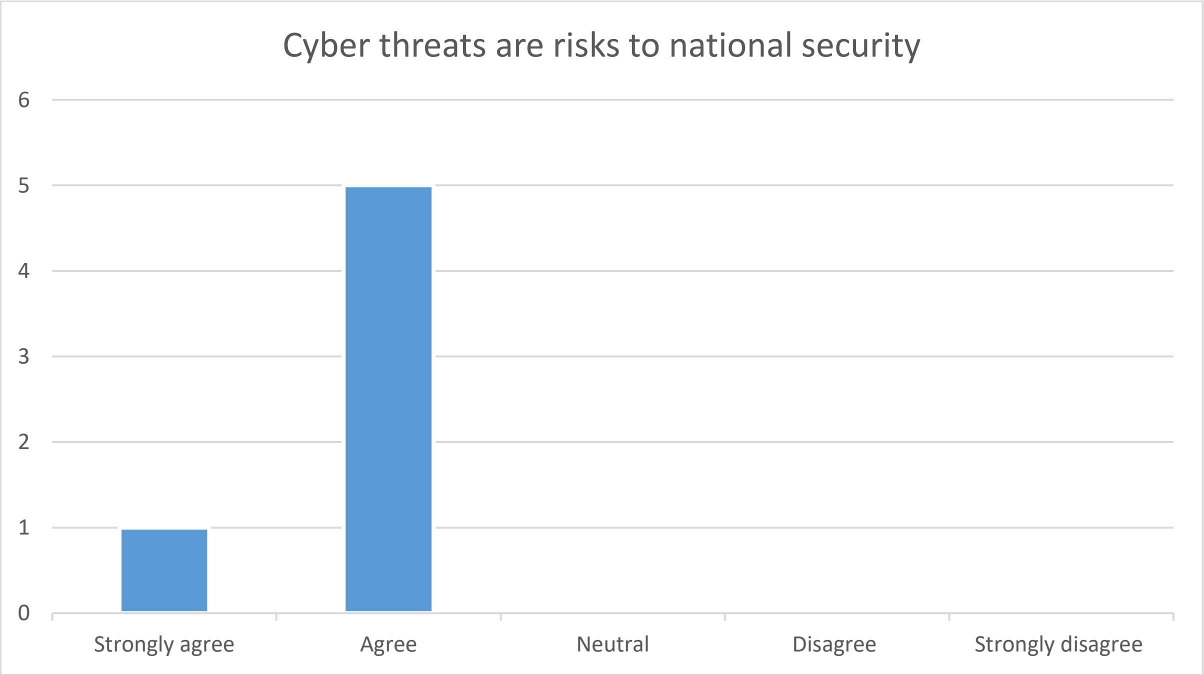


Figure D.362: Cyber threats are risks to national security (Business, consultancy and management)

Despite the security awareness training, 3 participants have a satisfactory level of understanding of the impact of cyber-attacks on the public and the organisation; 1 have no understanding; 2 did not score either way (See figure D.361). However, all participants realise the potential threats to national security from cyber-attacks (See figure D.362). In general, understanding cyber threats and their impact on national security will encourage people to act responsibly to minimise end-user errors, and in time they will have a strong voice in accepting and implementing a national, regional, and global level mechanism.

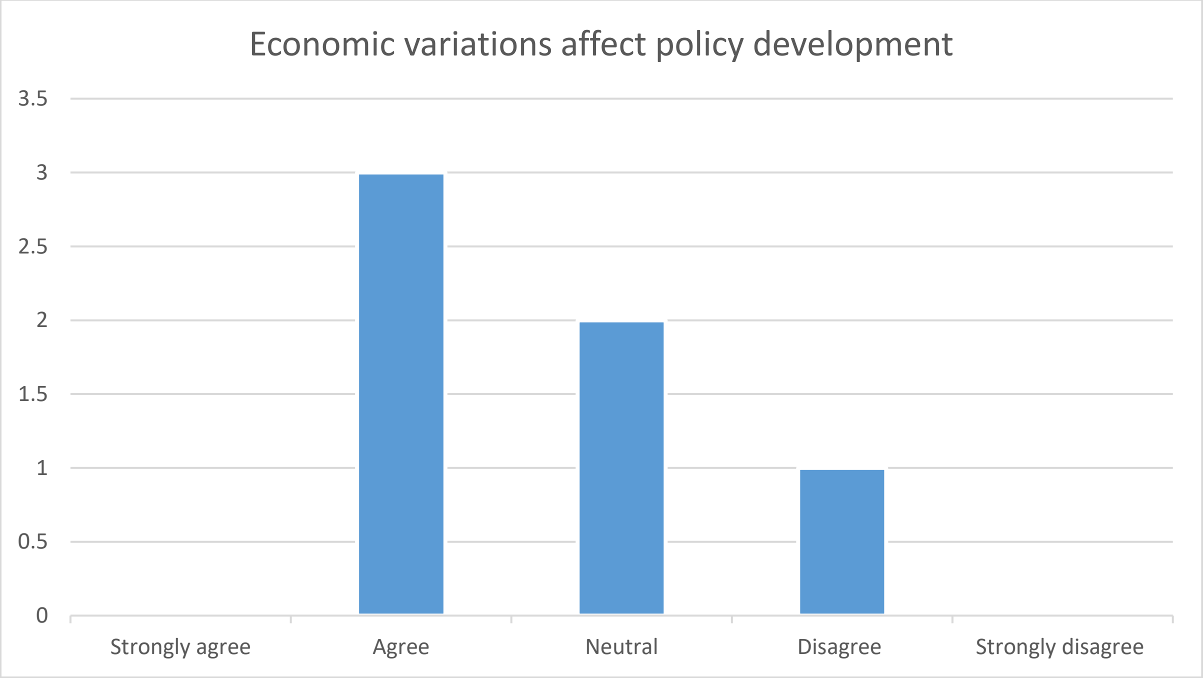


Figure D.363: Economic variations affect policy development (Business, consultancy and management)

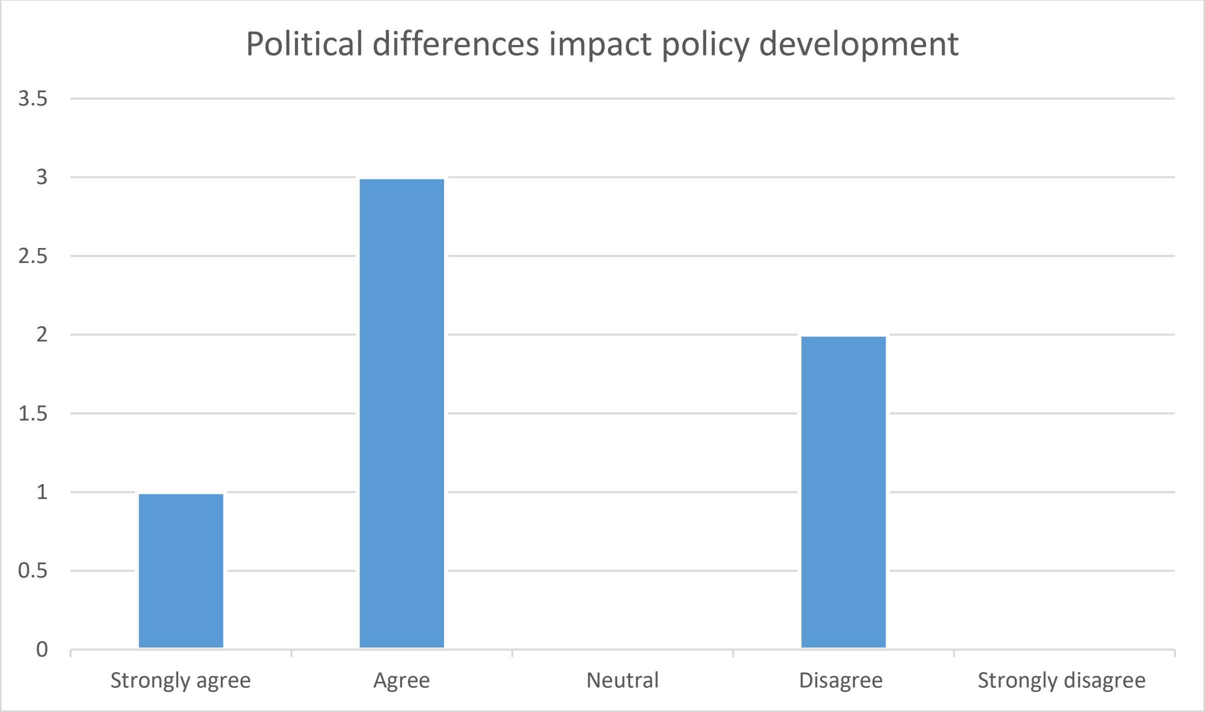


Figure D.364: Political differences impact policy development (Business, consultancy and management)

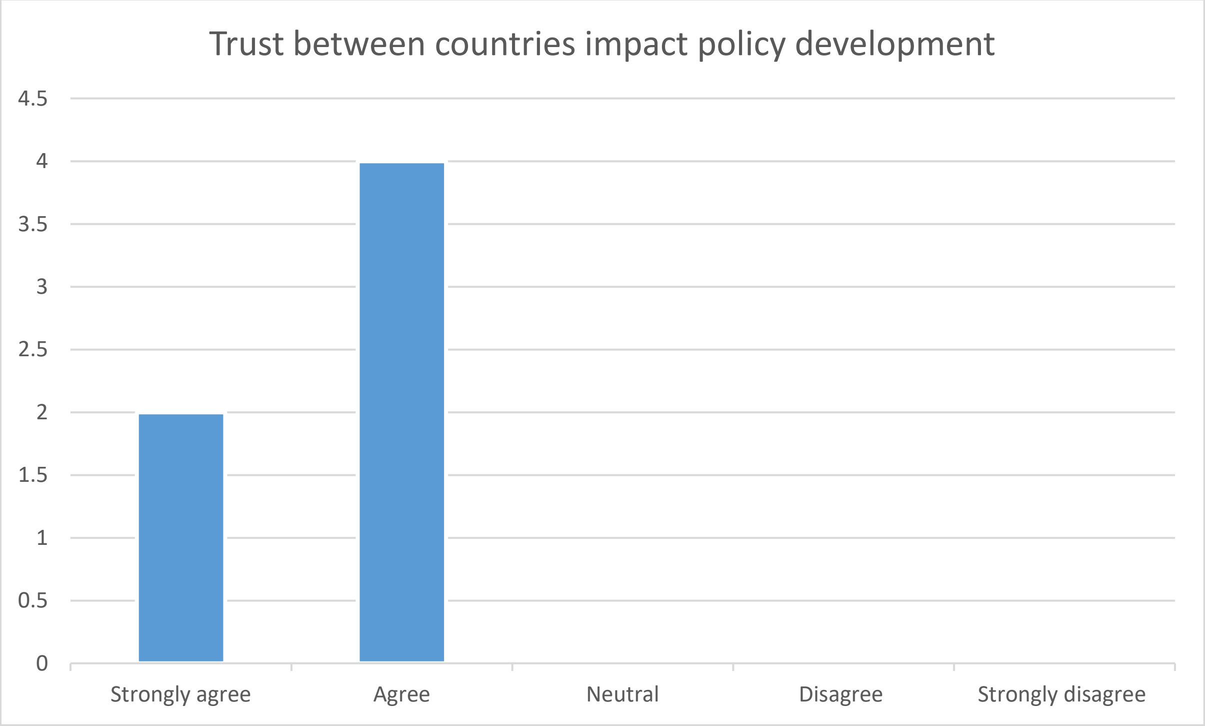


Figure D.365: Trust between countries impact policy development (Business, consultancy and management)

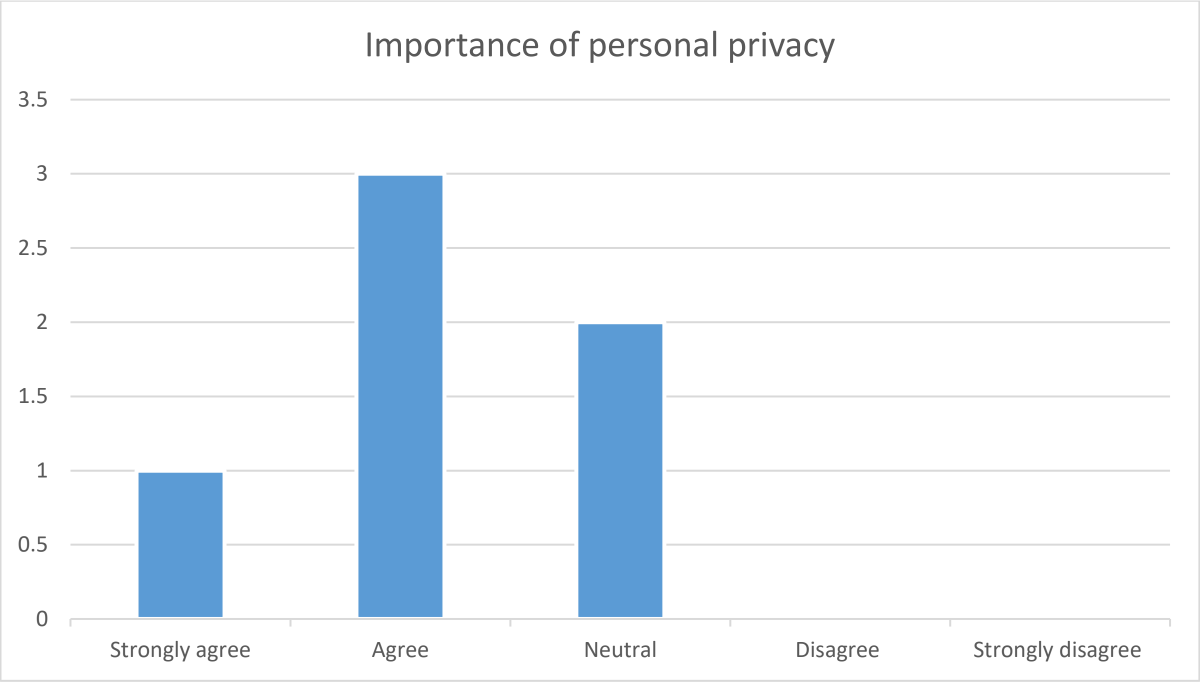


Figure D.366: Importance of personal privacy (Business, consultancy and management)

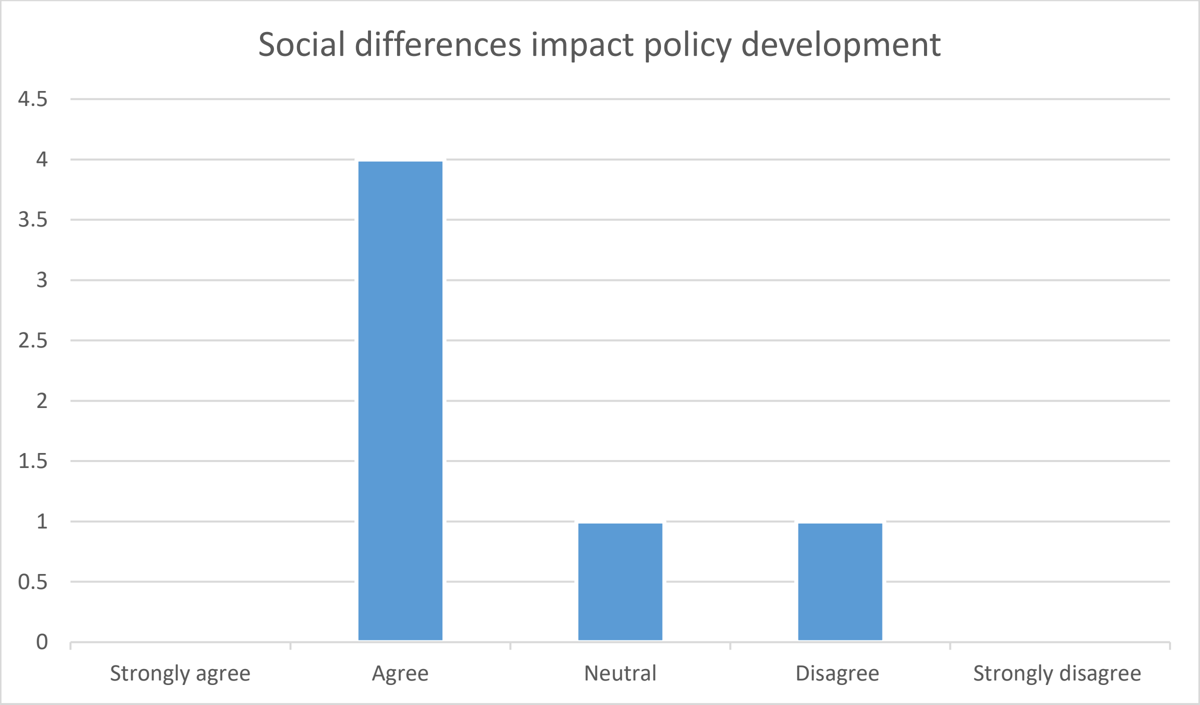


Figure D.367: Social differences impact policy development (Business, consultancy and management)

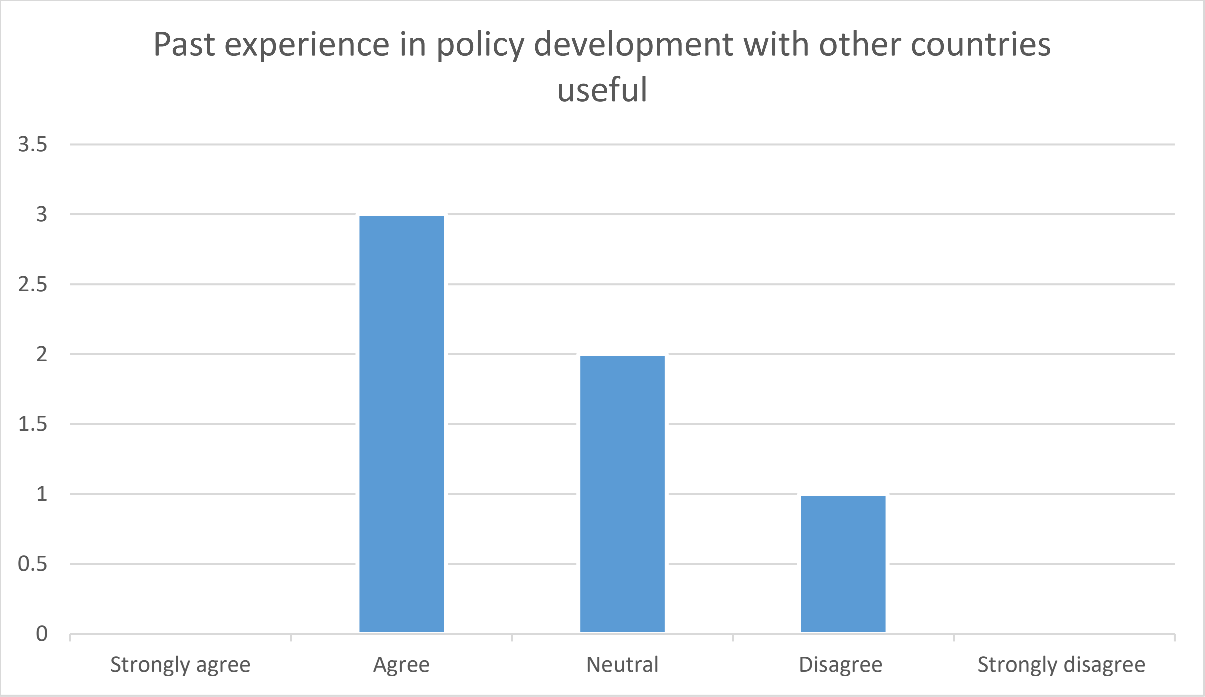


Figure D.368: Past experience in policy development with other countries useful (Business, consultancy and management)

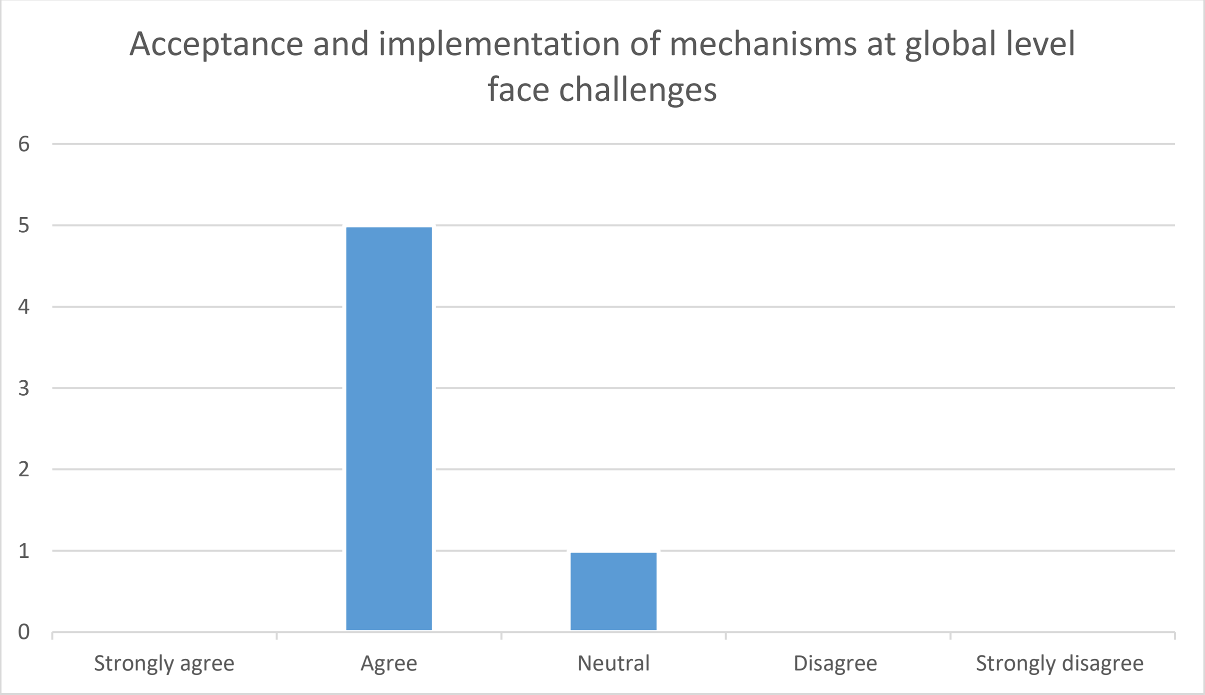


Figure D.369: Acceptance and implementation of mechanisms at global level face challenges (Business, consultancy and management)

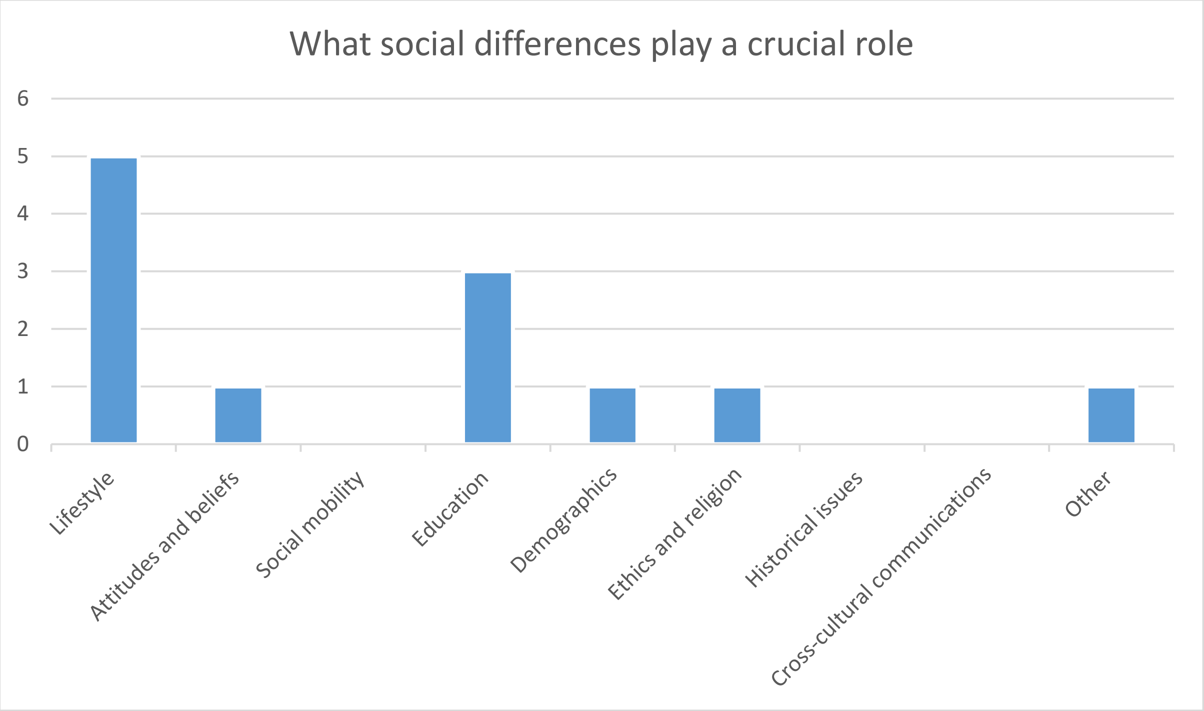


Figure D.370: What social differences play a crucial role (Business, consultancy and management)

The response to the social differences listed in the questionnaire, The majority have highlighted the importance of education and lifestyle (See figure D.370). The awareness of potential cyber threats, their impact on people and national security has an important part to play in accepting and implementing data privacy and security policies. Therefore, it is beneficial to provide cybersecurity awareness training at schools, and at the organisational level, and education training could be effective in making people understand the importance of privacy and the implications of privacy violations. People will have to make crucial choices when considering reliance on technology at the workplace. Therefore, the demand for accepting and implementing policies associated with data privacy and security also should be high.

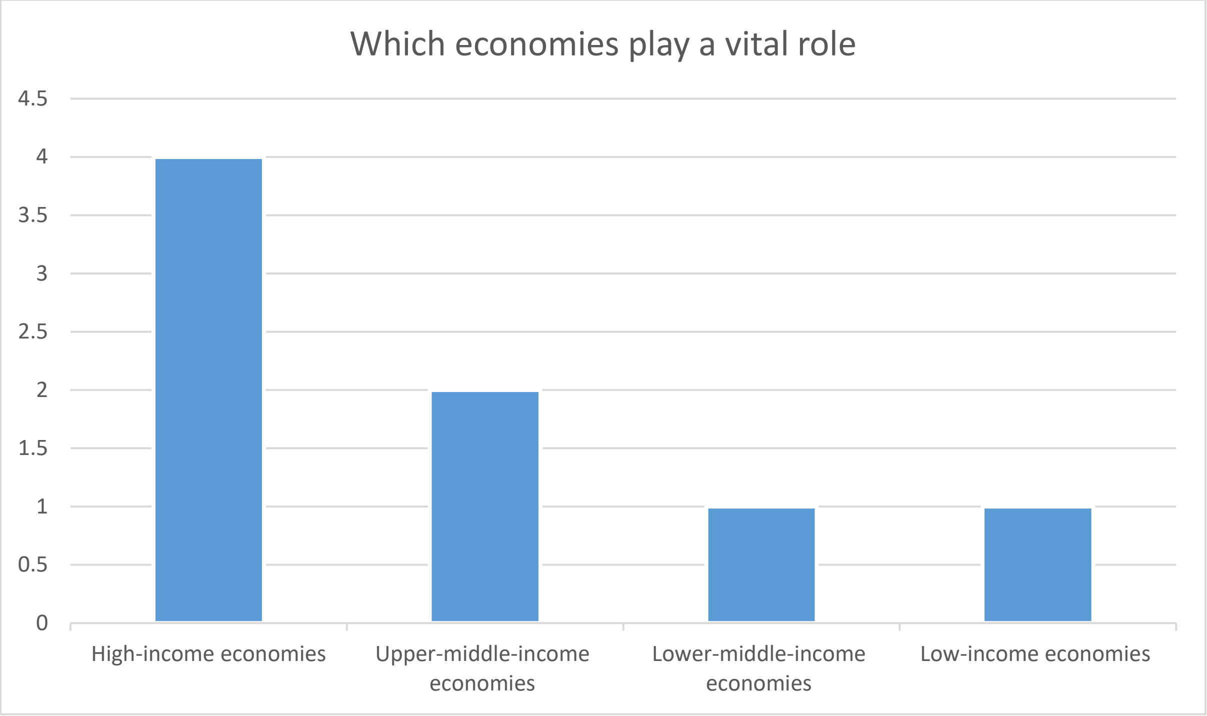


Figure D.371: Which economies play a vital role (Business, consultancy and management)

In the questionnaire, the majority has stated that high-income countries play a vital role (See figure D.371). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking. Employees put emphasis on high-income economies in comparison to others.

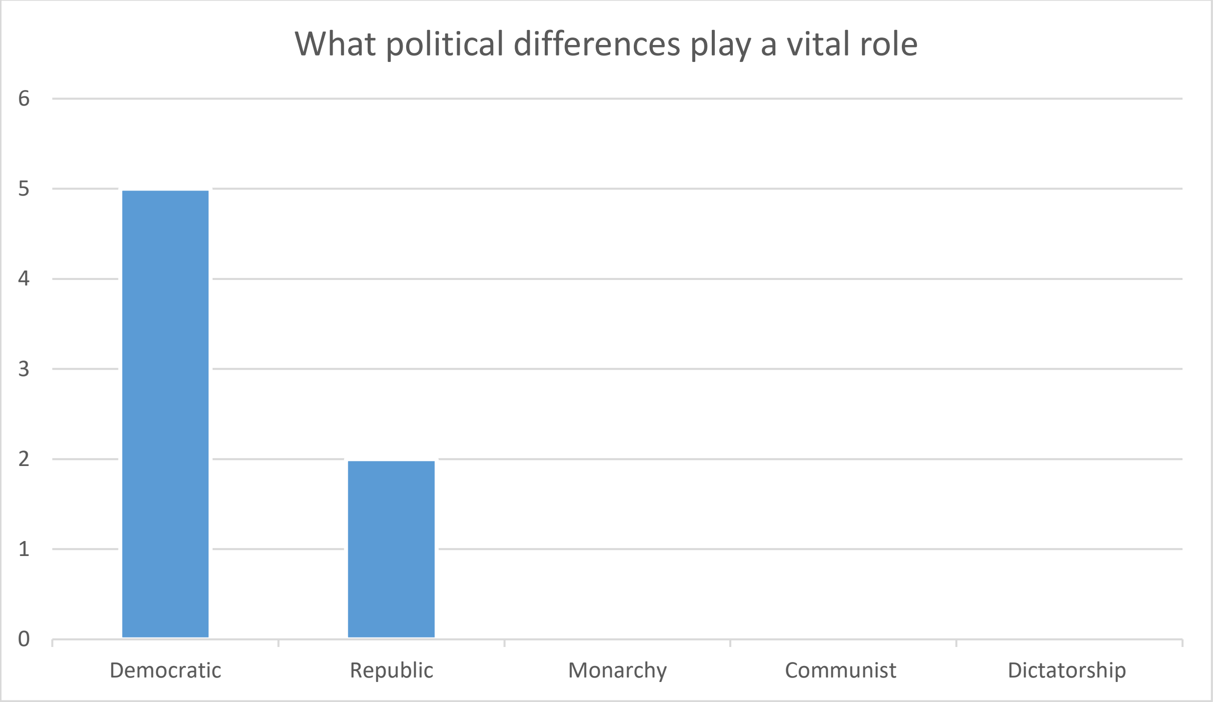


Figure D.372: What political differences play a vital role (Business, consultancy and management)

The majority have chosen a democratic political system (See figure D.372), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

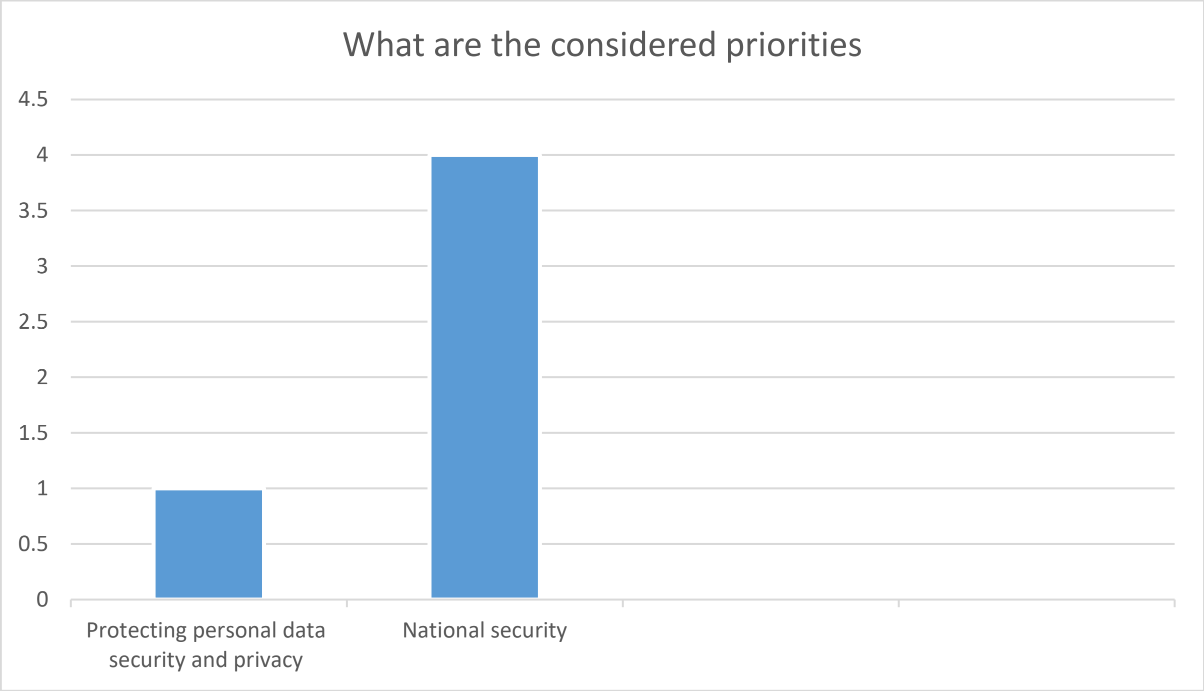


Figure D.373: What are the considered priorities (Business, consultancy and management)

In accepting and implementing a global data privacy and security policies, the participants focus far more on the importance of national security, and less on protecting personal data security and privacy (See figure D.373). However, in the case of a personal data breach incident, the repercussions will have a knock-on effect on personal data security and privacy as well, and it will also be felt right across the groups as well as the community alike.

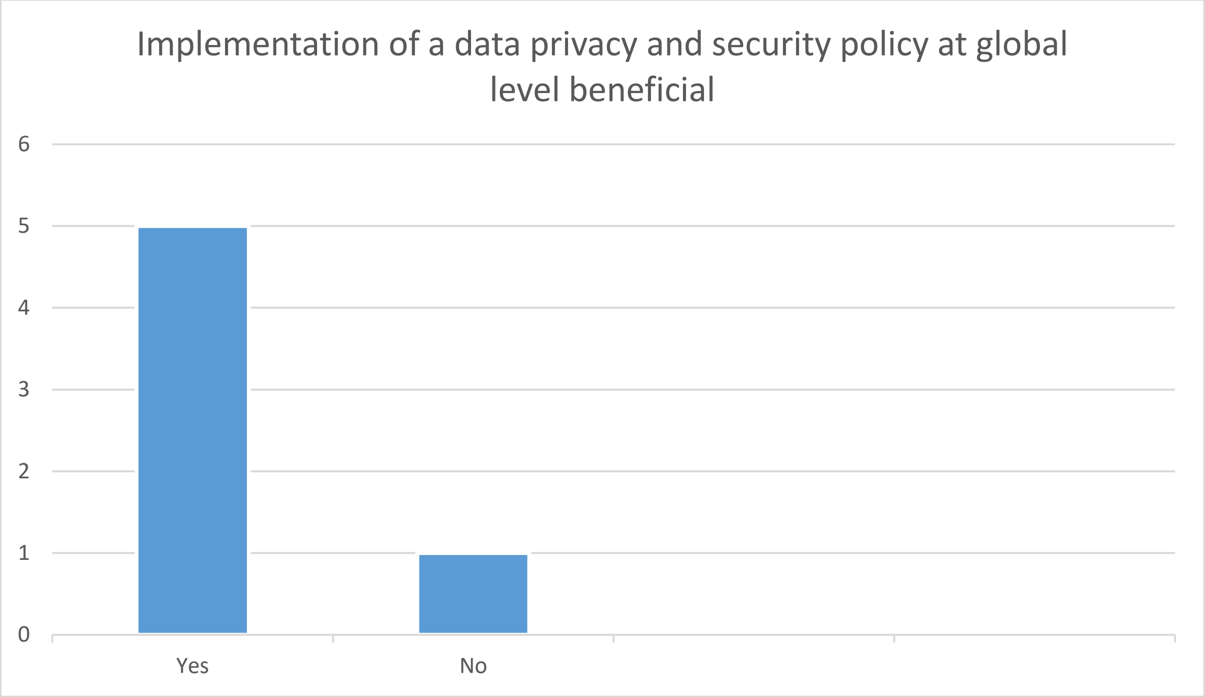


Figure D.374: Implementation of a data privacy and security policy at global level beneficial (Business, consultancy and management)

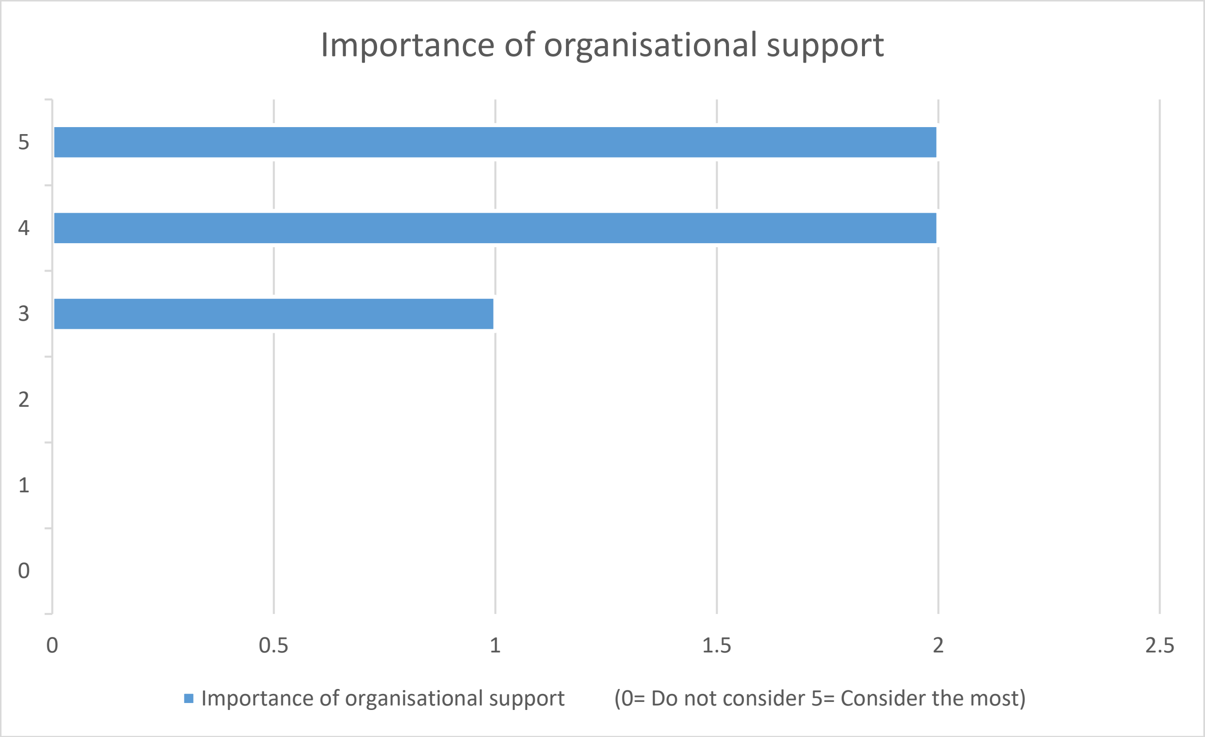


Figure D.375: Importance of organisational support (Business, consultancy and management)

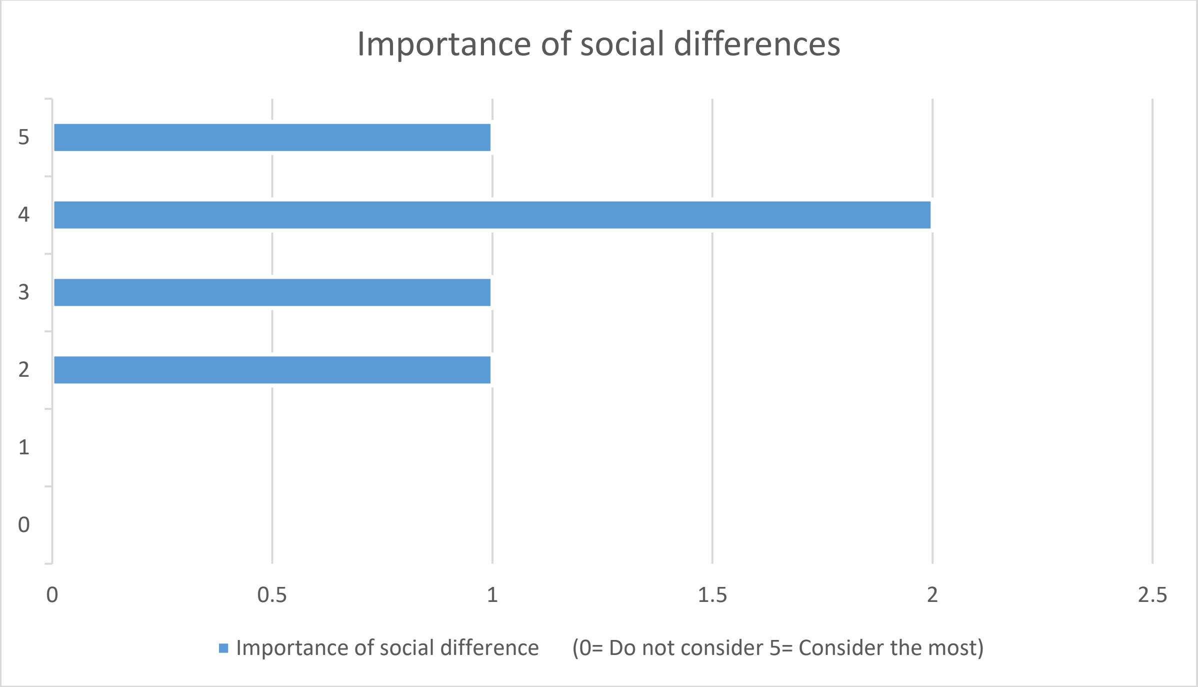


Figure D.376: Importance of social differences (Business, consultancy and management)

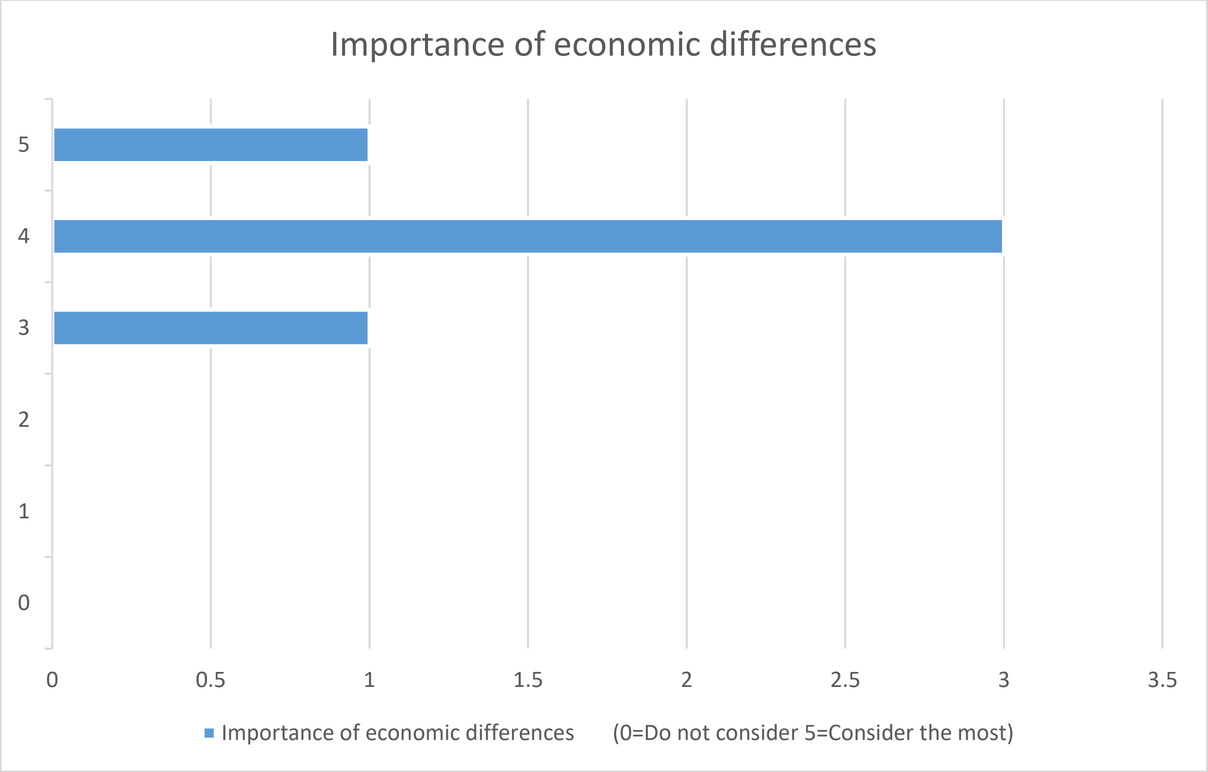


Figure D.377: Importance of economic differences (Business, consultancy and management)

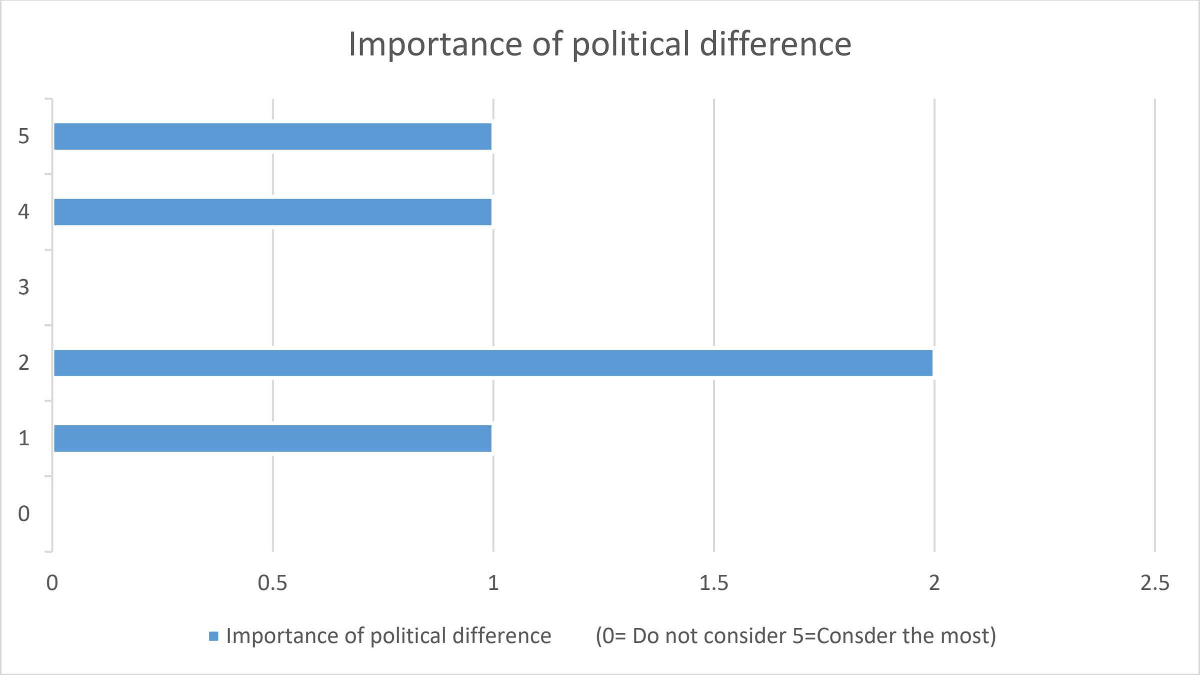


Figure D.378: Importance of political difference (Business, consultancy and management)

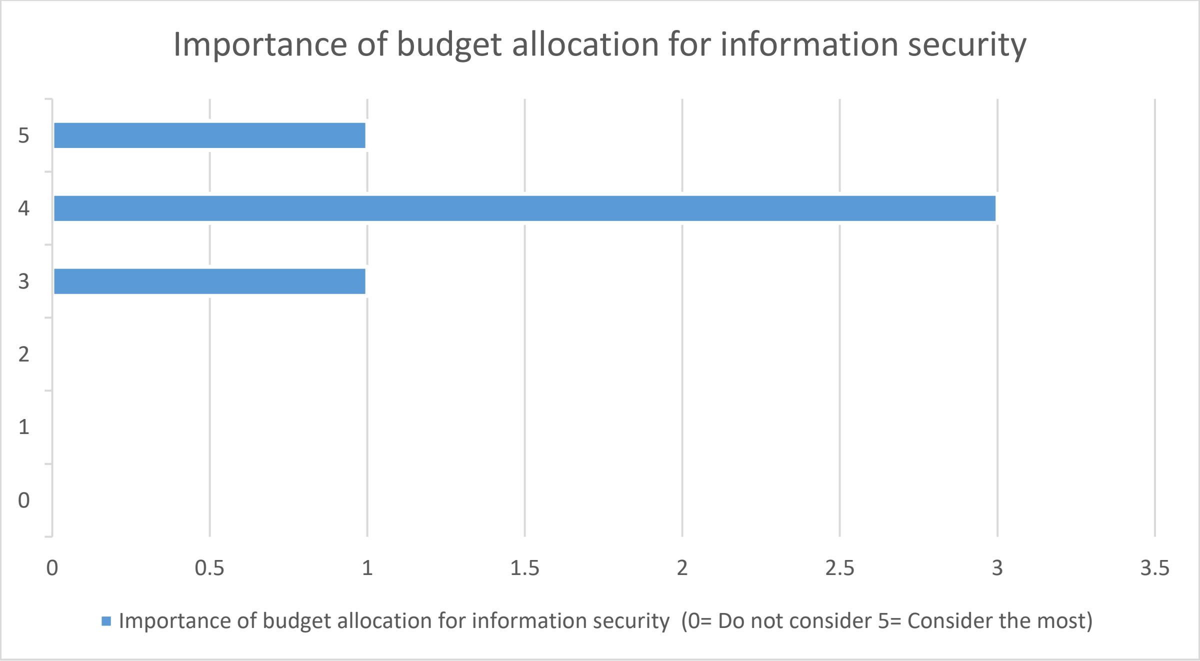


Figure D.379: Importance of budget allocation for information security (Business, consultancy and management)

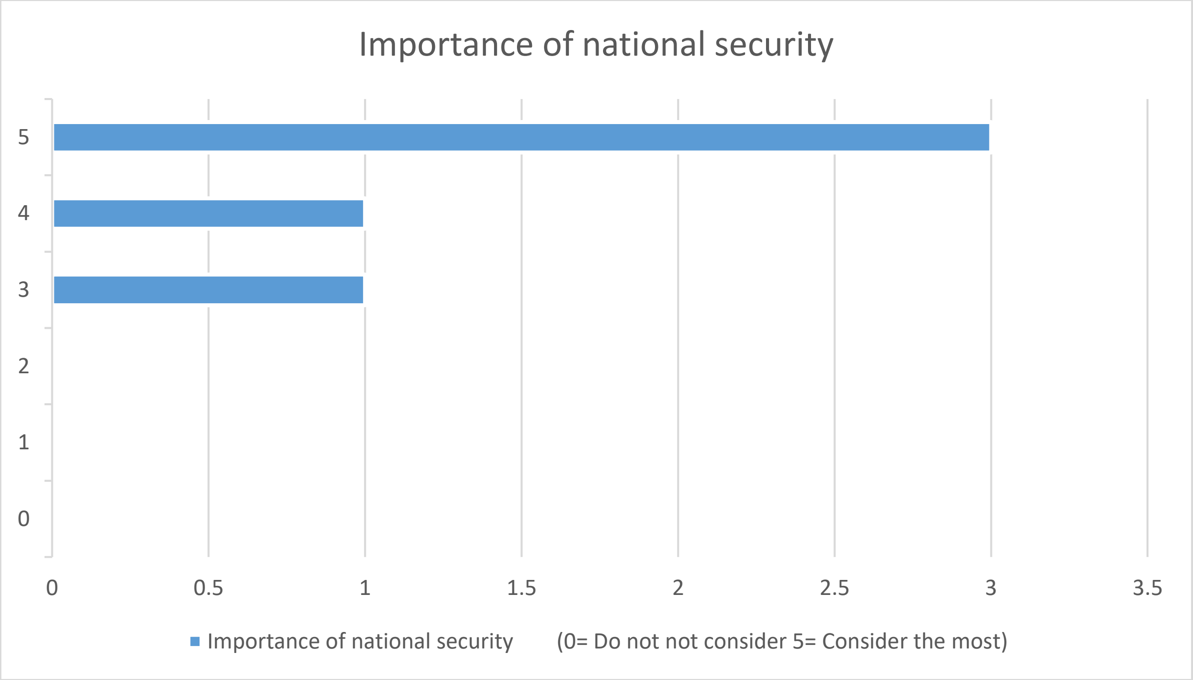


Figure D.380: Importance of national security (Business, consultancy and management)

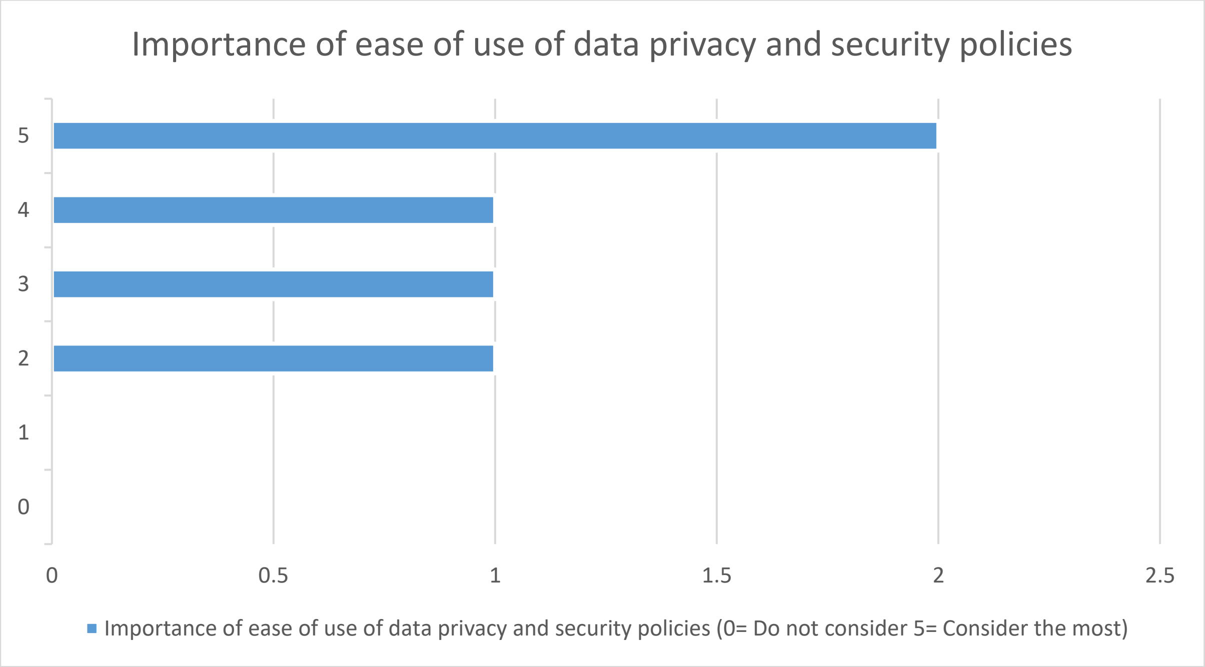


Figure D.381: Importance of ease of use of data privacy and security policies (Business, consultancy and management)

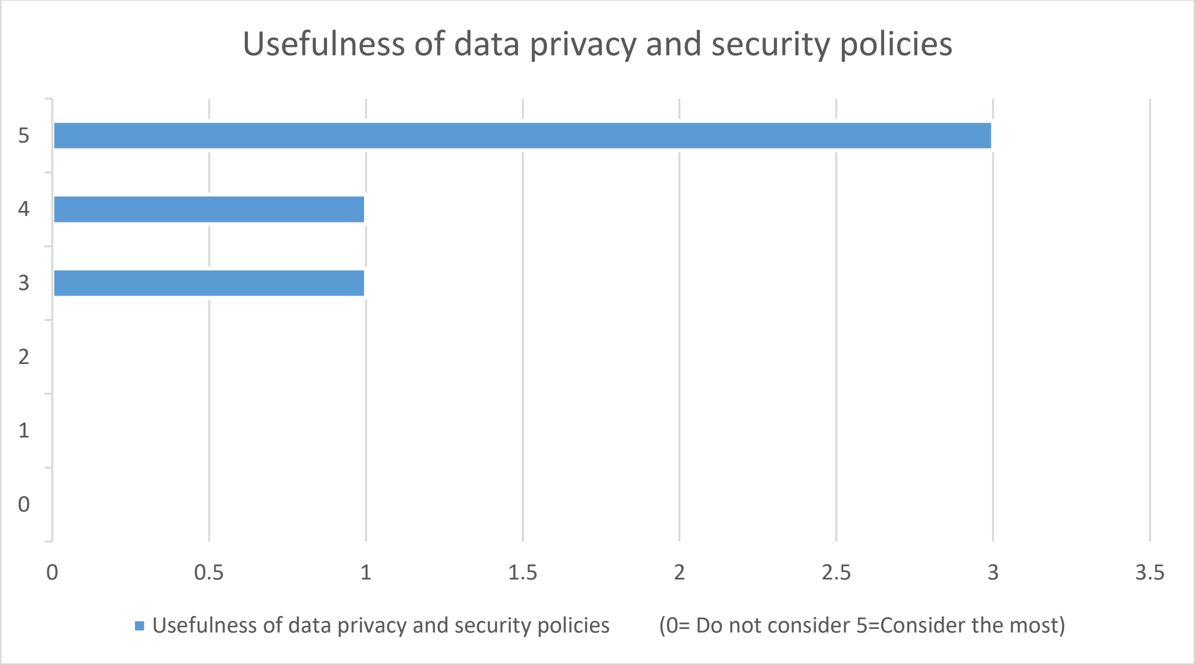


Figure D.382: Usefulness of data privacy and security policies (Business, consultancy and management)

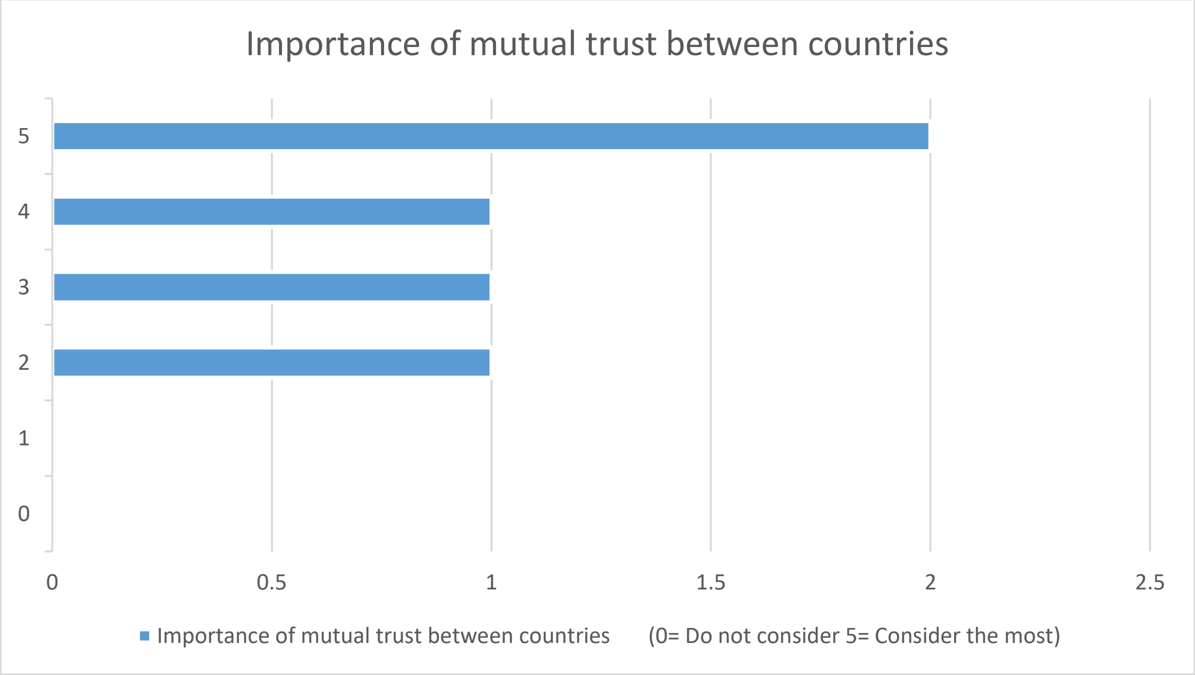


Figure D.383 Importance of mutual trust between countries (Business, consultancy and management)

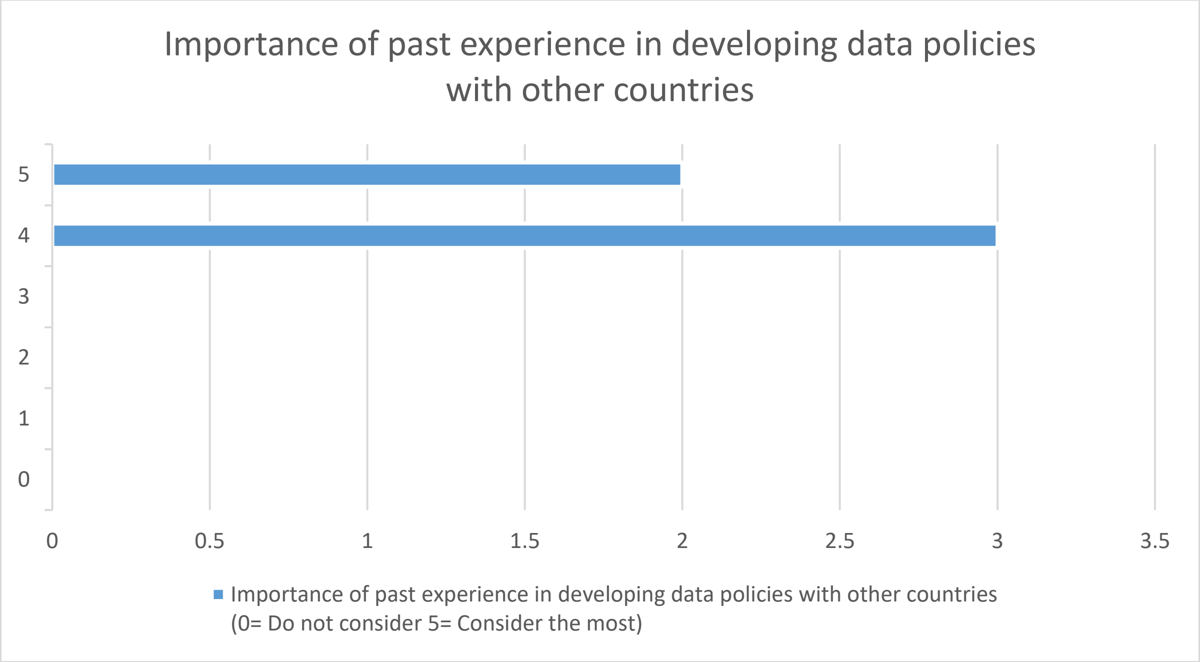


Figure D.384: Importance of past experience in developing data policies with other counties (Business, consultancy and management)

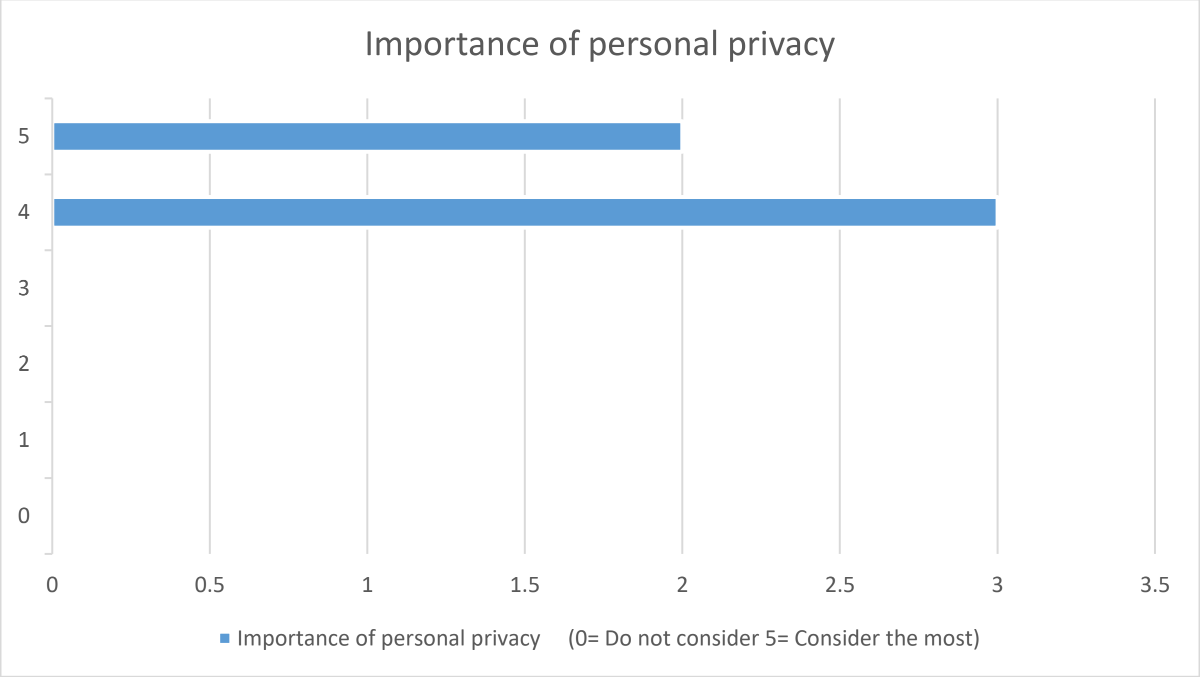


Figure D.385: Importance of personal privacy (Business, consultancy and management)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 83 percent of the respondents have endorsed (See figure D.374). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure D.363-373) (See figure D.375-385).

Sri Lanka – Education

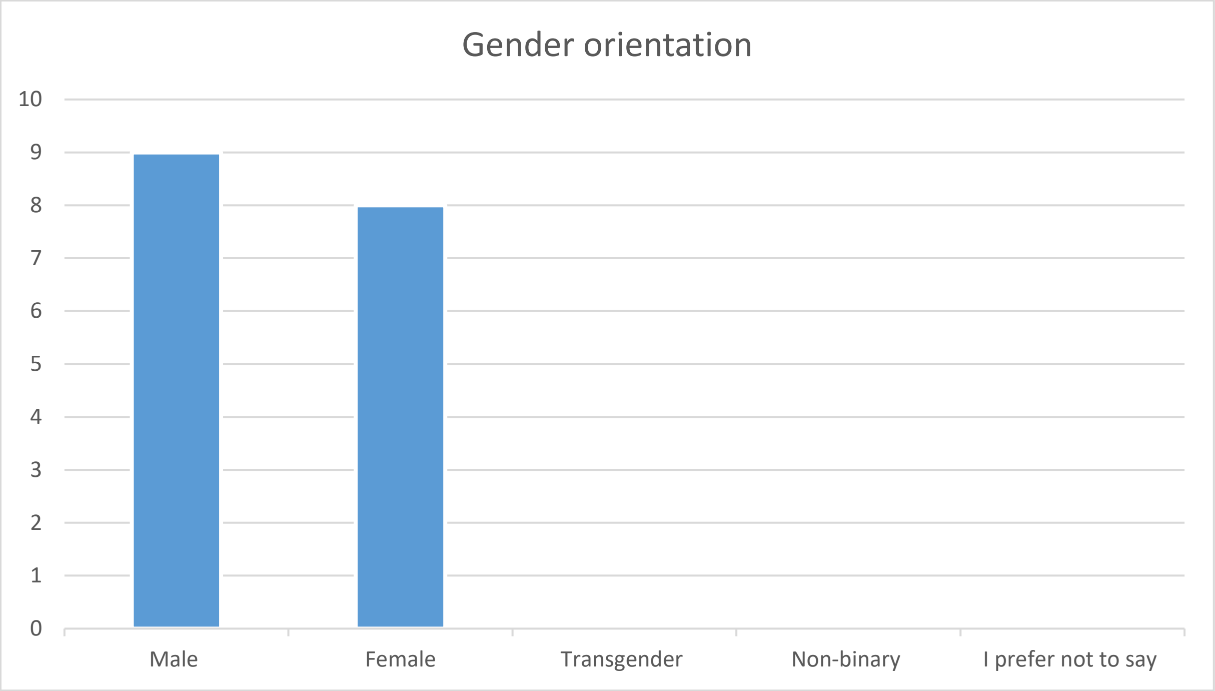


Figure D.386: Gender orientation (Education)

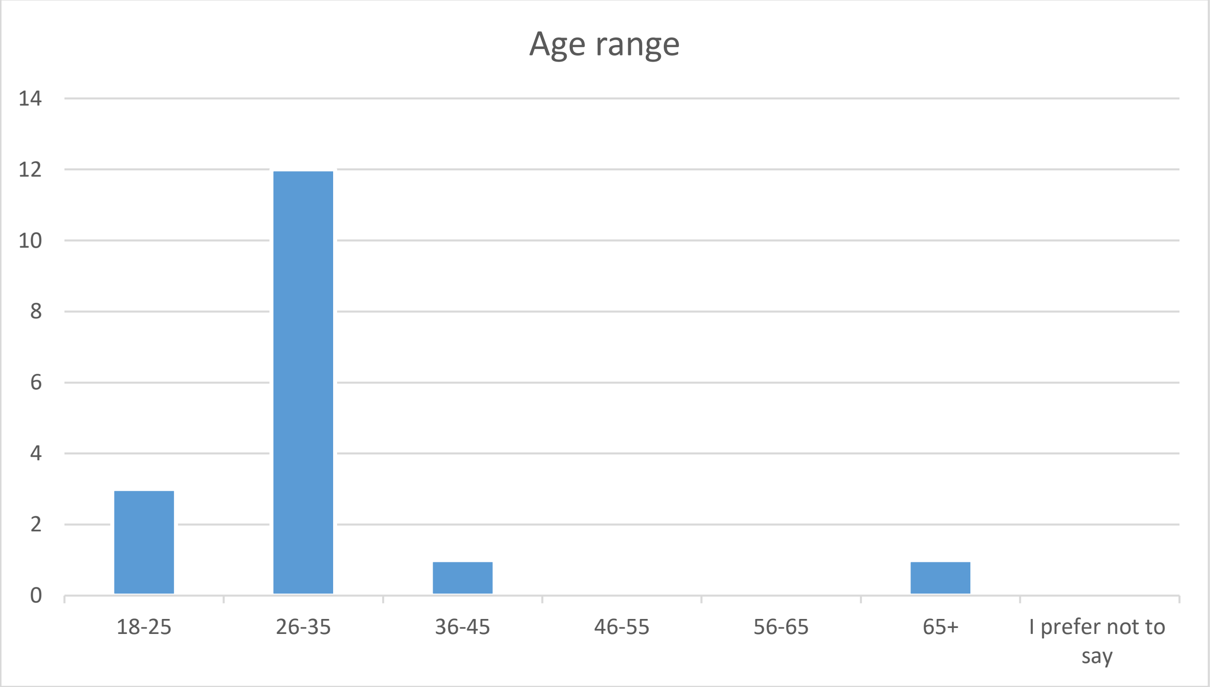


Figure D.387: Age range (Education)

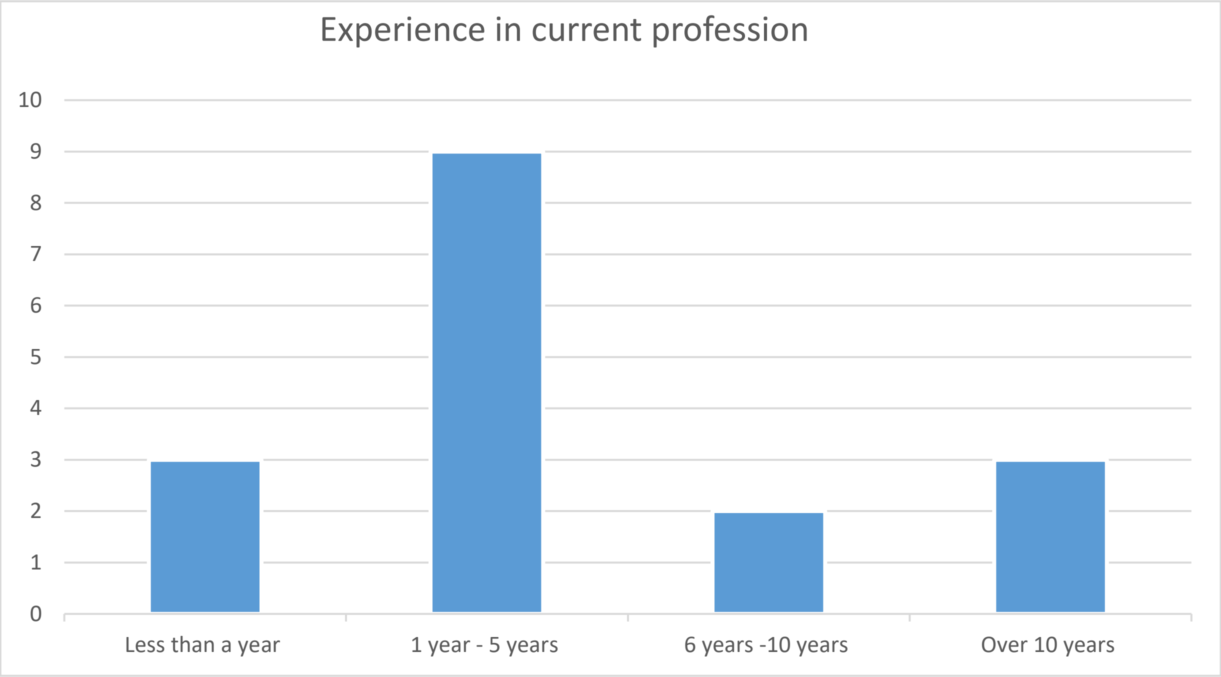


Figure D.388: Experience in current profession (Education)

This analysis is based on the responses received from Sri Lankan participants employed in the education sector. Total of 17 participants, 9 males and 8 females (See figure D.386); within 18-65 plus age range in groups of 3 in the 18-25, 12 in the 26-35, 1 in the 36-45, and 1 in the 65 plus range (See figure D.387). The participants employed in the industry between less than a year and over 10 years (See figure D.388).

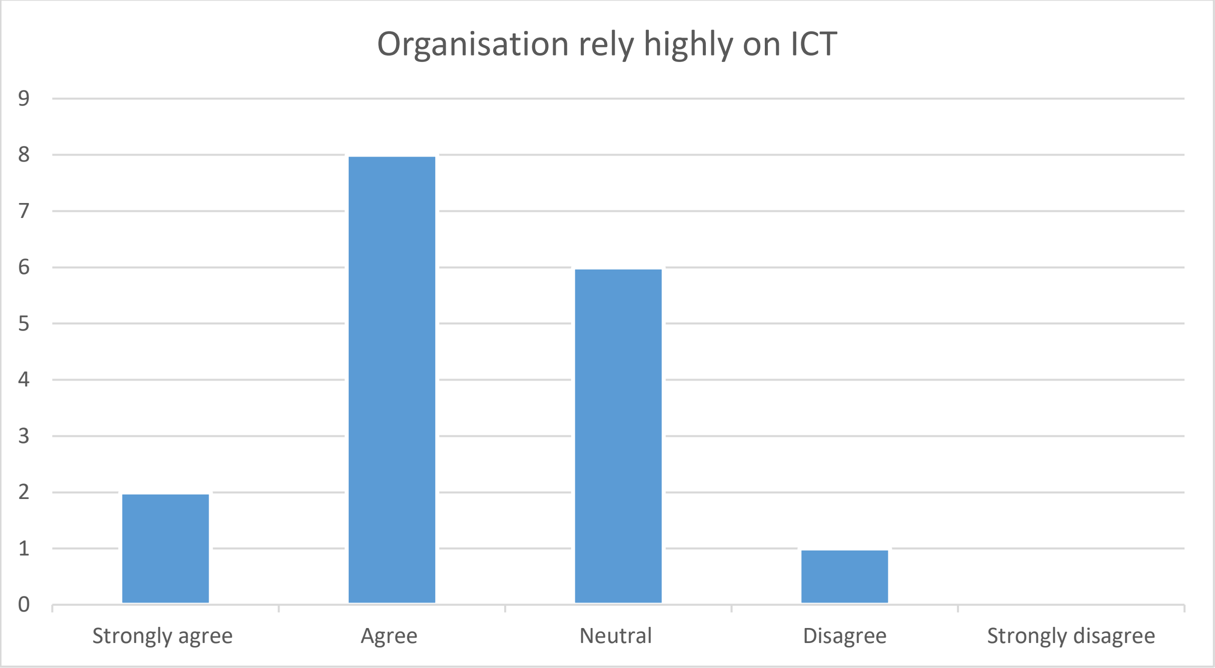


Figure D.389: Organisation rely highly on ICT (Education)

Out of the 17 respondents, 10 worked in a technology reliance working environment, 6 unaware because of the nature of the work assigned to them; 1 'disagreed' on ICT (See figure D.389). This indicates a majority engaged in the education sector with high reliance on ICT.

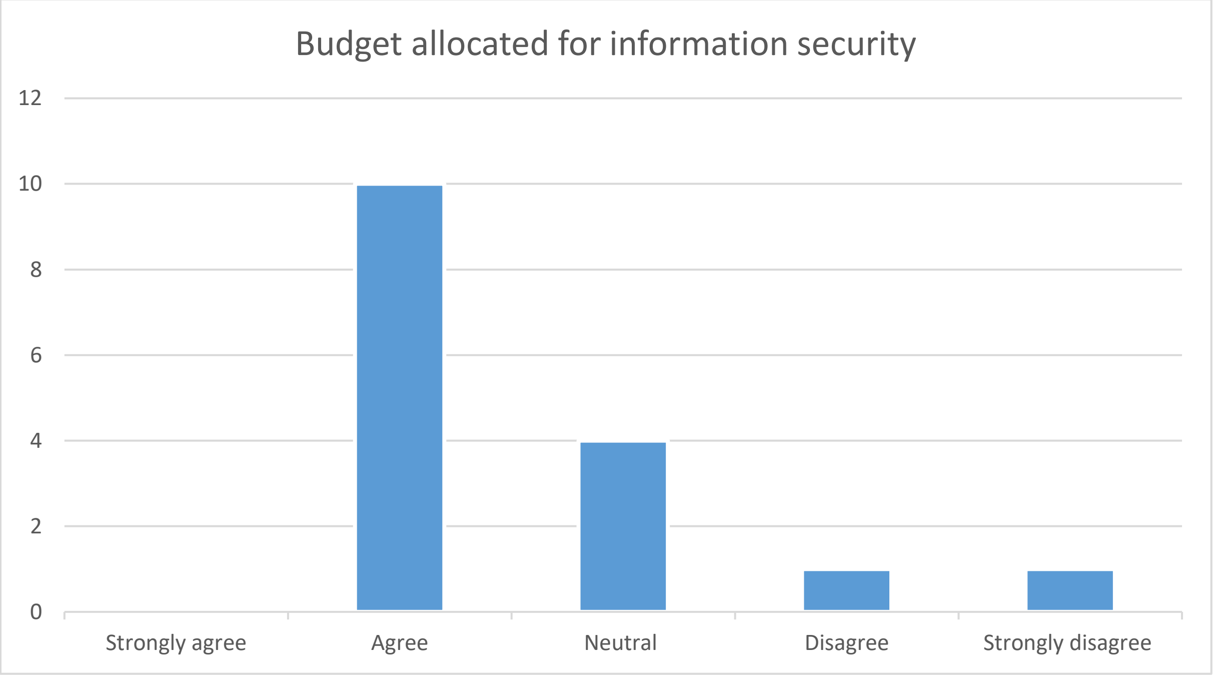


Figure D.390: Budget allocated for information security (Education)

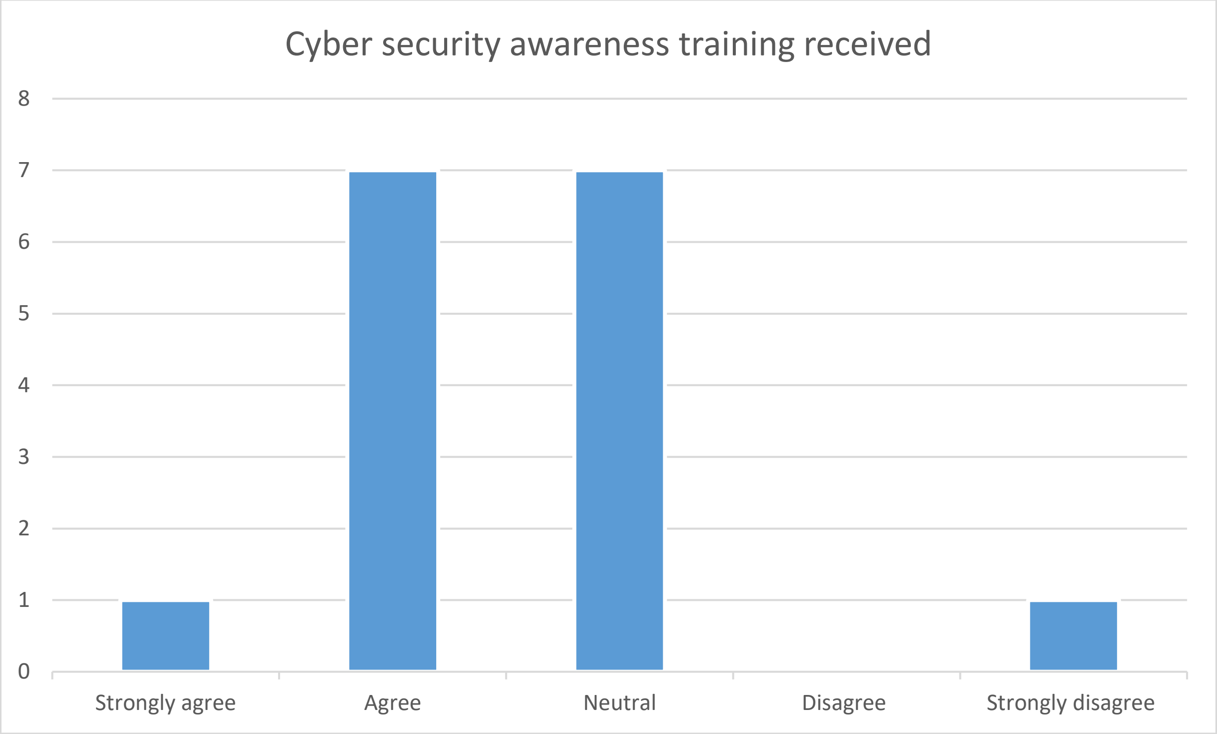


Figure D.391: Cyber security awareness training received (Education)

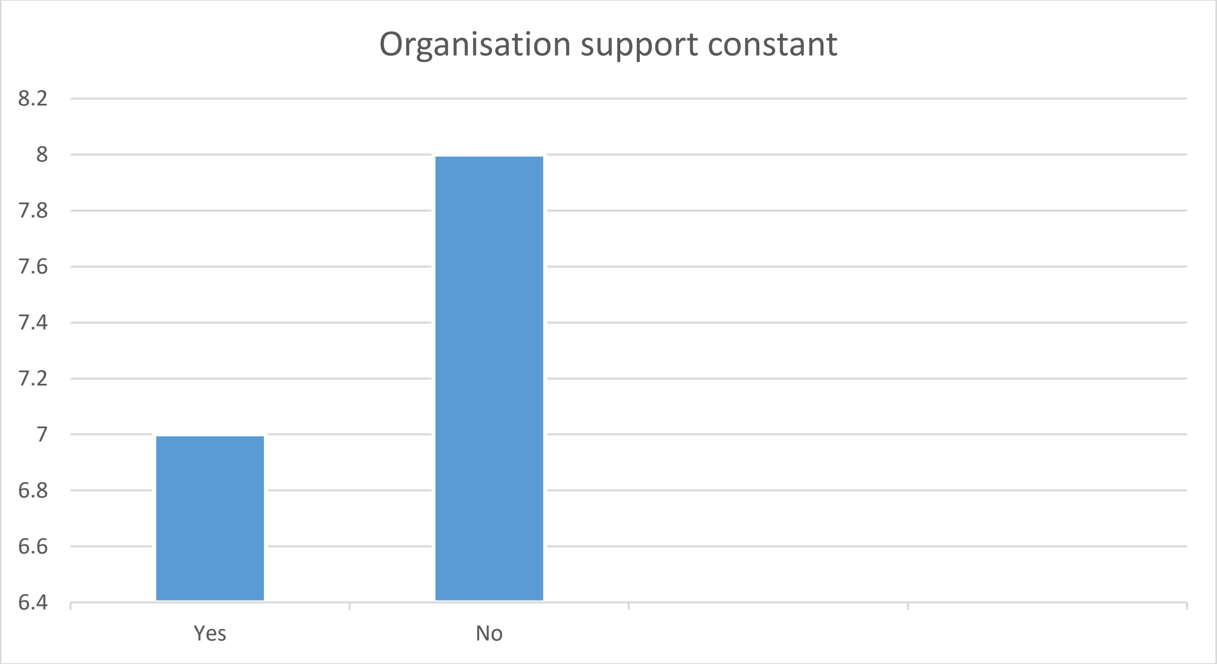


Figure D.392: Organisation support constant (Education)

10 out of the 17 scores suggest that the organisations had an allocated budget for information security; 4 did not specify either way; according to the 2 disagreed their organisations had no budget allocation for information security (See figure D.390). According to some participants, despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 8 participants received regular cybersecurity awareness training; 7 neither agreed nor disagreed; 1 participant had not received security awareness training regularly (See figure D.391). In addition, 8 participants had not received support from the organisation to protect personal information, whilst only 7 did (See figure D.392). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

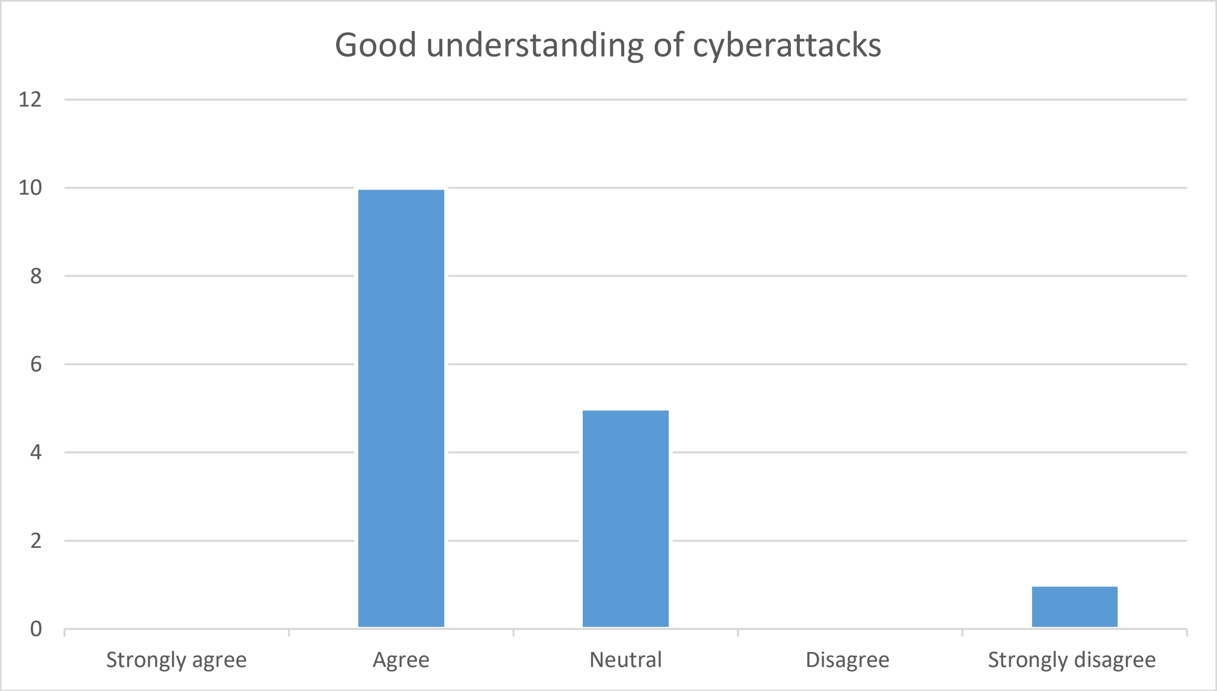


Figure D.393: Good understanding of cyberattacks (Education)

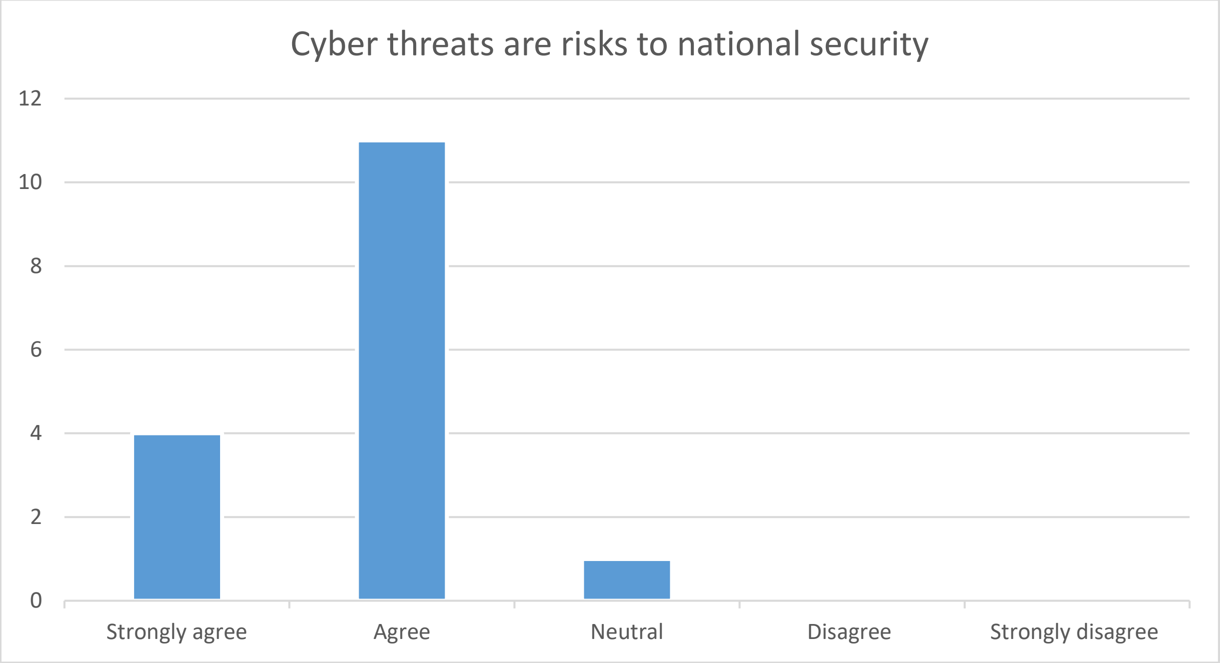


Figure D.394: Cyber threats are risks to national security (Education)

Despite the lack of security awareness training, 10 participants have a high understanding of the impact of cyber-attacks on the public and the organisation; 1 participant had no understanding; 5 did not specify either way (See figure D.393). Furthermore, 88 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure D.394). In general, understanding cyber threats and their impact on national security should make people act responsibly to minimise end-user errors, and in time, their voice would be an influencing factor in accepting and implementing a national, regional, and global level mechanism.

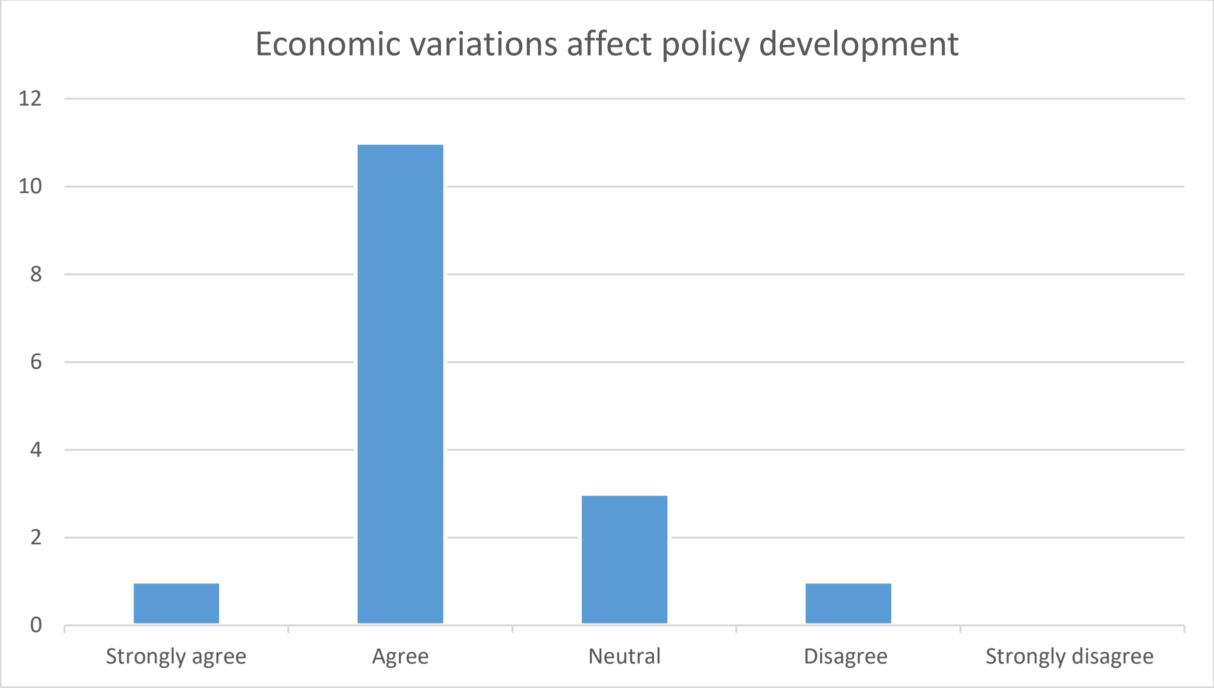


Figure D.395: Economic variations affect policy development (Education)

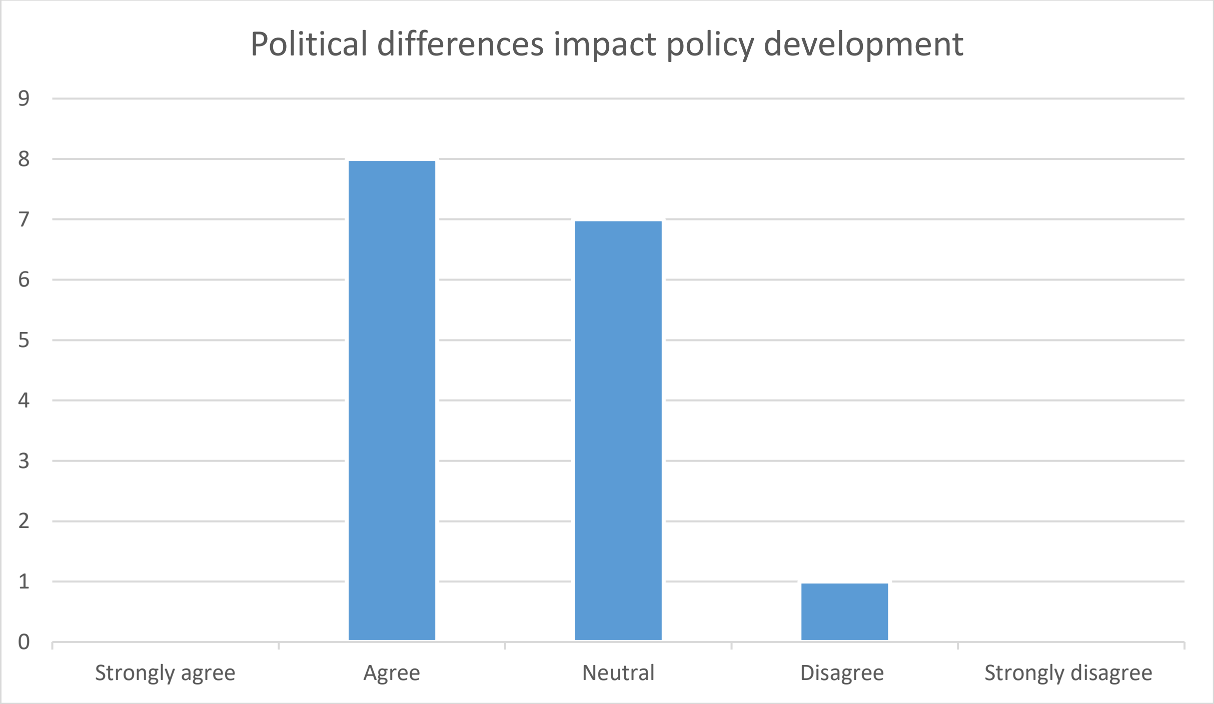


Figure D.396: Political differences impact policy development (Education)

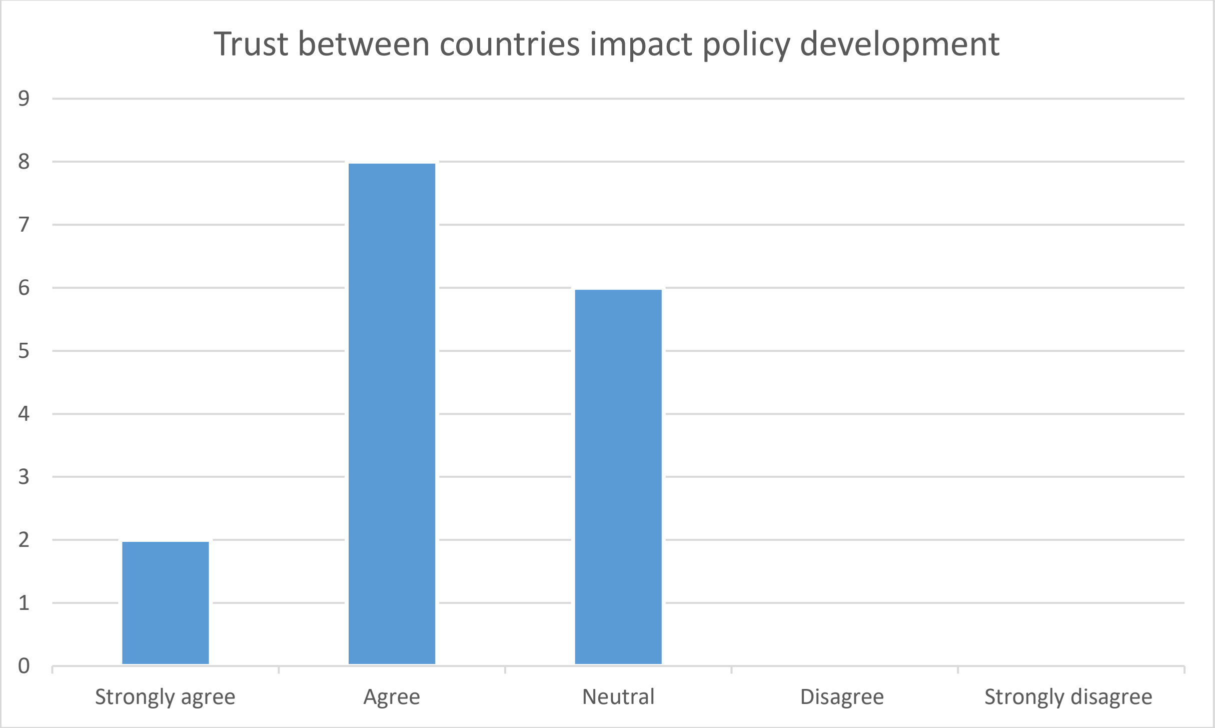


Figure D.397: Trust between countries impact policy development (Education)

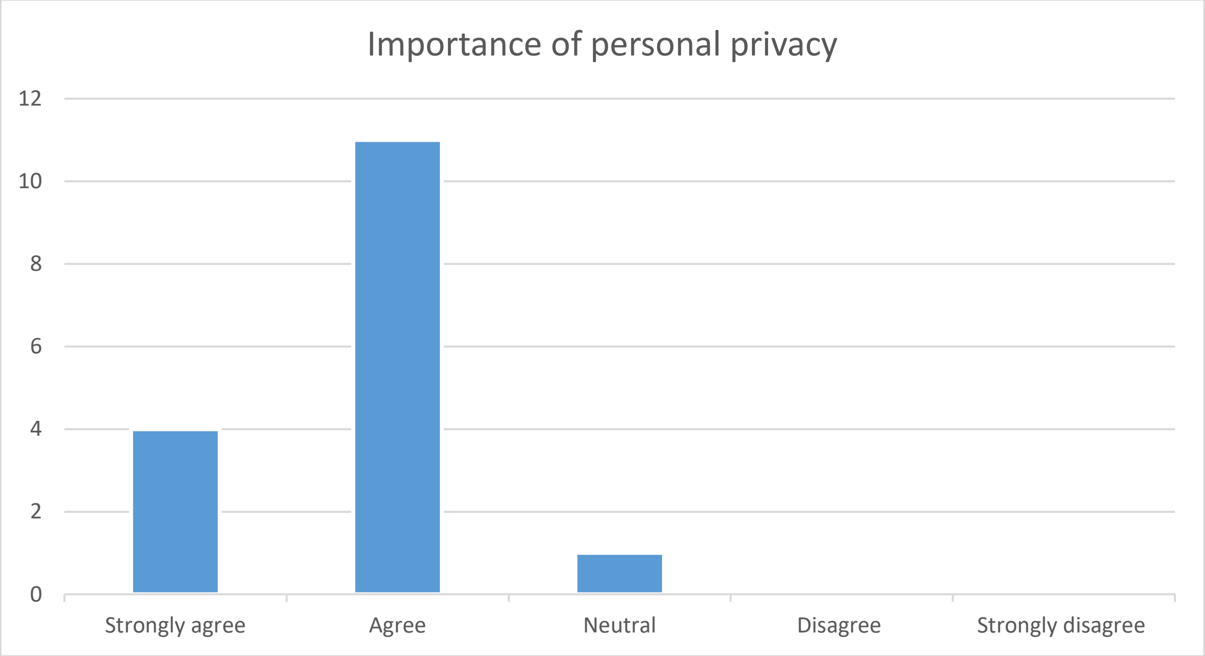


Figure D.398: Importance of personal privacy (Education)

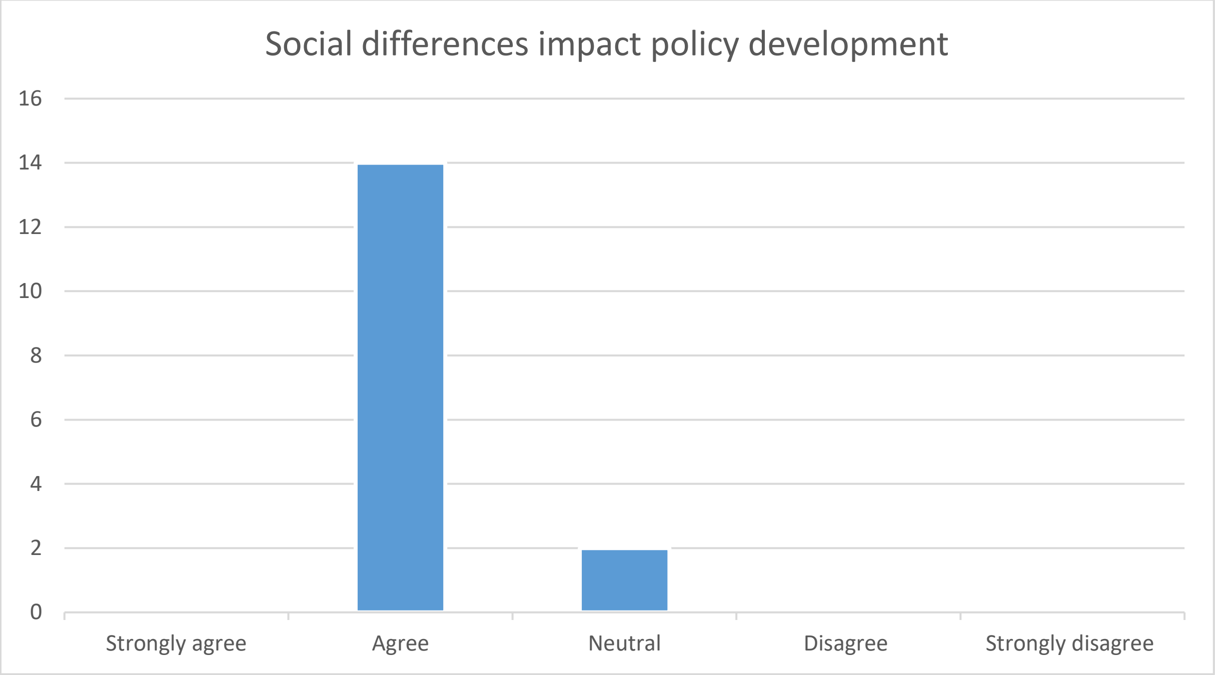


Figure D.399: Social differences impact policy development (Education)

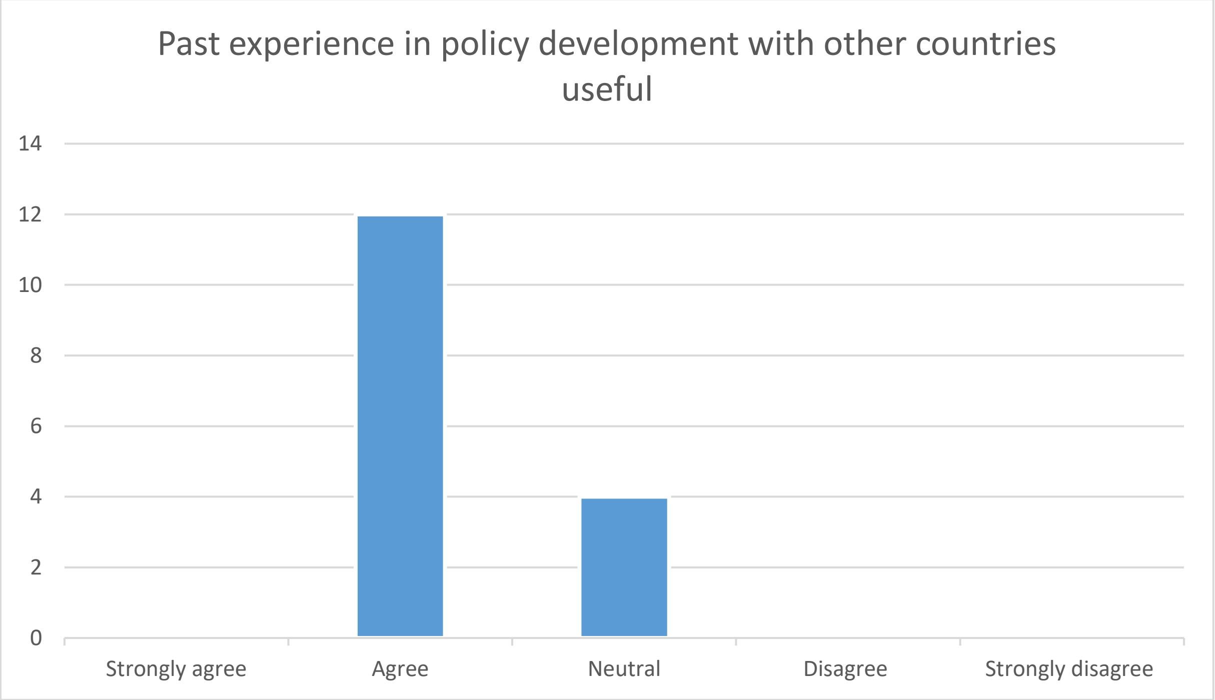


Figure D.400: Past experience in policy development with other countries useful (Education)

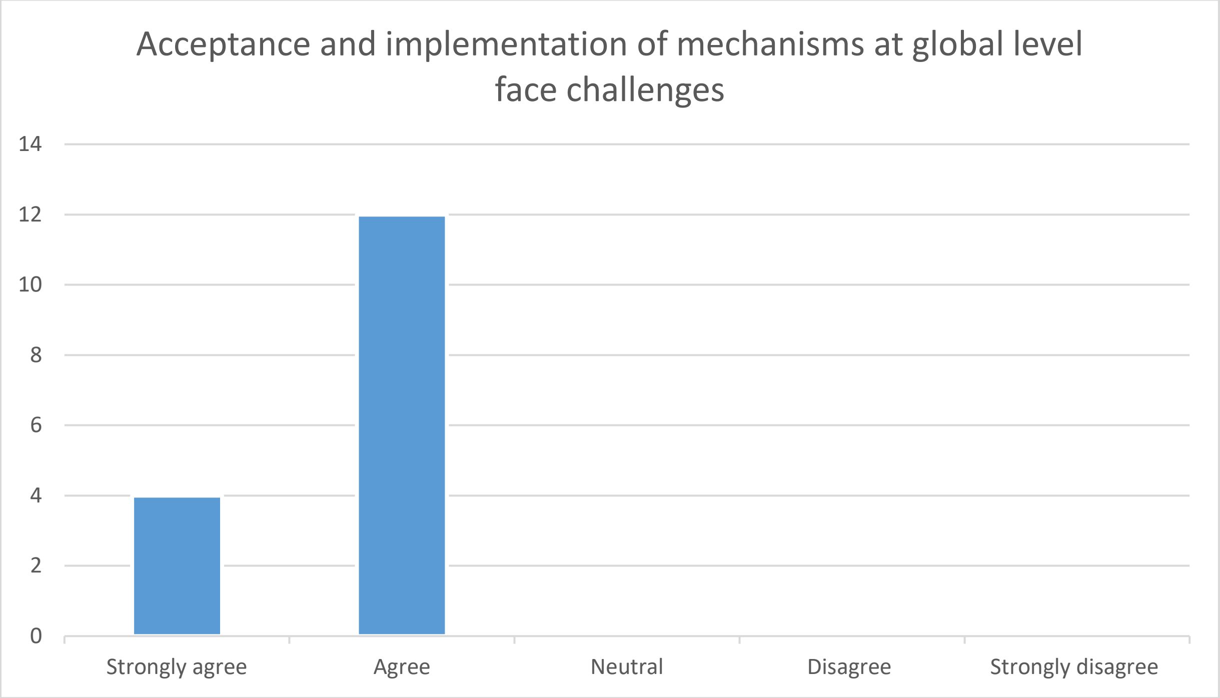


Figure D.401: Acceptance and implementation of mechanisms at global level face challenges (Education)

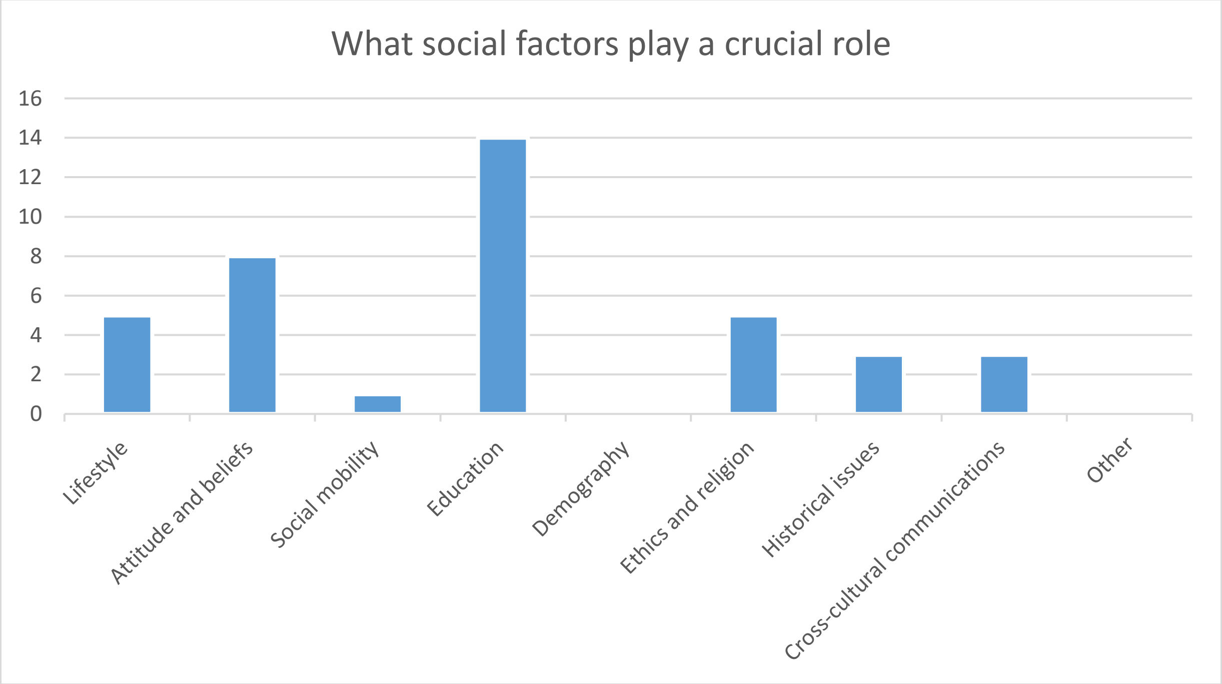


Figure D.402: What social differences play a crucial role (Education)

The responses from majority of the participants points to the relevance of education. (See figure D.402). This indicates that knowledge and familiarity with cyber threats, their impact on people and national security, is considered important in accepting and implementing data privacy and security policies. Therefore, the delivery of cybersecurity awareness training at schools, also at organisational level is of utmost importance.

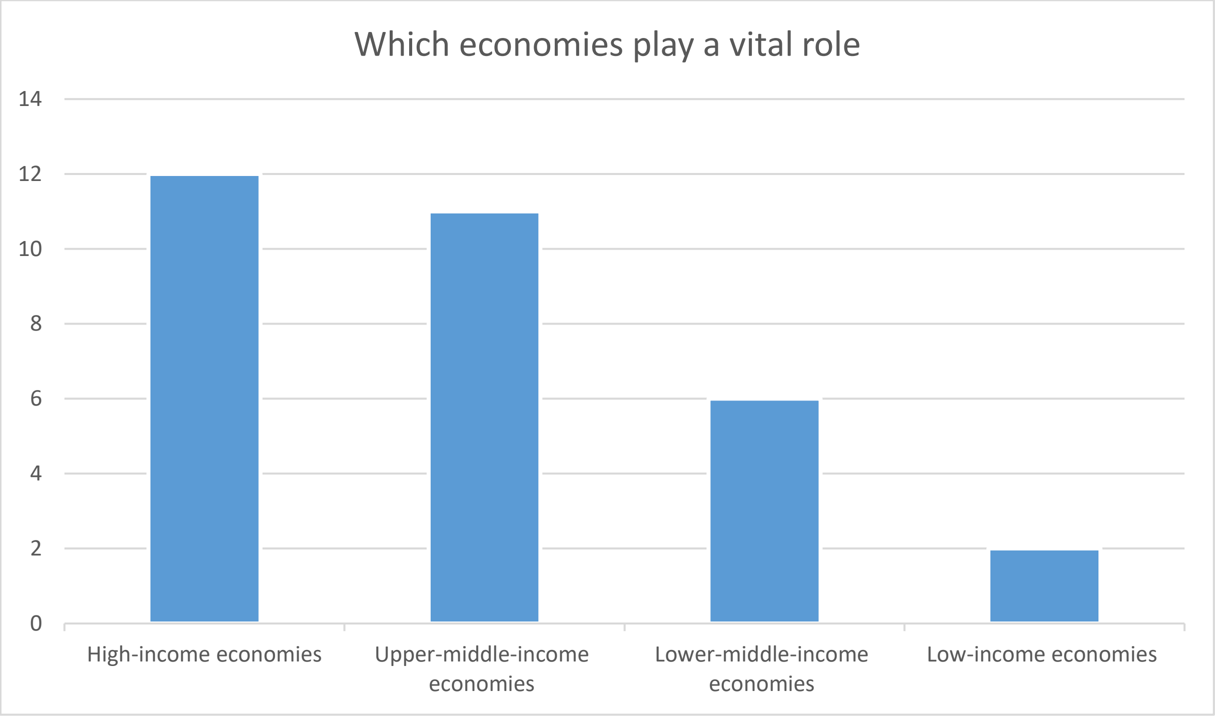


Figure D.403: Which economies play a vital role (Education)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure D.403). The key stages in the policymaking process aim to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the resources necessary, implement, and finally evaluate the policy. These stages are time-consuming and require sufficient funding and resources.

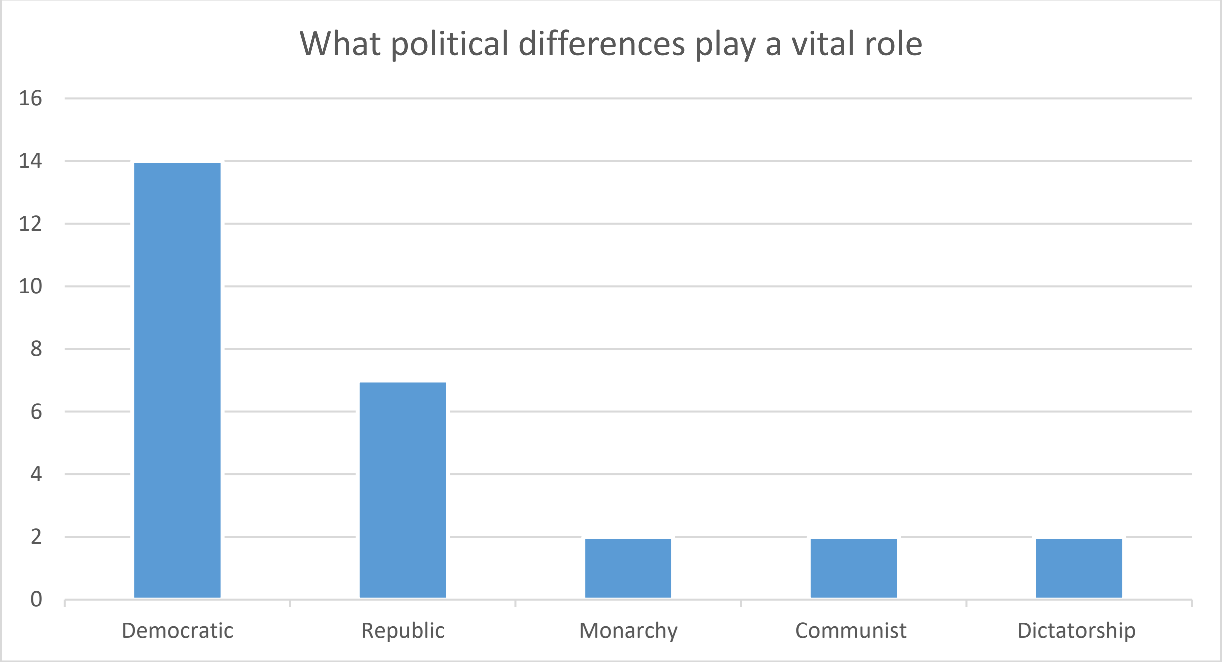


Figure D.404: What political differences play a vital role (Education)

The majority opts for a democratic political system (See figure D.404), in preference to others, as it allows public participation in the process and be influential in policy development, helps achieve consensus and collective responsibility for their actions. This forms the basis for developing trust between the organisations, and coherence and transparency in the policy development process.

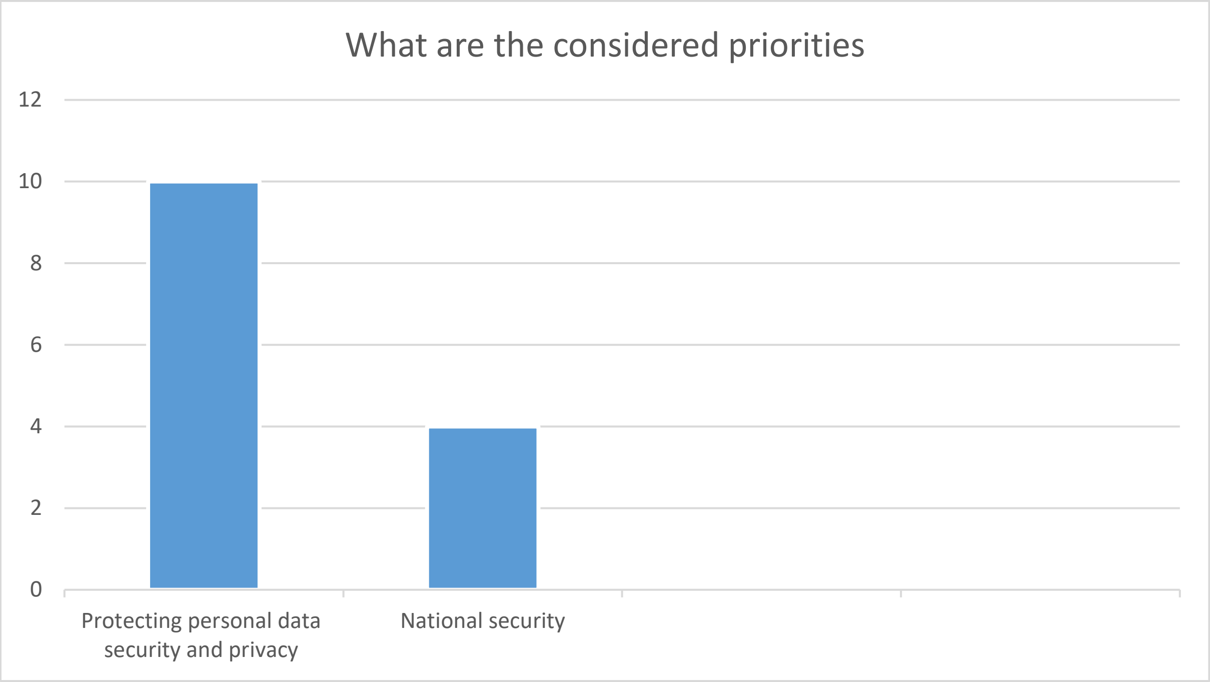


Figure D.405: What are the considered priorities (Education)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security (See figure D.405). However, in an incident of a personal data breach, there will potentially be a knock-on effect on national security, and it will also be felt right across the groups as well as the community alike.

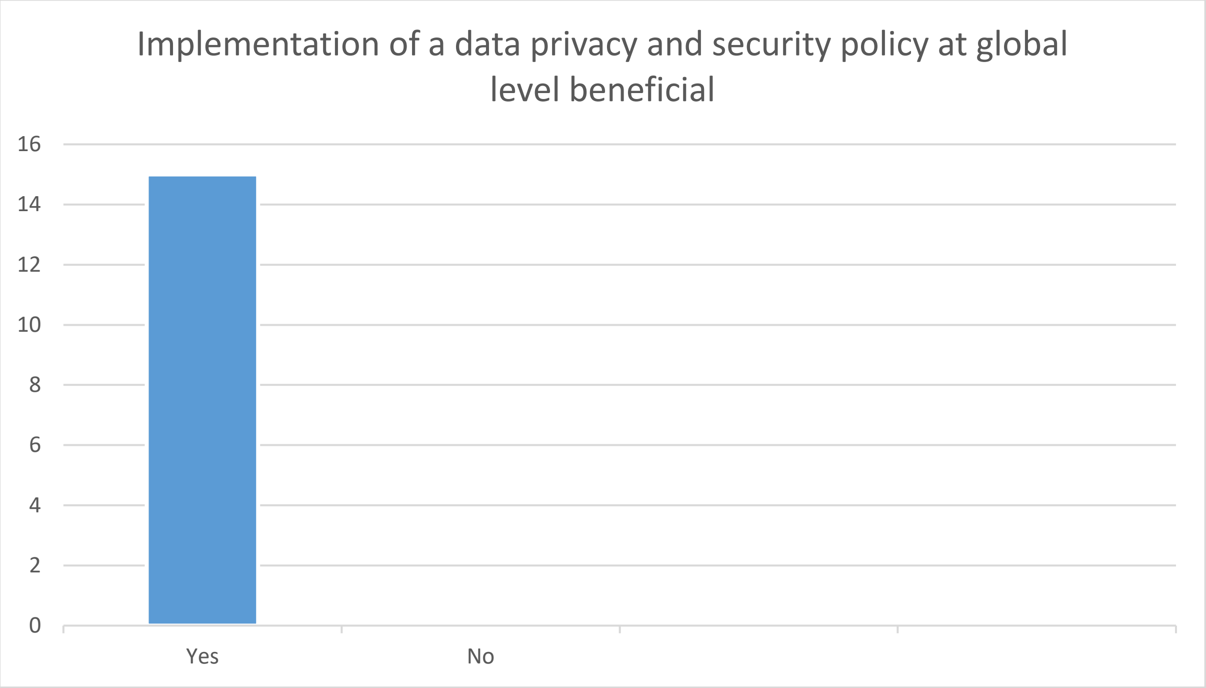


Figure D.406: Implementation of a data privacy and security policy at global level beneficial (Education)

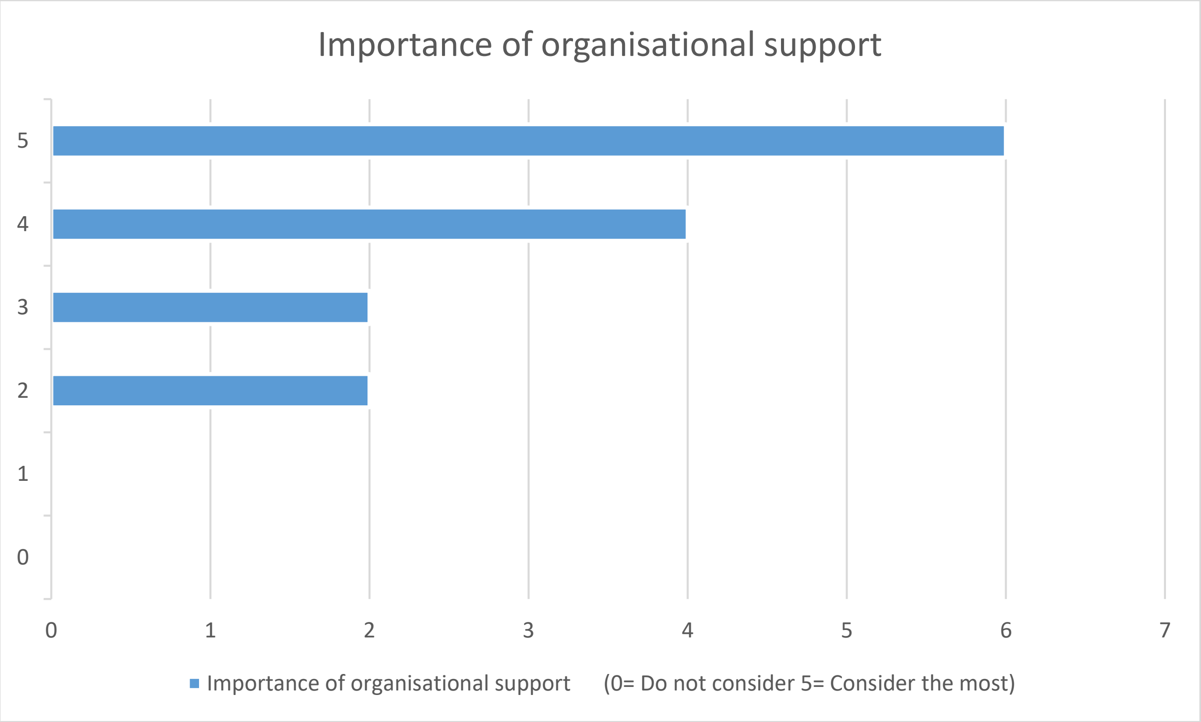


Figure D.407: Importance of organisational support (Education)

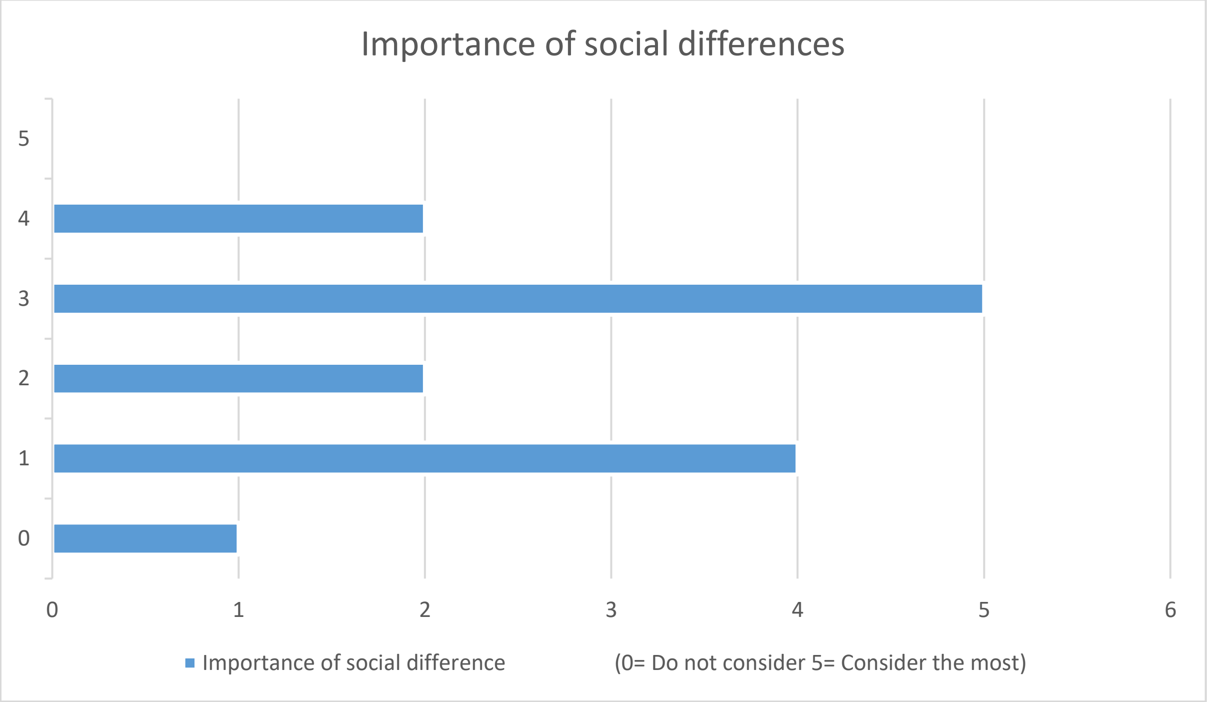


Figure D.408: Importance of social differences (Education)

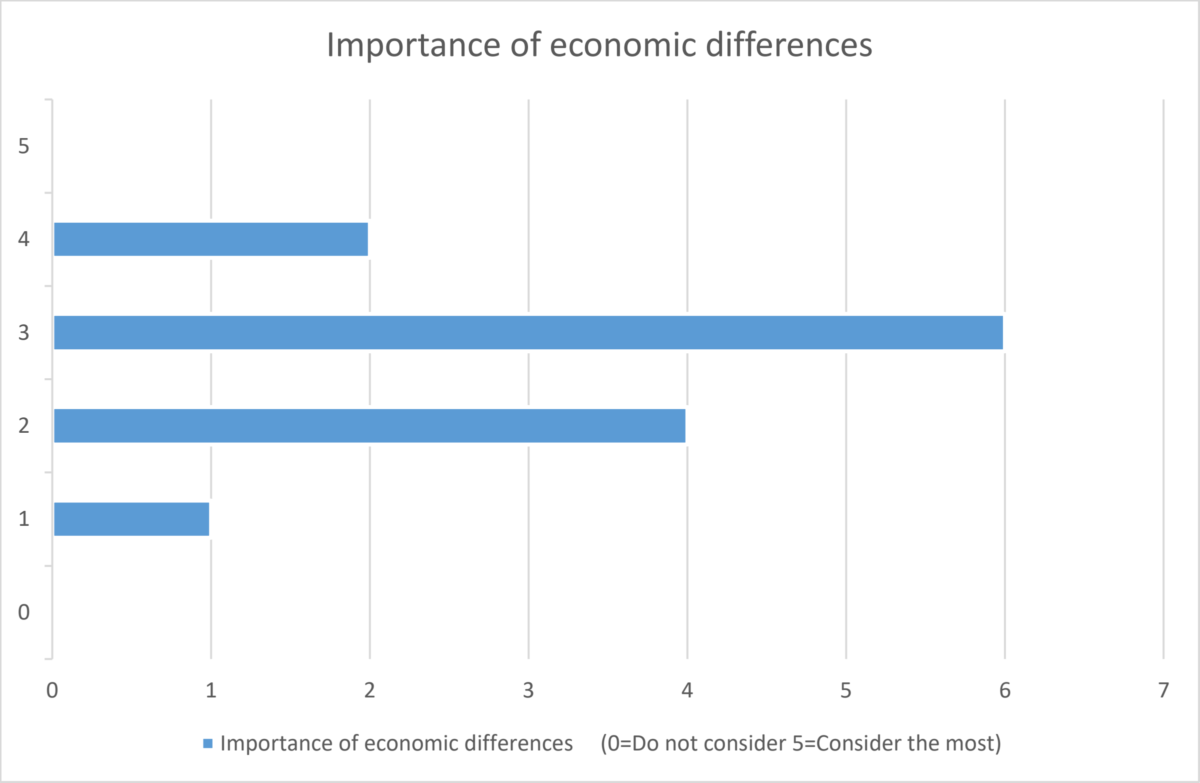


Figure D.409: Importance of economic differences (Education)

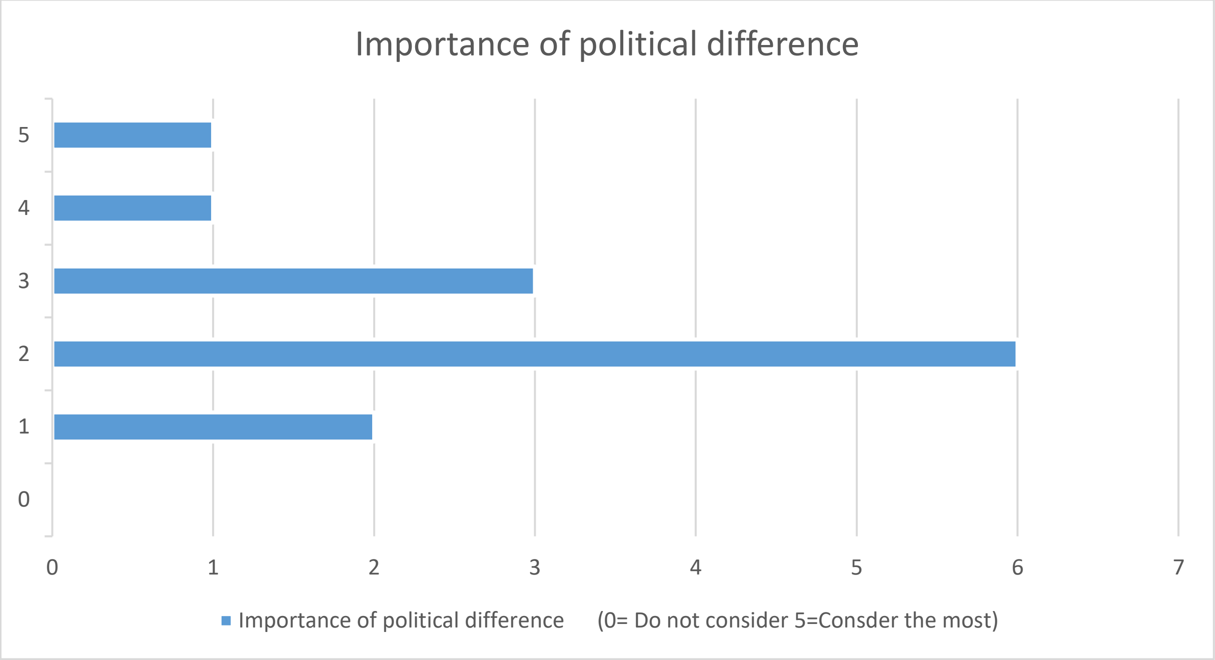


Figure D.410: Importance of political difference (Education)

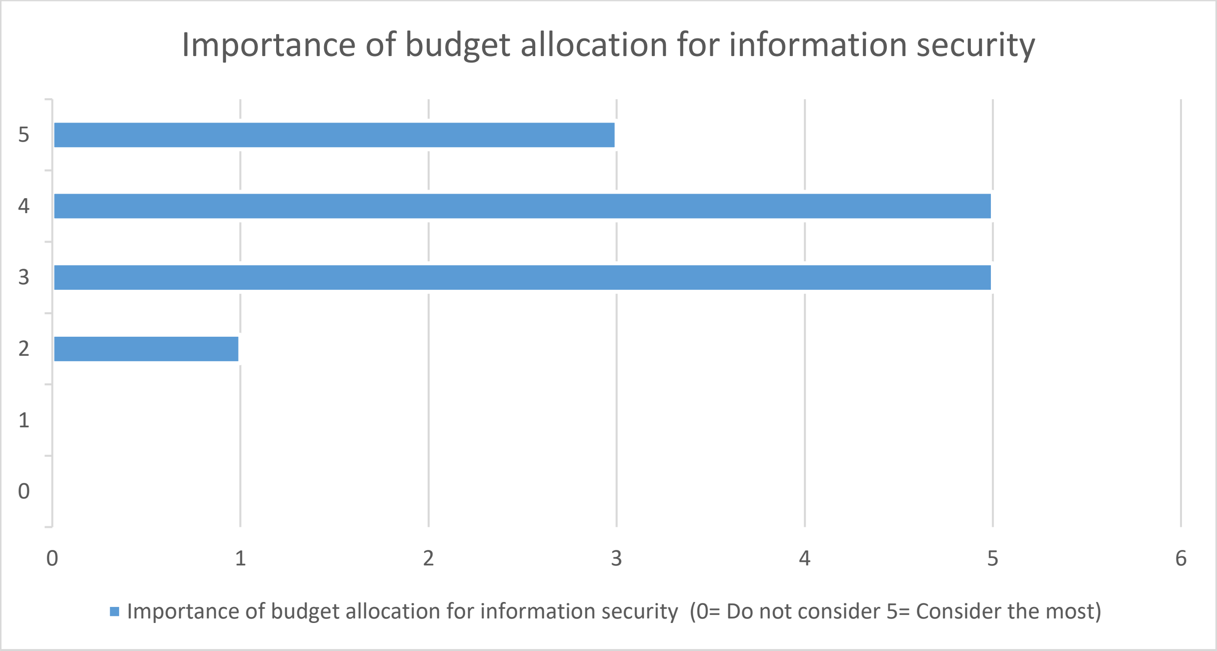


Figure D.411: Importance of budget allocation for information security (Education)

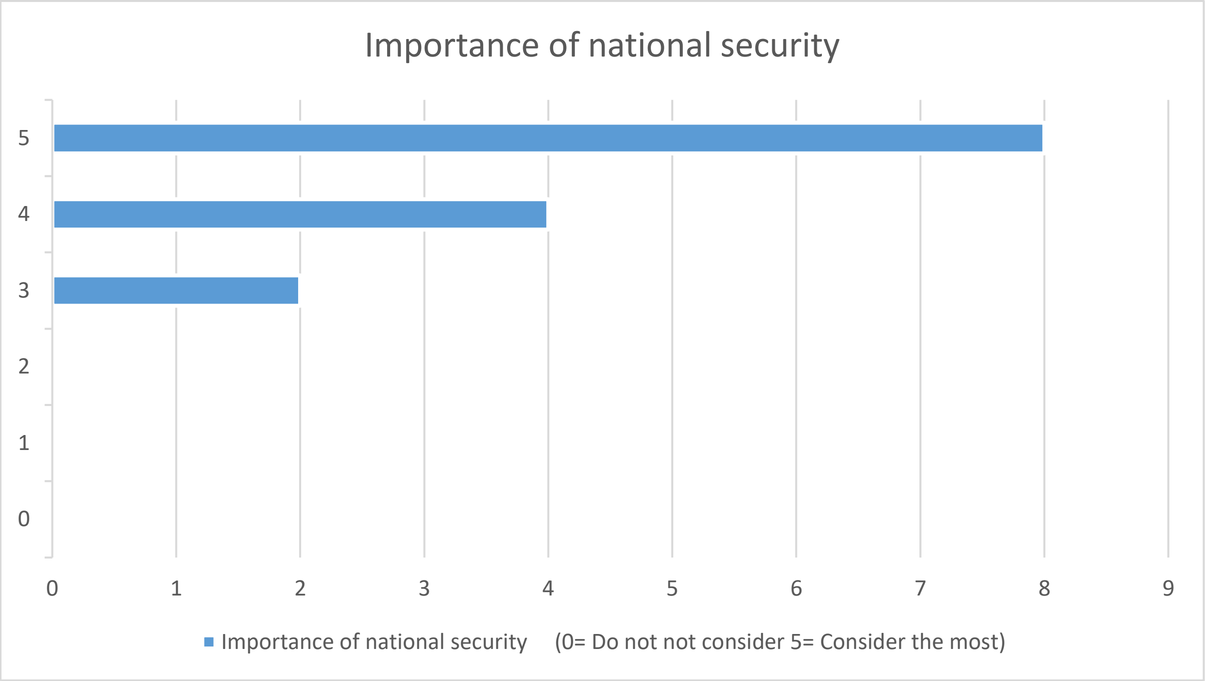


Figure D.412: Importance of national security (Education)

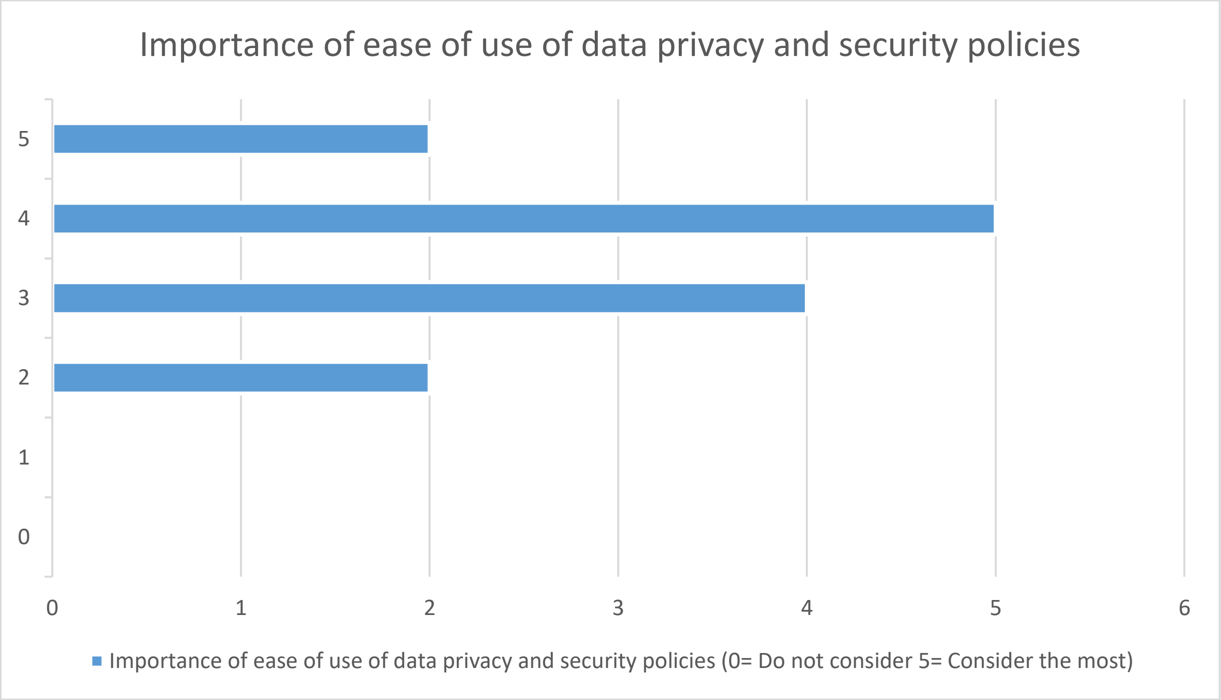


Figure D.113: Importance of ease of use of data privacy and security policies (Education)

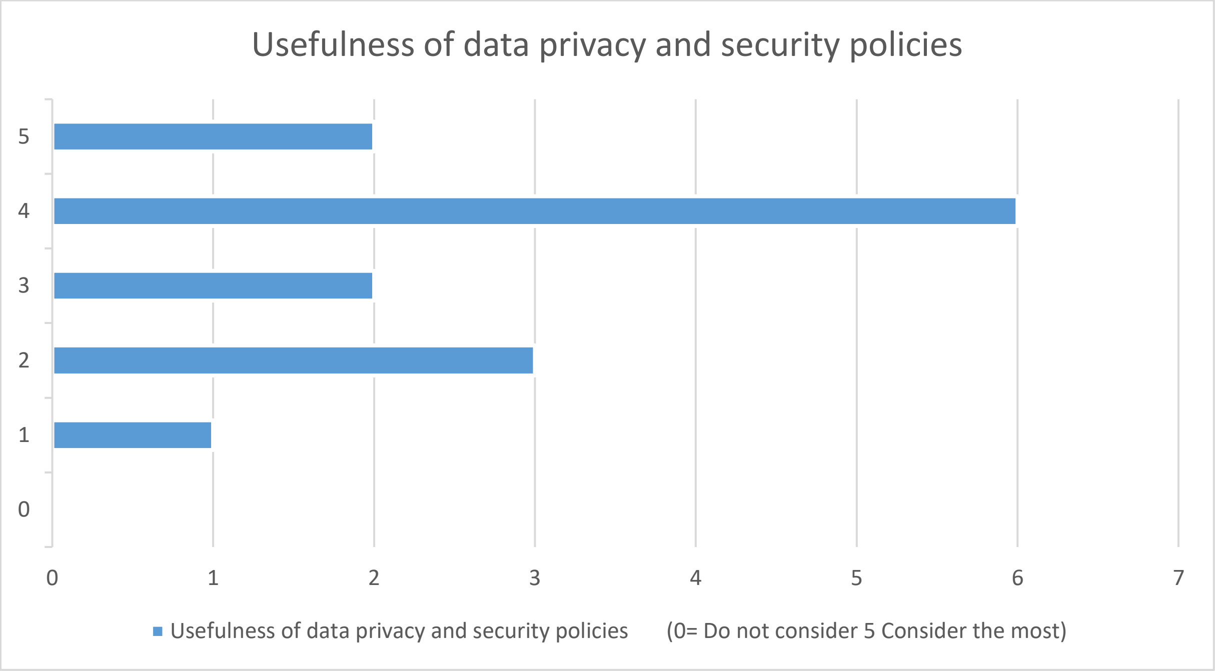


Figure D.414: Usefulness of data privacy and security policies (Education)

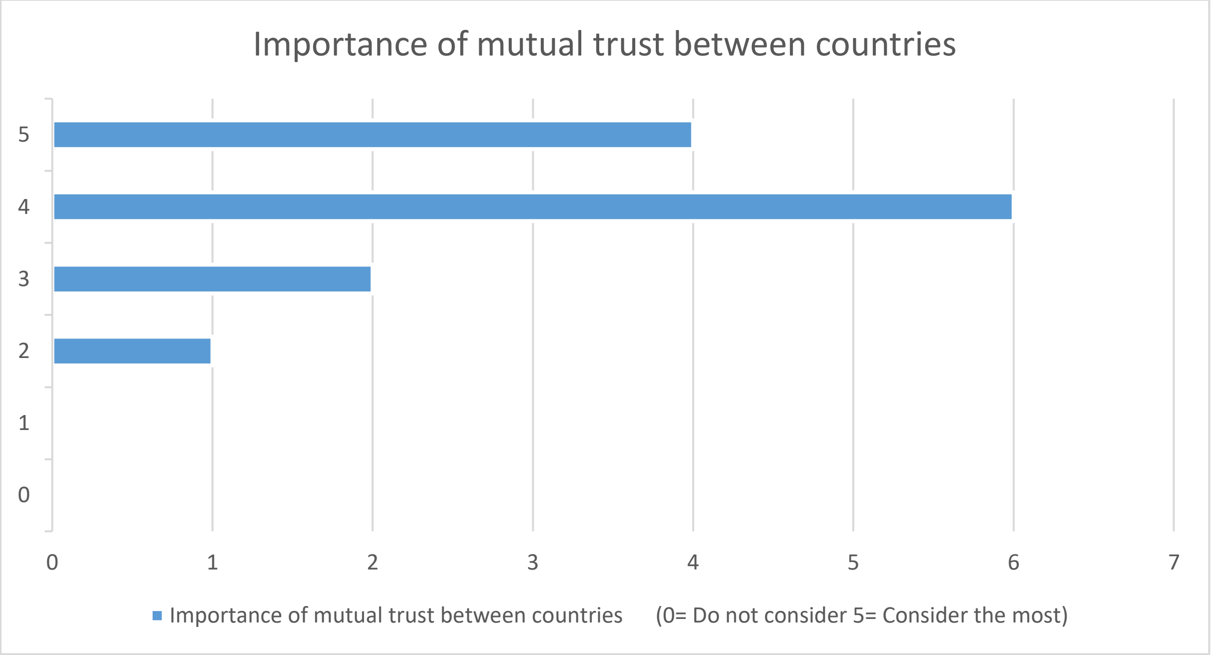


Figure D.415: Importance of mutual trust between countries (Education)

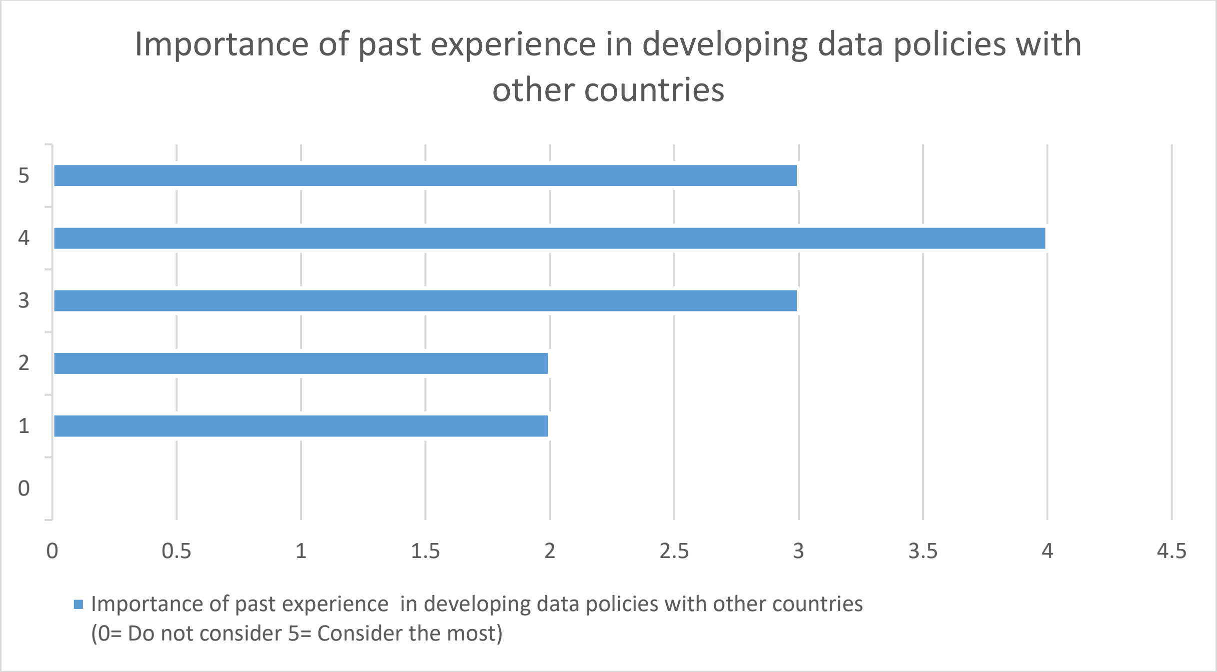


Figure D.416: Importance of past experience in developing data policies with other counties (Education)

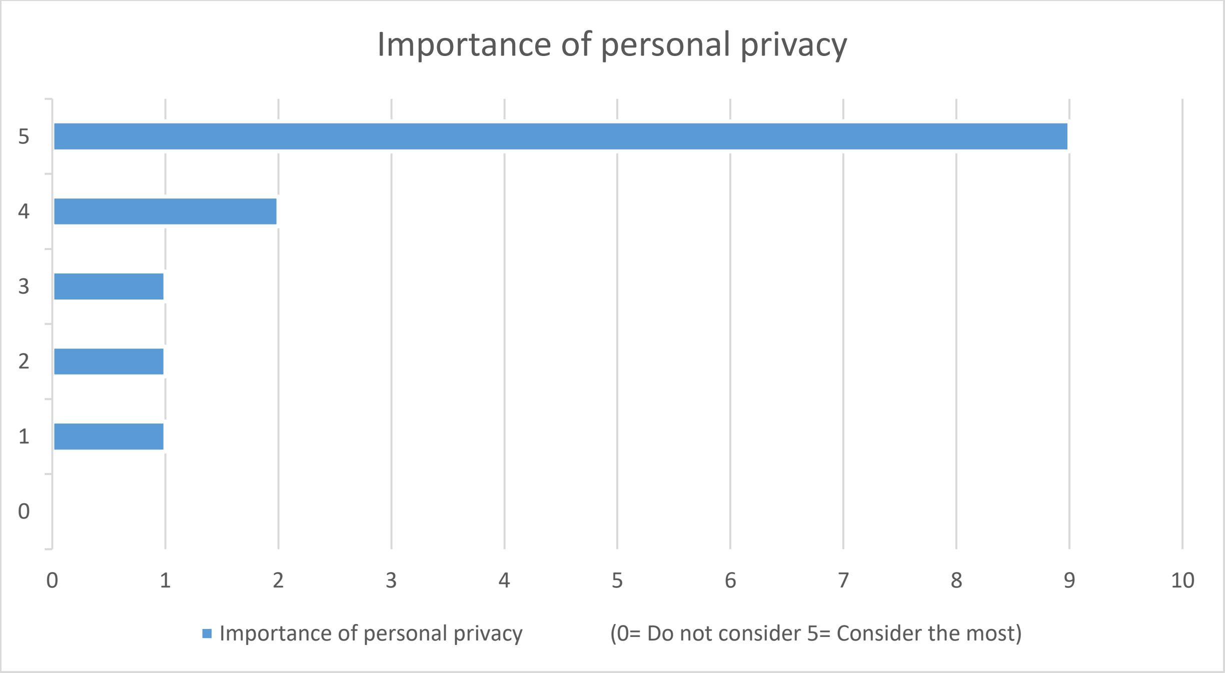


Figure D.417: Importance of personal privacy (Education)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 88 percent of the respondents have endorsed (See figure D.406). The other notable factors to come out of the survey are organisational support, budget allocation, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries, previous experience in developing policies with other countries (See figure D.395-405) (See figure D.407-417).

Sri Lanka – Healthcare

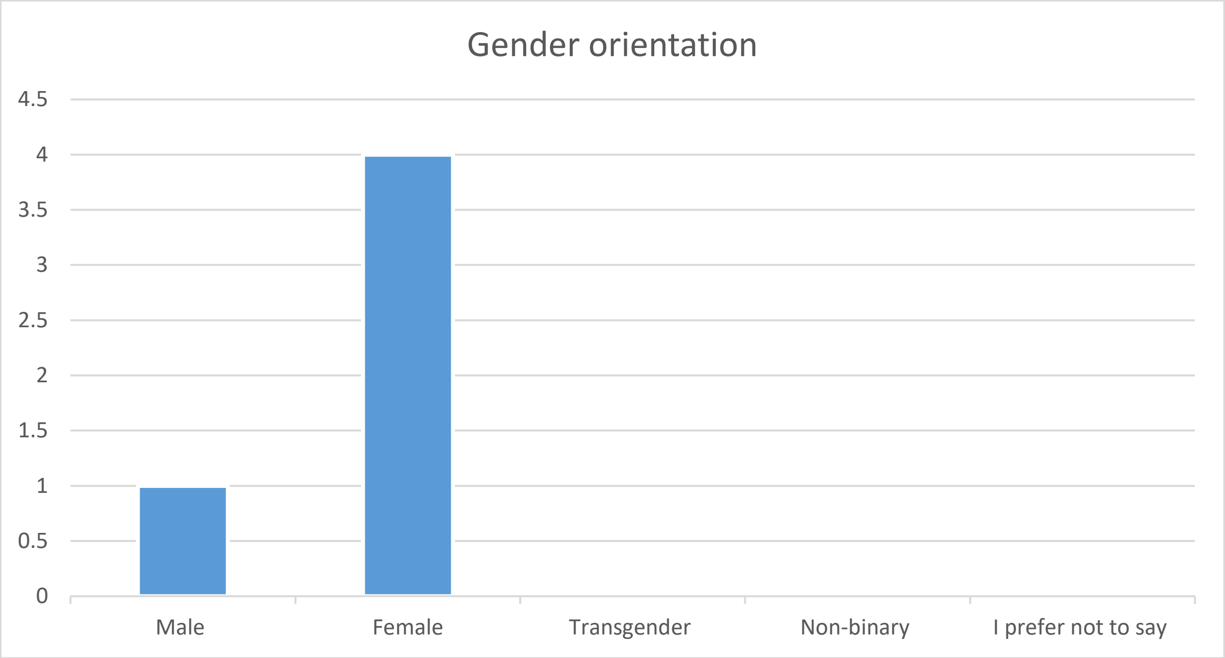


Figure D.418: Gender orientation (Healthcare)

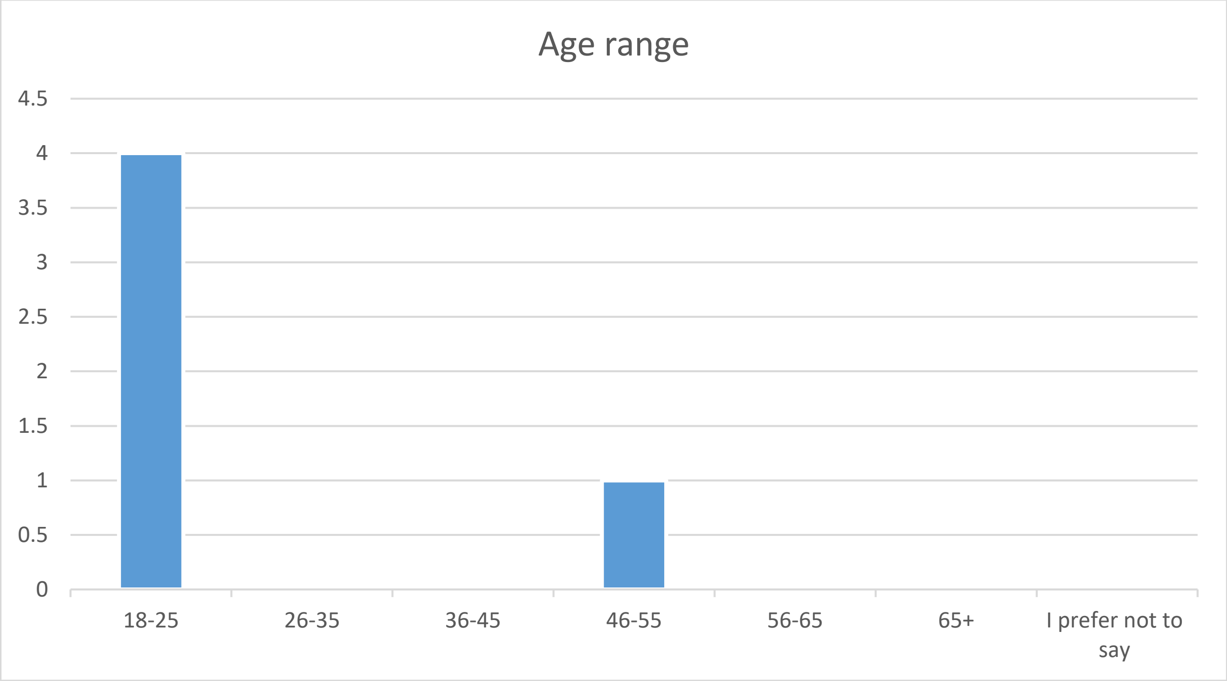


Figure D.419: Age range (Healthcare)

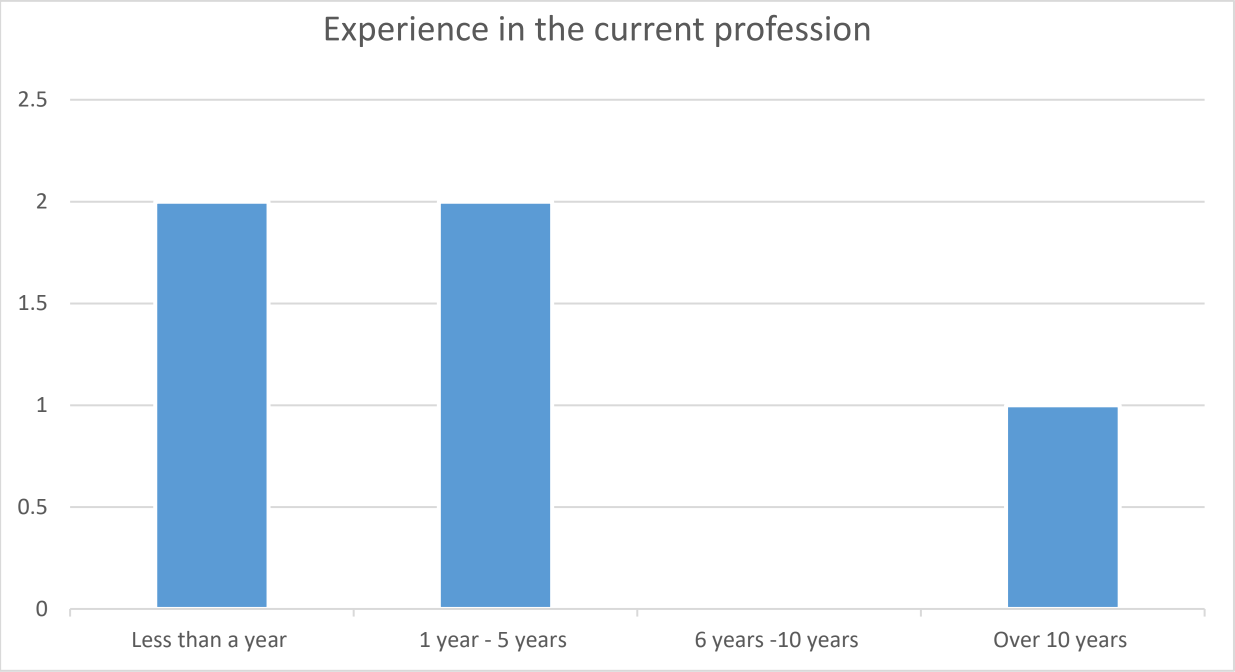


Figure D.420: Experience in current profession (Healthcare)

This analysis is based on the responses received from Sri Lankan participants working in the healthcare sector. Of the 5 participants, 4 are females and 1 male (See figure D.418). Their overall age range is within 18-55; 4 in the 18-25 and 1 in the 46-55 range (See figure D.419). The time duration in work is between less than a year to over 10 years (See figure D.420).

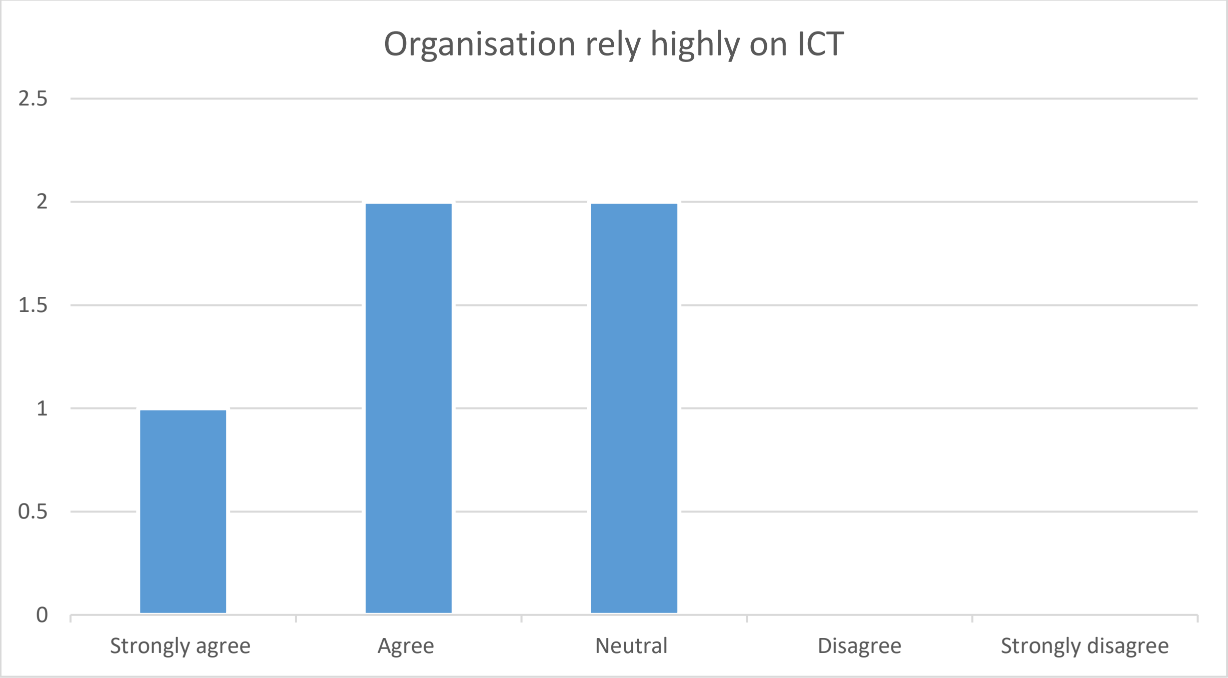


Figure D.421: Organisation rely highly on ICT (Healthcare)

Out of the 5 respondents, 3 work in a technology reliance working environment, 2 unaware due to the nature of the work assigned to them (See figure D.421). This indicates that the majority working in the healthcare sector has a high reliance on ICT.

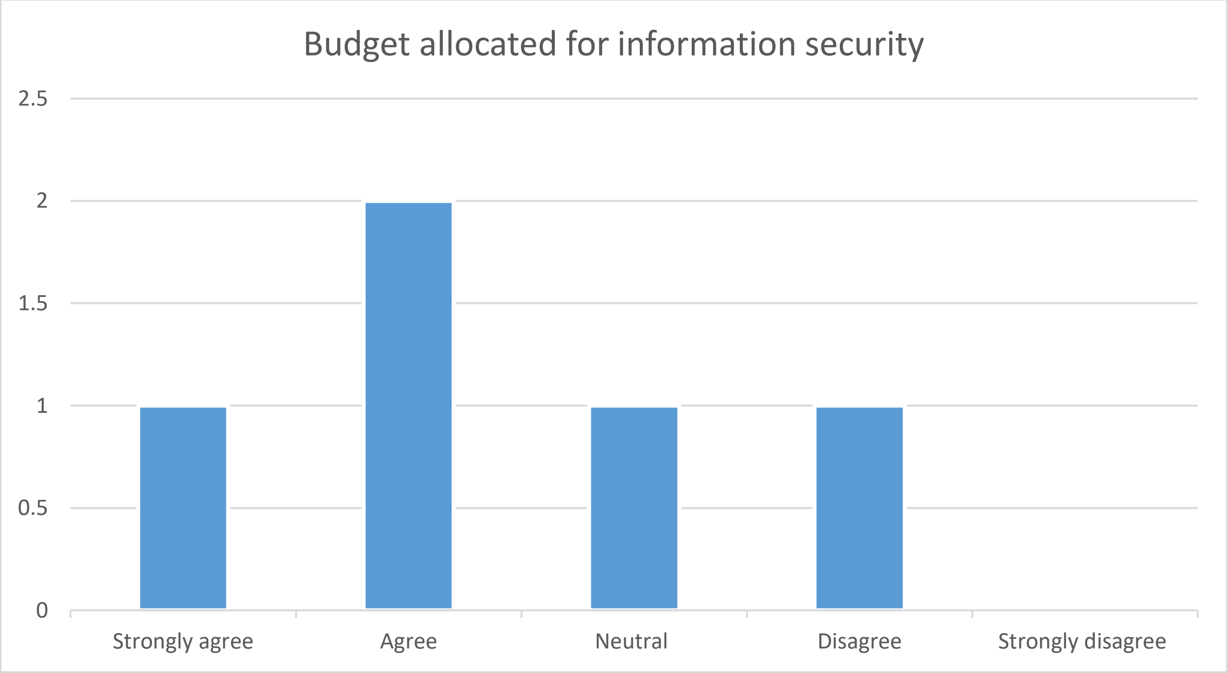


Figure D.422: Budget allocated for information security (Healthcare)

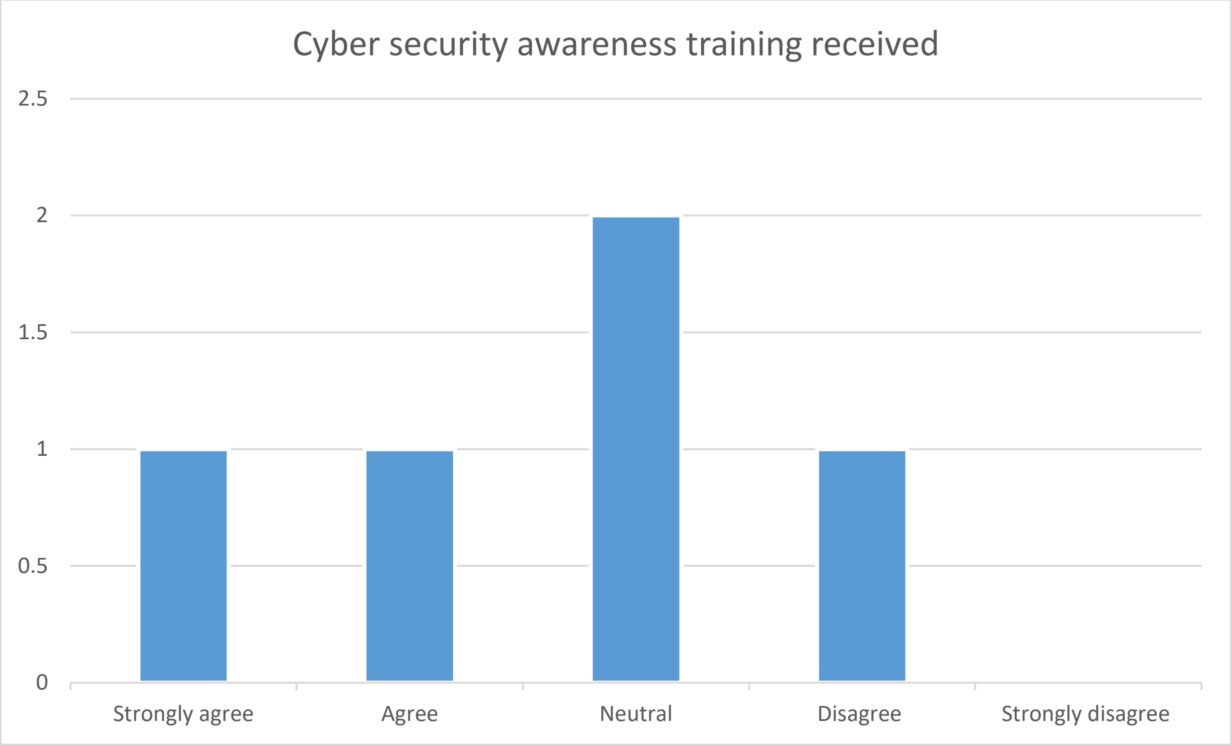


Figure D.423: Cyber security awareness training received (Healthcare)

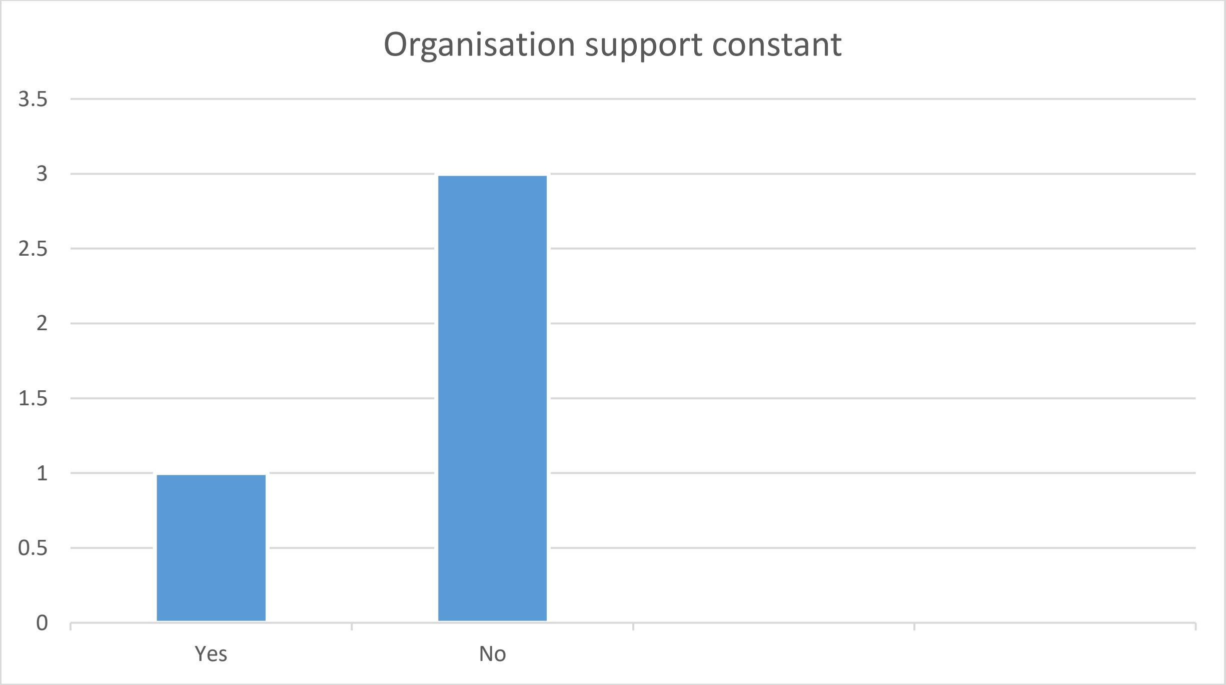


Figure D.424: Organisation support constant (Healthcare)

3 out of the 5 agree that their organisations have an allocated budget for information security, 1 neither agrees nor disagrees; according to the 1 disagreed, their organisations does not (See figure D.422). However, the response from some participants points out that despite the satisfactory level of resources allocated for information security, regular security awareness training received was inadequate. Only 2 participants received regular cybersecurity awareness training; 2 neither agreed nor disagreed; 1 had no training at all (See figure D.423). In respect of support from the organisation to protect personal information, 3 had not any; only 1 had (See figure D.424). This shows a lack of organisational support to protect personal information, despite financial resources being available for information security and high reliance on technology. Therefore, not providing resources to provide necessary support and training for their employees in the healthcare service could risk compromising the health records of the patients. Breaches of any will be detrimental and will jeopardise patient confidence and trust in the organisation.

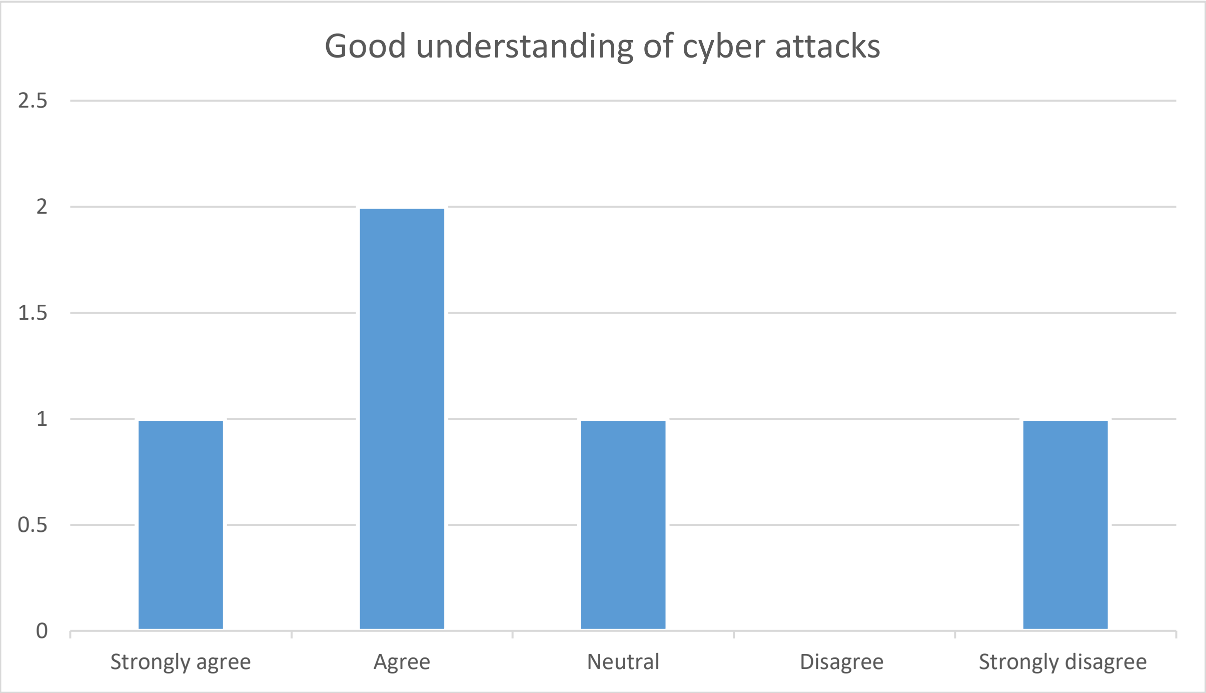


Figure D.425: Good understanding of cyberattacks (Healthcare)

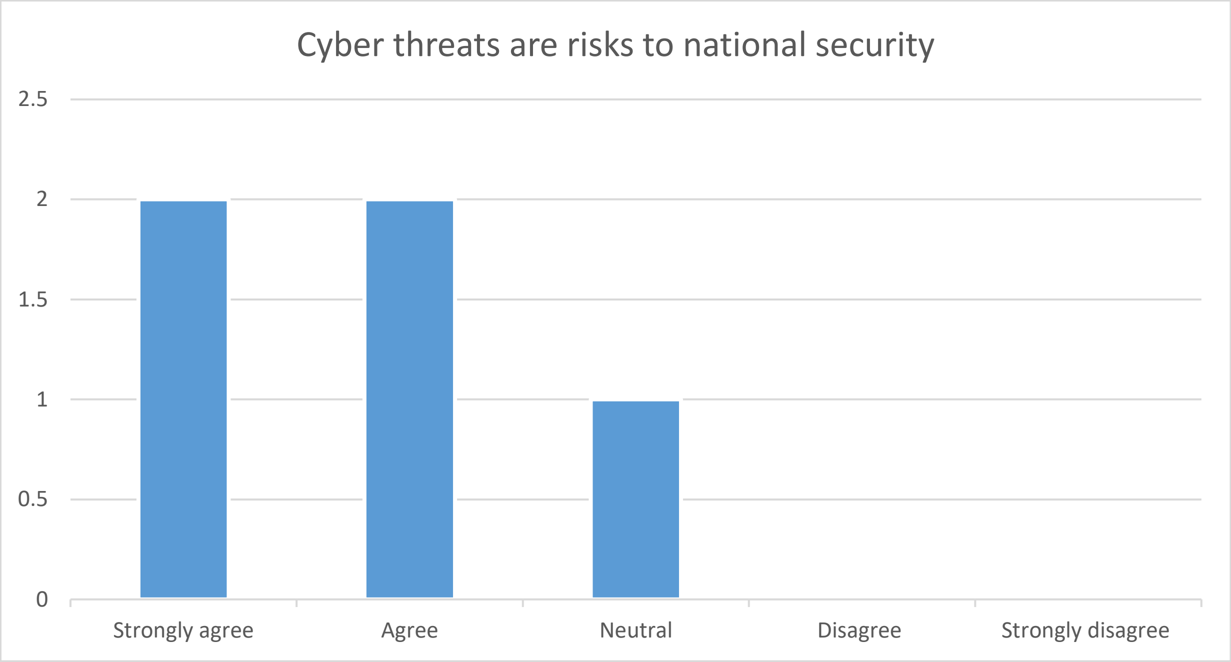


Figure D.426: Cyber threats are risks to national security (Healthcare)

The participants have a high understanding of the impact of cyber-attacks on the public and the organisation, despite the lack of security awareness training. Accordingly, 3 participants have a good understanding of cyber attacks; 1 had no understanding; 1 said neither (See figure D.425). Furthermore, 80 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure D.426). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in time, their concerns will influence the process of accepting and implementing a national, regional, and global level mechanism.

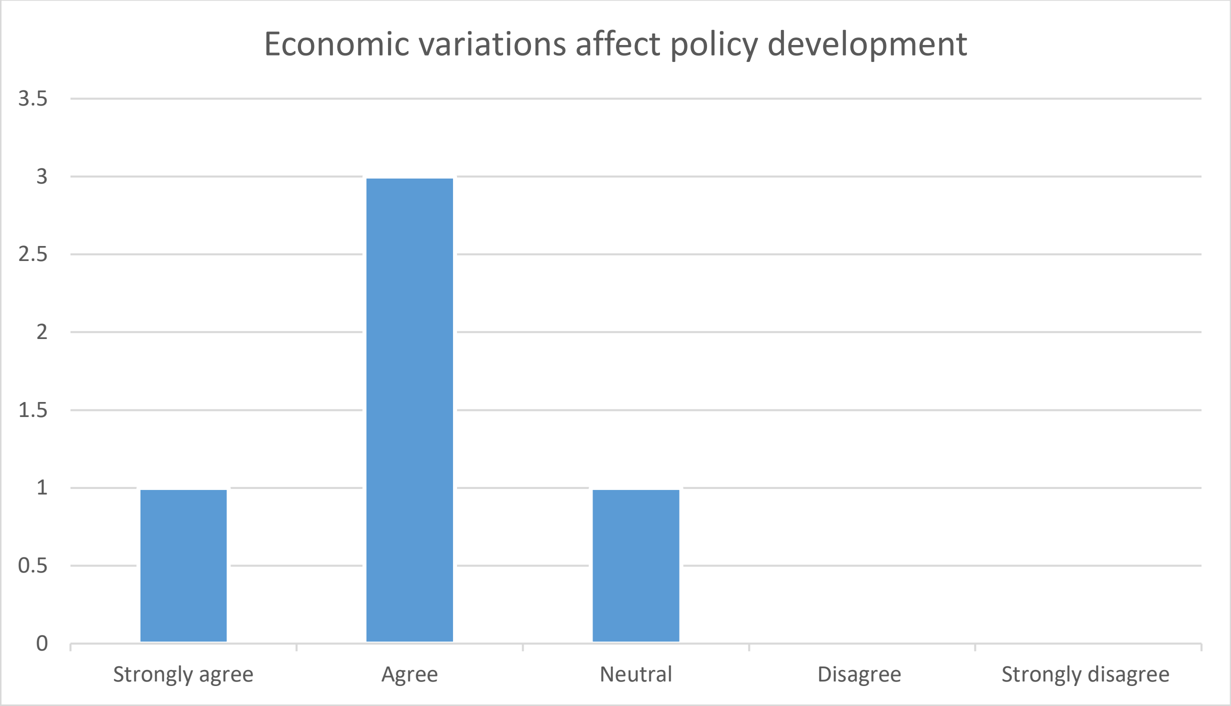


Figure D.427: Economic variations affect policy development (Healthcare)

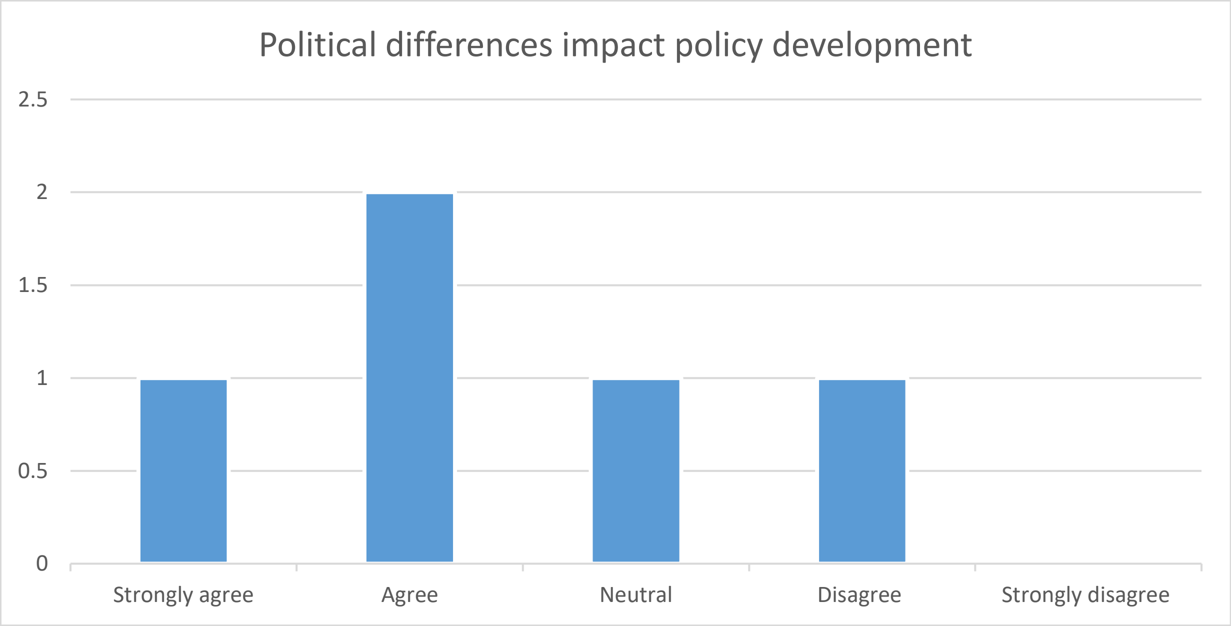


Figure D.428: Political differences impact policy development (Healthcare)

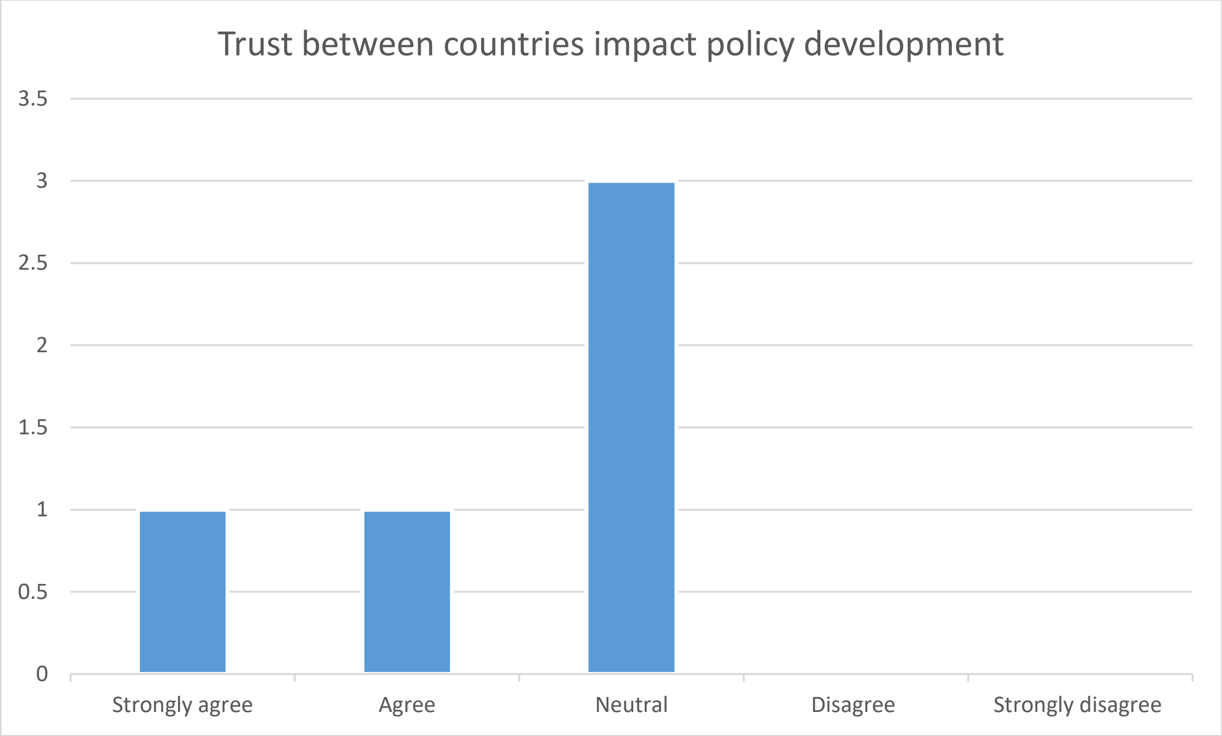


Figure D.429: Trust between countries impact policy development (Healthcare)

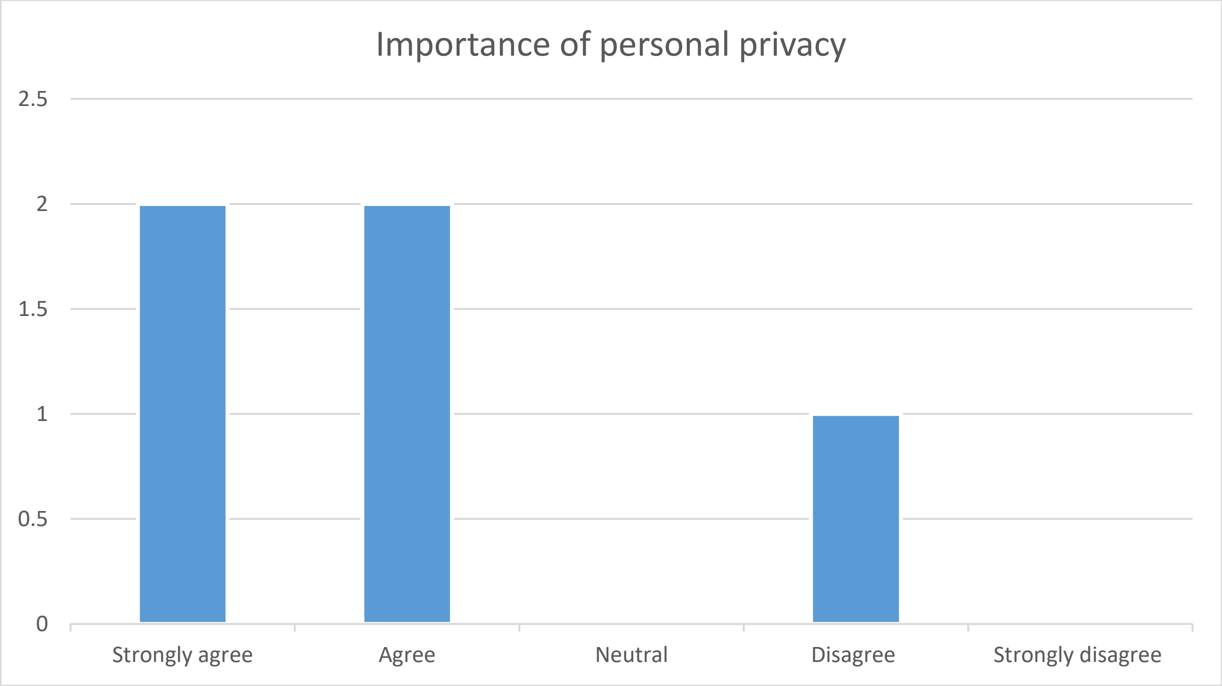


Figure D.430: Importance of personal privacy (Healthcare)

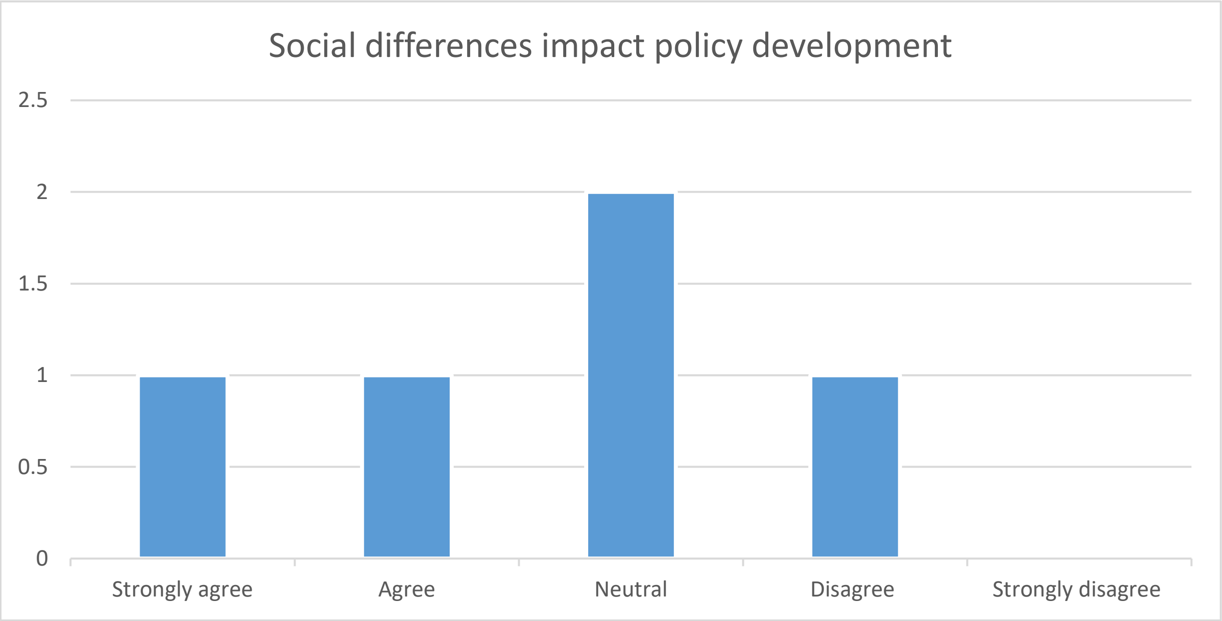


Figure D.431: Social differences impact policy development (Healthcare)

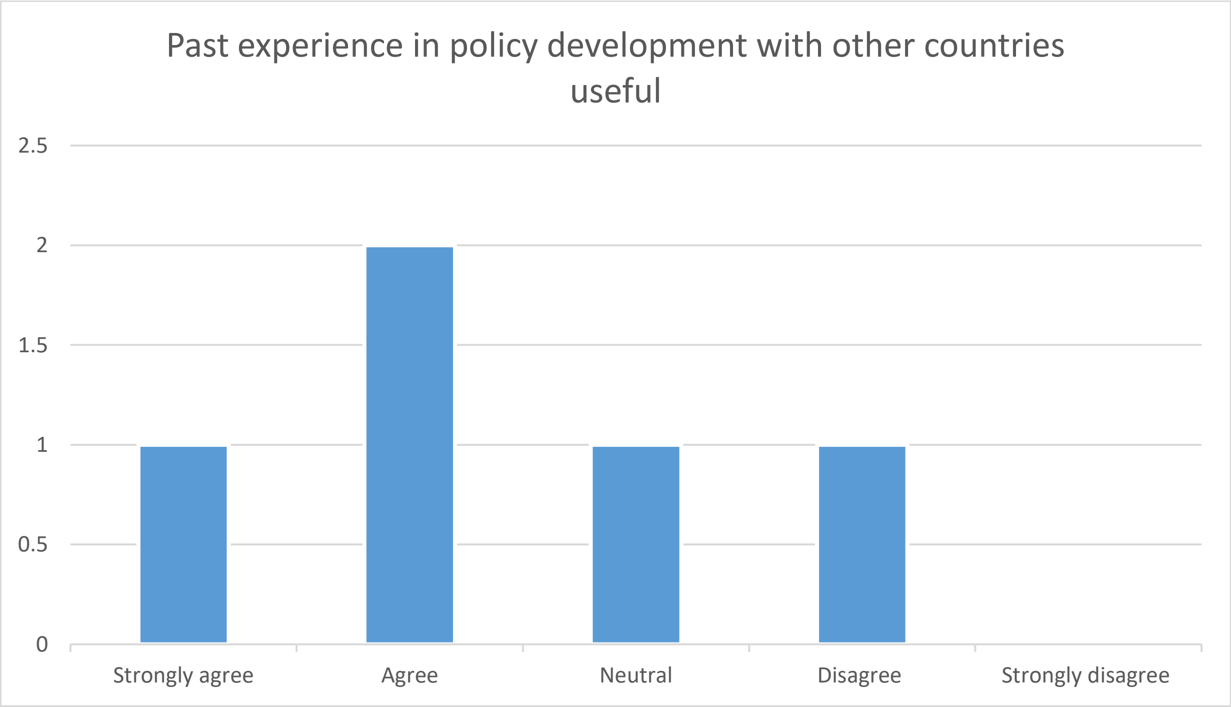


Figure D.432: Past experience in policy development with other countries useful (Healthcare)

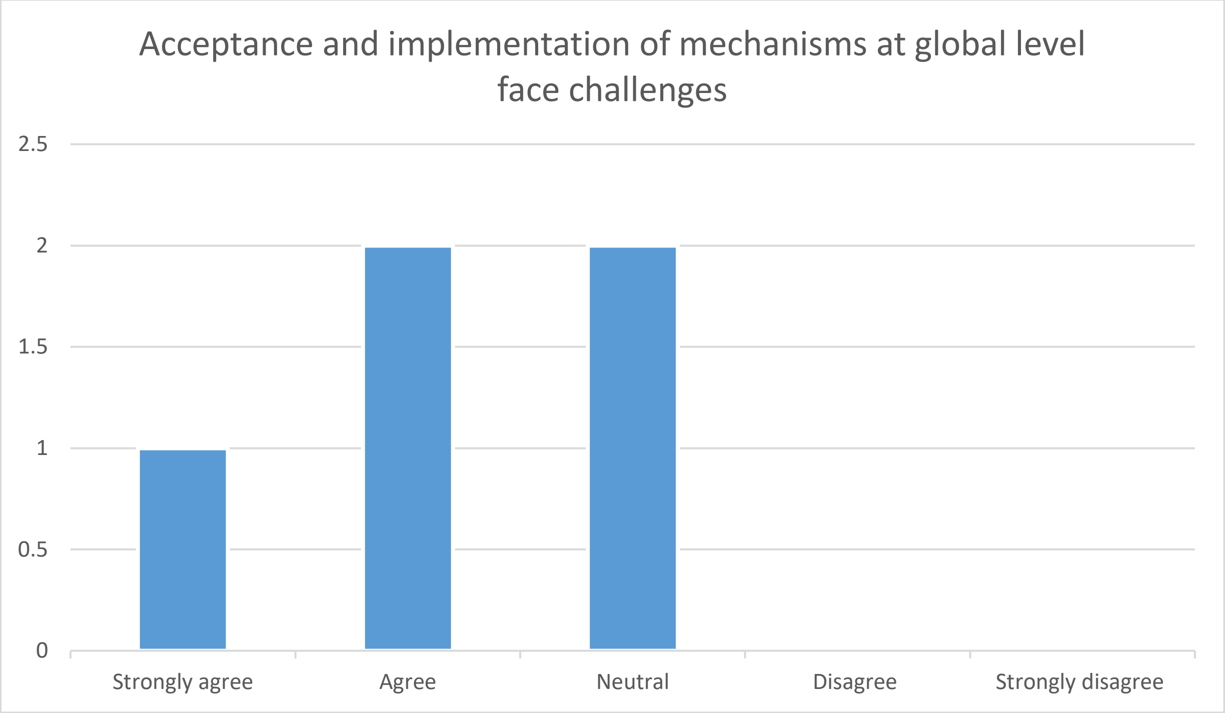


Figure D.433: Acceptance and implementation of mechanisms at global level face challenges (Healthcare)

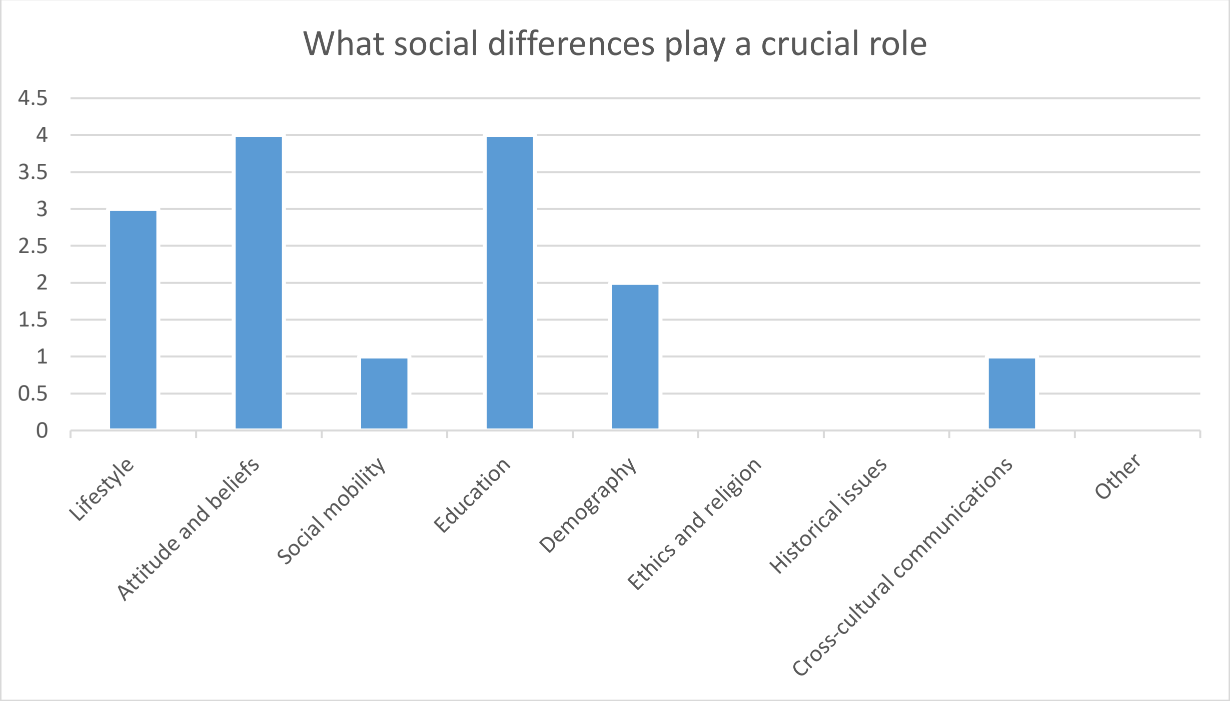


Figure D.434: What social differences play a crucial role (Healthcare)

The majority of the respondents feel positive about the importance of education, lifestyle and attitude and beliefs when considering social differences (See figure D.434), also there is an awareness of the importance of knowledge and familiarity with potential cyber threats, their impact on people and national security in accepting and implementing data privacy and security policies. That reflects the importance of providing cybersecurity awareness training at schools and at the organisational level. Also, the provision of educational training will be an effective way to make people understand the importance of privacy and the implications associated with privacy violations. If there is a high reliance on technology in sharing or handling personal information, the demand for accepting and implementing policies associated with data privacy and security also should be high. The contributory factors such as believing in privacy and respecting the privacy of self and others have been discussed under attitude and believes.

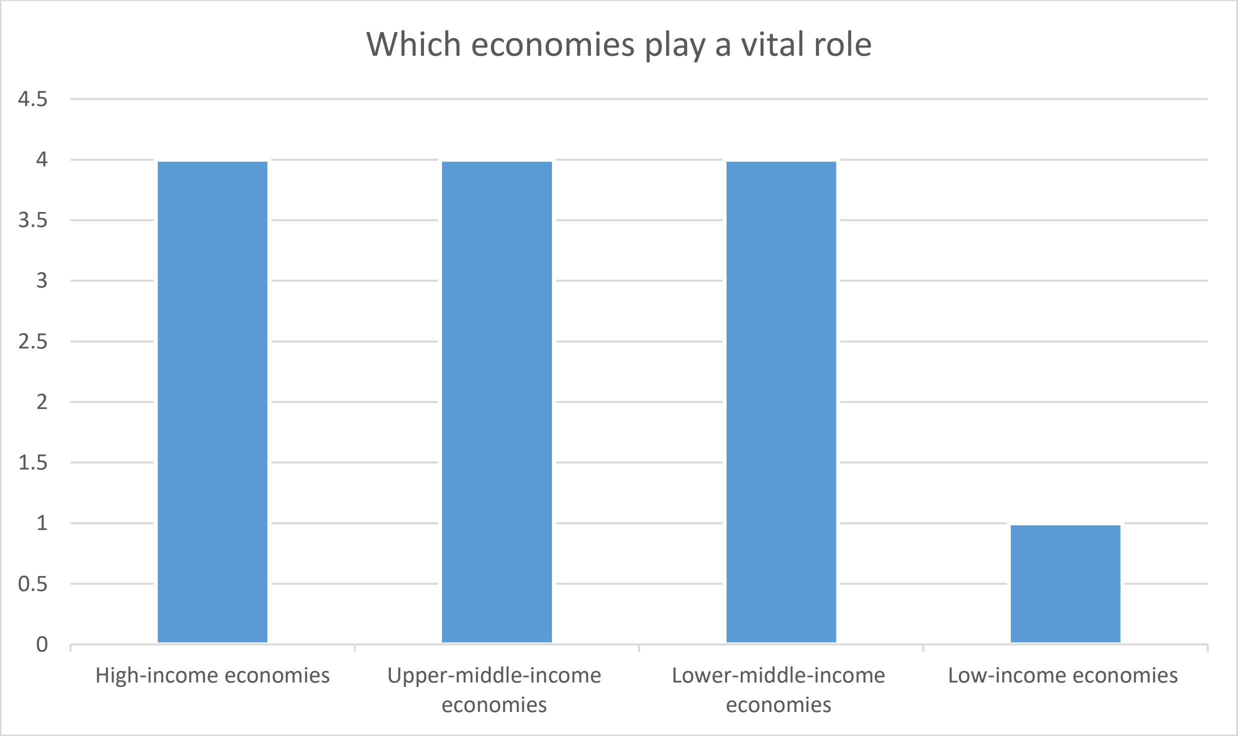


Figure D.435: Which economies play a vital role (Healthcare)

The majority indicates that high income, and upper-middle-income, and lower-middle-income countries play a vital role in the policy development process (See figure D.435). The key stages in policymaking are to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the necessary resources, and then implement and then evaluate the policy. Therefore, achieving success to a large extent depends on the economic stability of the country, which counts as a crucial factor in policymaking. The significant factor here is none of the participants in other sectors highlighted the importance of lower-middle-income economies.

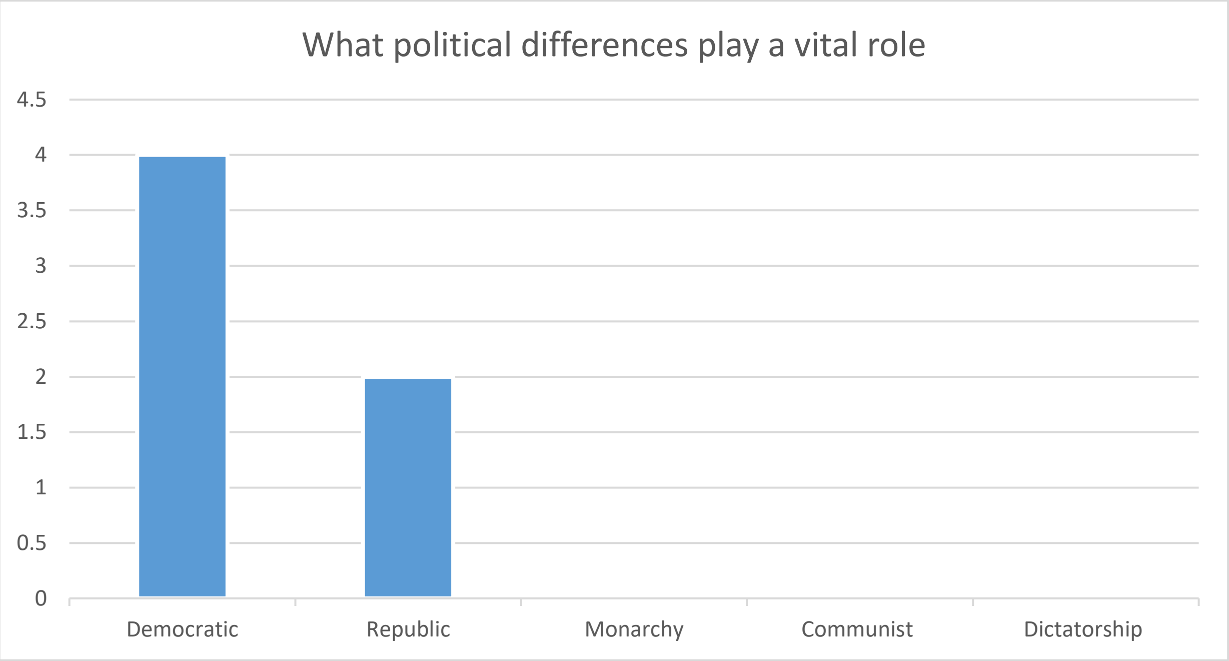


Figure D.436: What political differences play a vital role (Healthcare)

The majority have favoured the democratic political system in preference to others (See figure D.436) because it allows public participation in policy development, and influence the process of policy development, and promote consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

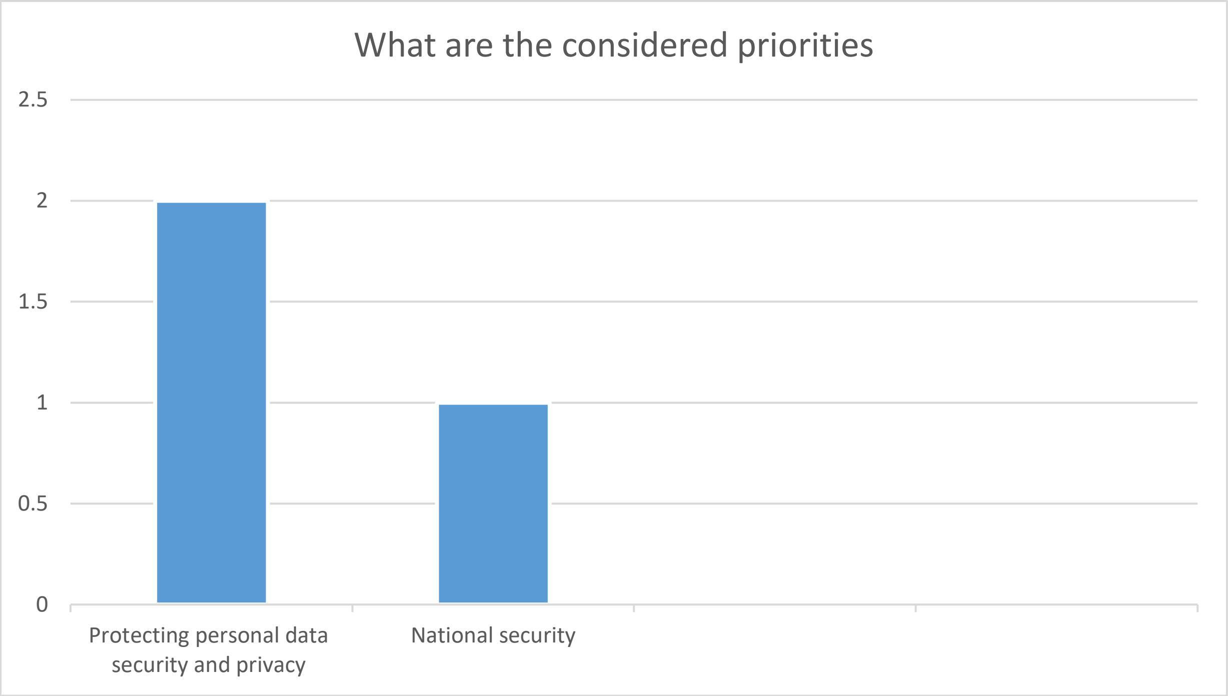


Figure D.437: What are the considered priorities (Healthcare)

The marked difference here is the majority not recognising the importance of protection of personal data security and privacy, and protection of national security (See figure D.437). In an incident of a personal data breach, there will potentially be a knock-on effect on both personal data security and privacy, and national security, and it will also be felt right across the groups as well as the community alike.

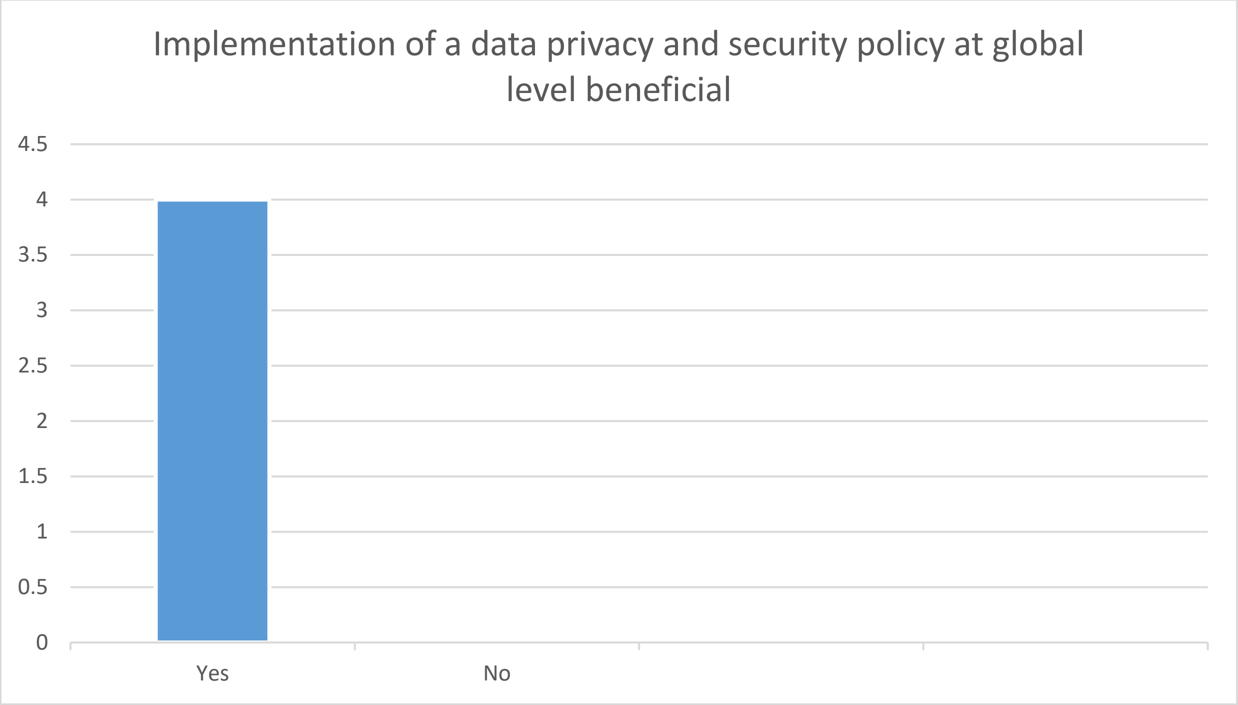


Figure D.438: Implementation of a data privacy and security policy at global level beneficial (Healthcare)

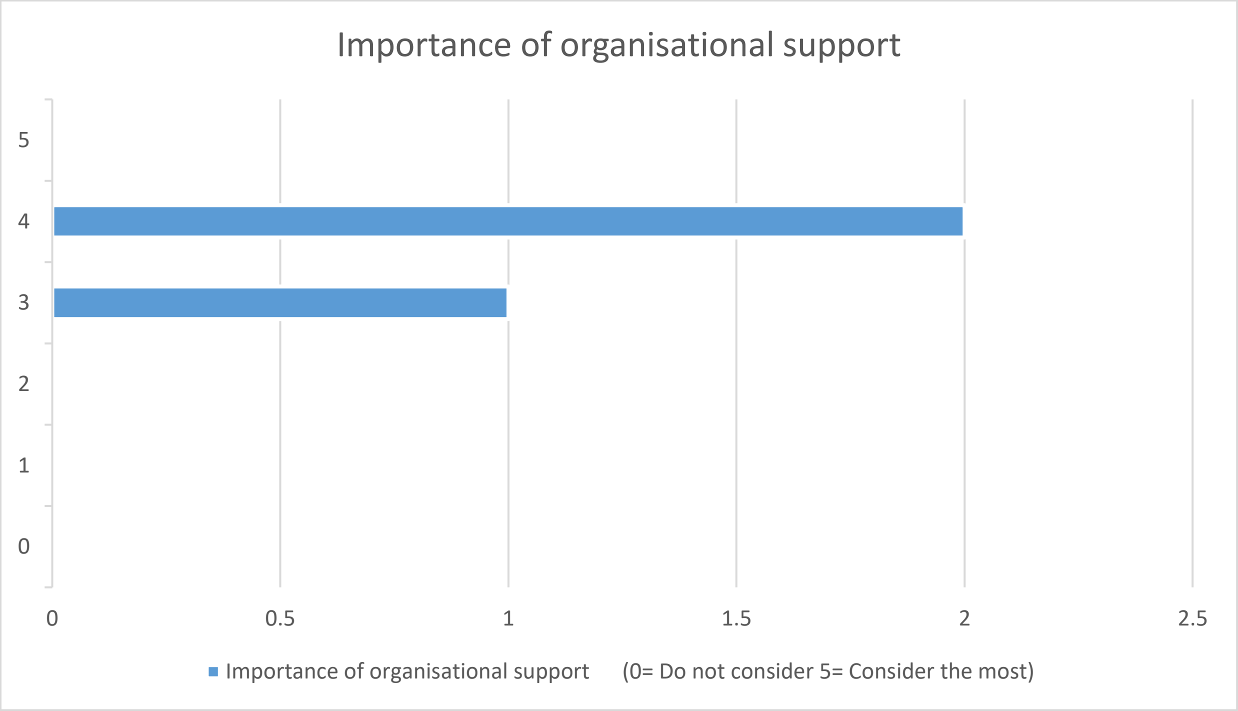


Figure D.439: Importance of organisational support (Healthcare)

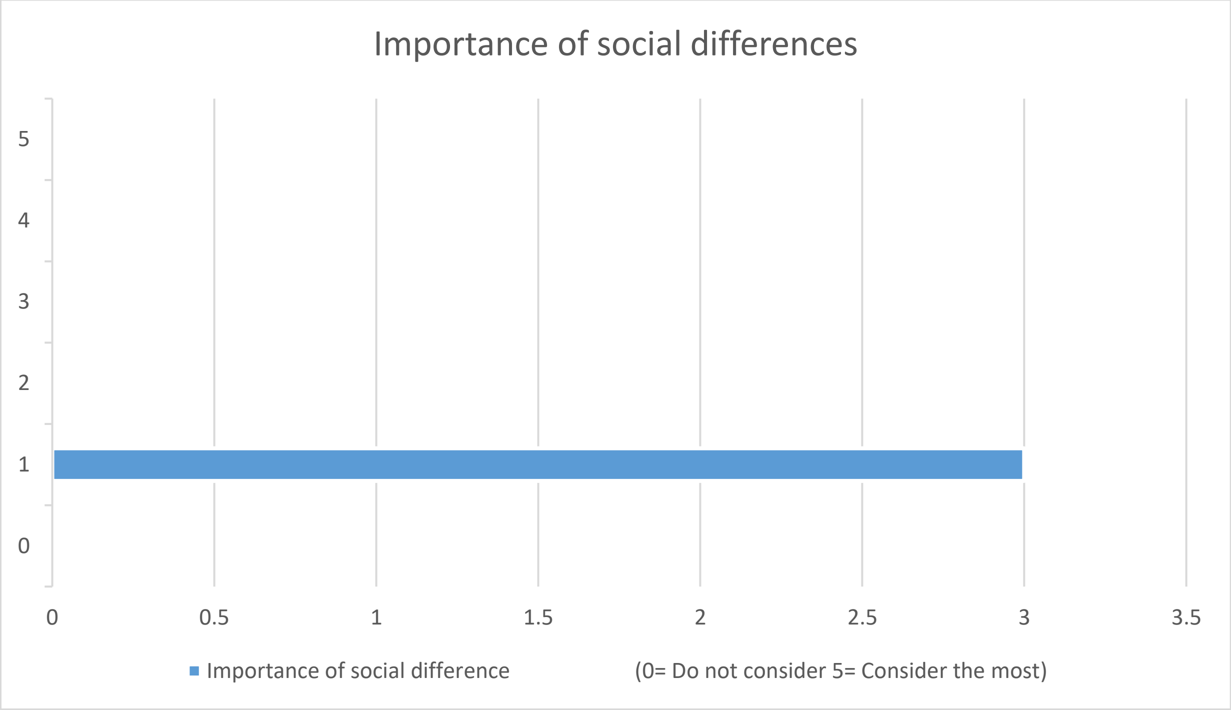


Figure D.440: Importance of social differences (Healthcare)

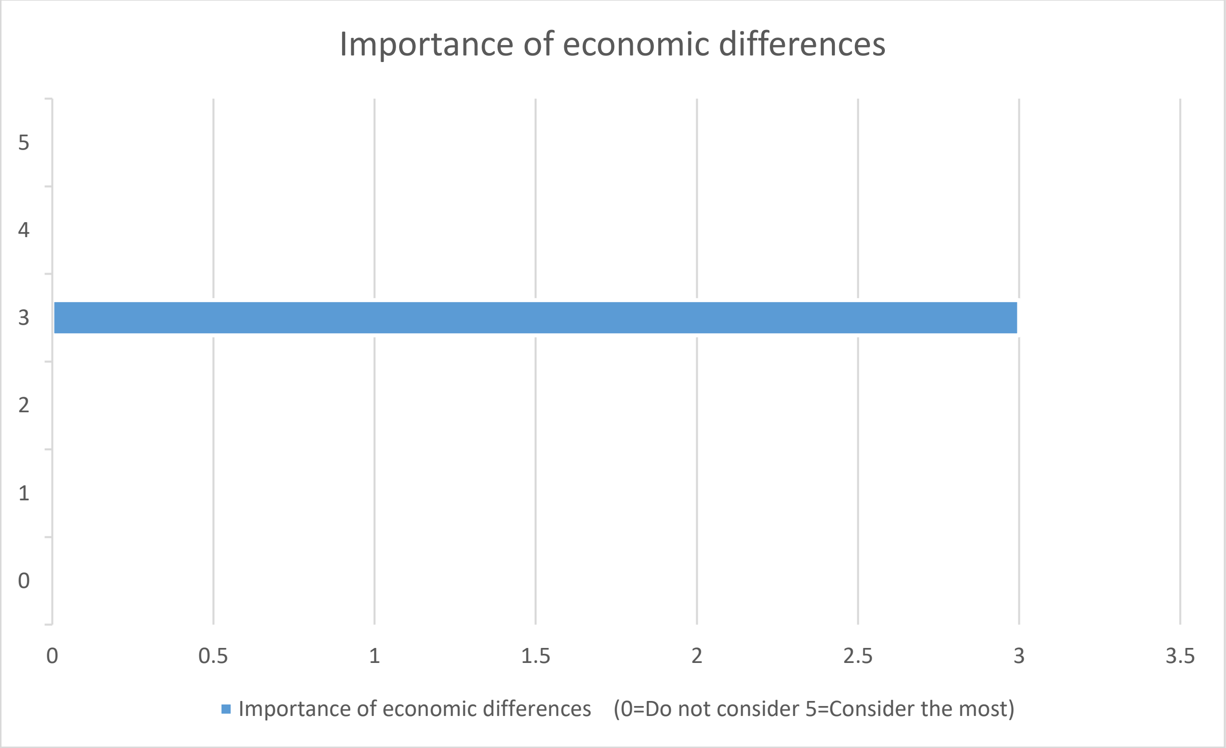


Figure D.441: Importance of economic differences (Healthcare)

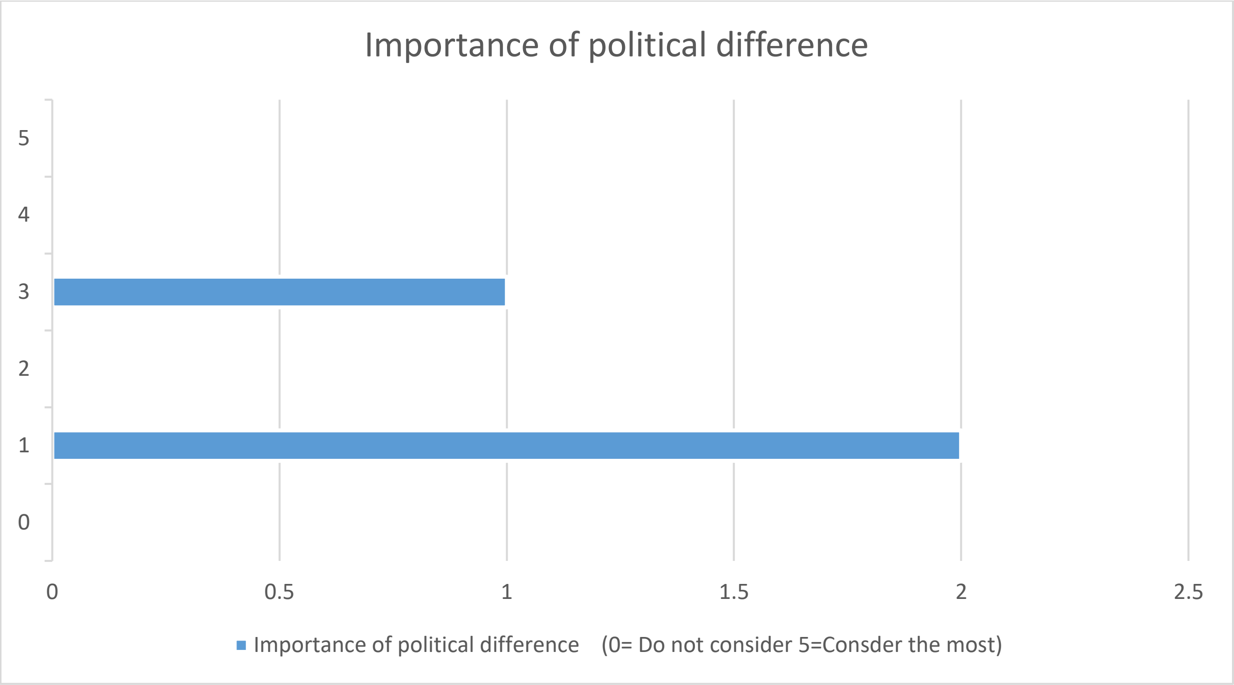


Figure D.442: Importance of political difference (Healthcare)

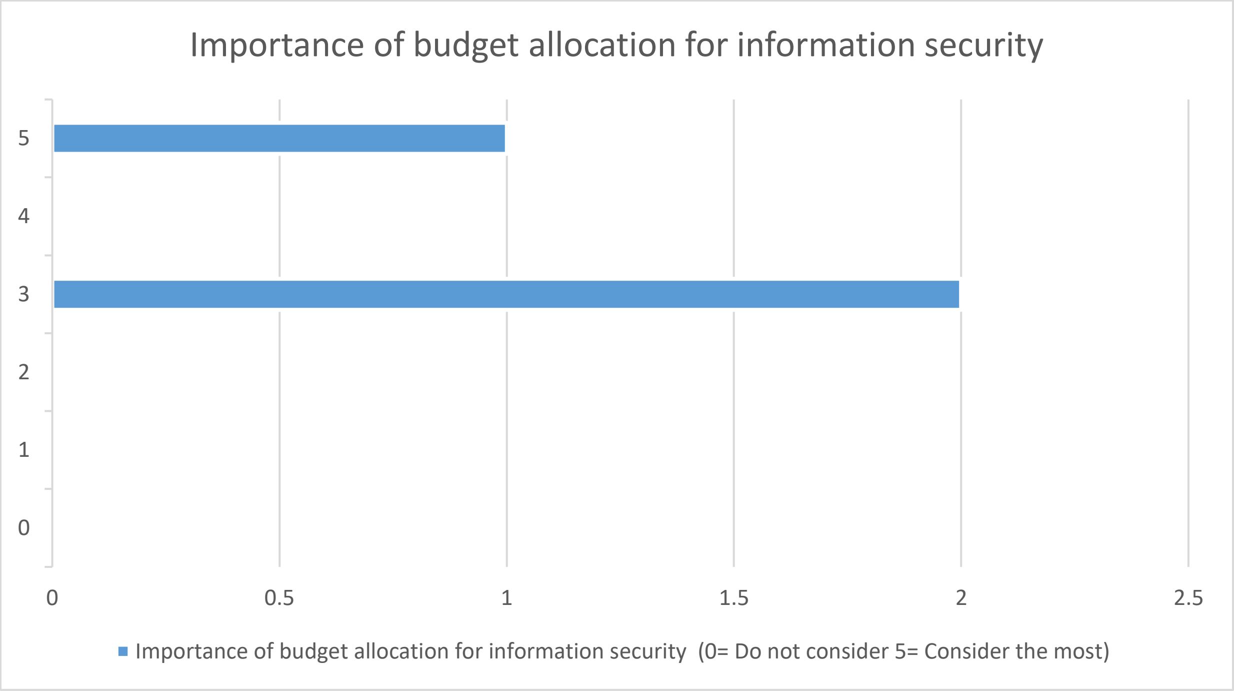


Figure D.443: Importance of budget allocation for information security (Healthcare)

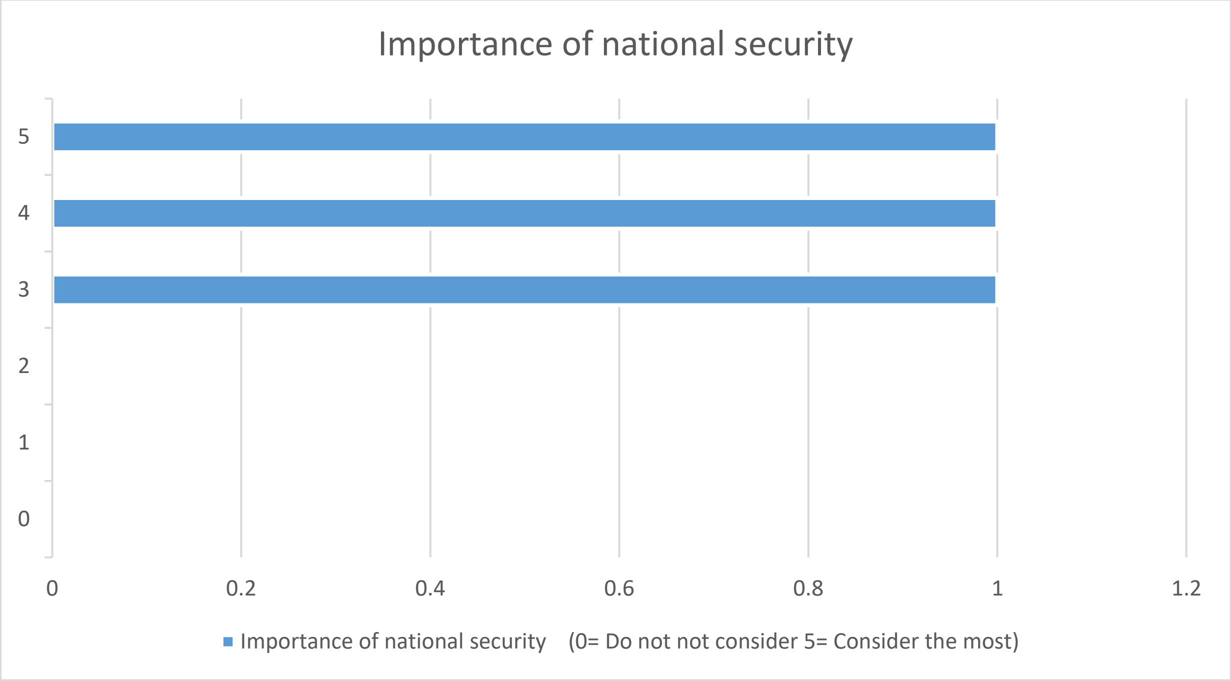


Figure D.444: Importance of national security (Healthcare)

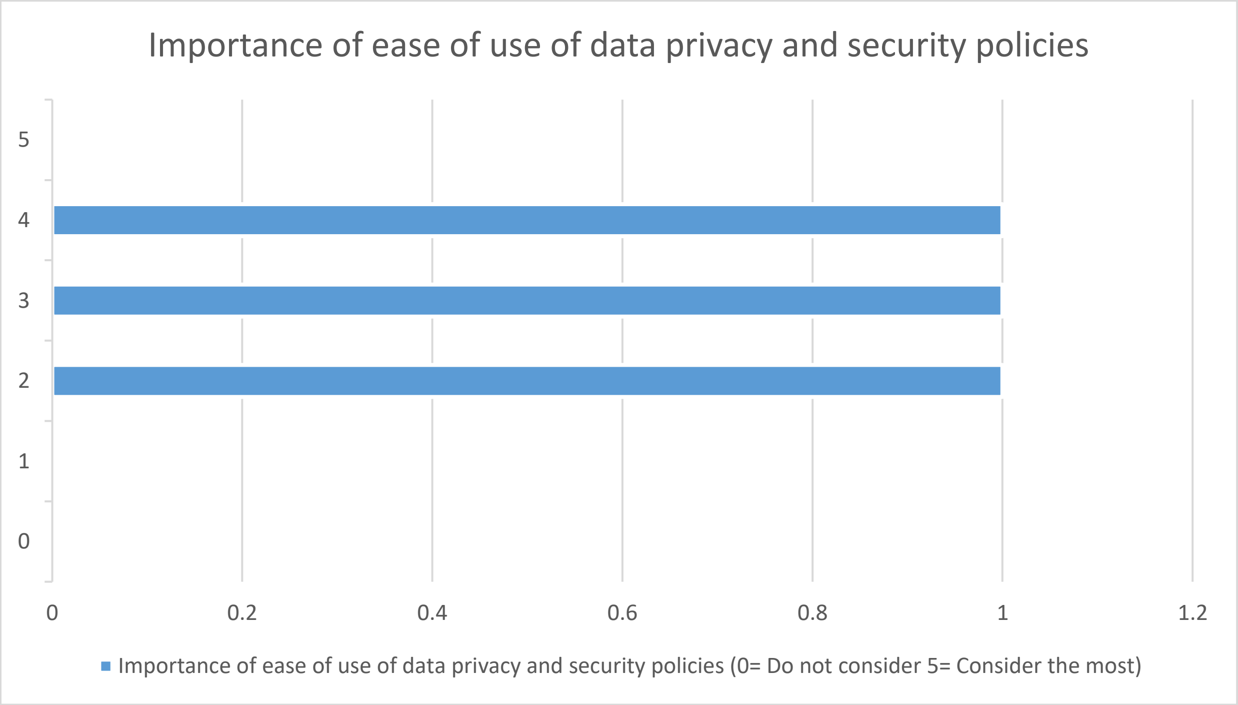


Figure D.445: Importance of ease of use of data privacy and security policies (Healthcare)

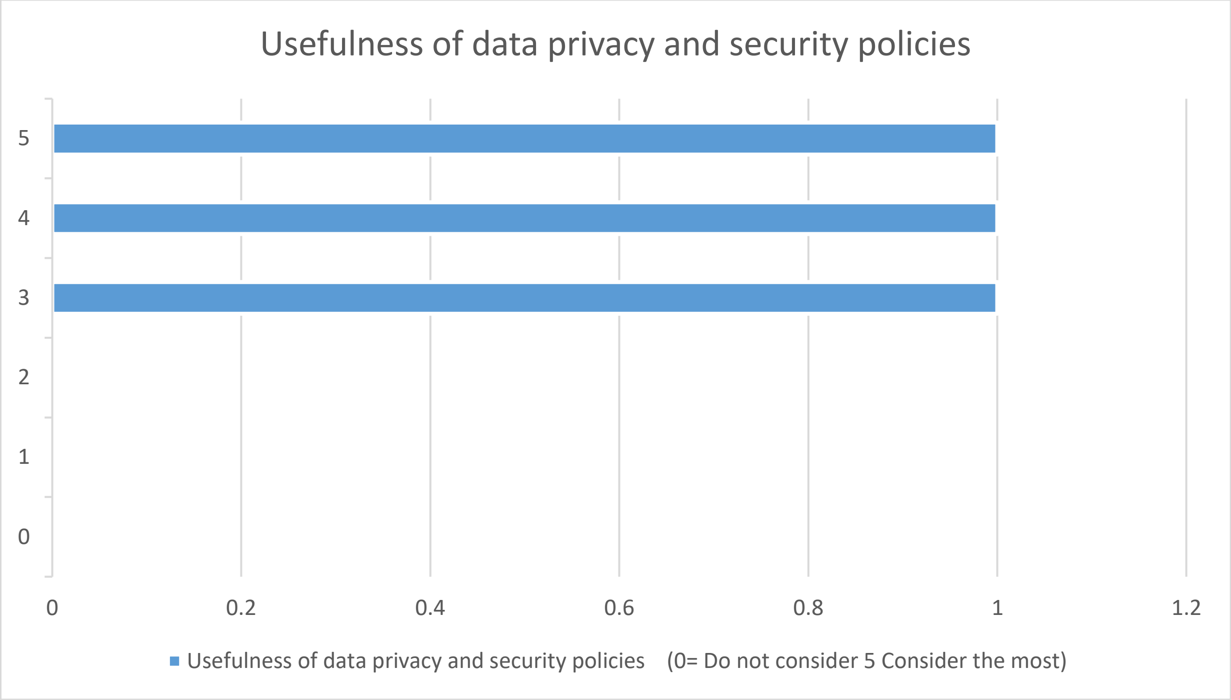


Figure D.446: Usefulness of data privacy and security policies (Healthcare)

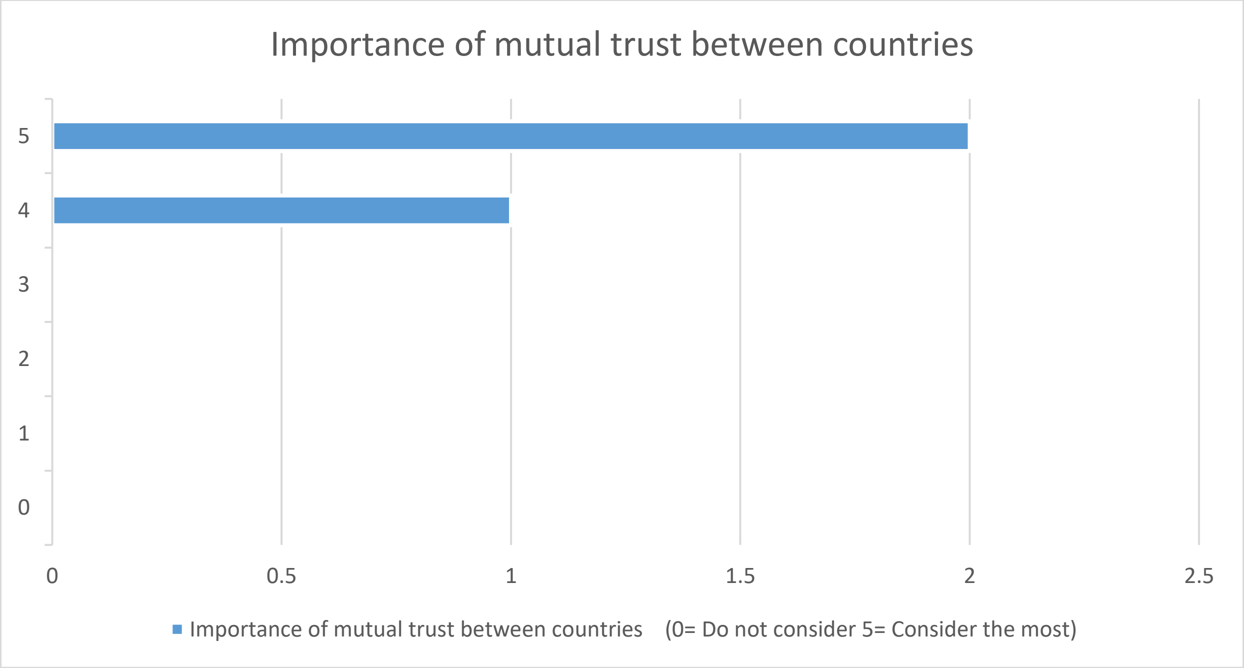


Figure D.447: Importance of mutual trust between countries (Healthcare)

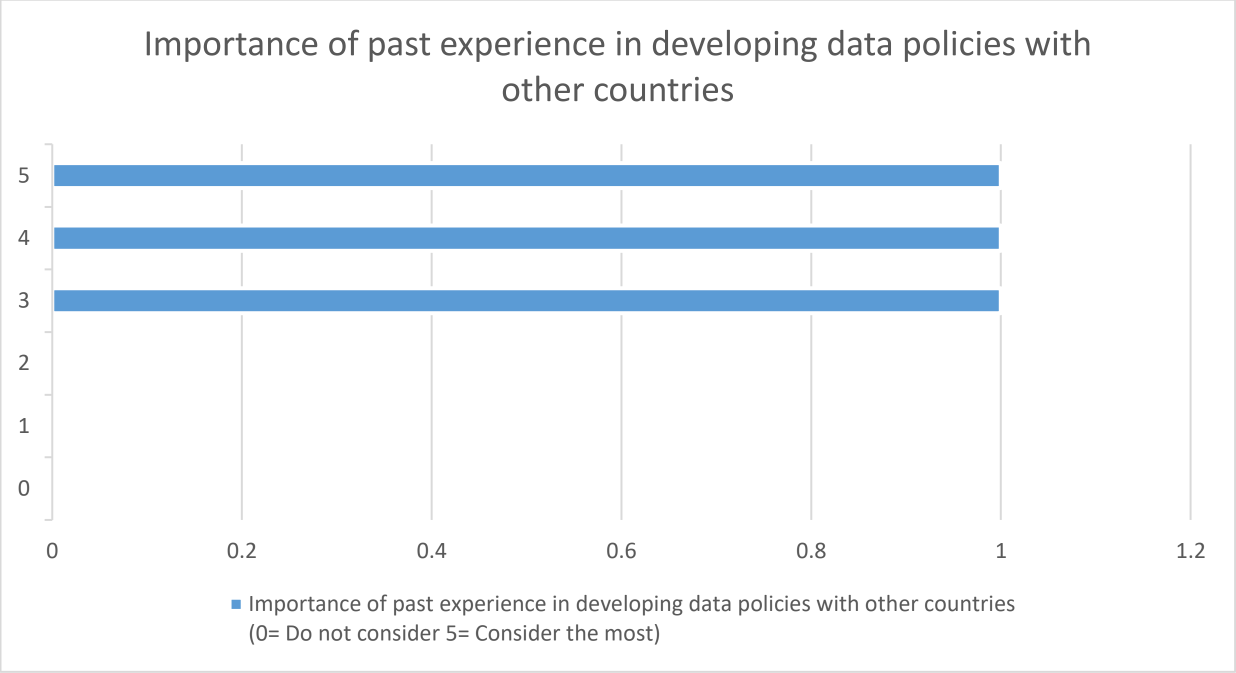


Figure D.448: Importance of past experience in developing data policies with other counties (Healthcare)

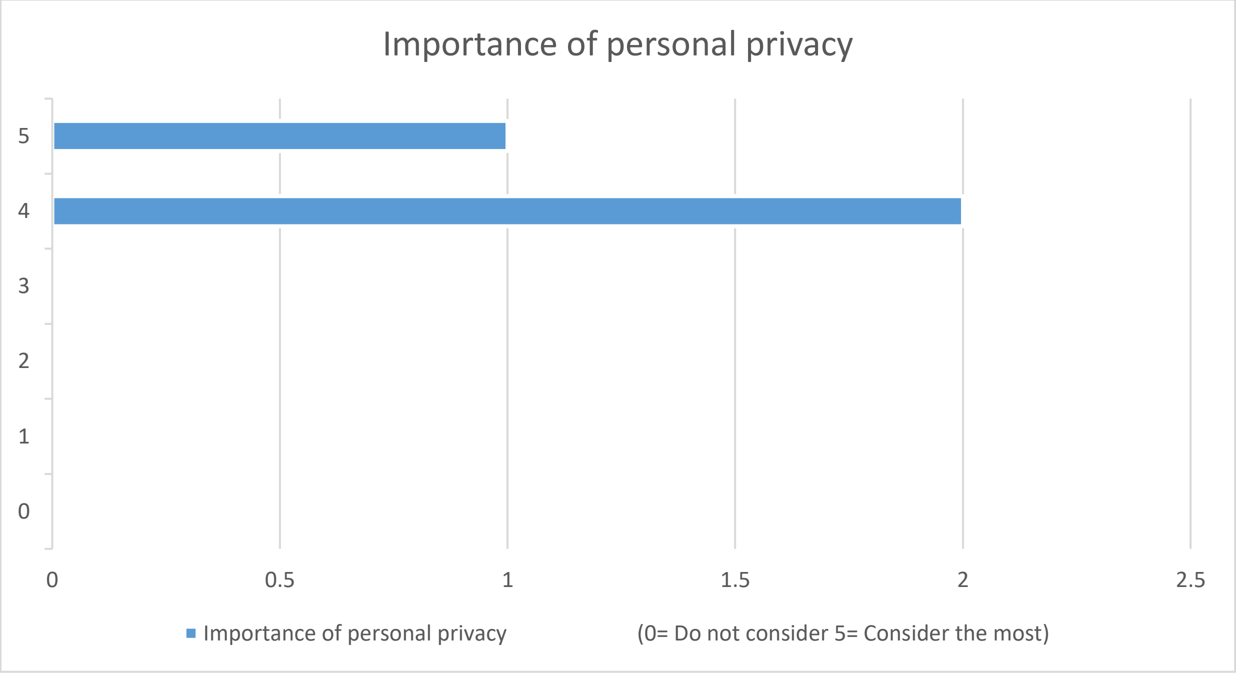


Figure D.449: Importance of personal privacy (Healthcare)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 80 percent of the respondents have endorsed (See figure D.438). The other notable factors coming out of the survey are organisational support, budget allocation, economical differences, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure D.427-437) (See figure D.439-449).

Sri Lanka – Information Security

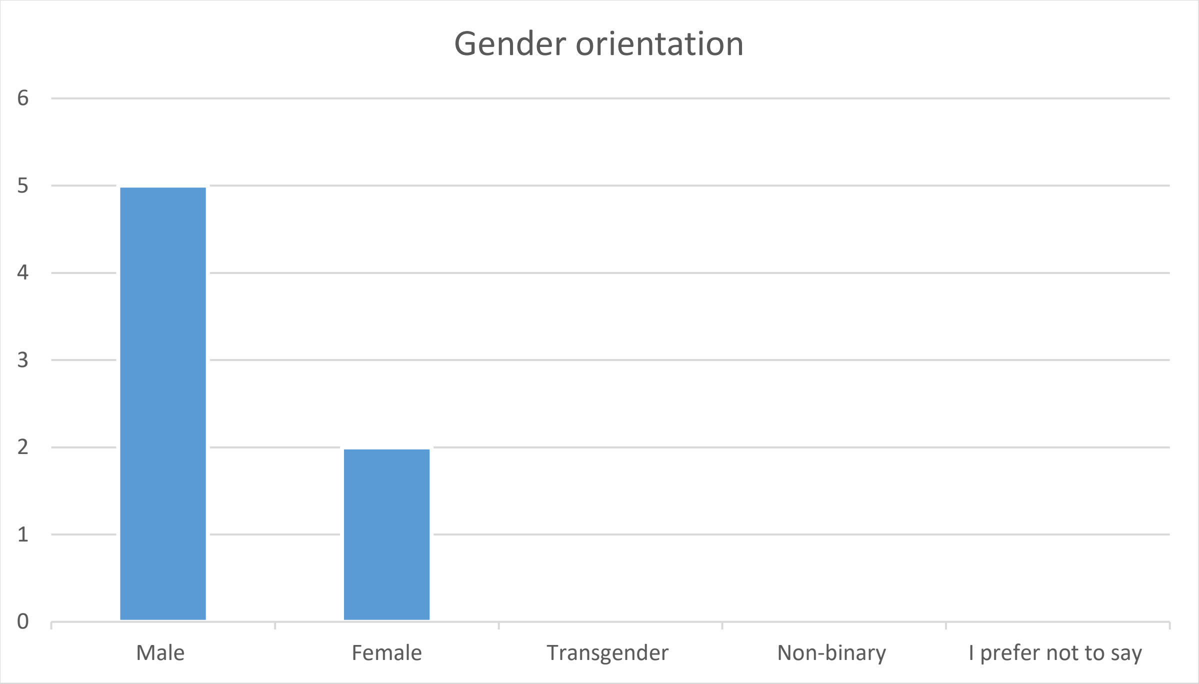


Figure D.450: Gender orientation (Information Security)

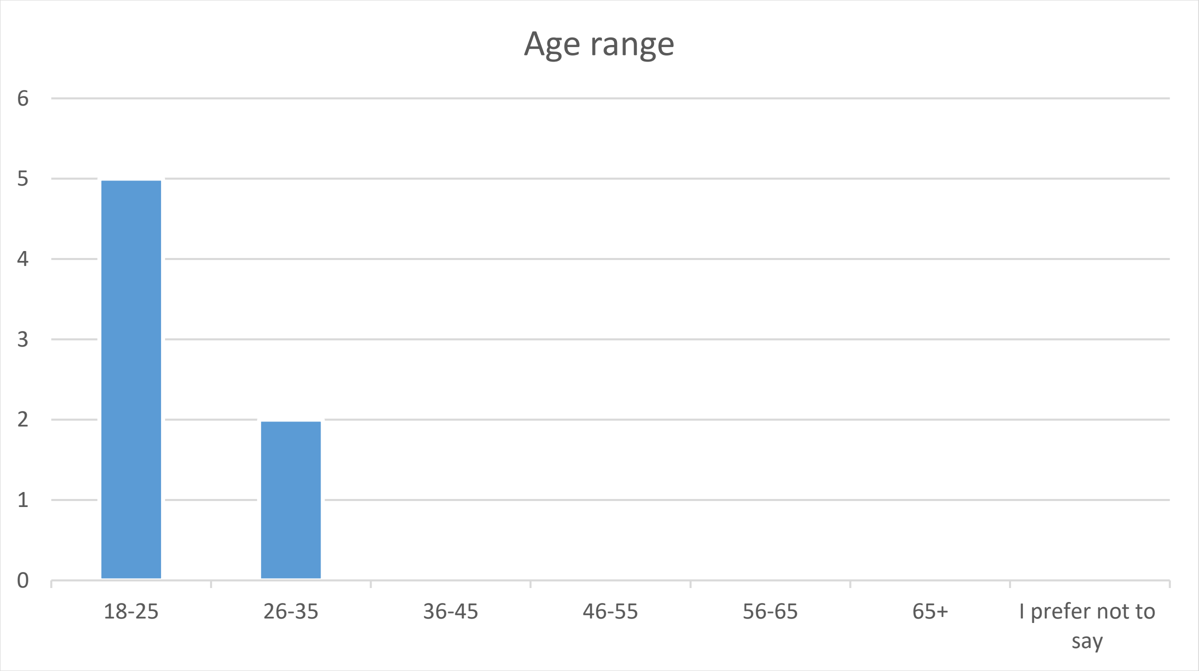


Figure D.451: Age range (Information Security)

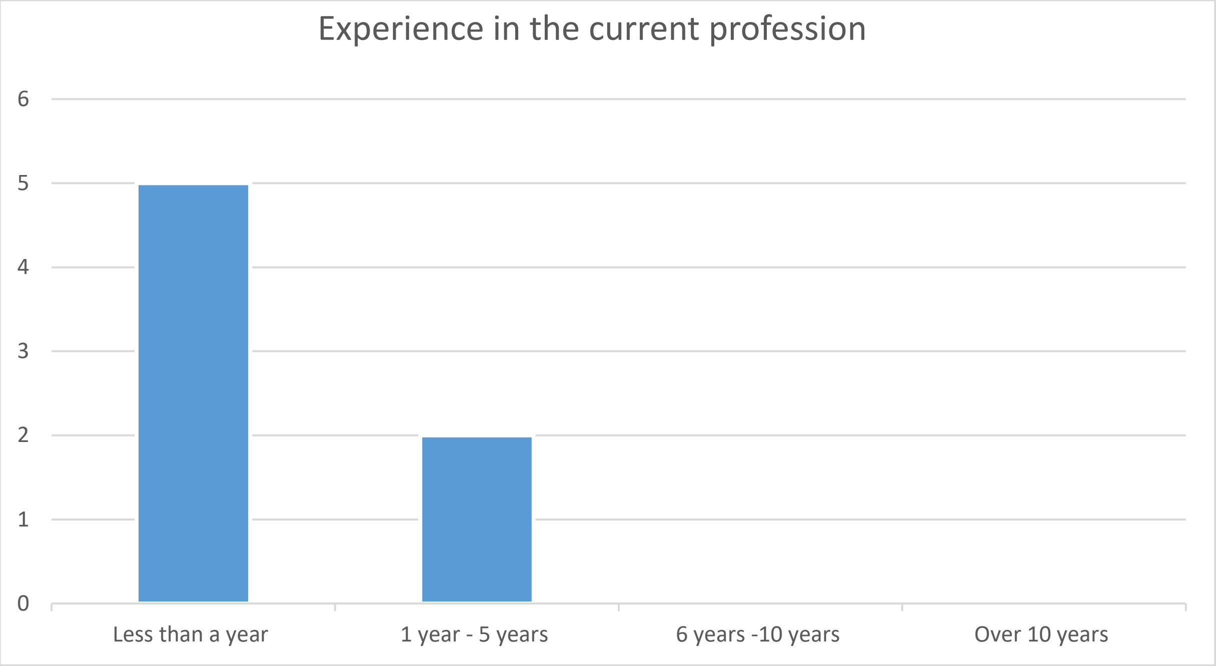


Figure D.452: Experience in current profession (Information Security)

This analysis is based on the responses received from Sri Lankan participants working in the information security sector. There were 7 participants, 5 males and 2 females (See figure D.450). They were within the age range 18-35; broken down groups, 5 in the 18-25, and 2 in the 26-35 range (See figure D.451). The participants with less than a year to 5 years of employment in the industry (See figure D.452).

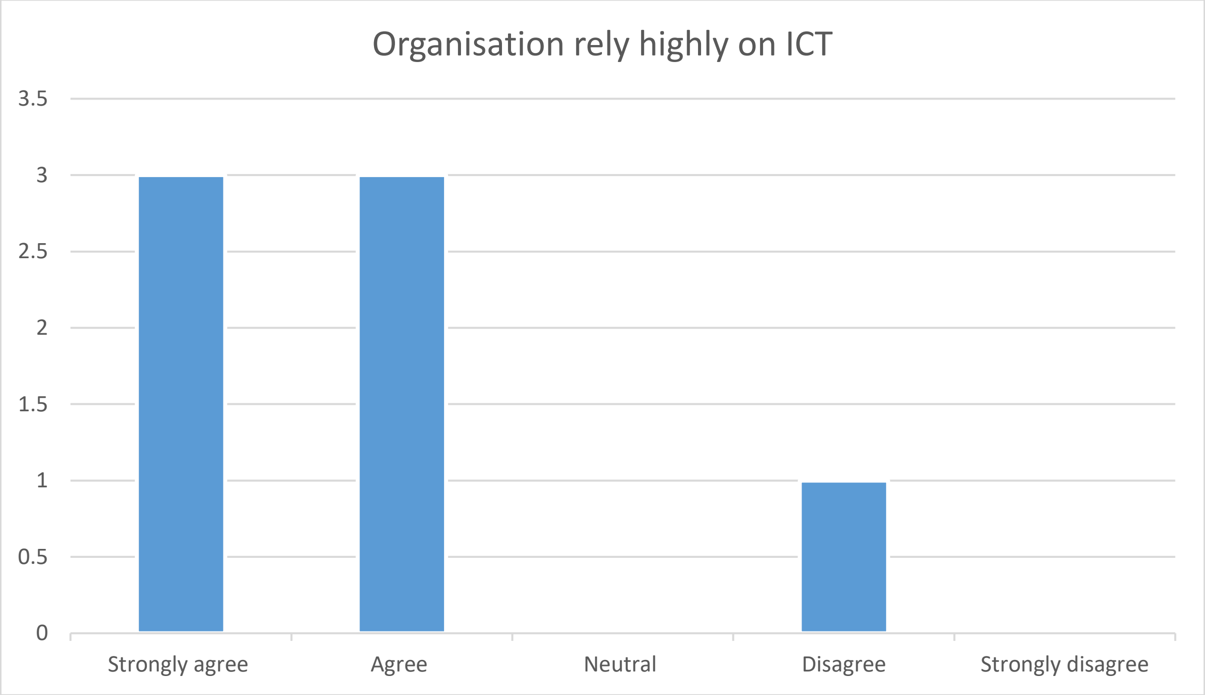


Figure D.453: Organisation rely highly on ICT (Information Security)

Out of the 7 respondents, 6 employed in a technology reliance working environment, and 1 marked ‘disagree’ (See figure D.453). This shows that the majority of employees work in the information security sector with high reliance on ICT.

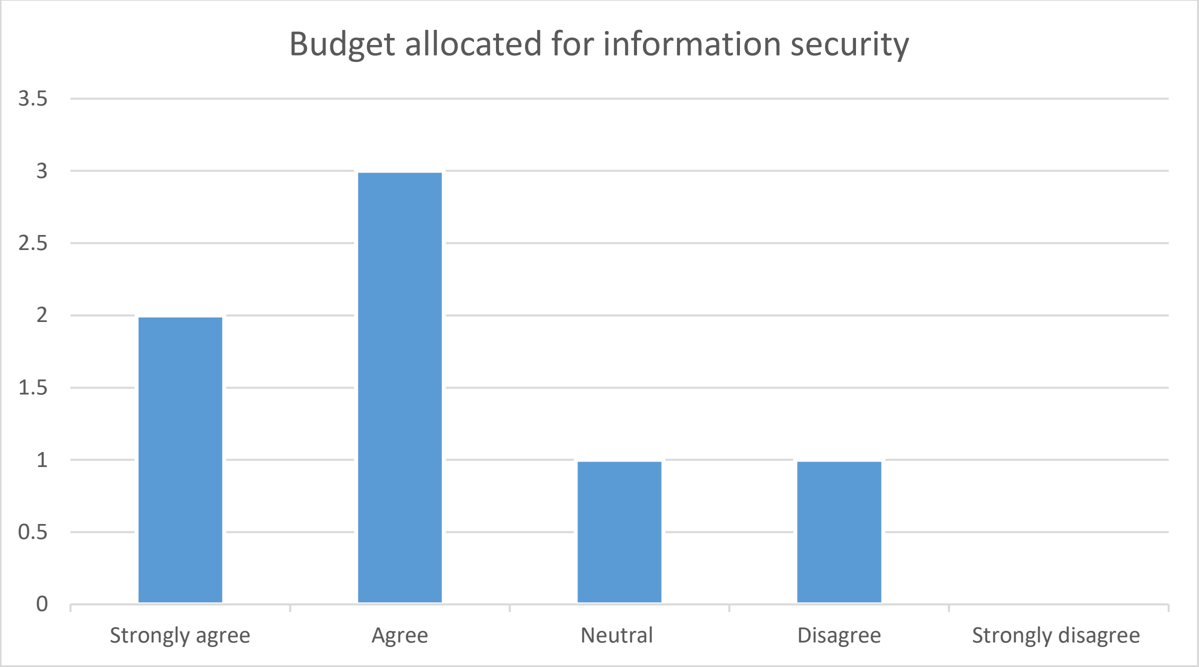


Figure D.454: Budget allocated for information security (Information Security)

5 out of the 7 have indicated that their organisations had an allocated budget for information security; 1 chose not to score yes or no, and 1 notably felt their organisations had no budget allocation for information security (See figure D.454).

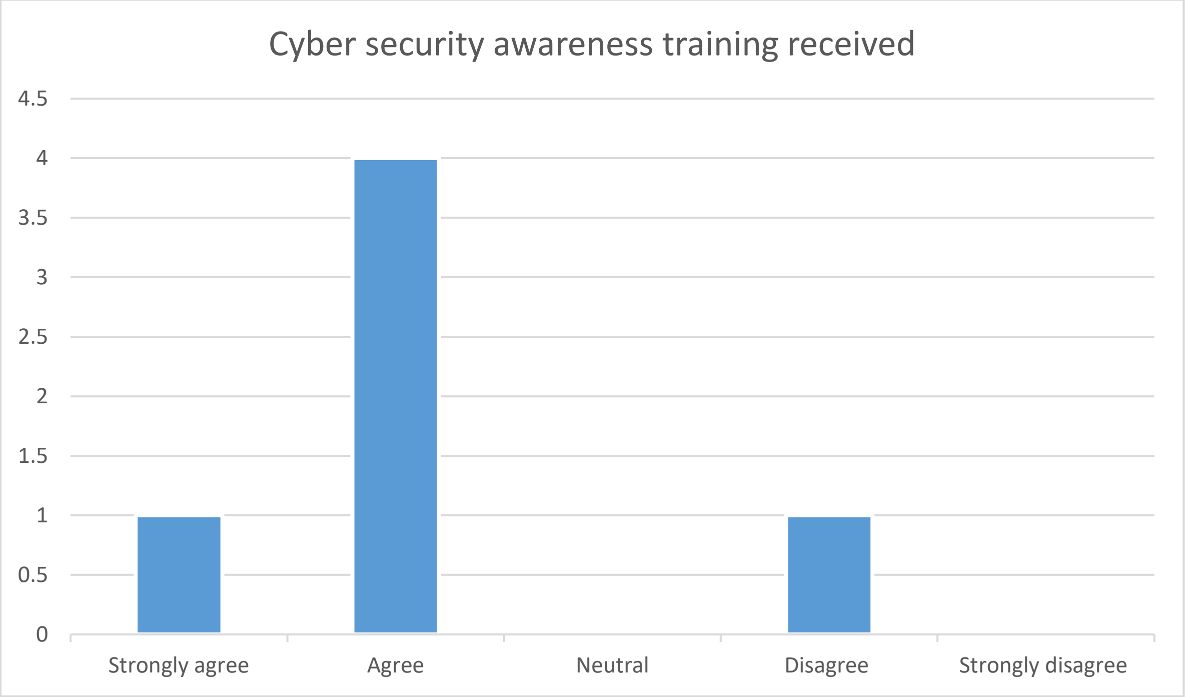


Figure D.455: Cyber security awareness training received (Information Security)

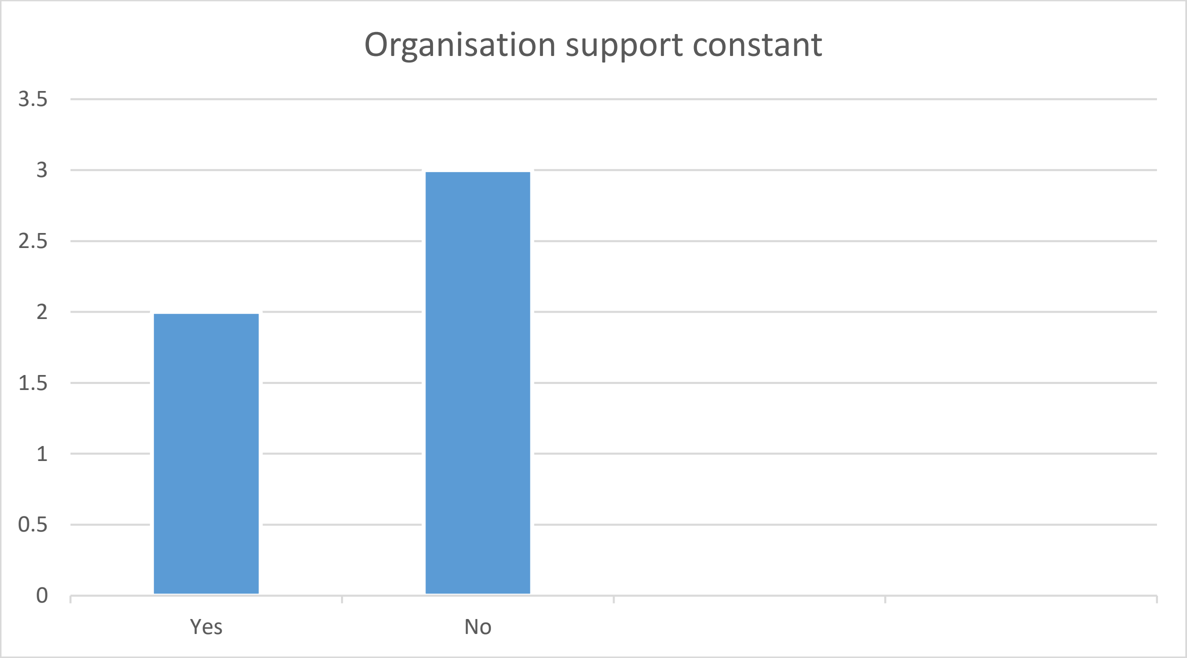


Figure D.456: Organisation support constant (Information Security)

Also, some of the participants agree that the regular security awareness training they received was adequate. 5 participants received regular cybersecurity awareness training; 1 participant did not receive security awareness training regularly (See figure D.455). Furthermore, only 2 did receive organisational support to protect personal information, and 3 participants did not (See figure D.456). This shows that even though the organisations have budget allocations providing training, there is also lack of support for the protection of personal information. However, the organisations should consider making improvement to resource allocation to meet the needs of the training programs.

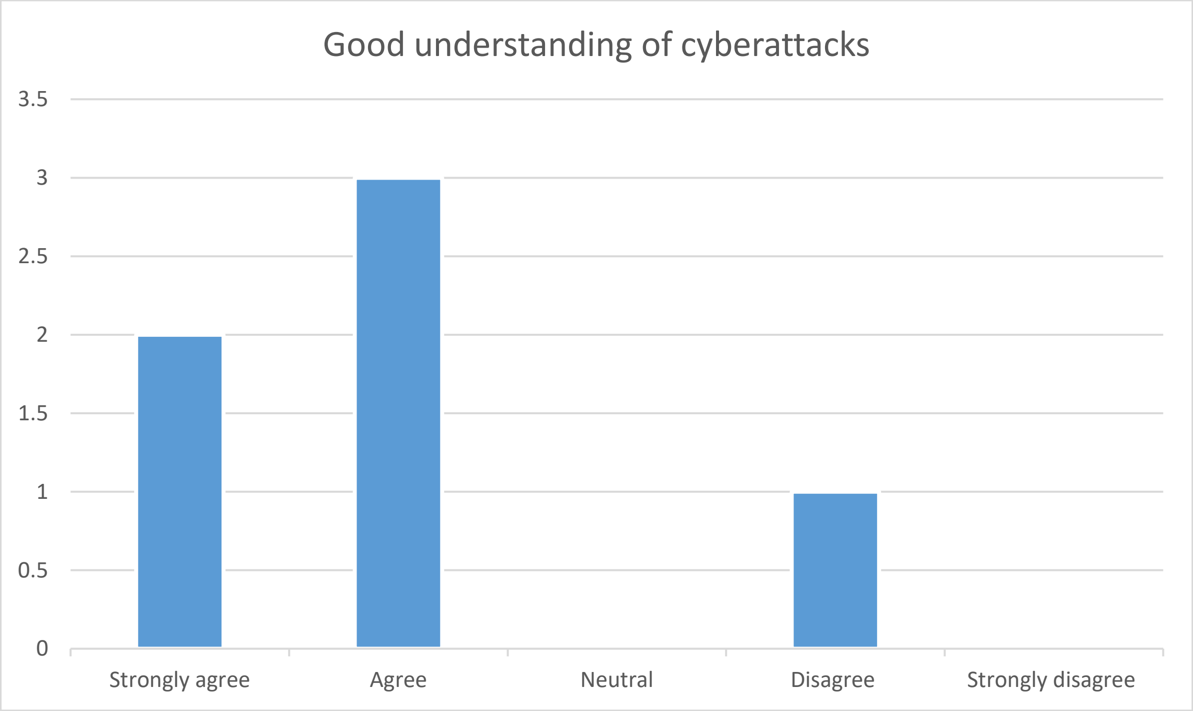


Figure D.457: Good understanding of cyberattacks (Information Security)

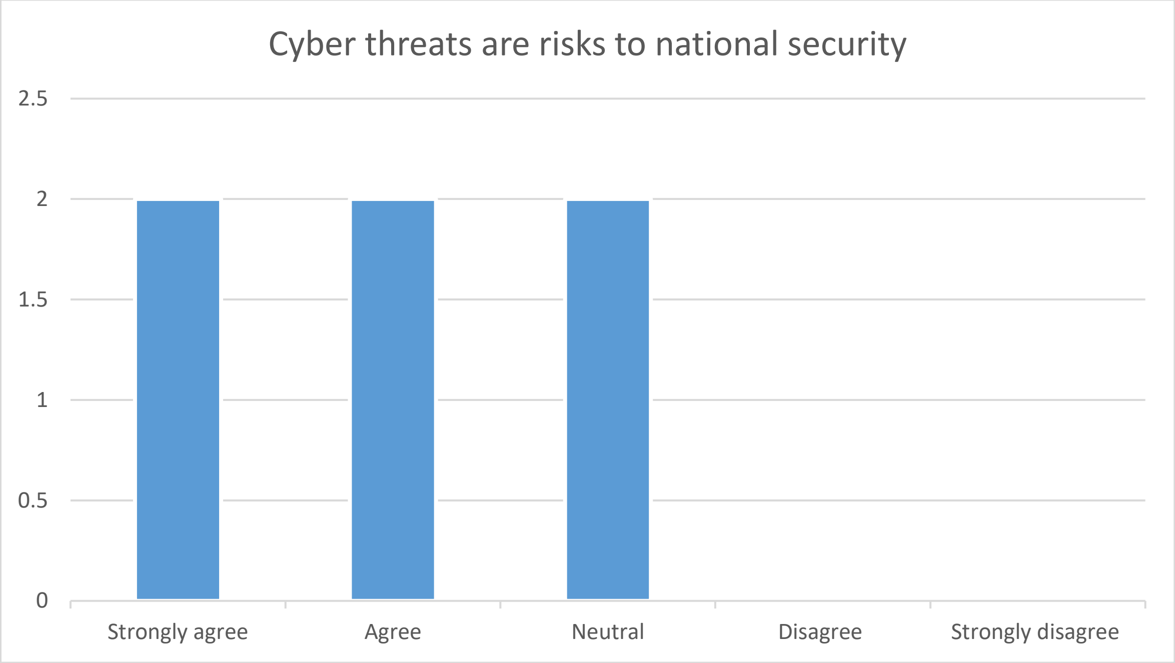


Figure D.458: Cyber threats are risks to national security (Information Security)

Despite the security awareness training, 5 of the participants except 1, show a high understanding of the impact of cyber-attacks on the public and the organisation (See figure D.457). Furthermore, 57 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure D.458). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in time, they will have the opportunity to voice their views and influence the process of accepting and implementing a national, regional, and global level mechanism.

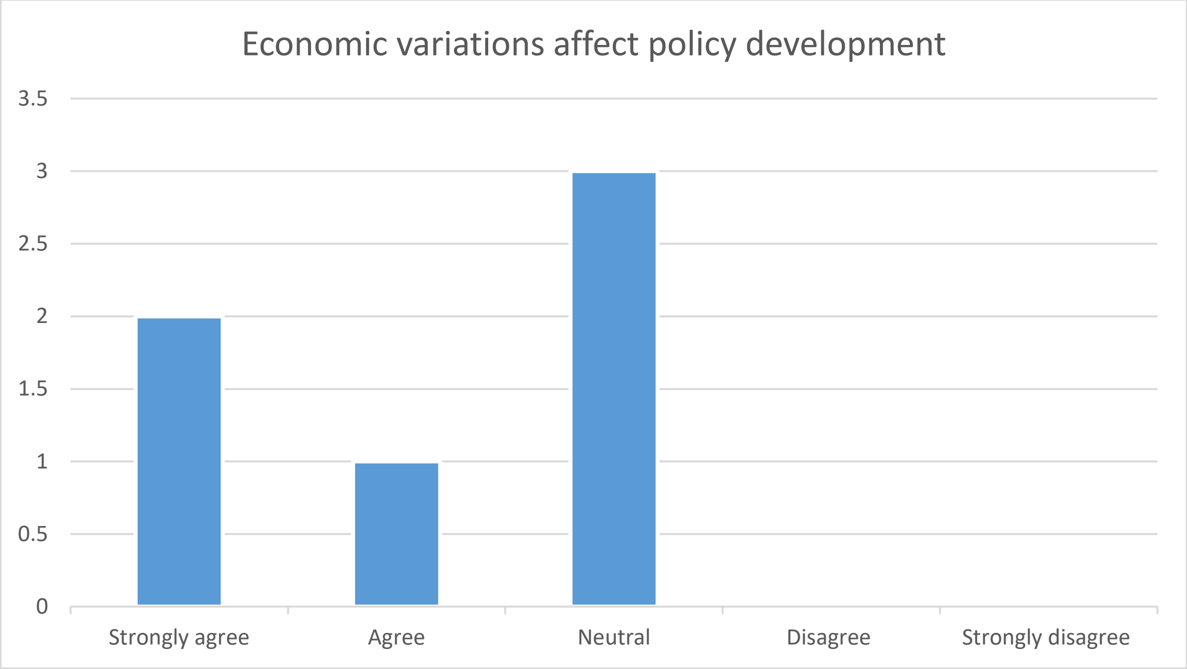


Figure D.459: Economic variations affect policy development (Information Security)

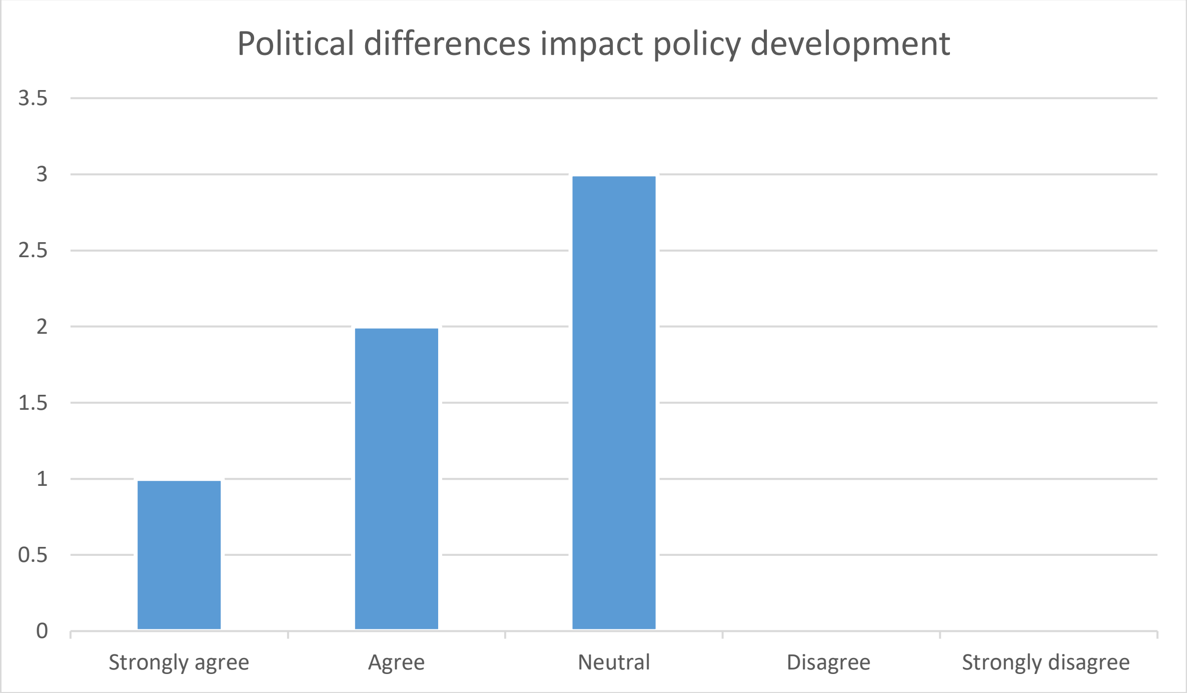


Figure D.460: Political differences impact policy development (Information Security)

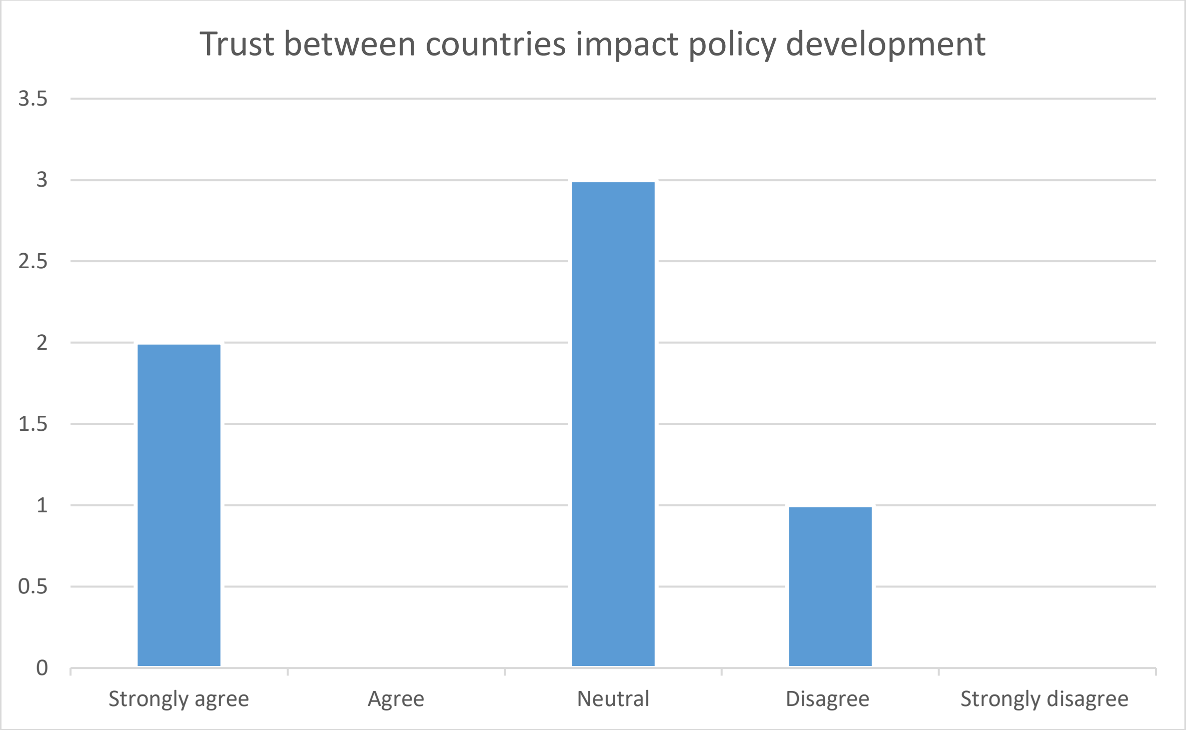


Figure D.461: Trust between countries impact policy development (Information Security)

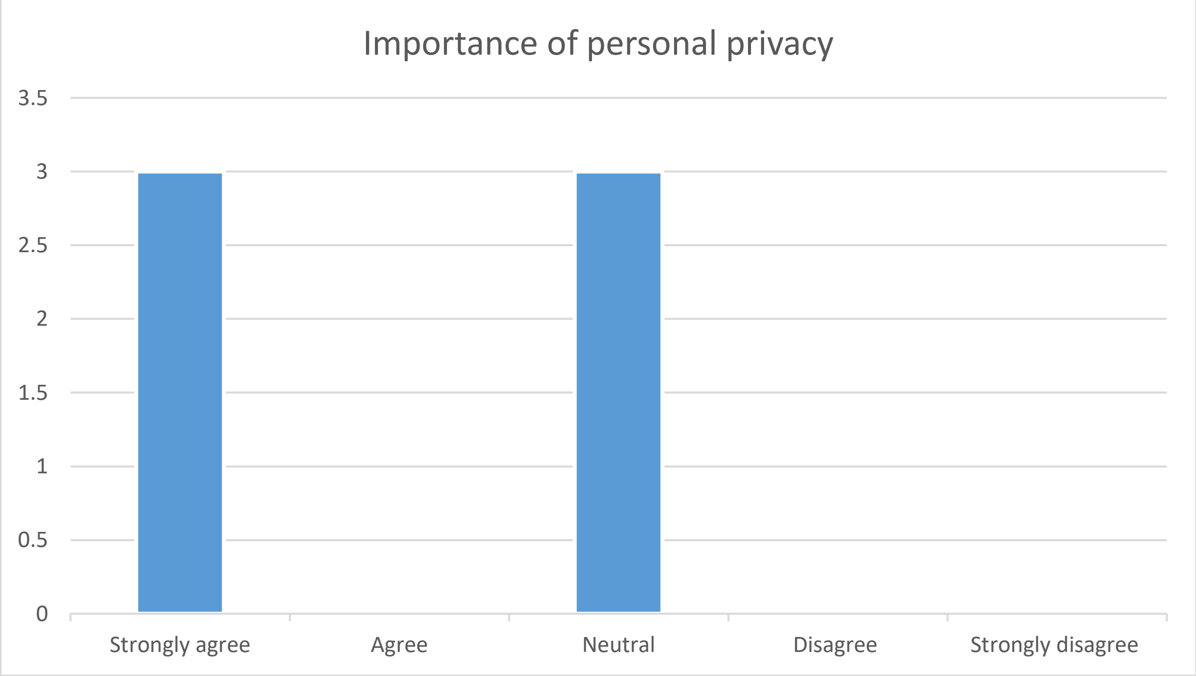


Figure D.462: Importance of personal privacy (Information Security)

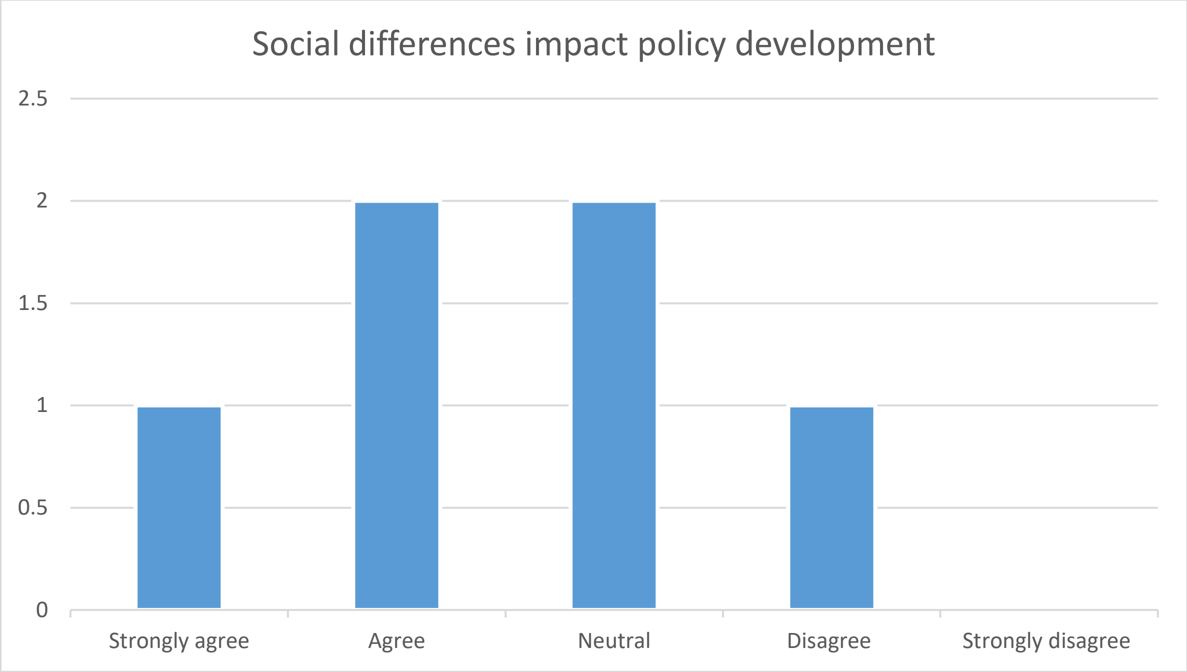


Figure D.463: Social differences impact policy development (Information Security)

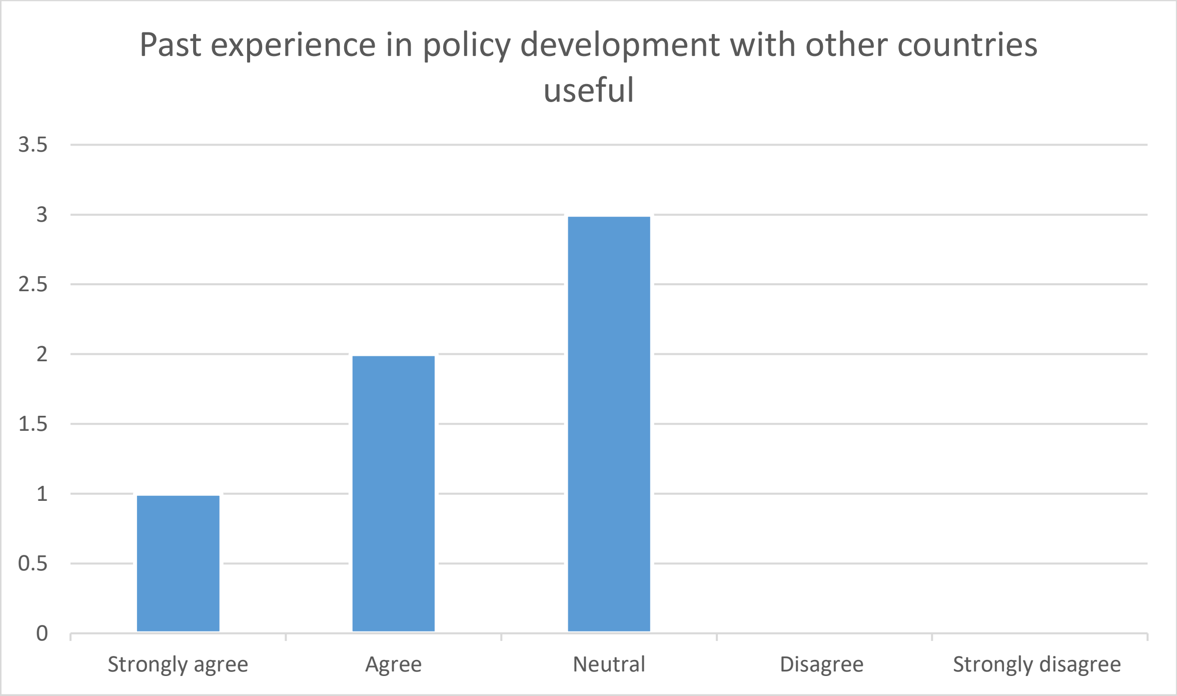


Figure D.464: Past experience in policy development with other countries useful (Information Security)

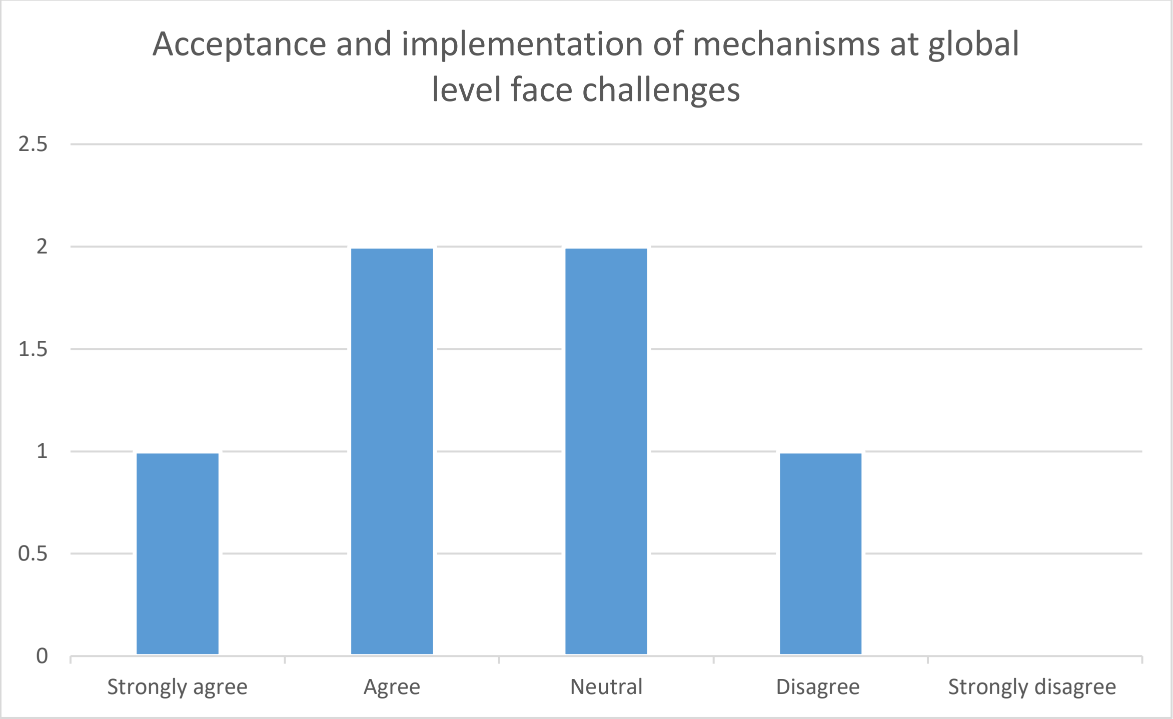


Figure D.465: Acceptance and implementation of mechanisms at global level face challenges (Information Security)

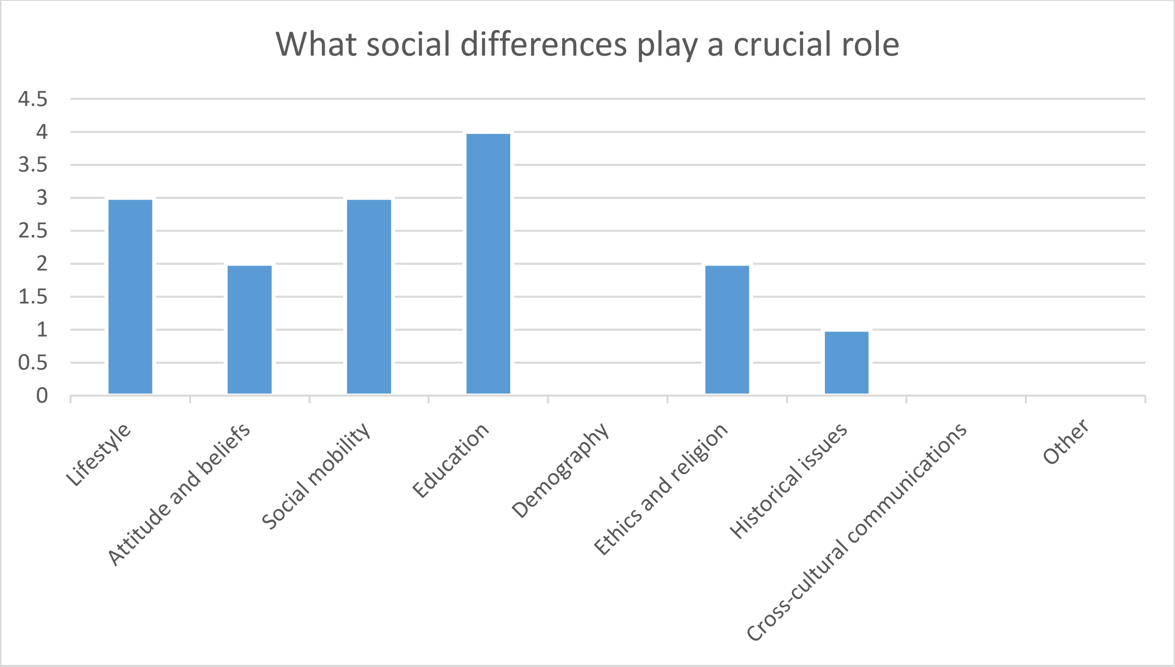


Figure D.466: What social differences play a crucial role (Information Security)

The response to the social differences component of the survey shows that the majority sees the importance of education (See figure D.466), and there is an awareness of the importance of knowledge and familiarity with potential cyber threats, their impact on people and national security in accepting and implementing data privacy and security policies. That reflects the importance of providing cybersecurity awareness training at schools and at the organisational level. Also, the provision of educational training will be an effective way to make people understand the importance of privacy and the implications associated with privacy violations.

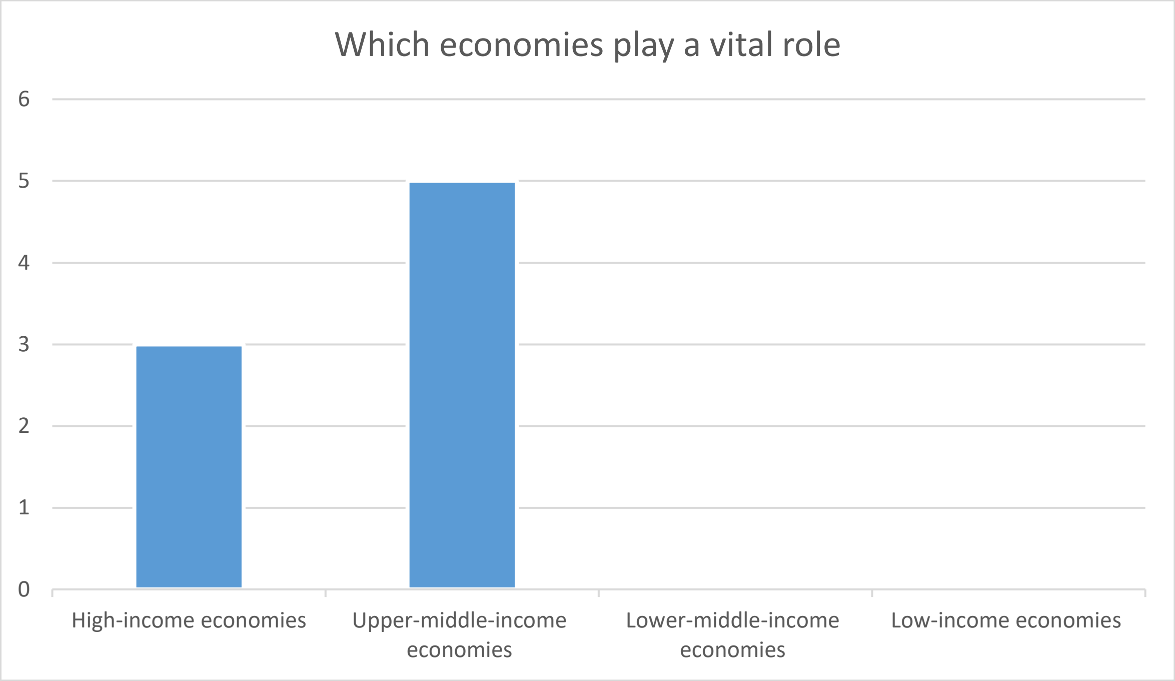


Figure D.467: Which economies play a vital role (Information Security)

In the questionnaire, the majority has stated that the upper-middle-income countries play a vital role (See figure D.467). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking. It is interesting to note that only those employed in the information security sector specifically choose upper-middle-income economies in comparison to the others employed in the industry. One possible explanation for this could be recognition of Sri Lanka's status as an upper-middle-income country, and that may have influenced the majority to select upper-middle-income economies.

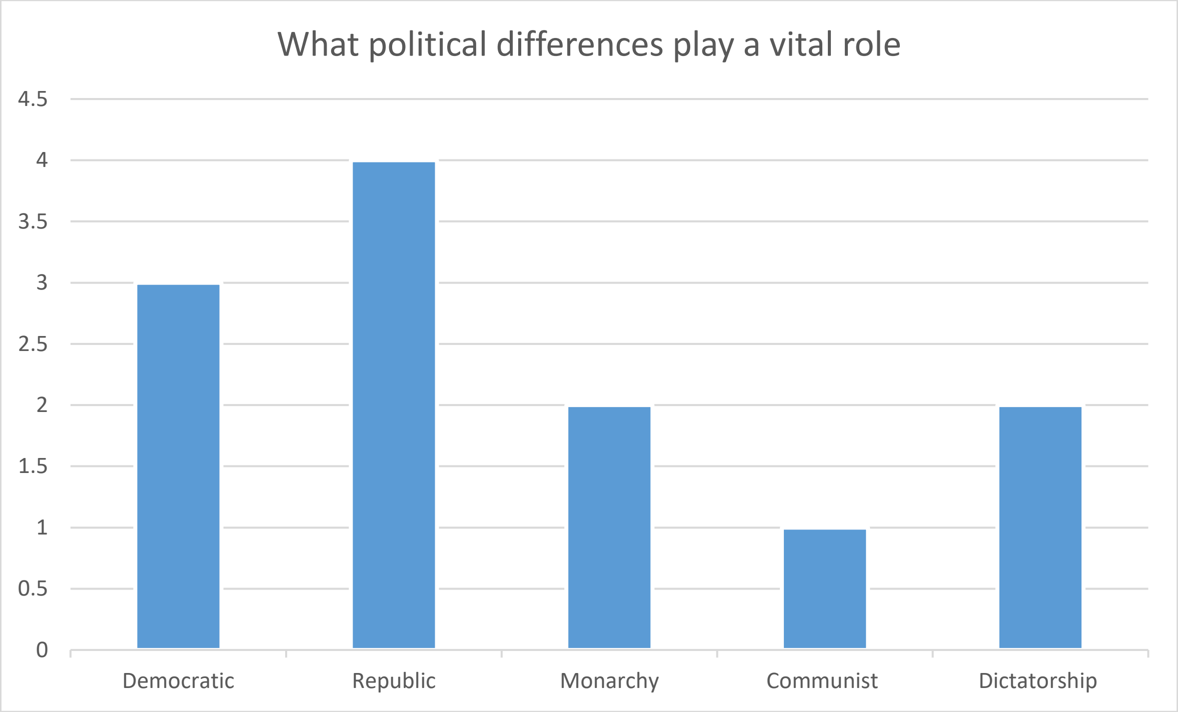


Figure D.468: What political differences play a vital role (Information Security)

The majority have chosen republic political system, in preference to others (See figure D.468). In a Republican Model Administration, it is common practice for the public to contribute to policy development. That is an effective way to ensures collective responsibility for their actions. This forms the basis for developing trust between the organisations and ensured transparency and coherence in the policy development process. Also, the constitutional rights of the public give assurance that the organisations collecting, storing, and sharing personal information will not be compromised for any reason.

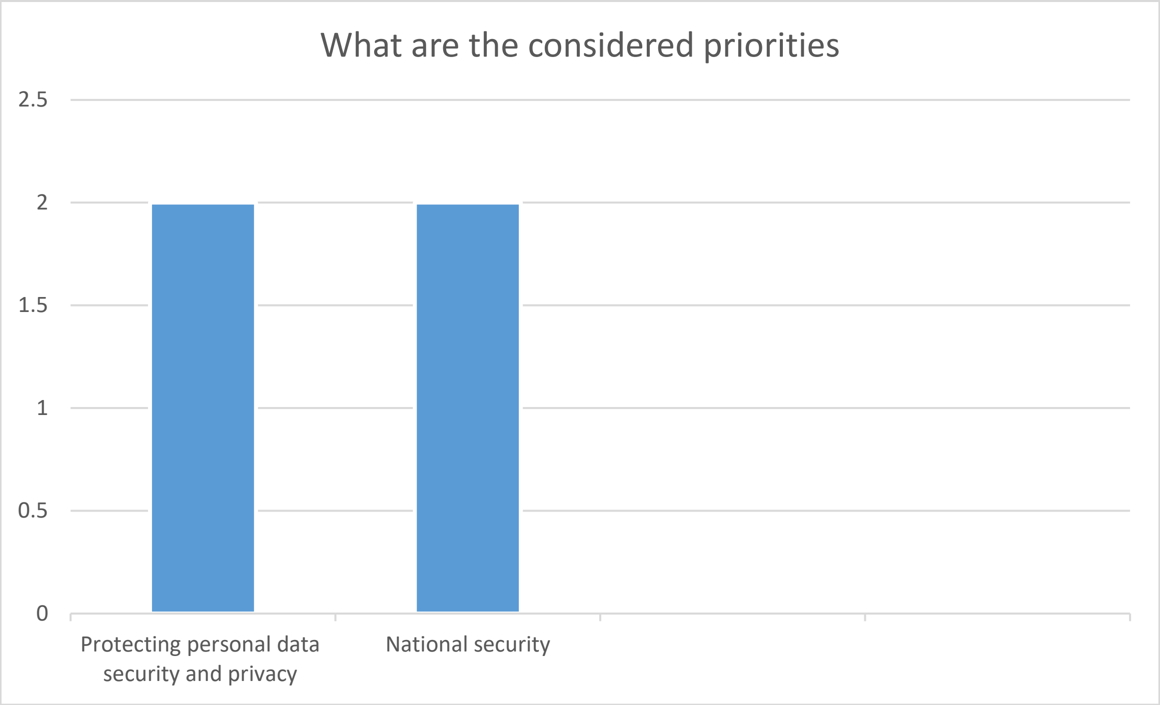


Figure D.469: What are the considered priorities (Information Security)

The majority has not given attention to either the importance of protection of personal data security and privacy or protection of national security, in accepting and implementing a global data privacy and security policies (See figure D.469).

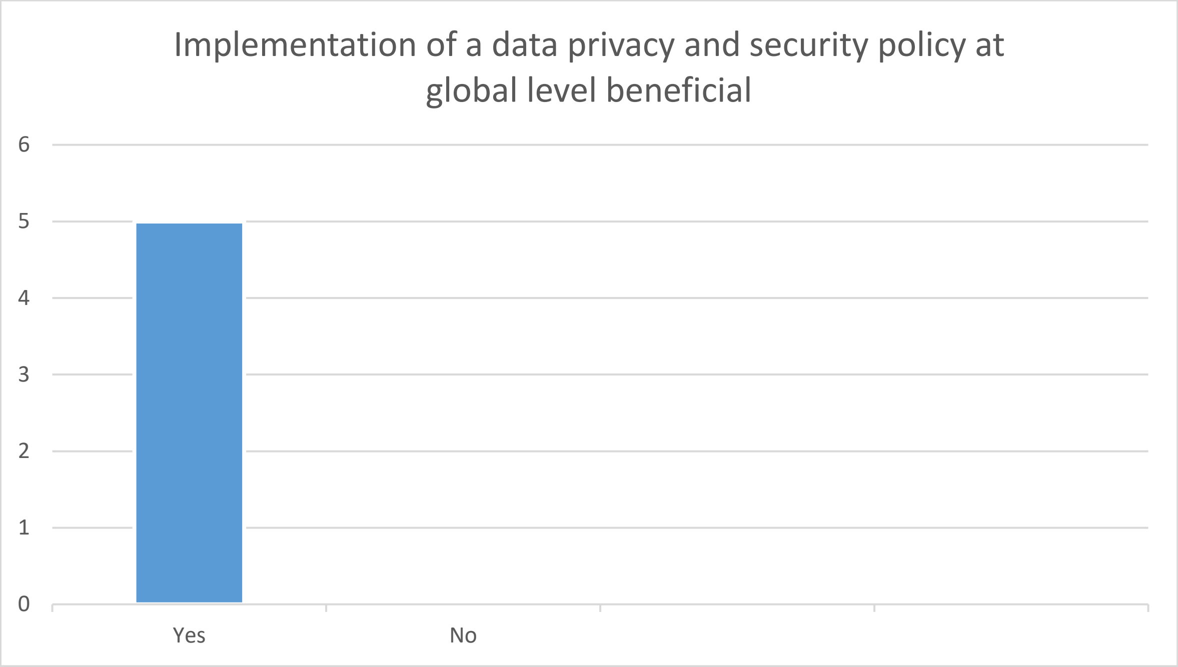


Figure D.470: Implementation of a data privacy and security policy at global level beneficial (Information Security)

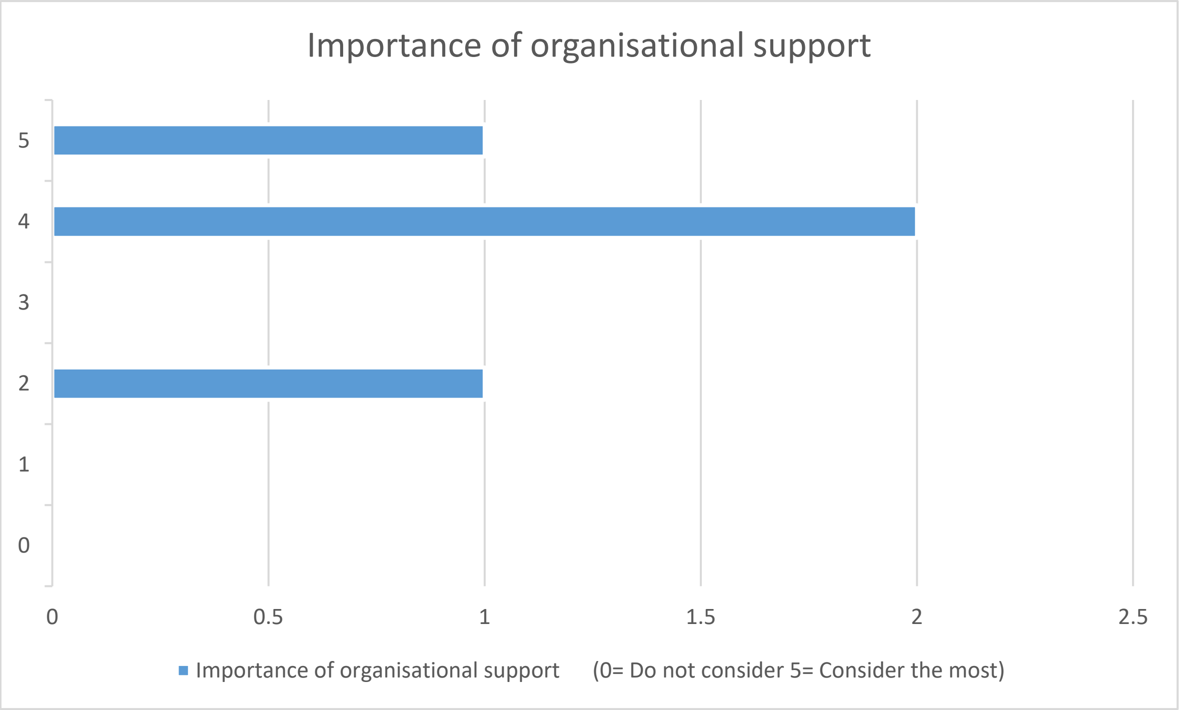


Figure D.471: Importance of organisational support (Information Security)

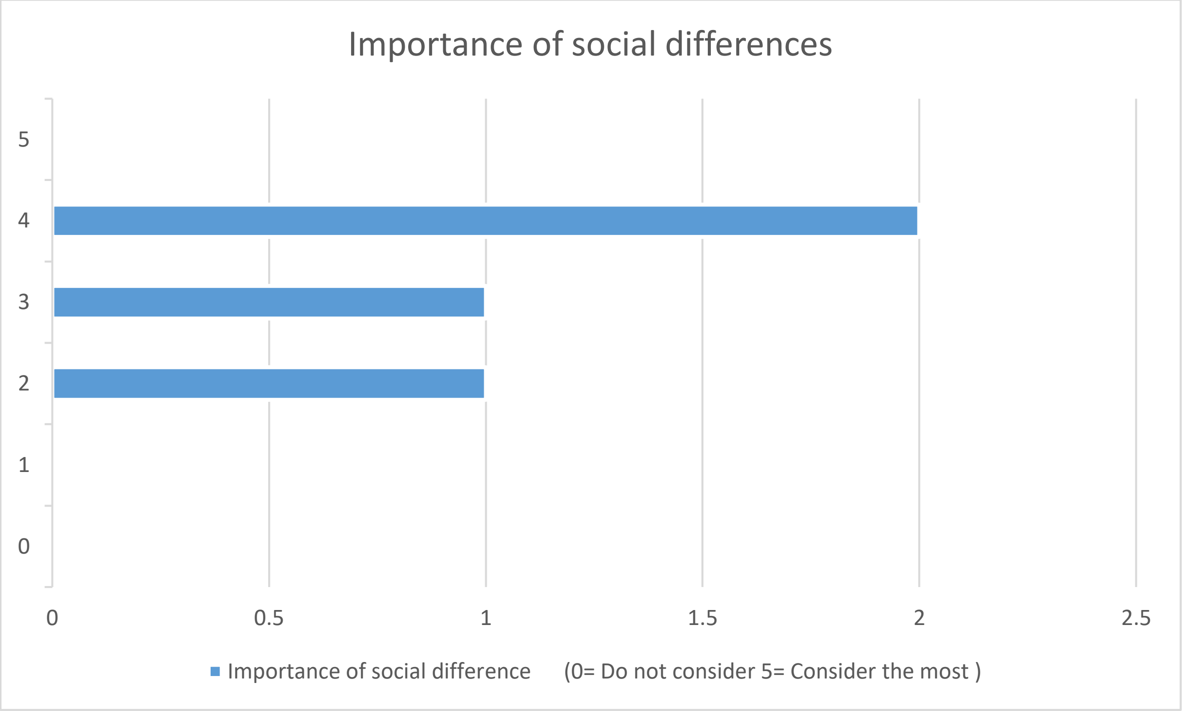


Figure D.472: Importance of social differences (Information Security)

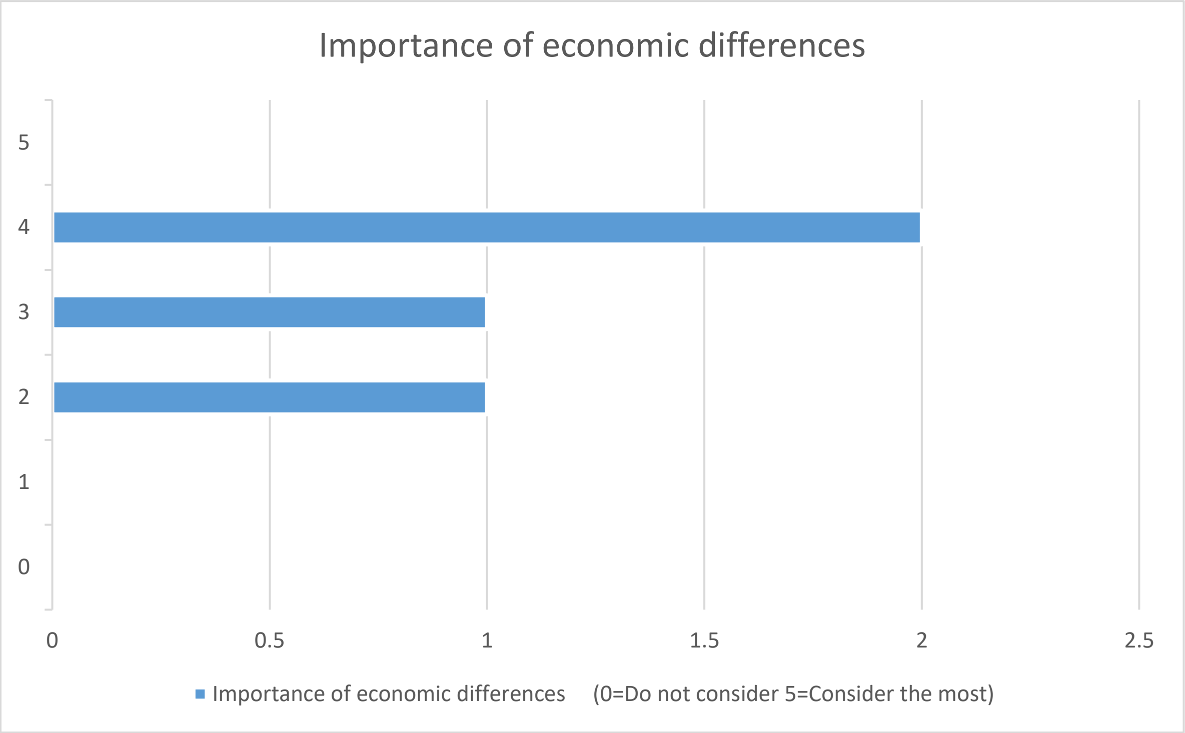


Figure D.473: Importance of economic differences (Information Security)

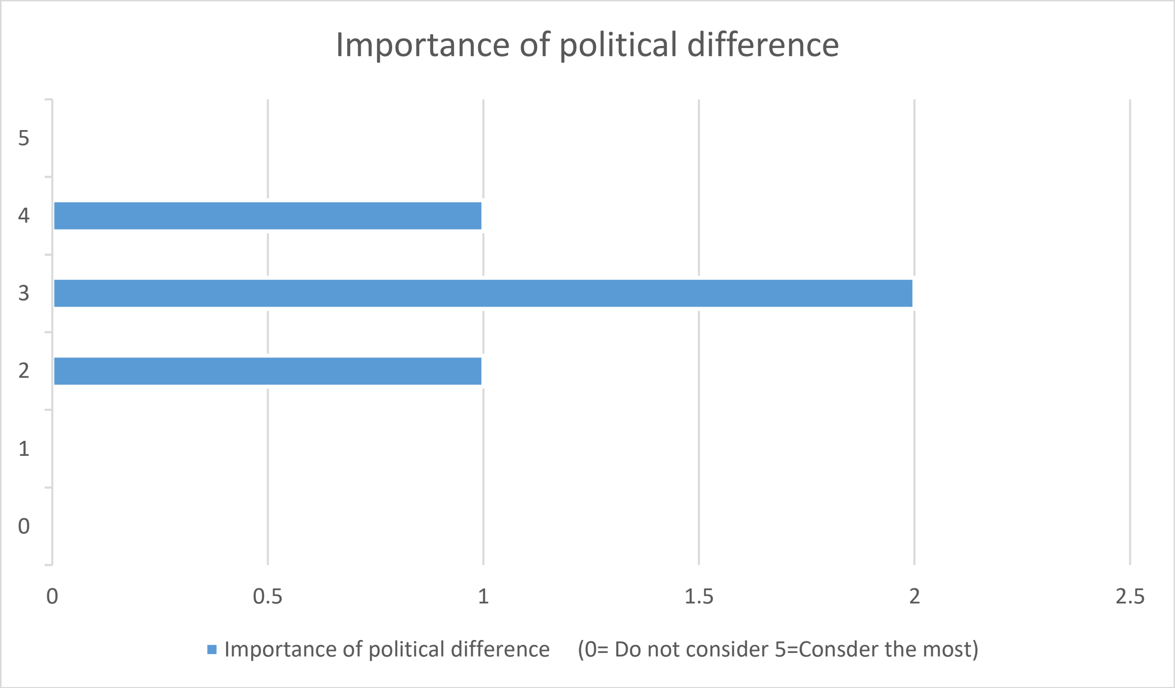


Figure D.474: Importance of political difference (Information Security)

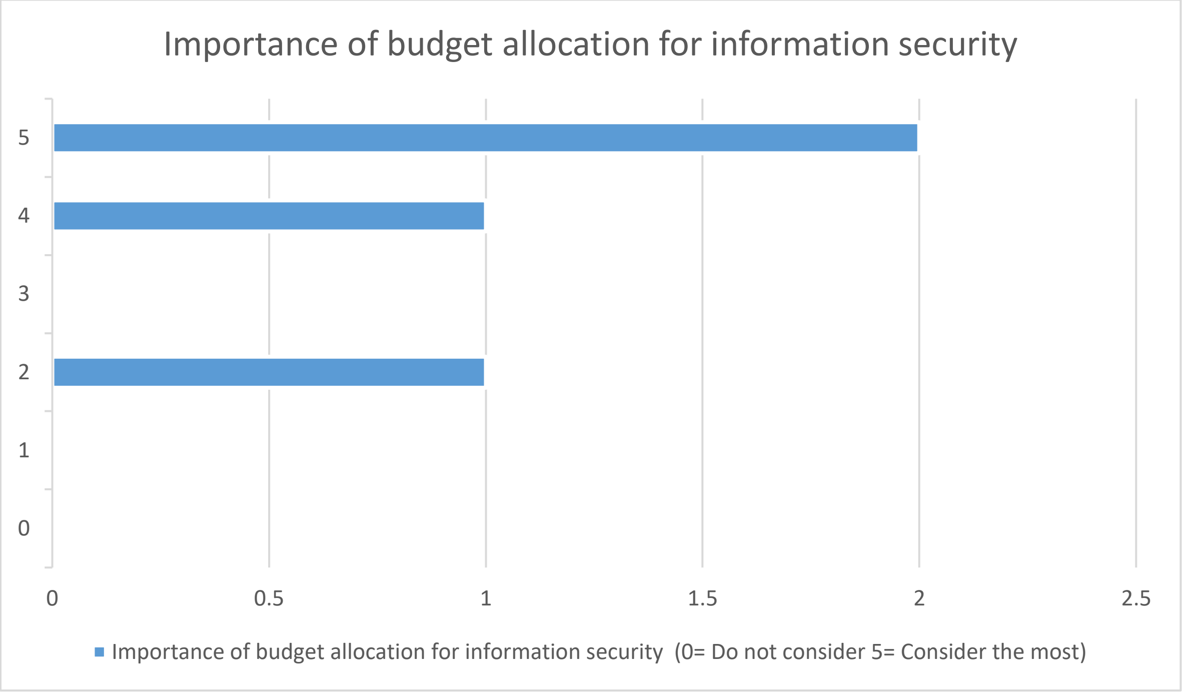


Figure D.475: Importance of budget allocation for information security (Information Security)

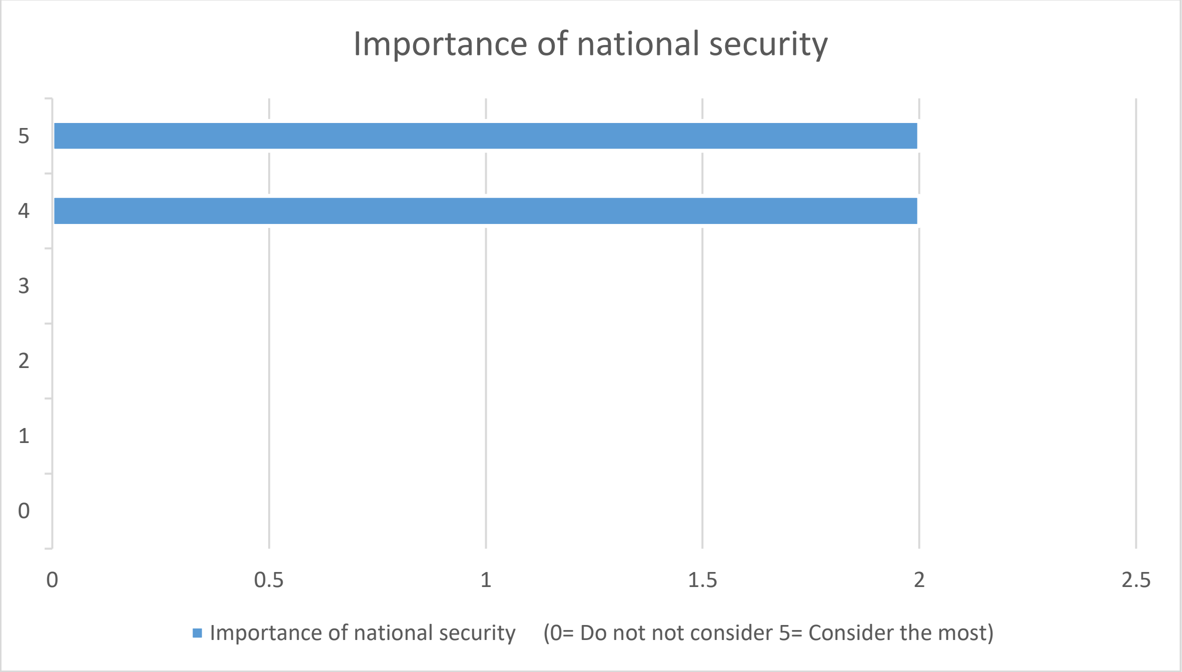


Figure D.476: Importance of national security (Information Security)

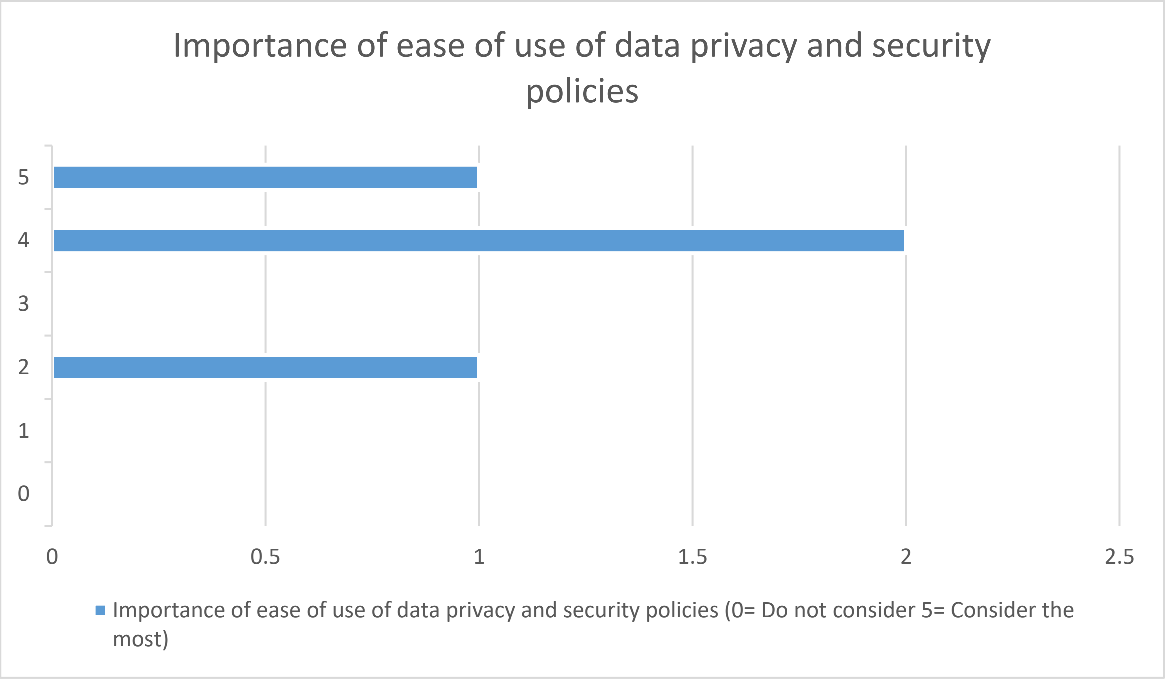


Figure D.477: Importance of ease of use of data privacy and security policies (Information Security)

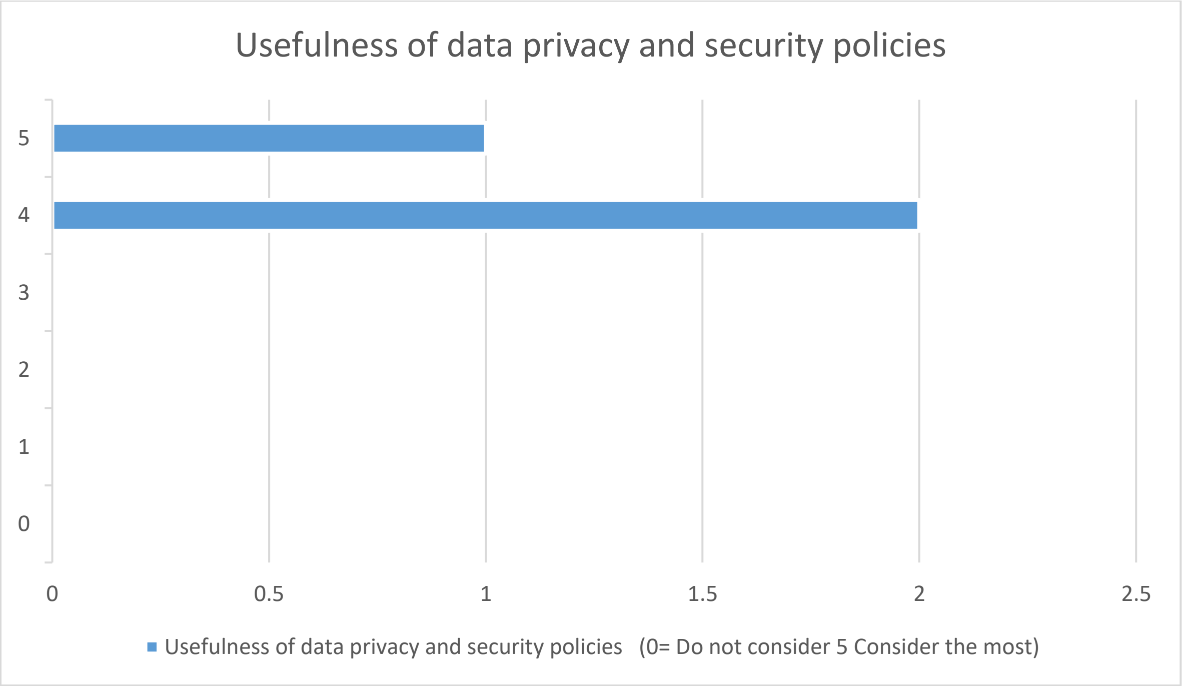


Figure D.478: Usefulness of data privacy and security policies (Information Security)

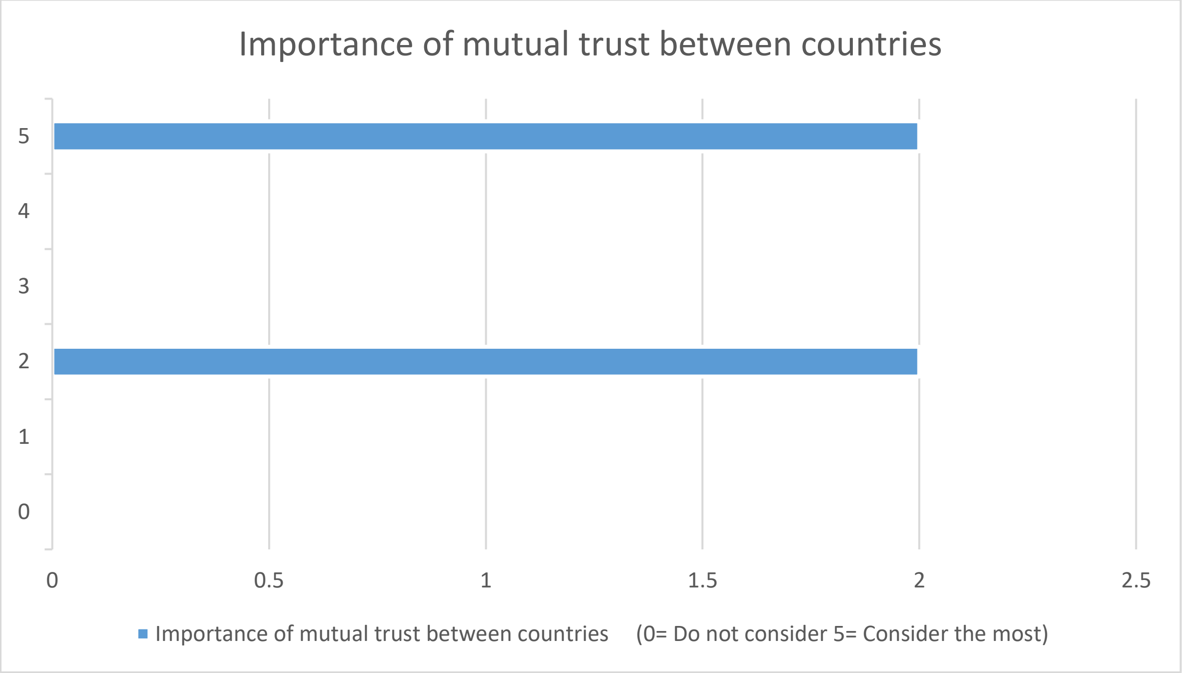


Figure D.479: Importance of mutual trust between countries (Information Security)

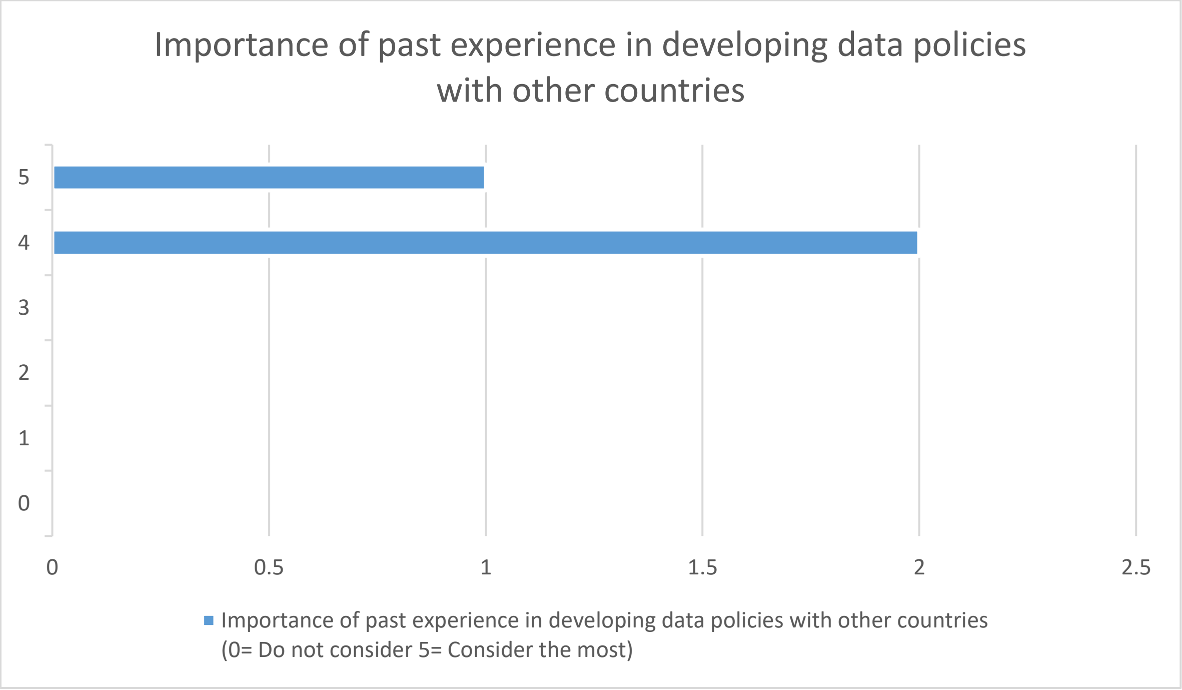


Figure D.480: Importance of past experience in developing data policies with other counties (Information Security)

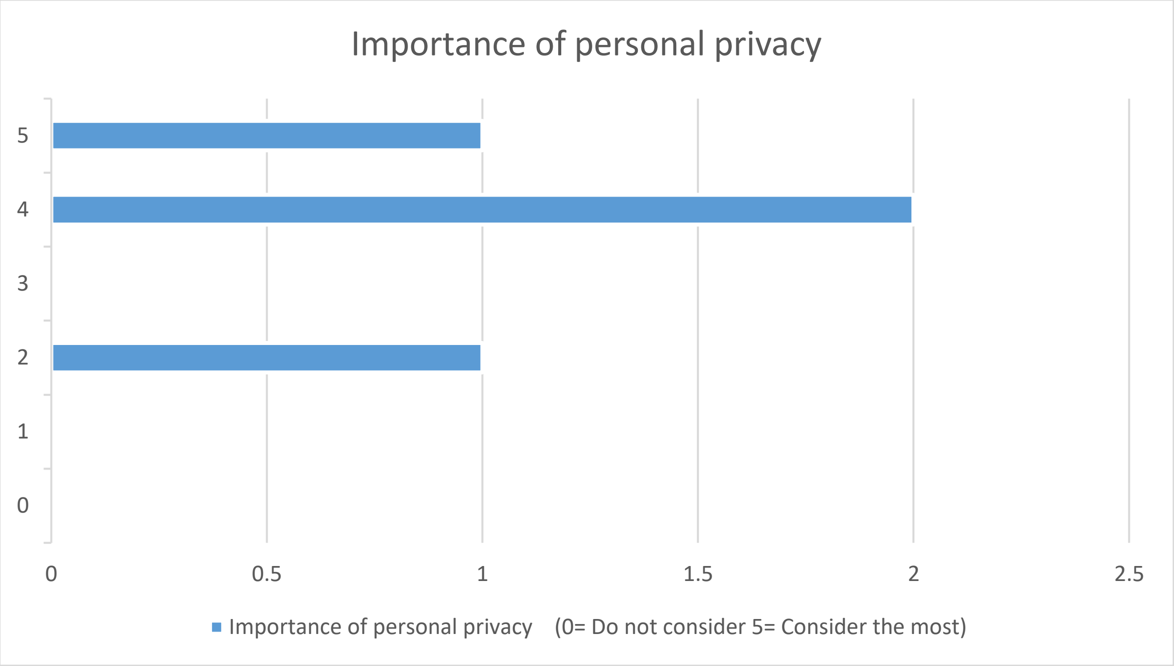


Figure D.481: Importance of personal privacy (Information Security)

The message from the respondents makes the case for having a global level data protection mechanism, which 71 percent of the participants agrees with (See figure D.470). The participants show their interest in the importance of national security in developing and accepting a global level data protection mechanism (See figure D.476)

Sri Lanka – Media

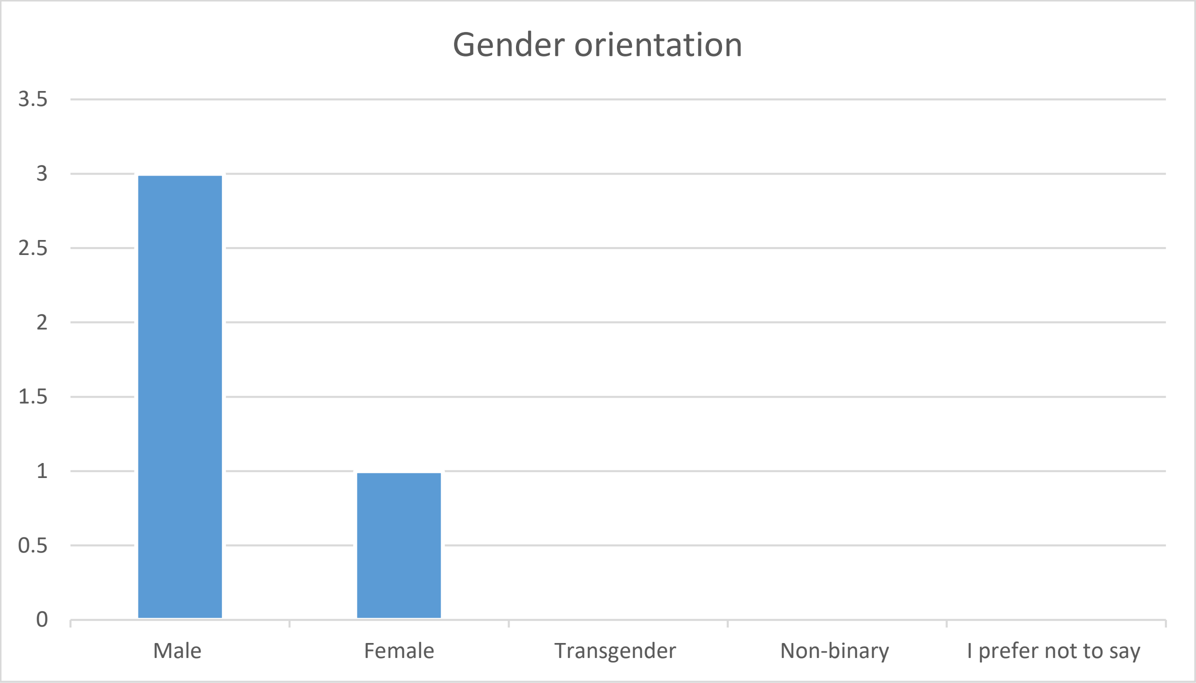


Figure D.482: Gender orientation (Media)

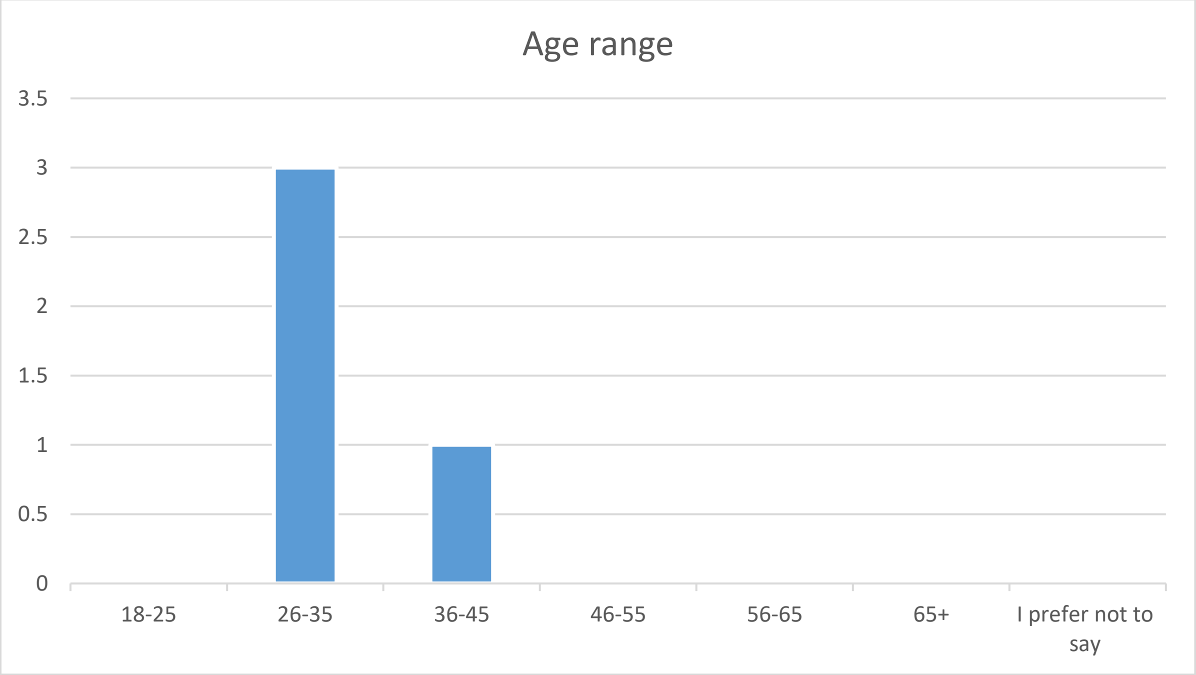


Figure D.483: Age range (Media)

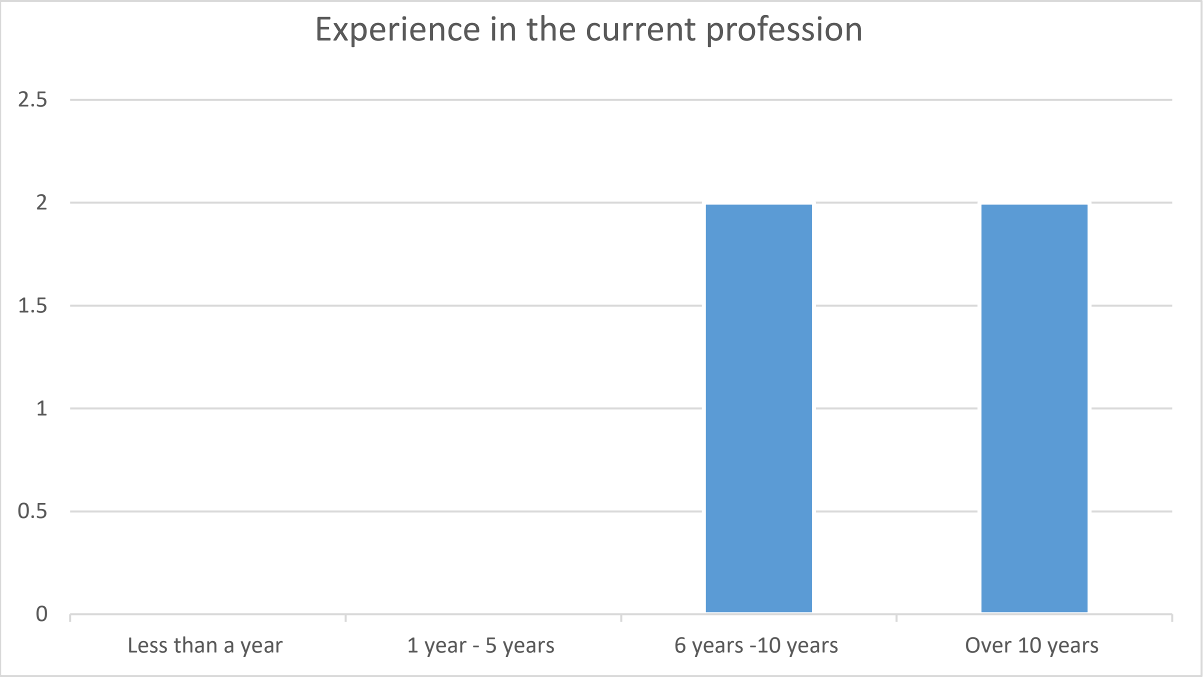


Figure D.484: Experience in current profession (Media)

This analysis is based on the responses received from Sri Lankans engaged in the media sector. There were 4 participants, 3 males and 1 female (See figure D.482), all in the 26-45 age range. Split into two groups, 3 in the 26-35; and 1 in the 36-45 age range (See figure D.483). All with 6 years or more than 10 years of experience in the current profession (See figure D.484).

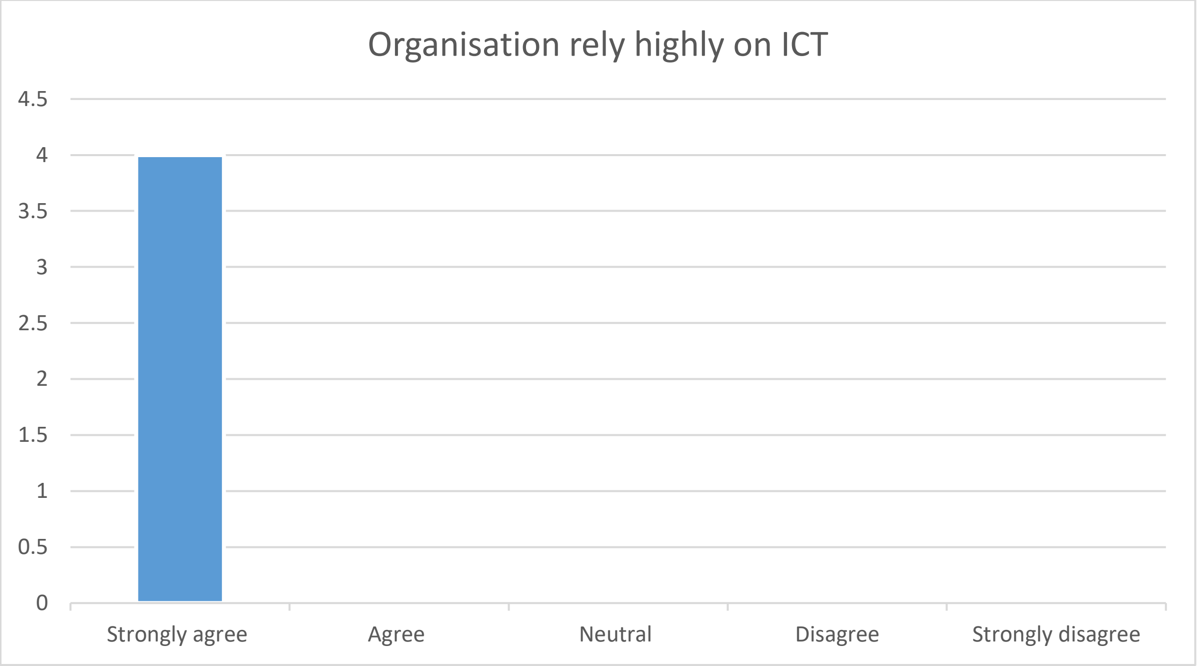


Figure D.485: Organisation rely highly on ICT (Media)

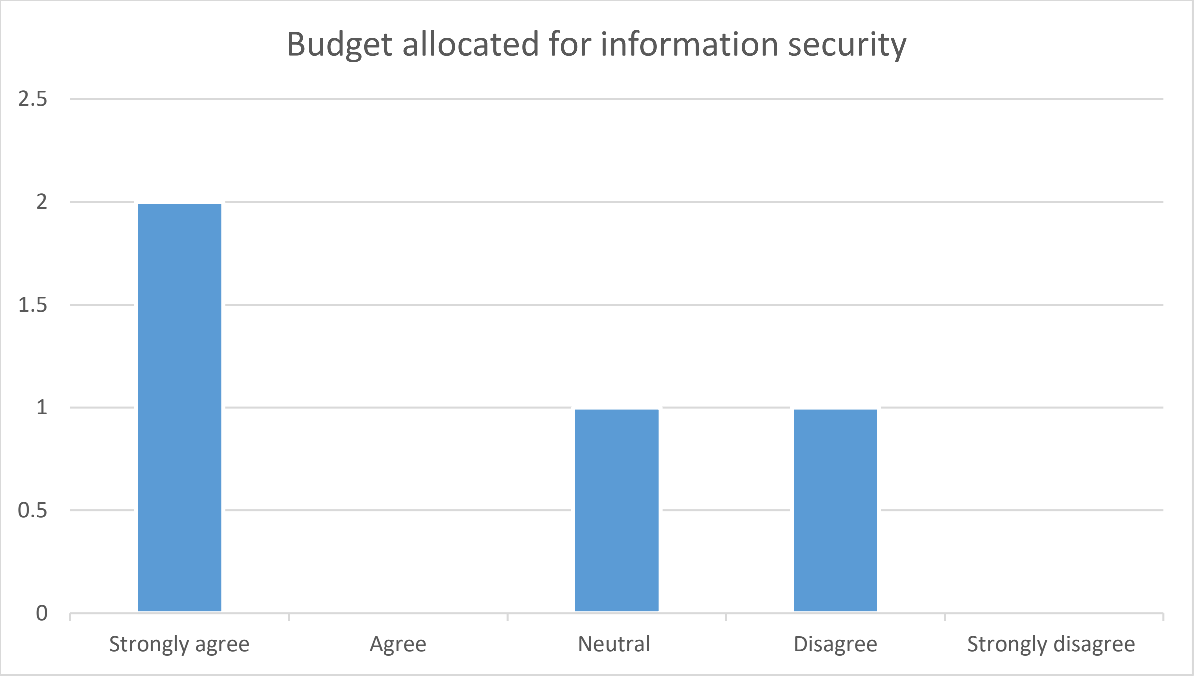


Figure D.486: Budget allocated for information security (Media)

All 4 respondents employed in a technology reliance working environment (See figure D.485). 2 agree their organisations have a budget allocation for information security; 1 does not know; 1 disagreed (See figure D.486).

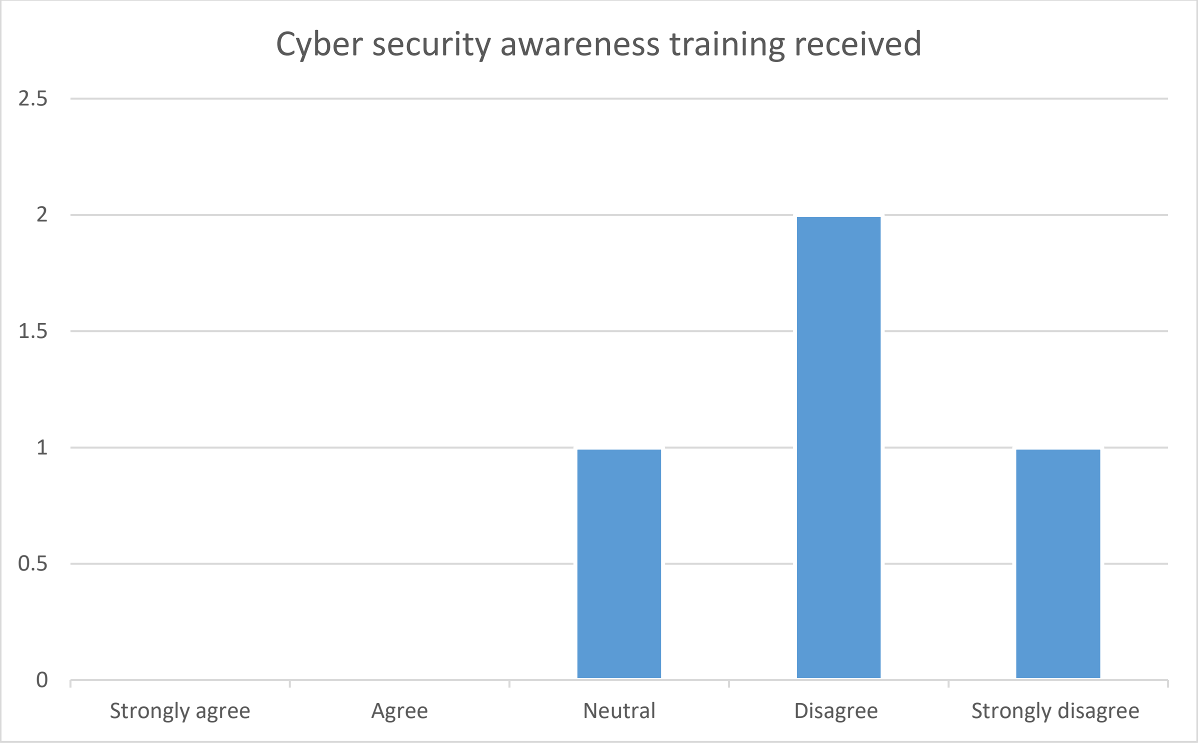


Figure D.487: Cyber security awareness training received (Media)

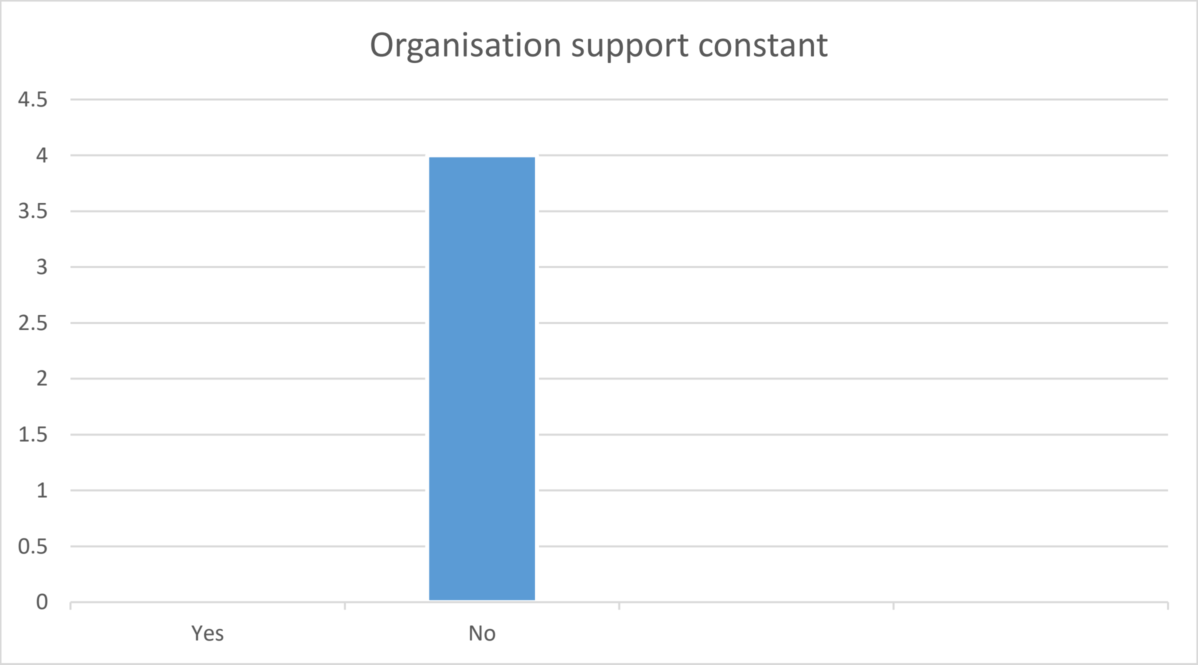


Figure D.488: Organisation support constant (Media)

Despite the level of resources allocated, regular training in security awareness received inadequate. None received regular cybersecurity awareness training; 1 neither agreed nor disagreed; 3 participants who had not regularly received security awareness training (See figure D.487). None of the participants received support from the organisation to protect personal information (See figure D.488). That clearly suggests insufficient organisational support to protect personal information despite funds being available for information security and high reliance on technology.

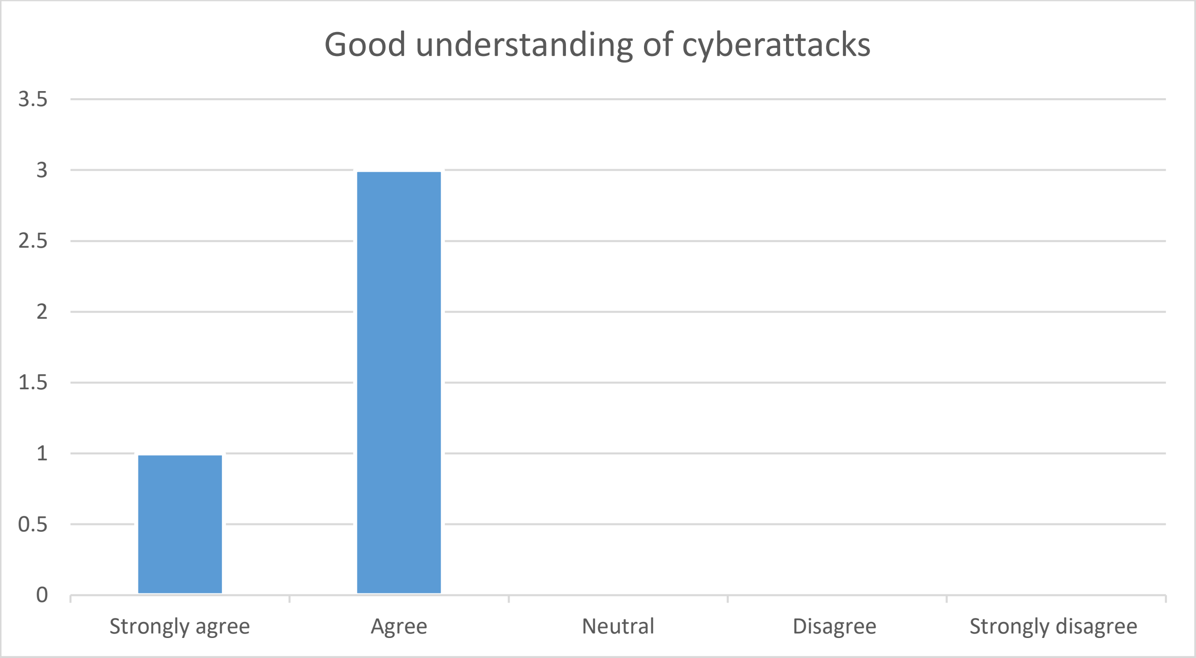


Figure D.489: Good understanding of cyberattacks (Media)

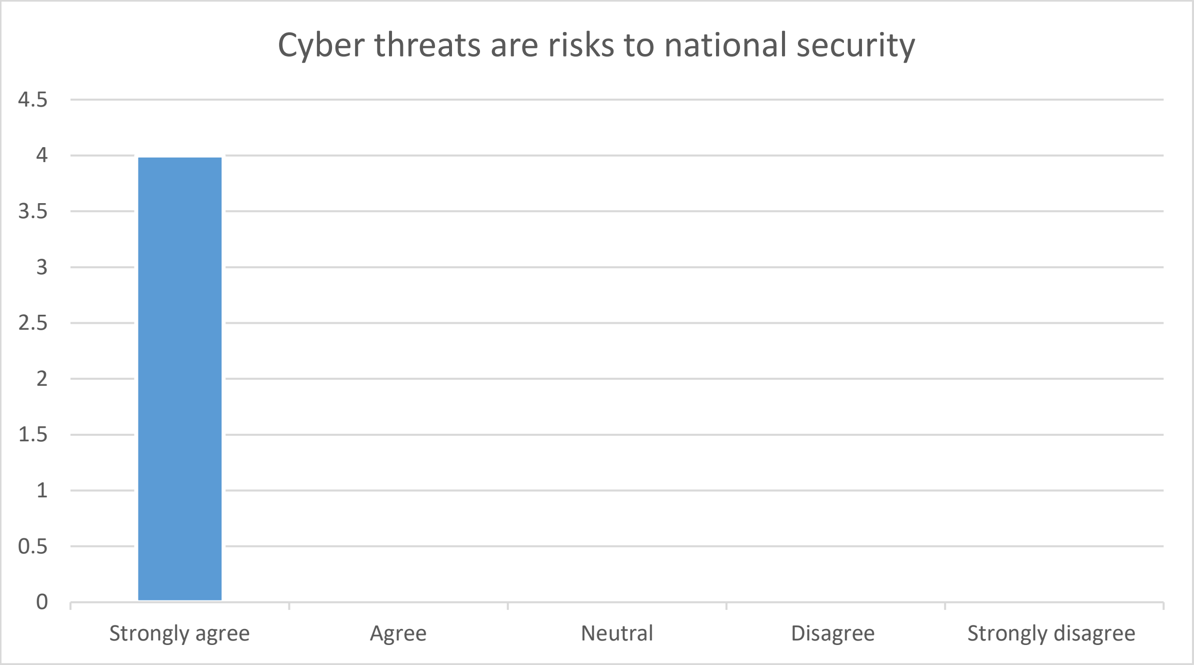


Figure D.490: Cyber threats are risks to national security (Media)

Despite the lack of security awareness training, all 4 participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation (See figure D.489), and the potential threats to national security from cyber-attacks (See figure D.490). In general, understanding cyber threats and their impact on national security encourage people to act responsibly to minimise end-user errors, and in time, they would be in a strong position to influence the process of accepting and implementing a national, regional, and global level mechanism.

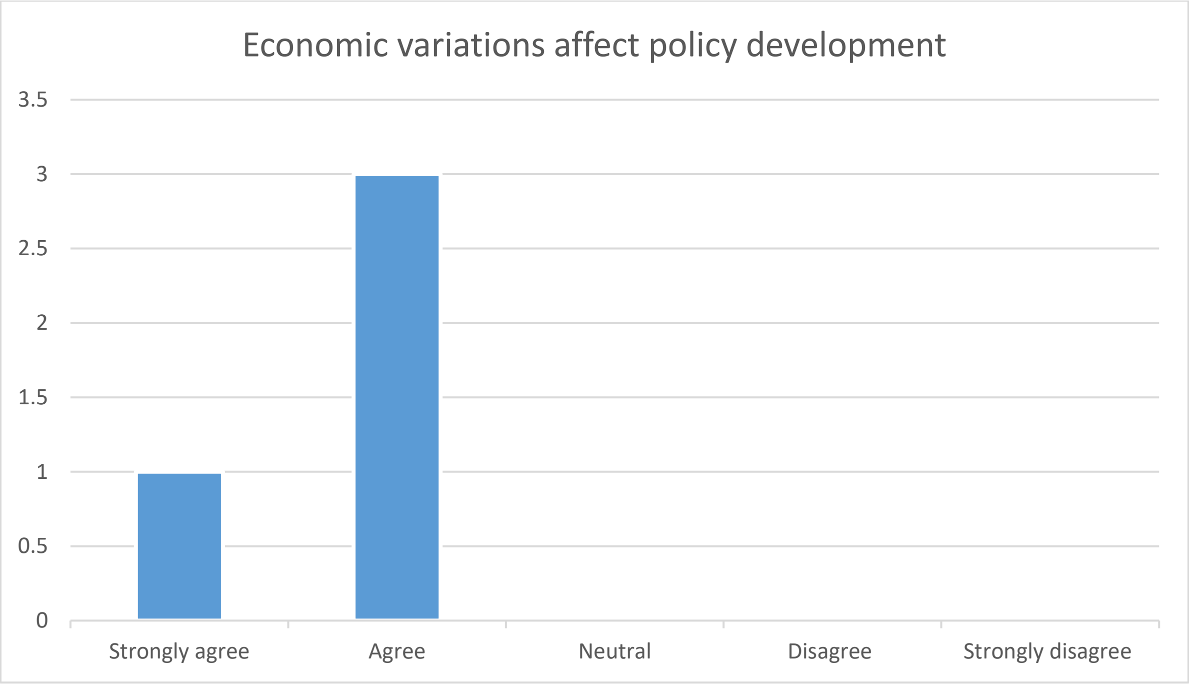


Figure D.491: Economic variations affect policy development (Media)

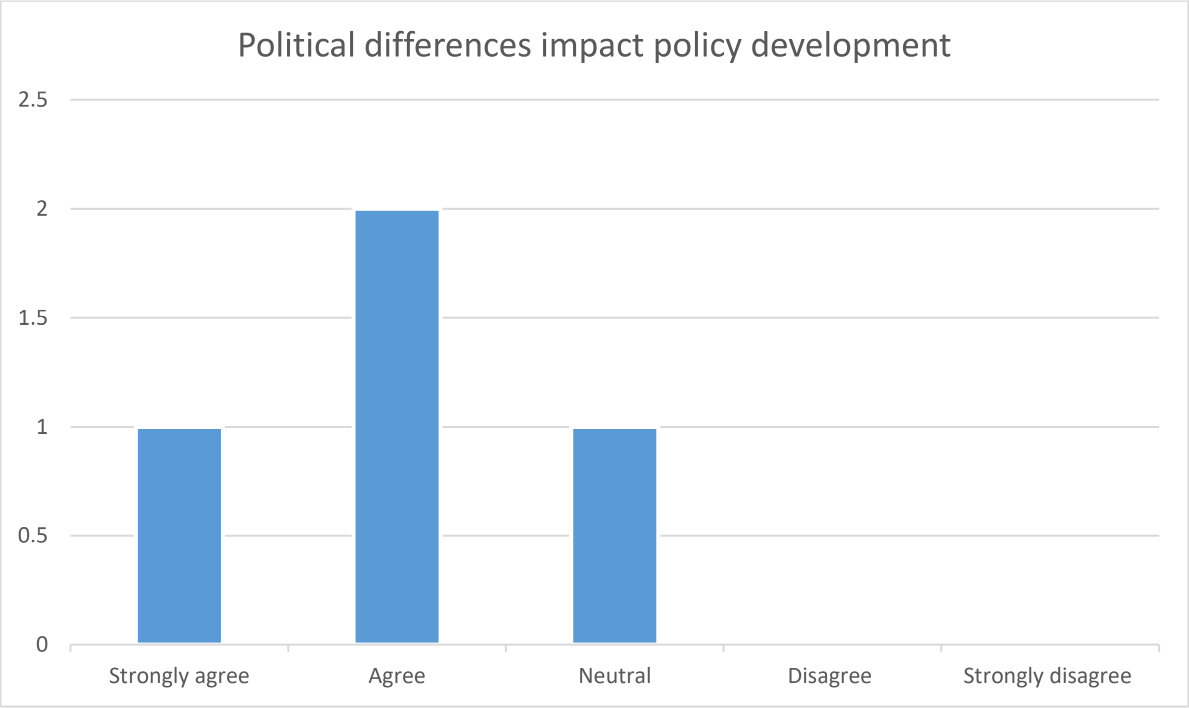


Figure D.492: Political differences impact policy development (Media)

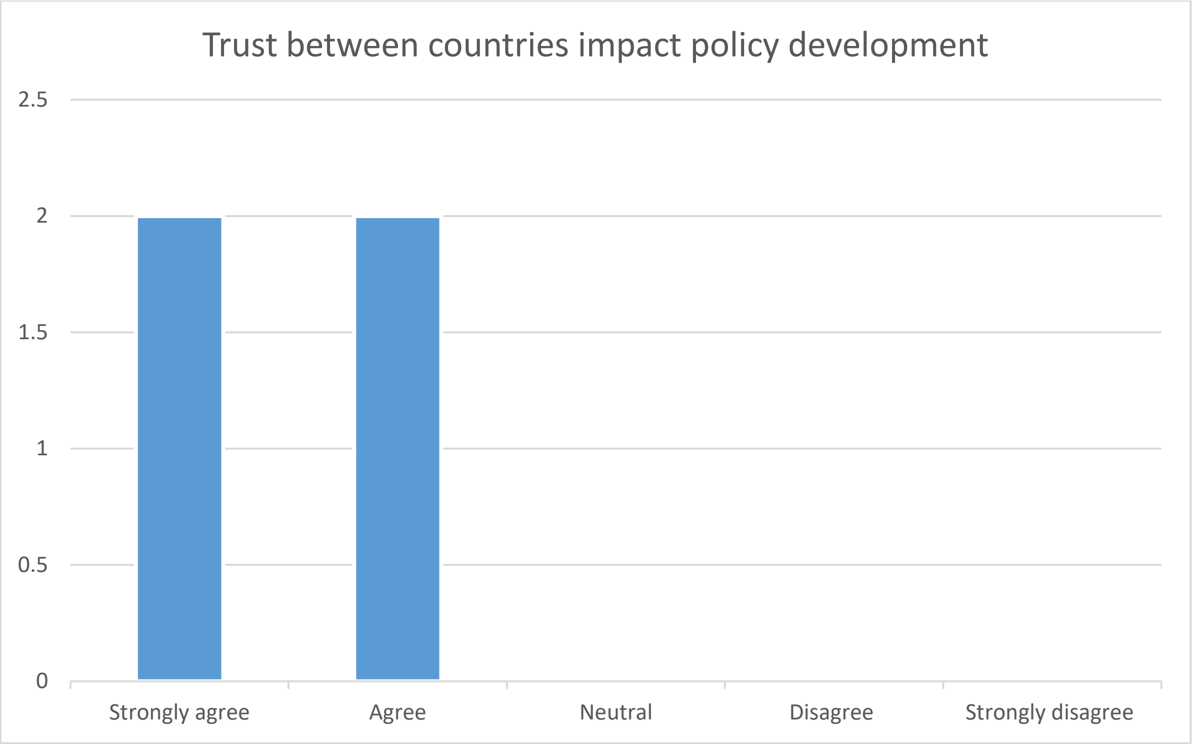


Figure D.493: Trust between countries impact policy development (Media)

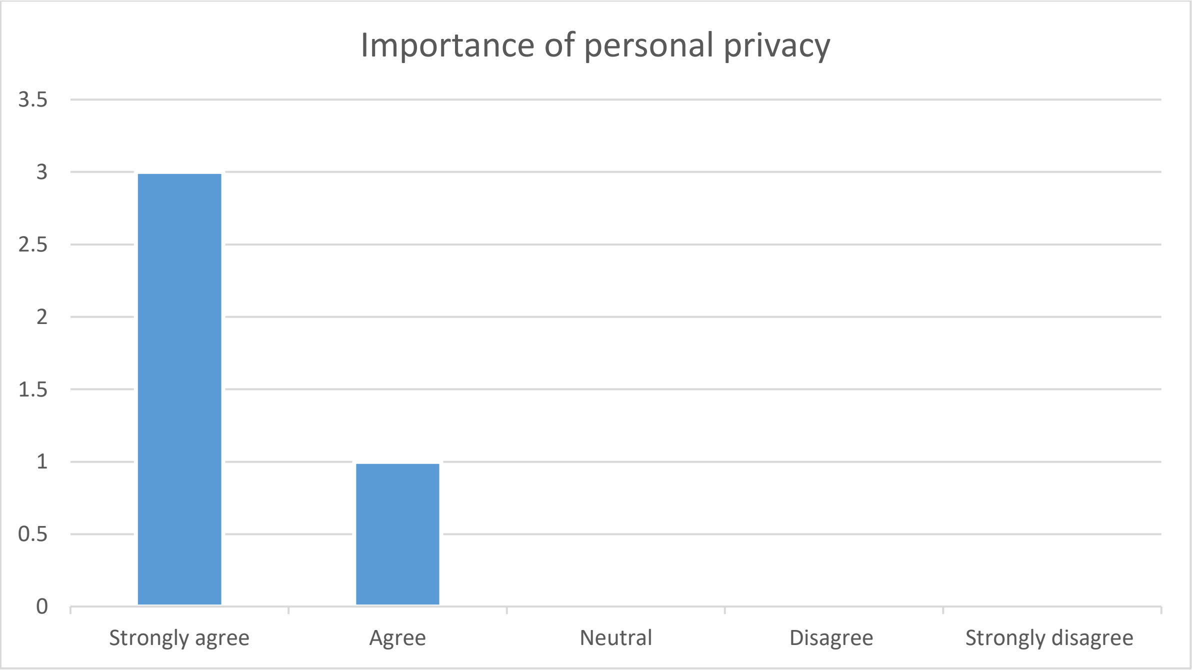


Figure D.494: Importance of personal privacy (Media)

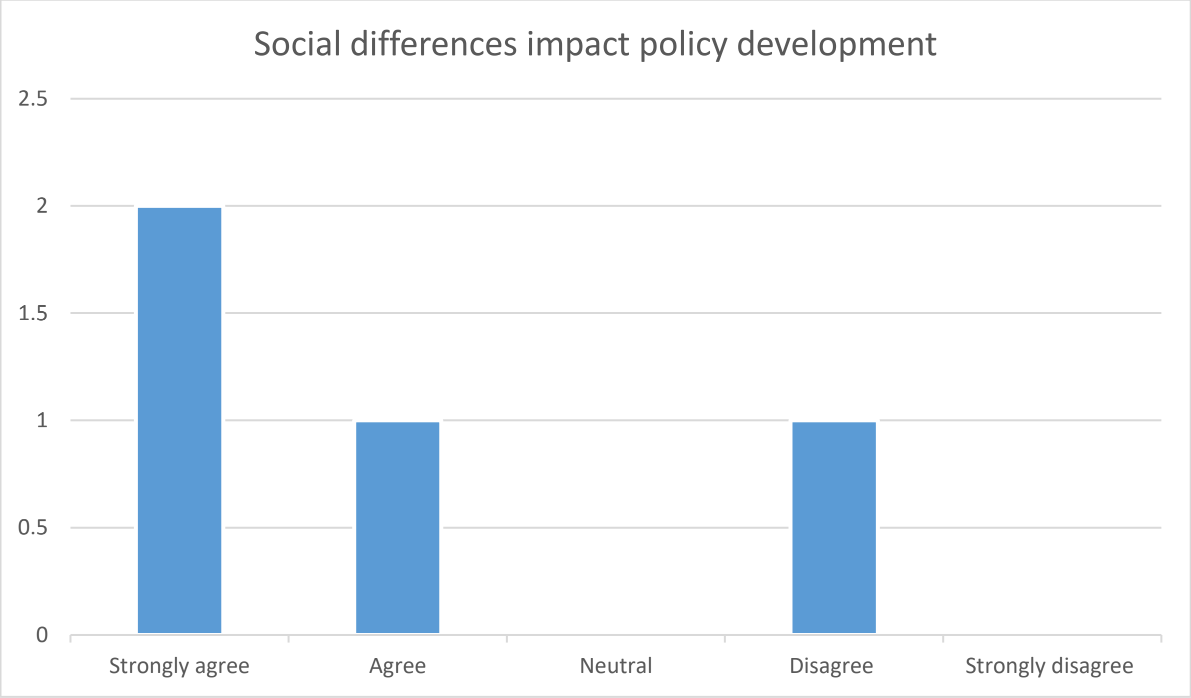


Figure D.495: Social differences impact policy development (Media)

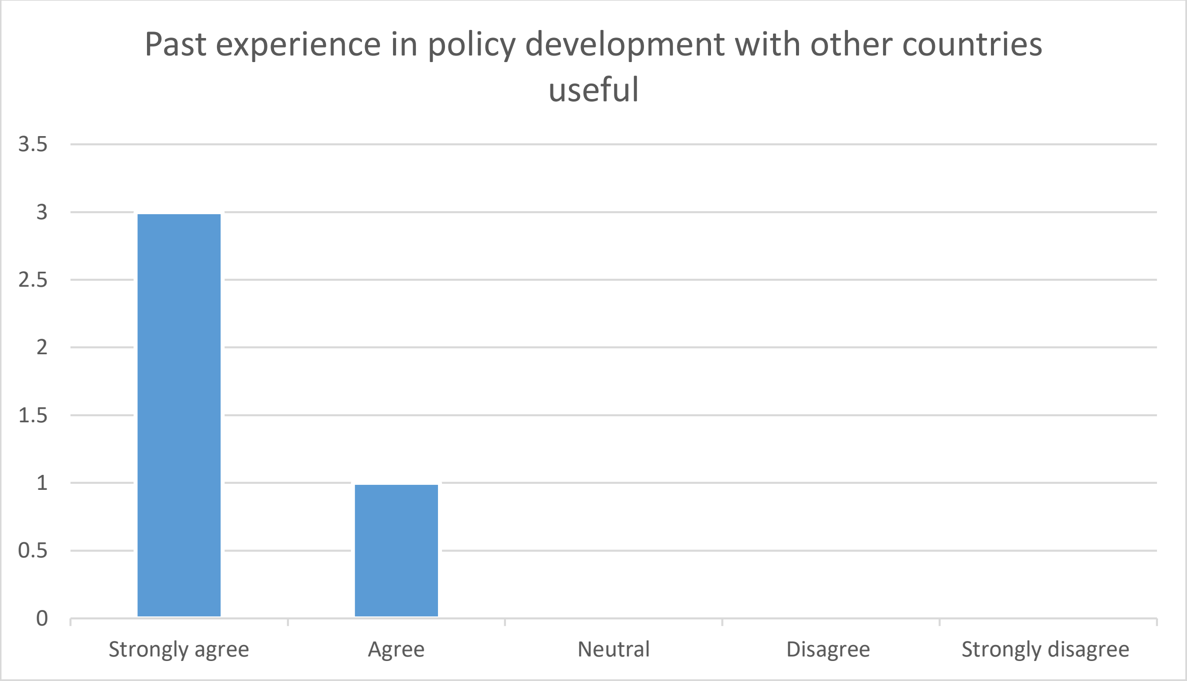


Figure D.496: Past experience in policy development with other countries useful (Media)

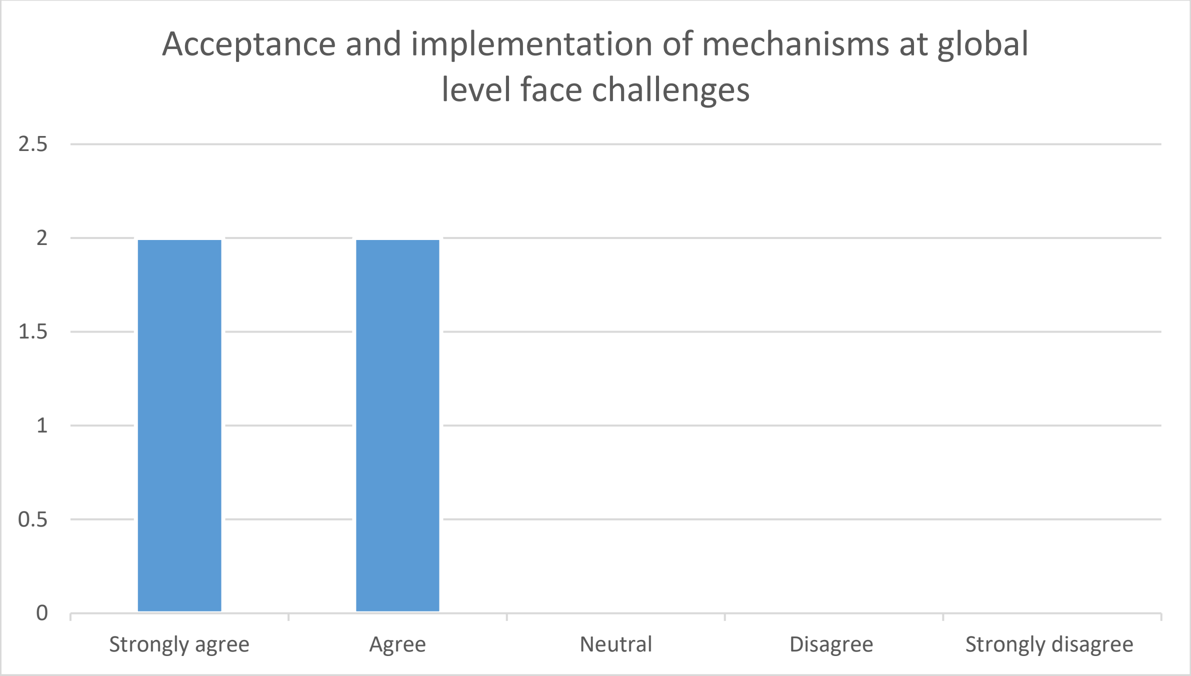


Figure D.497: Acceptance and implementation of mechanisms at global level face challenges (Media)

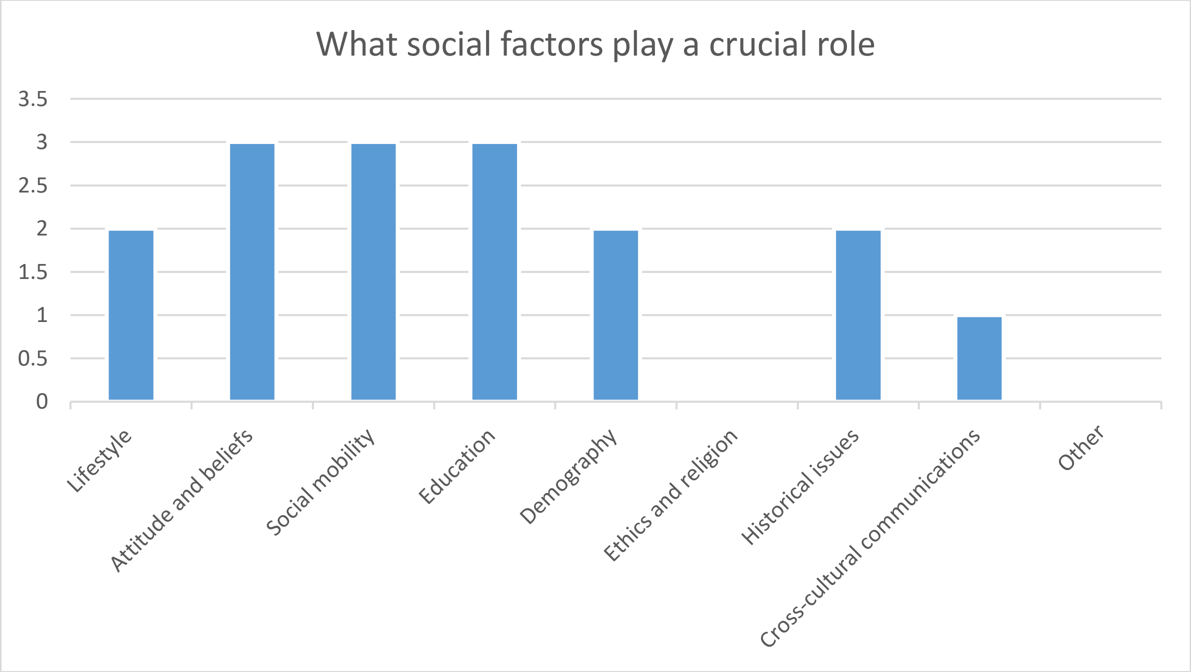


Figure D.498: What social differences play a crucial role (Media)

In response to the survey on social differences, the majority flag up the importance of education, lifestyle and attitude and beliefs, social mobility, demography, and historical issues (See figure D.498). There could be several reasons for the views expressed by this group, one being their social interaction with diverse groups of people due to the nature of the work that does, and the other being the demographical areas they cover. That gives them a deep understanding of the issues and attitudes of those who they come across in their daily life, and belief that it is of importance to consider social diversity in the wides form in accepting and implementing policies.

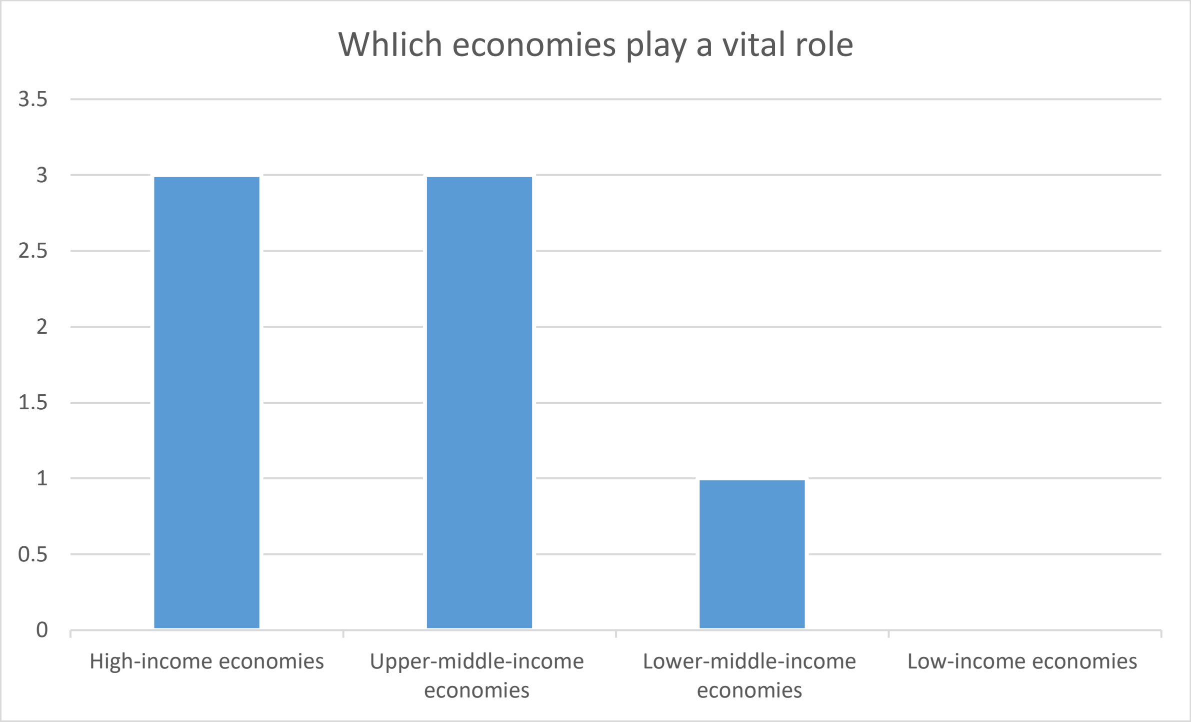


Figure D.499: Which economies play a vital role (Media)

Majority believes that the high income and upper-middle-income countries play a vital role in the policy development process (See figure D.499). The key stages in the policymaking process aim to identify policymaker aims, identify policies to achieve those aims, select a policy measure, identify the resources necessary, implement, and finally evaluate the policy. These stages are time-consuming and require sufficient funding and resources. Therefore, the economic stability of the country is considered an important contributory factor towards achieving success in policymaking.

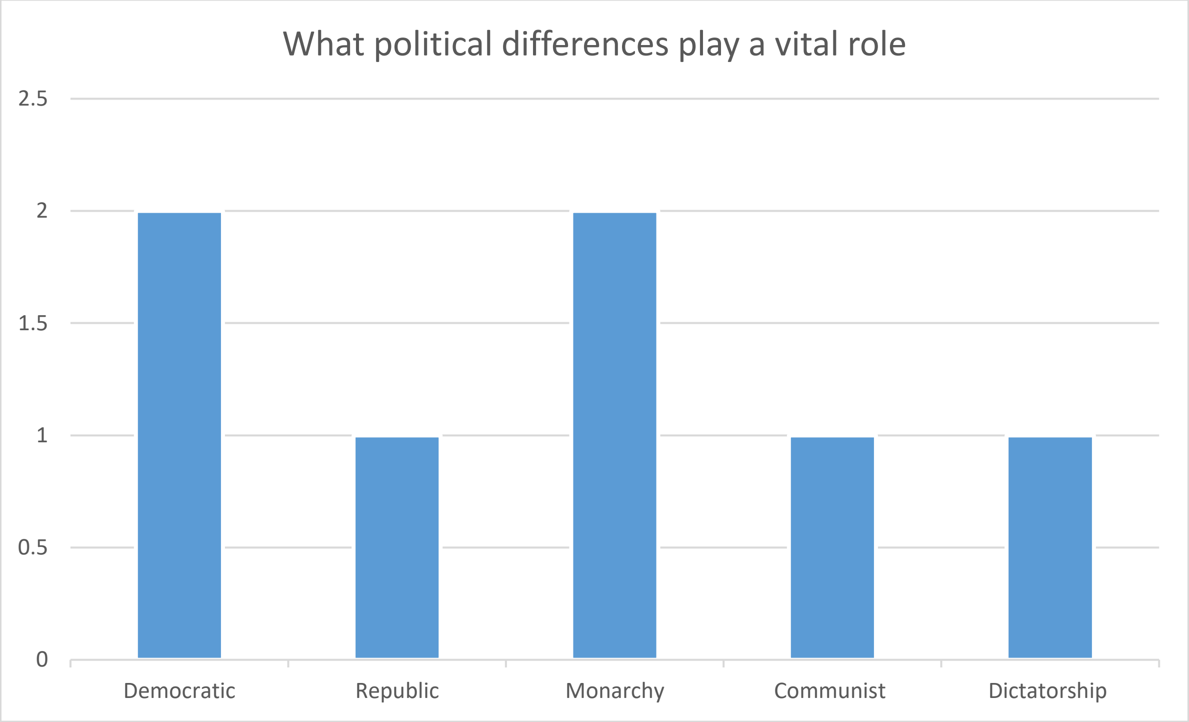


Figure D.500: What political differences play a vital role (Media)

The majority agree with both democratic and monarch political systems (See figure D.500). They allow the public an influential voice in policy development and encourages consensus and collective responsibility for their actions, and it helps to develop trust between the organisations and ensures coherence and transparency in the policy development process. The monarchist system has an individual ruler as head of state having functional power to sustain his/or her hereditary status. This system does not provide space for public participation and expression of opinions prohibited, and the power of the ruler is unquestionable. The reason for choosing Monarchist system is likely to be the failures and shortcomings of democratic systems of governance.

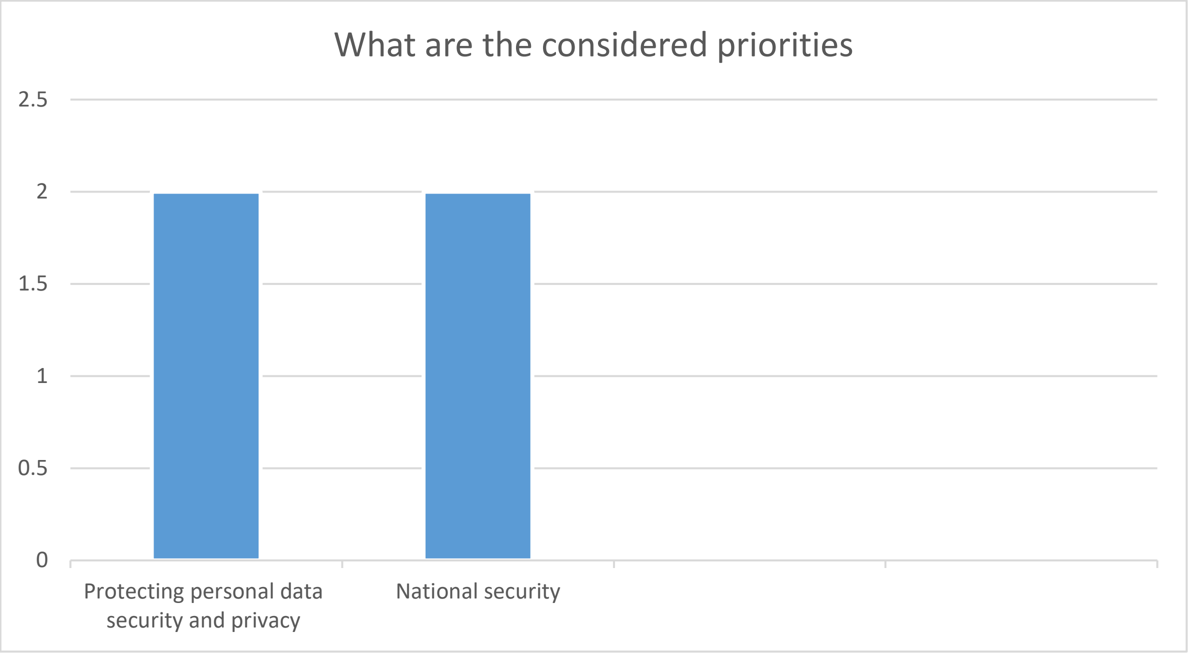


Figure 4.501: What are the considered priorities (Media)

The majority mentions neither the importance of protection of personal data security and privacy nor protection of national security in accepting and implementing global data privacy and security policies (See figure D.501). The implications of a personal data breach incident will have a knock-on effect on national security, and it will also be felt right across the groups as well as the community alike.

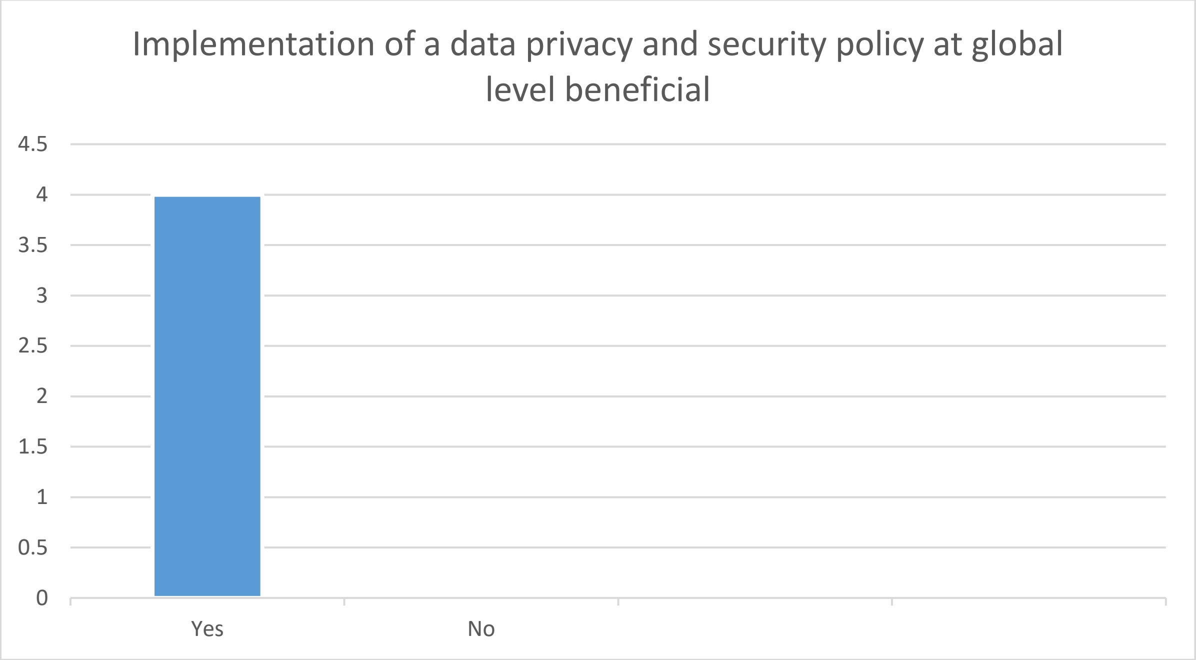


Figure D.502: Implementation of a data privacy and security policy at global level beneficial (Media)

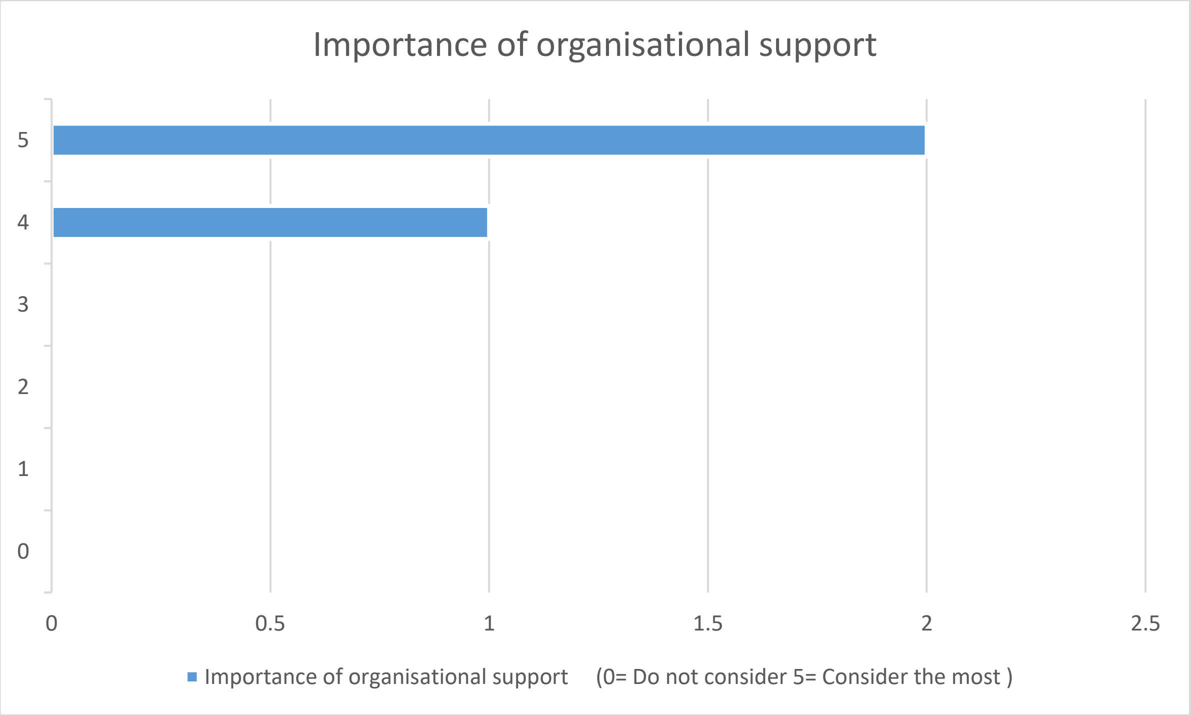


Figure D.503: Importance of organisational support (Media)

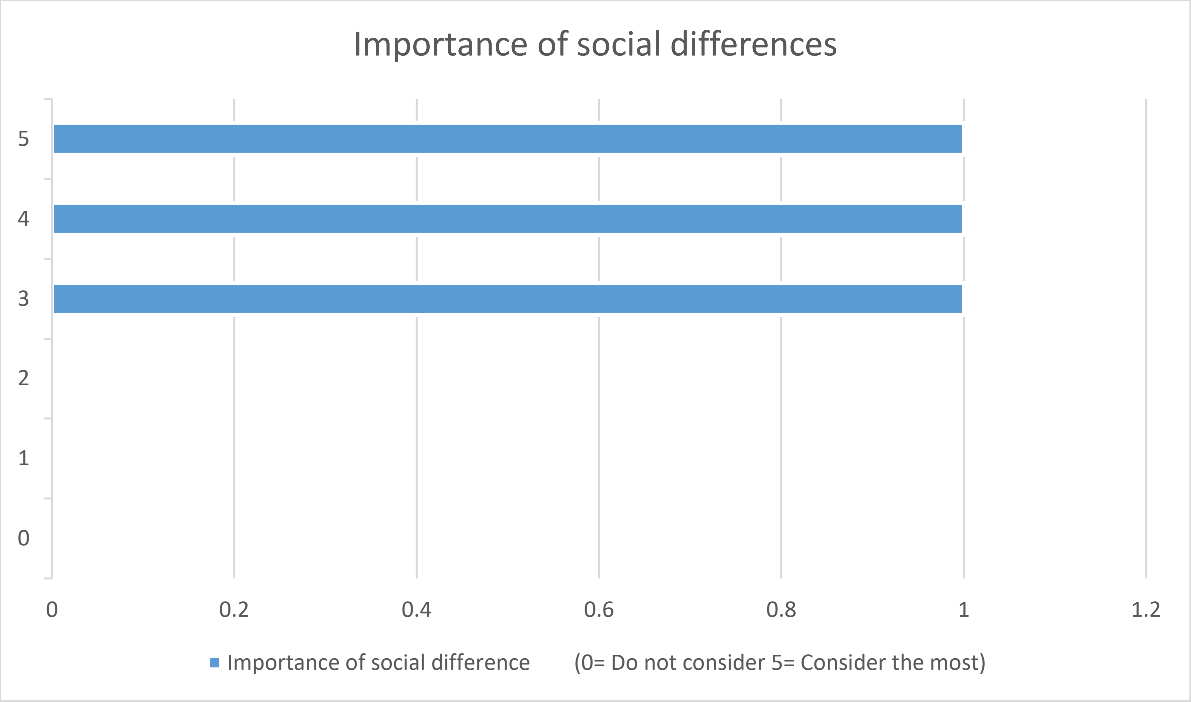


Figure D.504: Importance of social differences (Media)

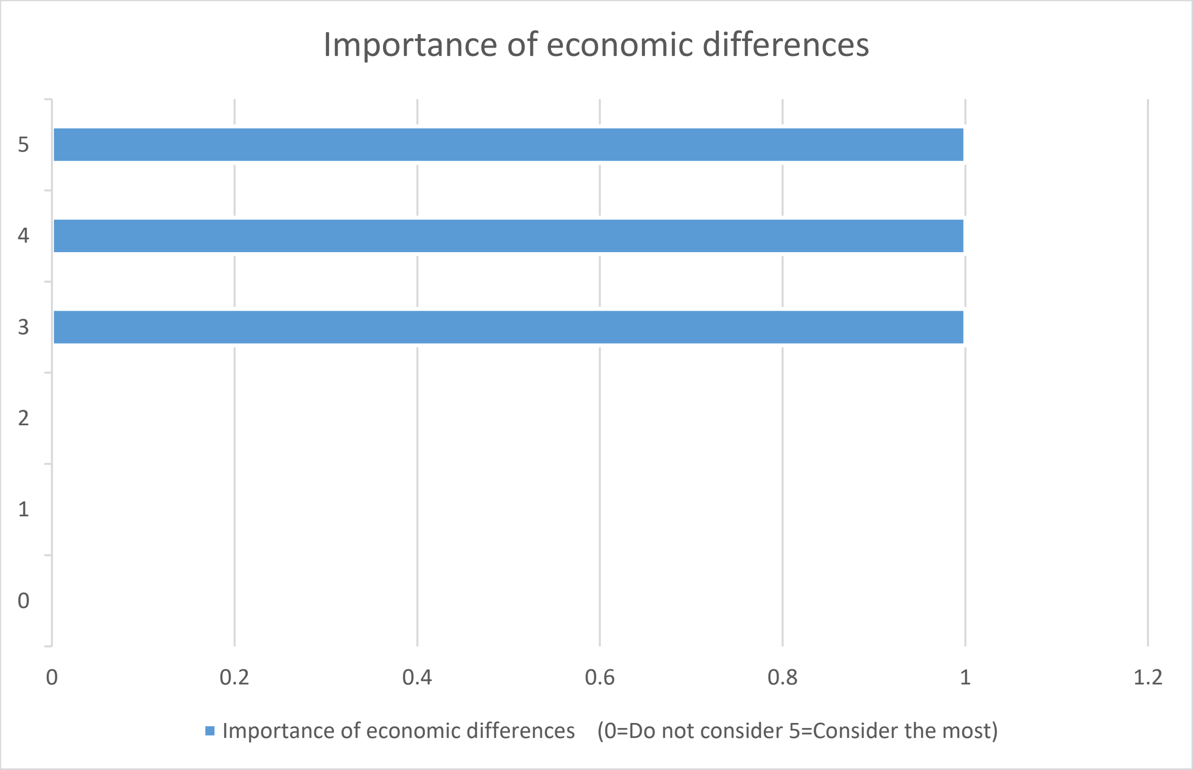


Figure D.505: Importance of economic differences (Media)

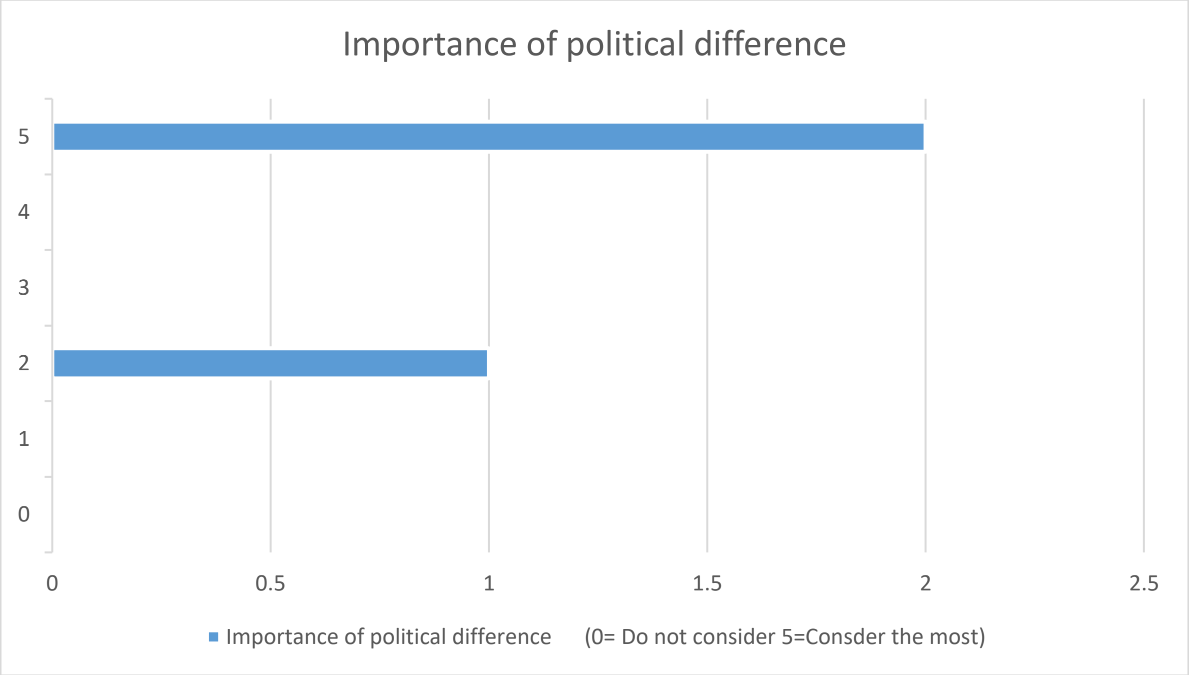


Figure D.506: Importance of political difference (Media)

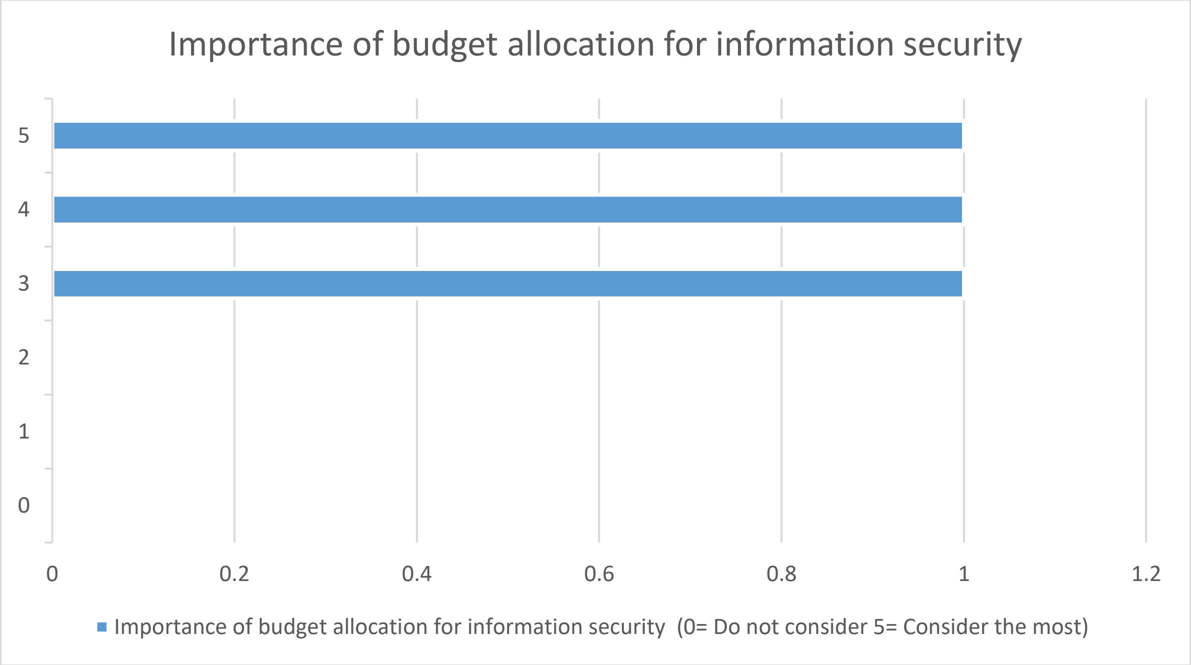


Figure D.507: Importance of budget allocation for information security (Media)

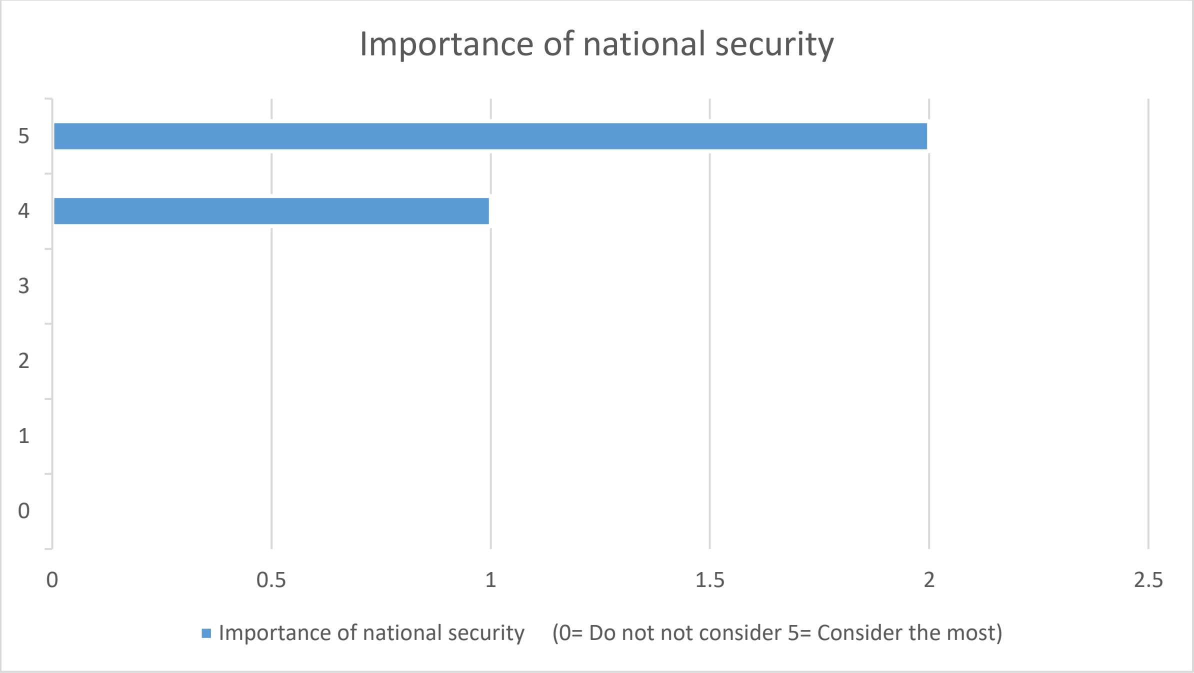


Figure D.508: Importance of national security (Media)

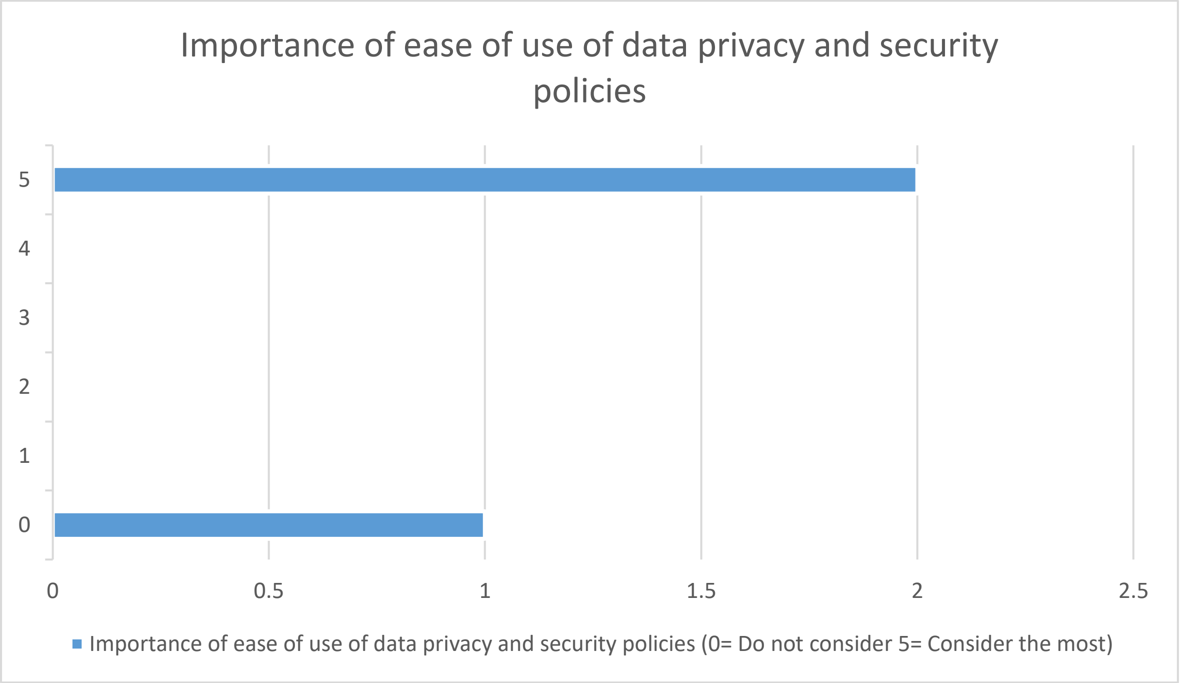


Figure D.509: Importance of ease of use of data privacy and security policies (Media)

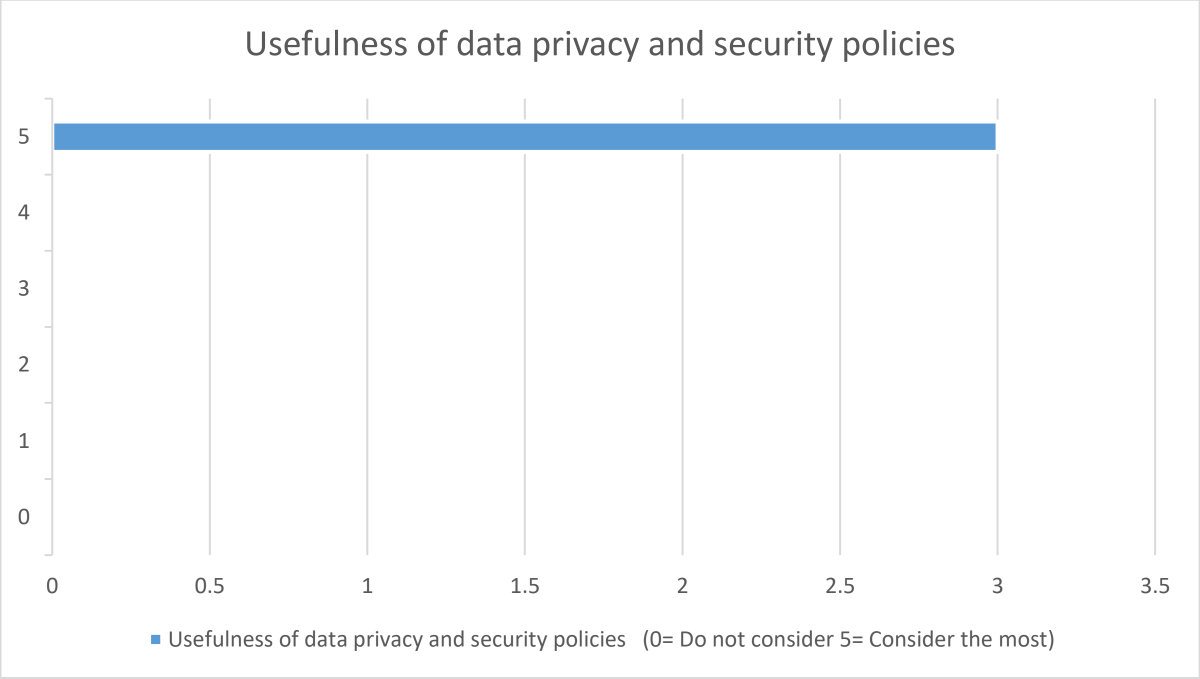


Figure D.510: Usefulness of data privacy and security policies (Media)

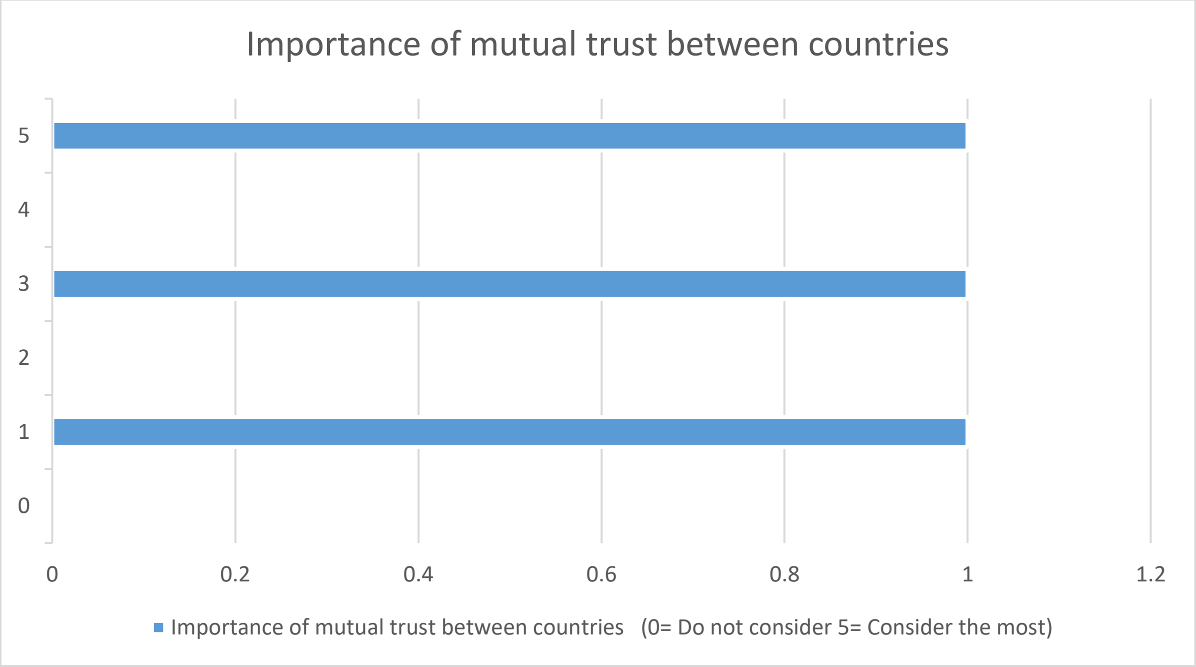


Figure D.511: Importance of mutual trust between countries (Media)

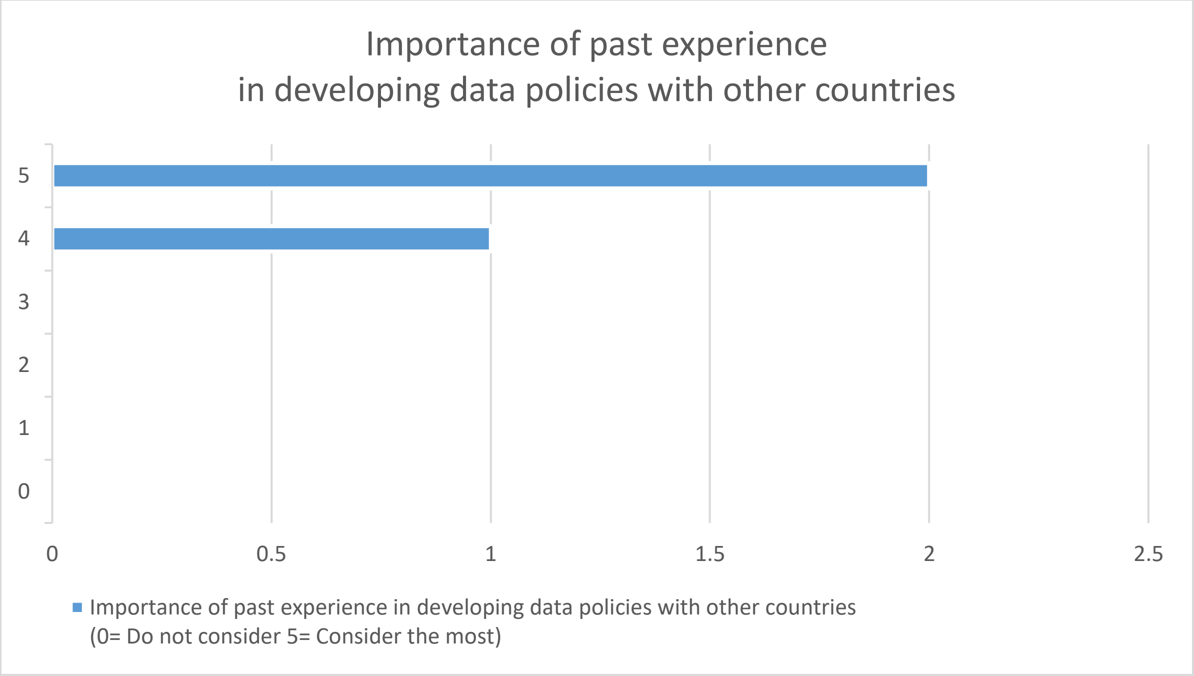


Figure D.512: Importance of past experience in developing data policies with other counties (Media)

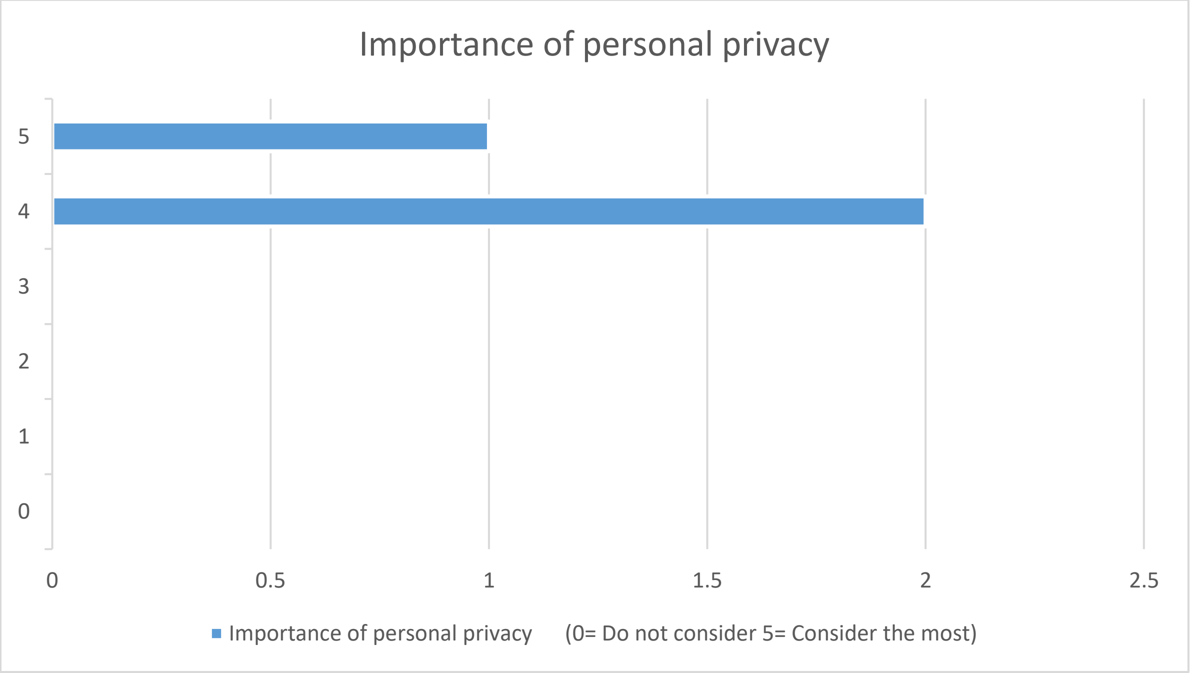


Figure D.513: Importance of personal privacy (Media)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 100 percent of the respondents have endorsed (See figure D.502). There is overwhelming consensus on organisational support, budget allocation, social differences, political differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure D.491-501) (See figure D.503-513).

Sri Lanka – Public services and administration

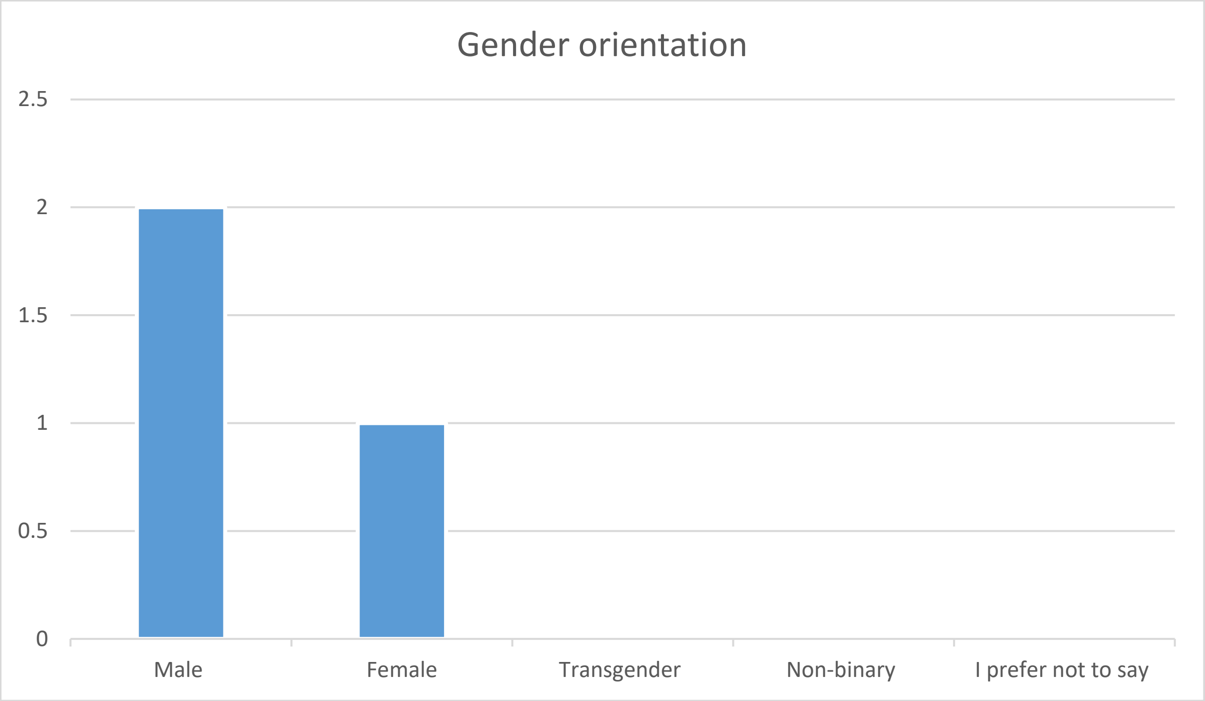


Figure D.514: Gender orientation (Public services and administration)

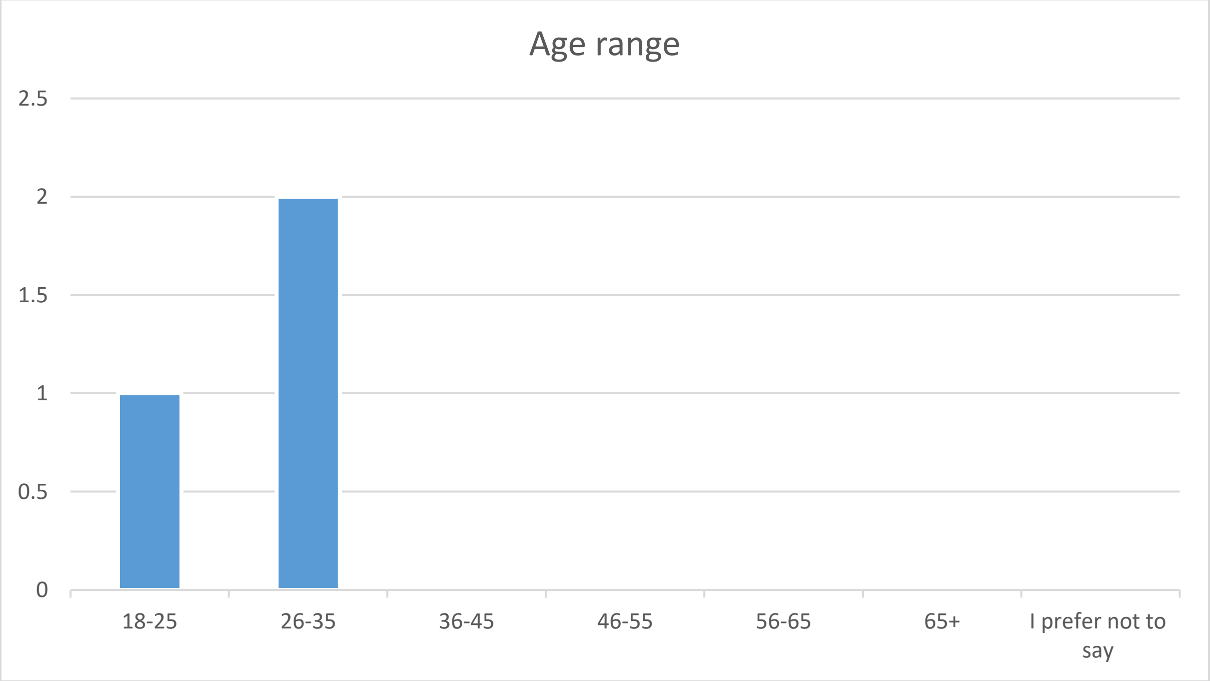


Figure D.515: Age range (Public services and administration)

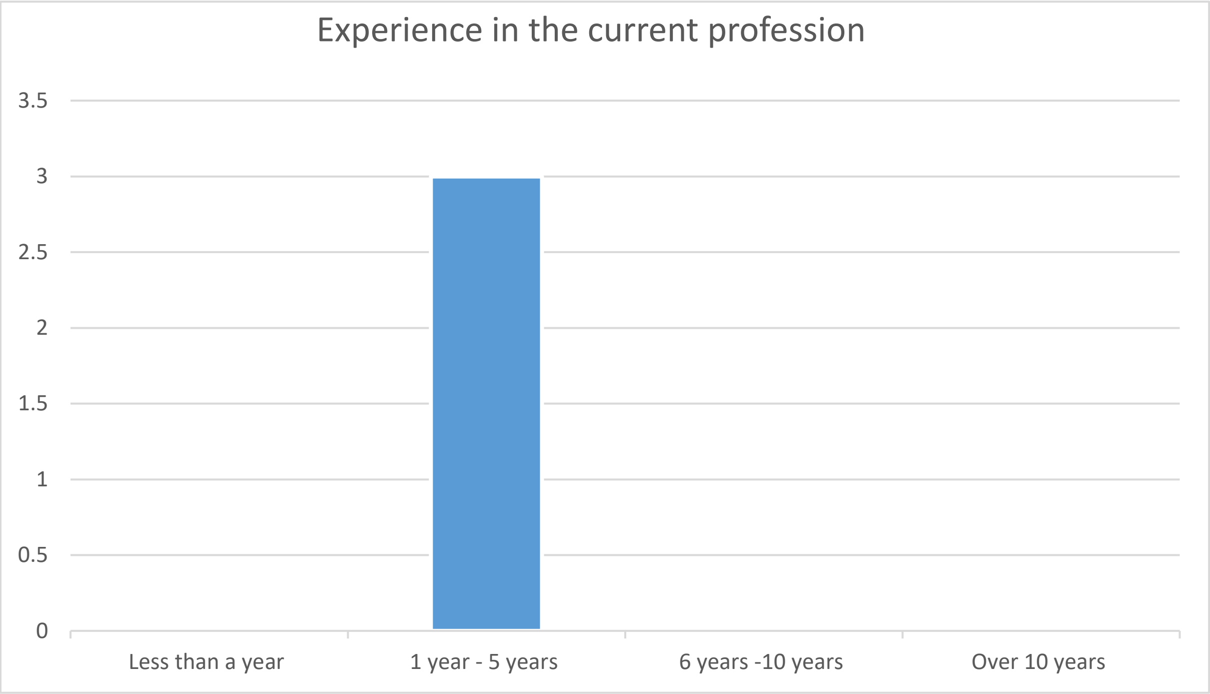


Figure D.516: Experience in current profession (Public services and administration)

This analysis is based on the responses received from Sri Lankans working in the public sector administration services. A total of 3 respondents include 2 males and 1 female (See figure D.514). All in the 18-35 age range; 1 between 18-25 range, and 2 between 26-35 range (See figure D.515), all having 1 to 5-year experience in the industry (See figure D.516).

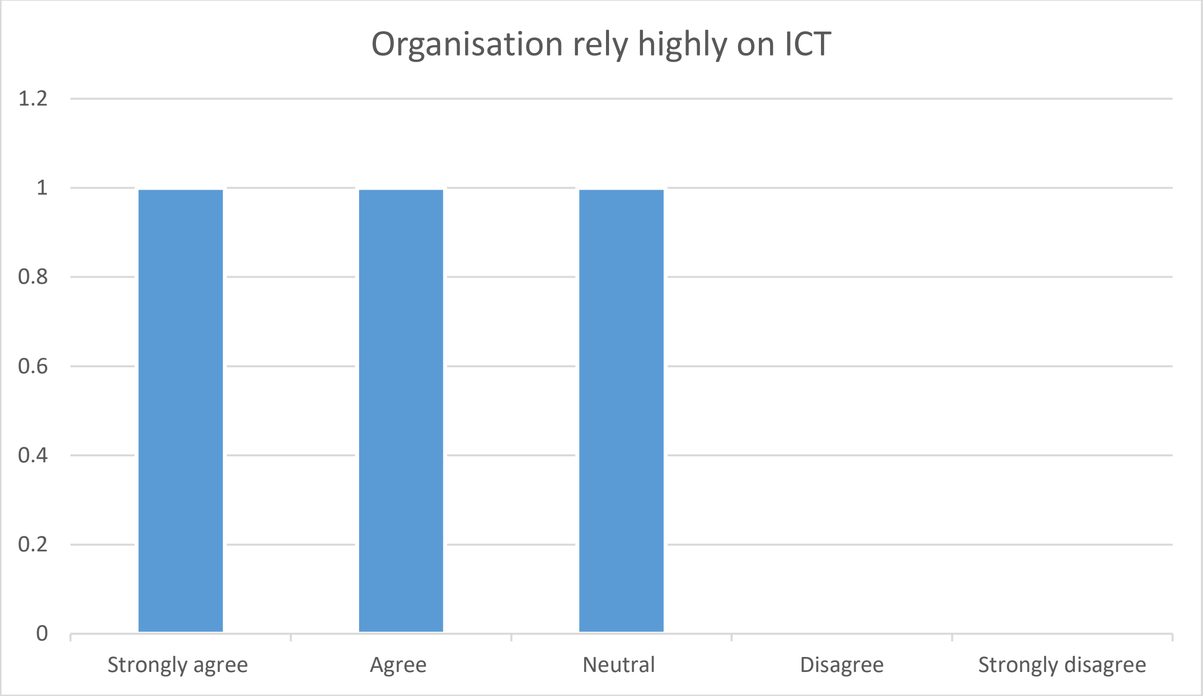


Figure D.517: Organisation rely highly on ICT (Public services and administration)

Out of the 3 respondents, 2 employed in a technology reliance working environment, 1 unaware due to the nature of the work assigned to them (See figure D.517). This suggests that the majority working in the public services administration have a high reliance on ICT.

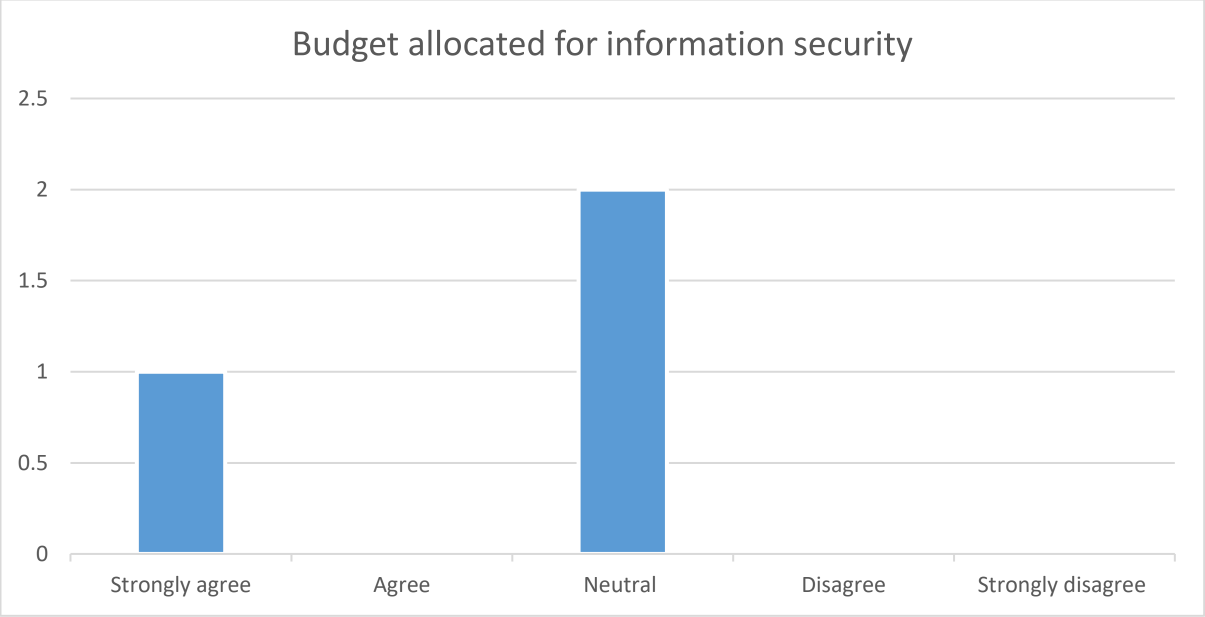


Figure D.518: Budget allocated for information security (Public services and administration)

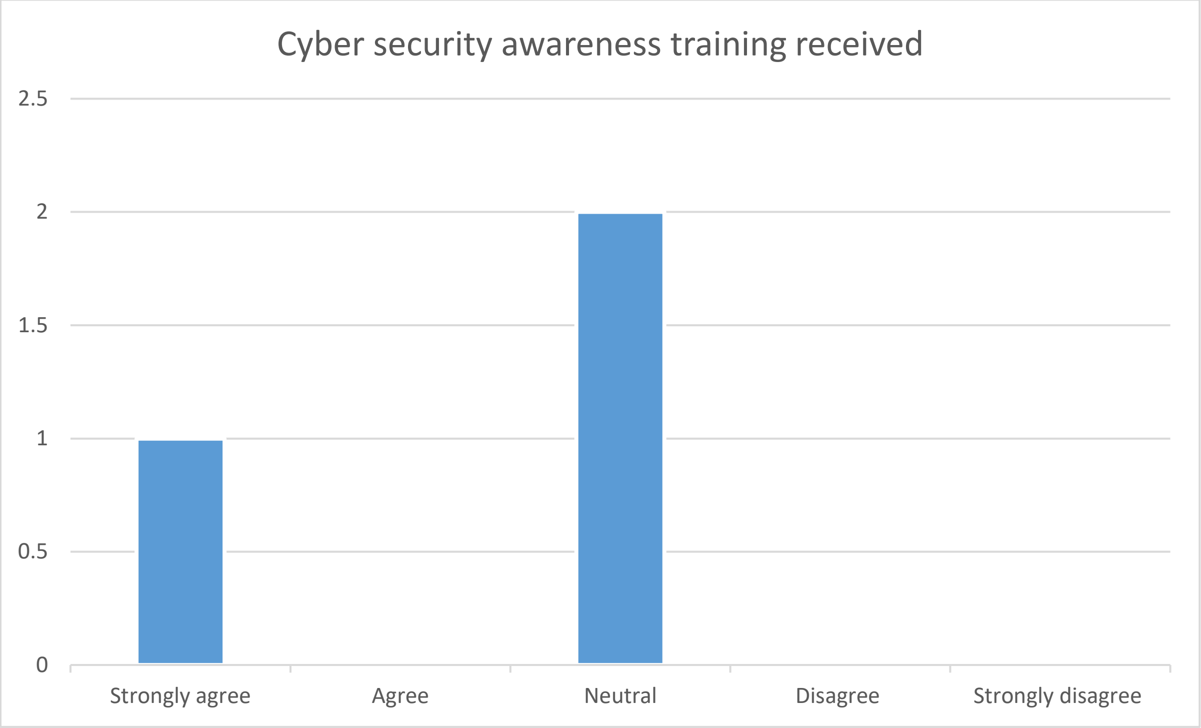


Figure D.519: Cyber security awareness training received (Public services and administration)

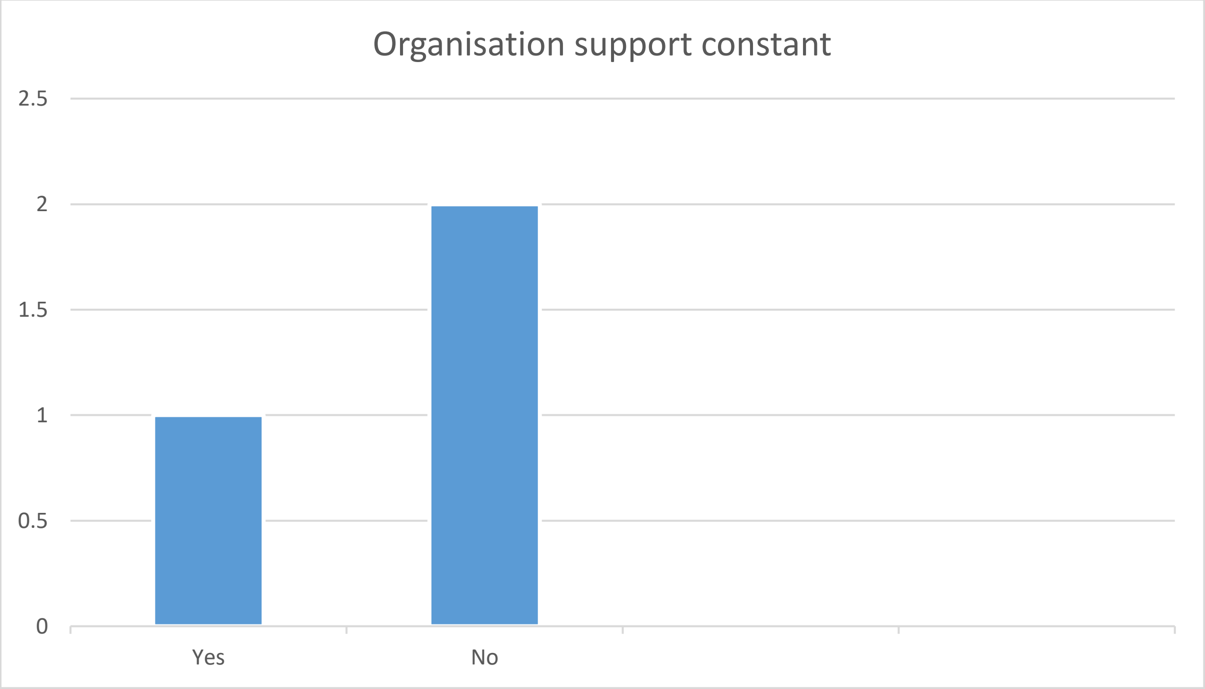


Figure D.520: Organisation support constant (Public services and administration)

According to 1 respondent, the organisations has a budget allocated for information security, and 2 have no opinion either way (See figure D.518). According to some of the participants, regular security awareness training received was inadequate, except for 1 who received regular cybersecurity awareness training, and 2 neither agreed nor disagreed (See figure D.519). Also, 2 participants have not received support from the organisation to protect personal information, except for only 1 who had. In comparison to the responses received from other sectors, this is the only sector without an allocated budget for information security(See figure D.520). The likely reason is the lack of funds, and the organisations find unable to provide awareness training regularly, and necessary support to protect personal information despite the high reliance on technology.

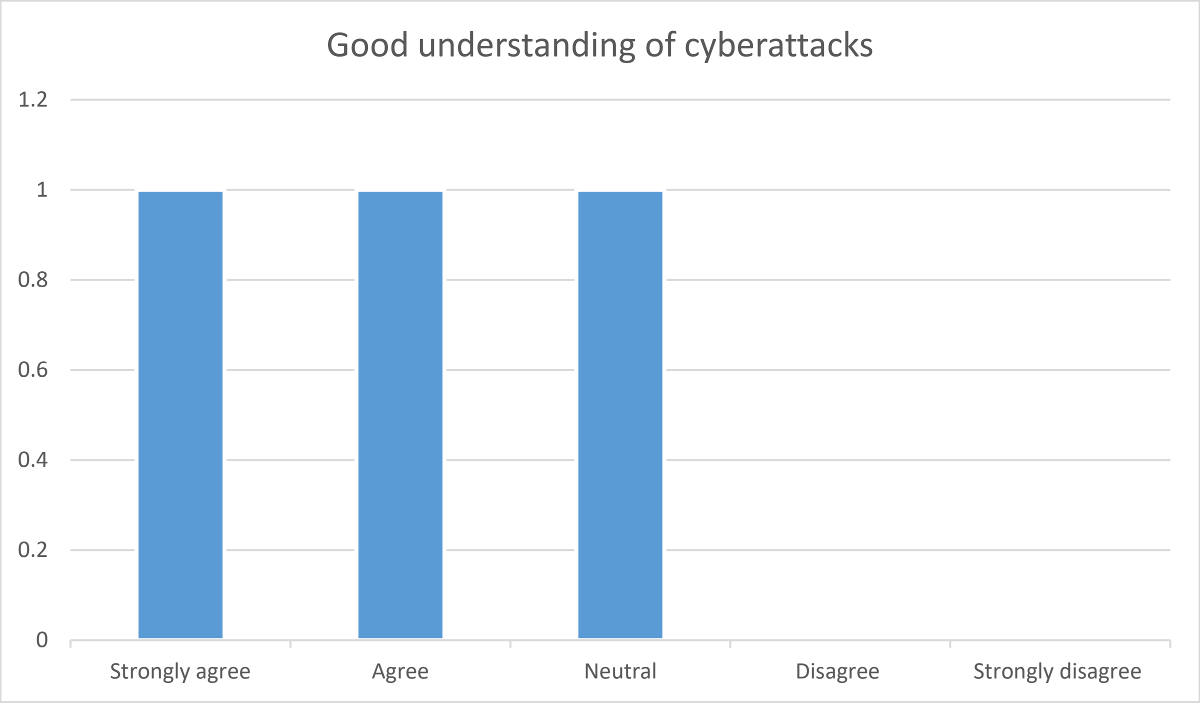


Figure D.521: Good understanding of cyberattacks (Public services and administration)

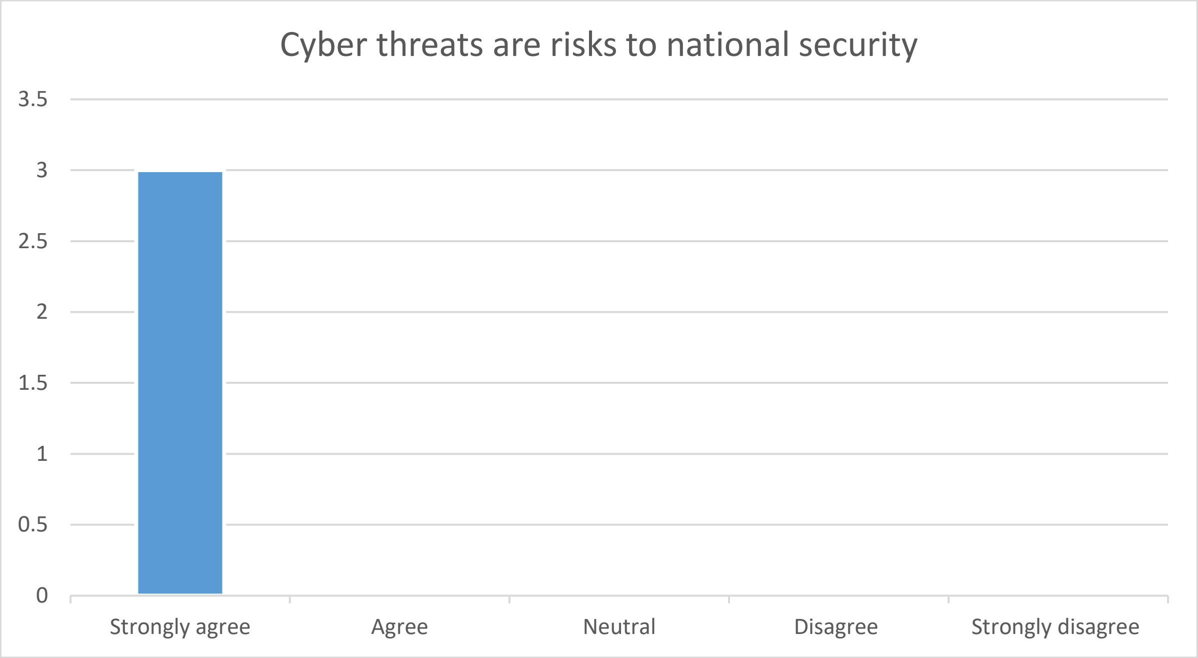


Figure D.522: Cyber threats are risks to national security (Public services and administration)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 2 participants have, and 1 gave no opinion either way (See figure D.521). Furthermore, the majority of the participants also realises the potential threats to national security from cyber-attacks (See figure D.522). In general, understanding cyber threats and their impact on national security should encourage people to act responsibly to minimise end-user errors, and in time, they will be in a strong position to influence the process of accepting and implementing a national, regional, and global level mechanism.

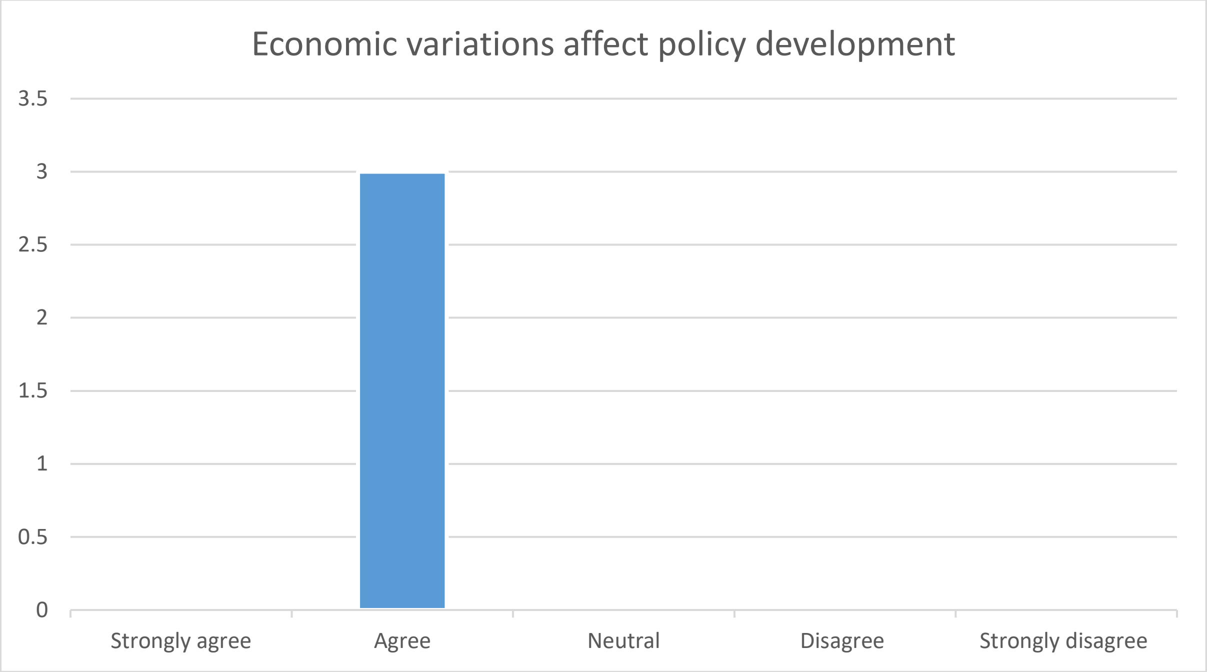


Figure D.523: Economic variations affect policy development (Public services and administration)

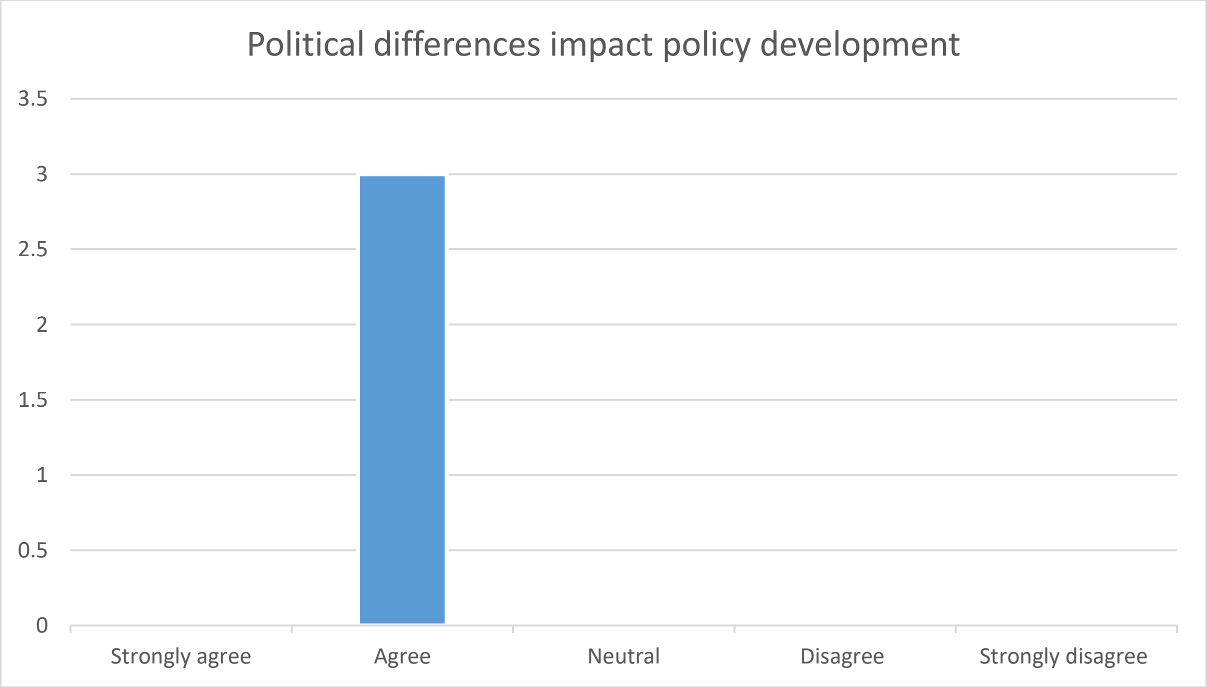


Figure D.524: Political differences impact policy development (Public services and administration)

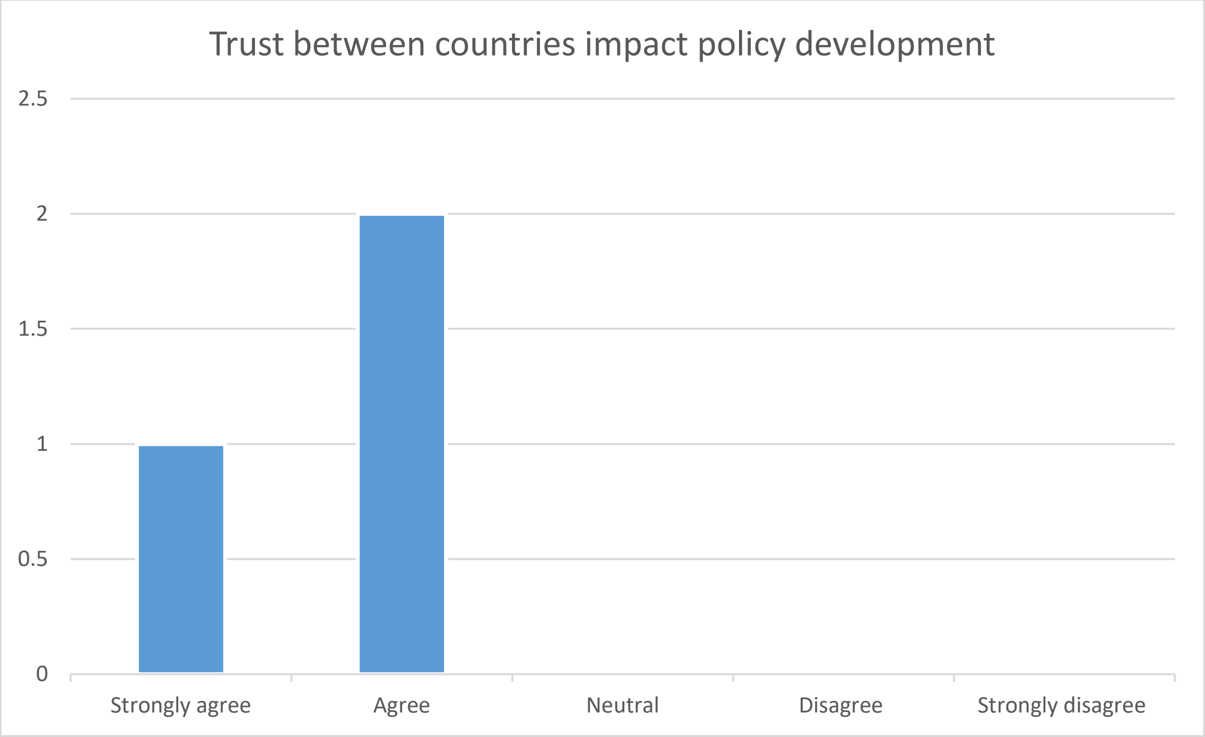


Figure D.525: Trust between countries impact policy development (Public services and administration)

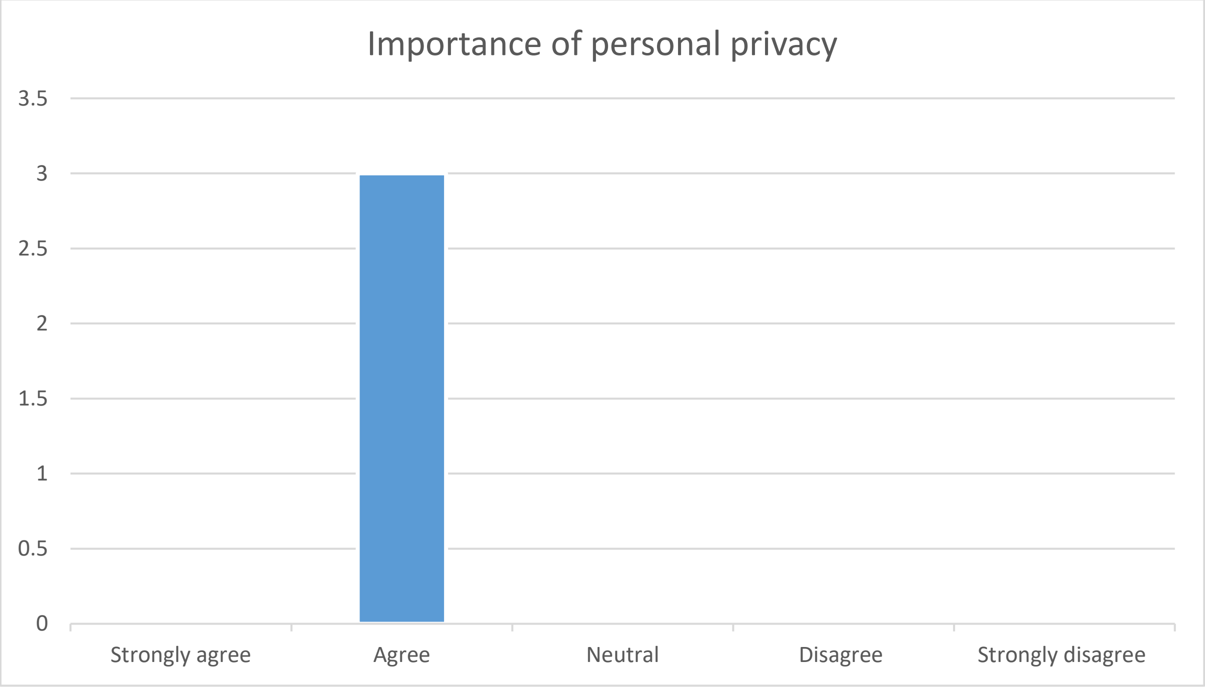


Figure D.526: Importance of personal privacy (Public services and administration)

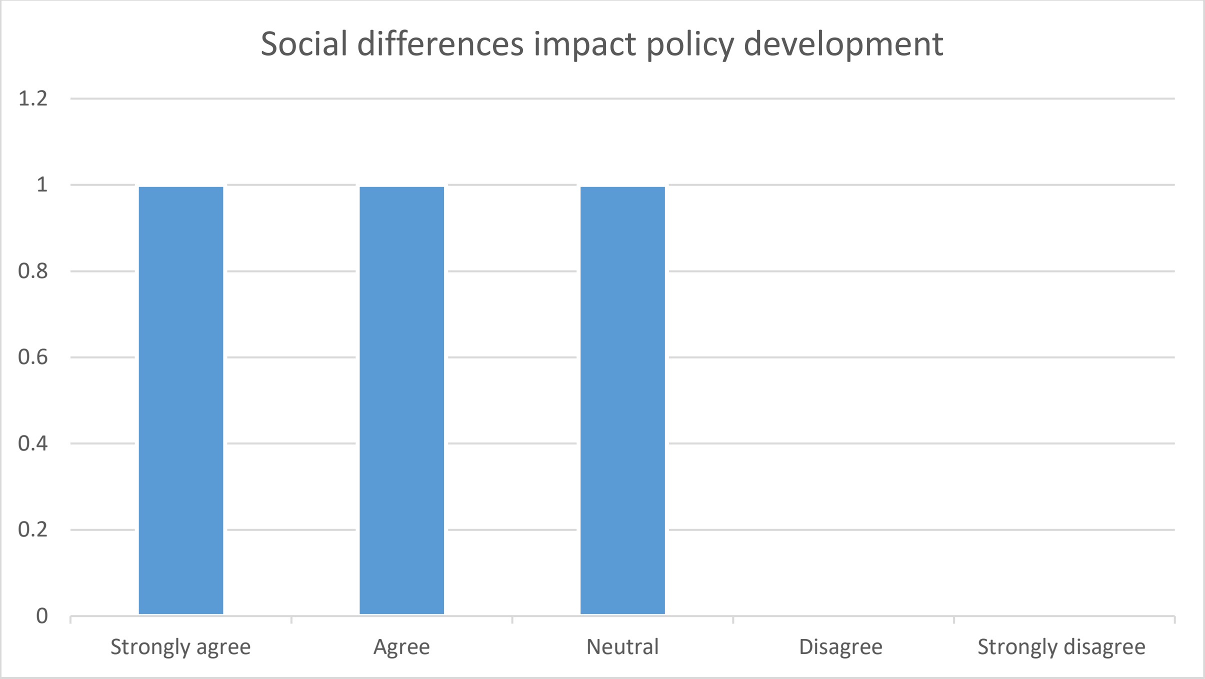


Figure D.527: Social differences impact policy development (Public services and administration)

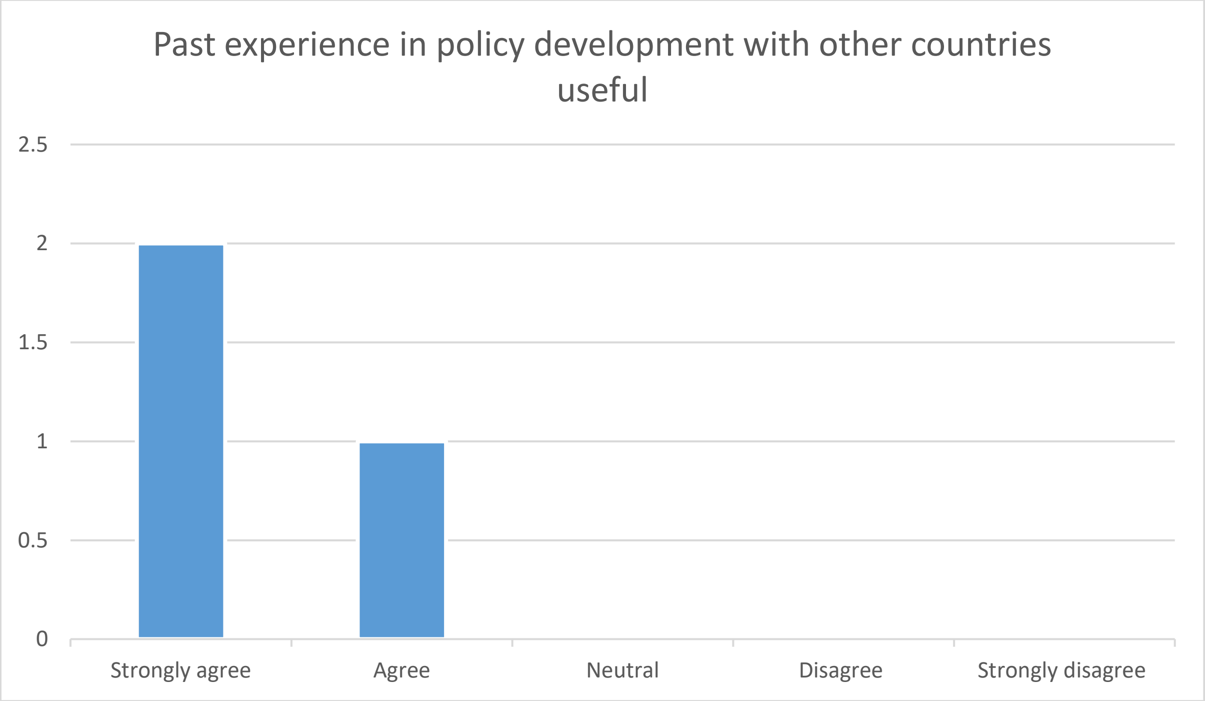


Figure D.528: Past experience in policy development with other countries useful (Public services and administration)

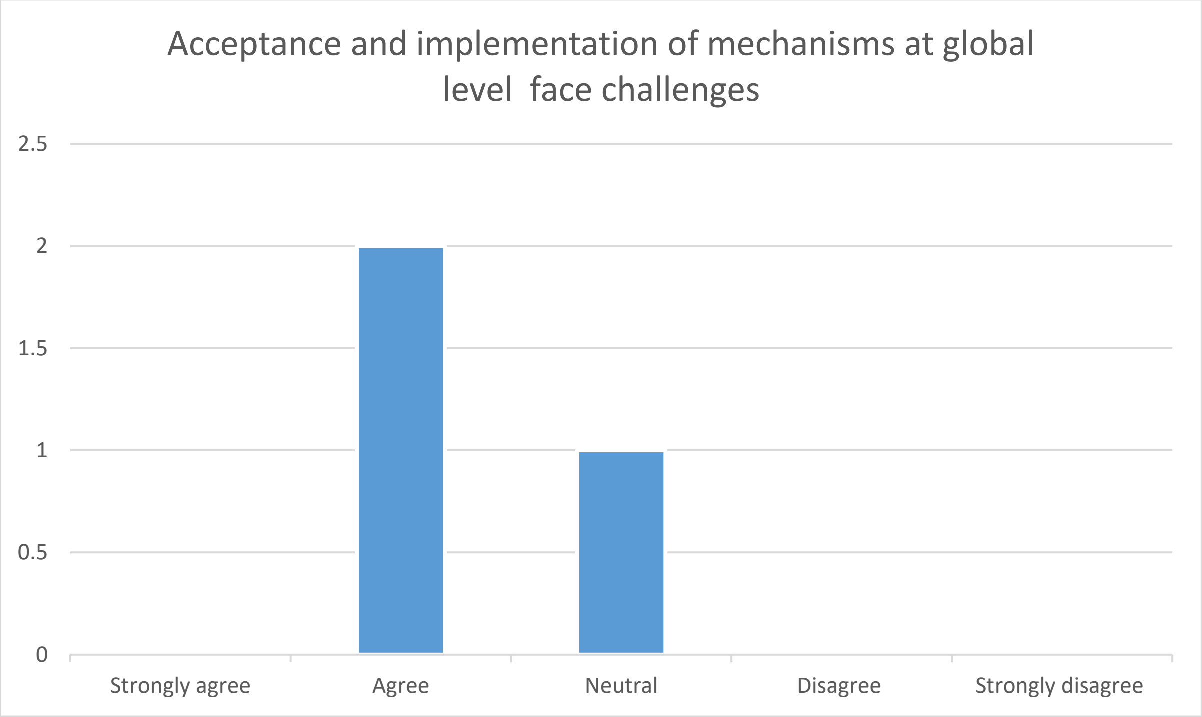


Figure D.529: Acceptance and implementation of mechanisms at global level face challenges (Public services and administration)

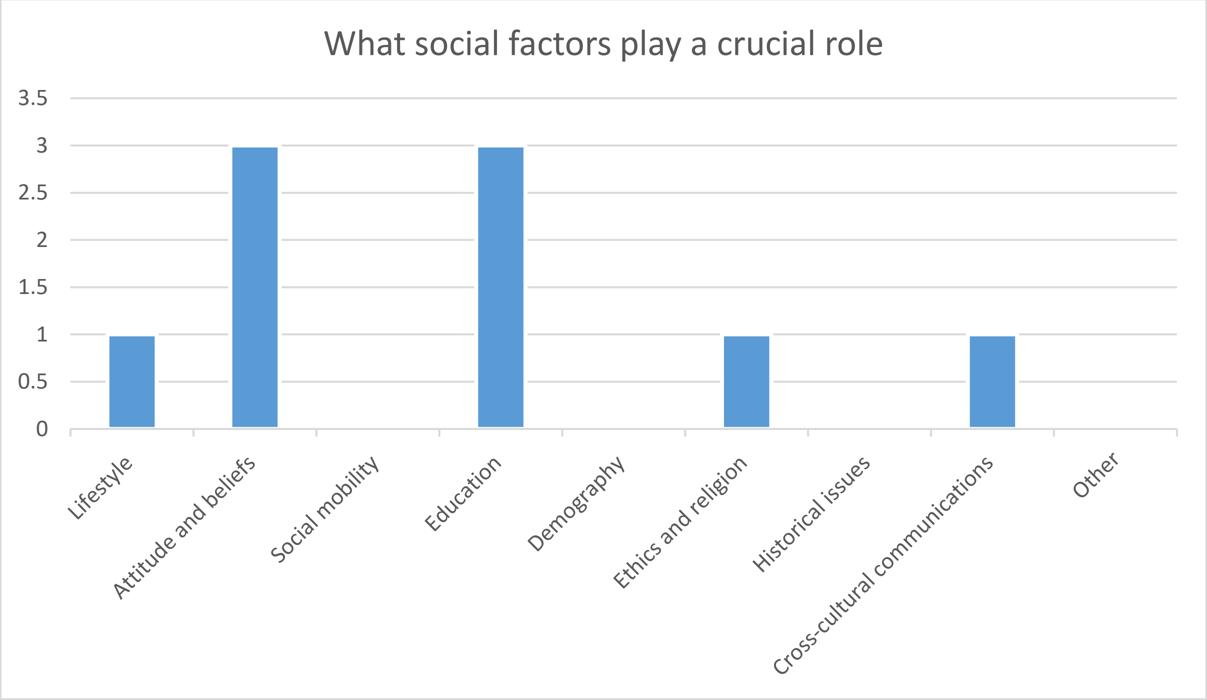


Figure D.530: What social differences play a crucial role (Public services and administration)

In response to the social differences component of the survey, the majority mark importance of education and attitude and beliefs (See figure D.530). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

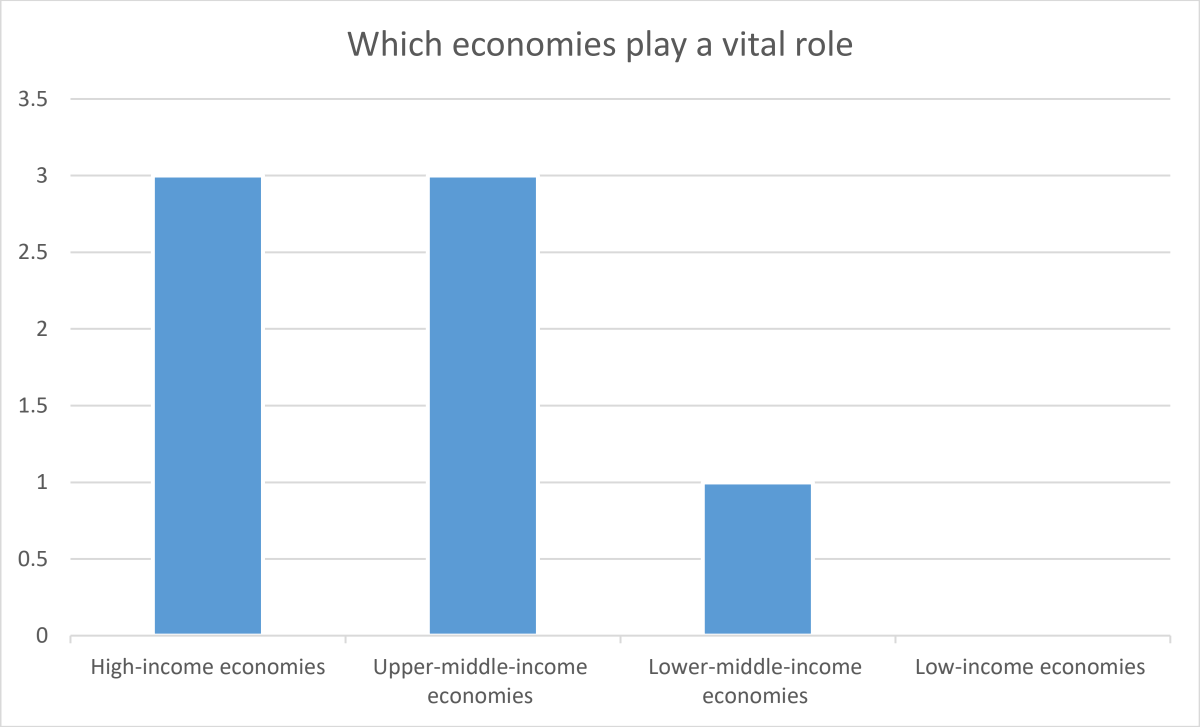


Figure D.531: Which economies play a vital role (Public services and administration)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure D.531). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

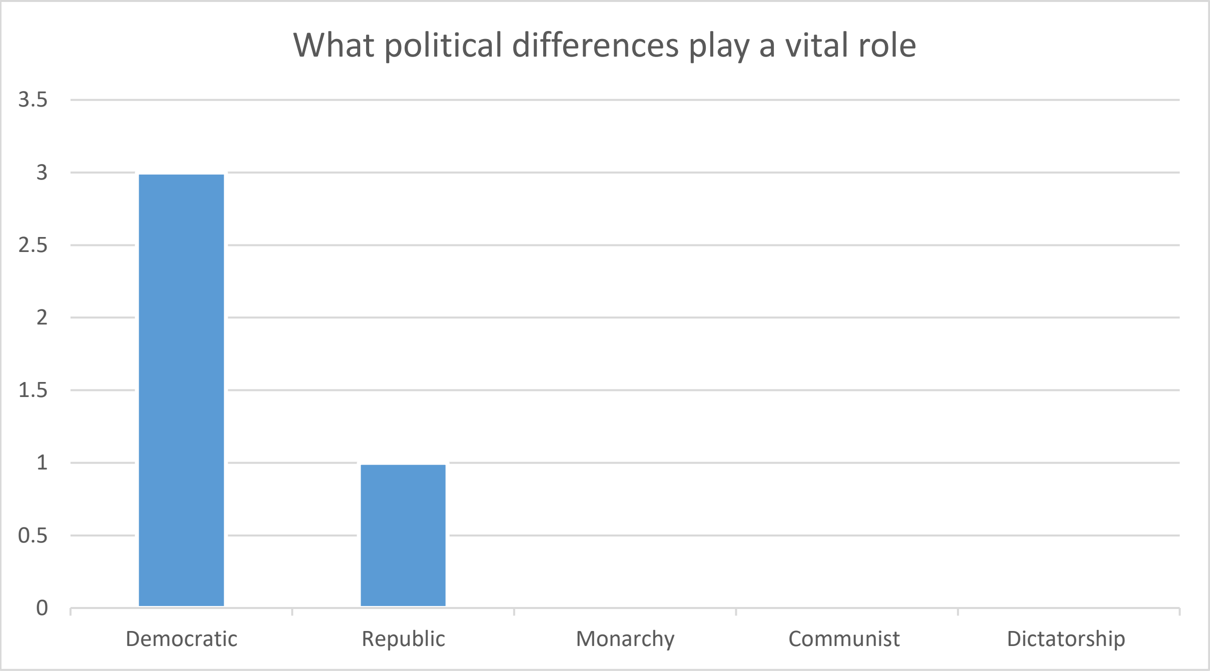


Figure D.532: What political differences play a vital role (Public services and administration)

The majority have chosen a democratic political system (See figure D.532), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

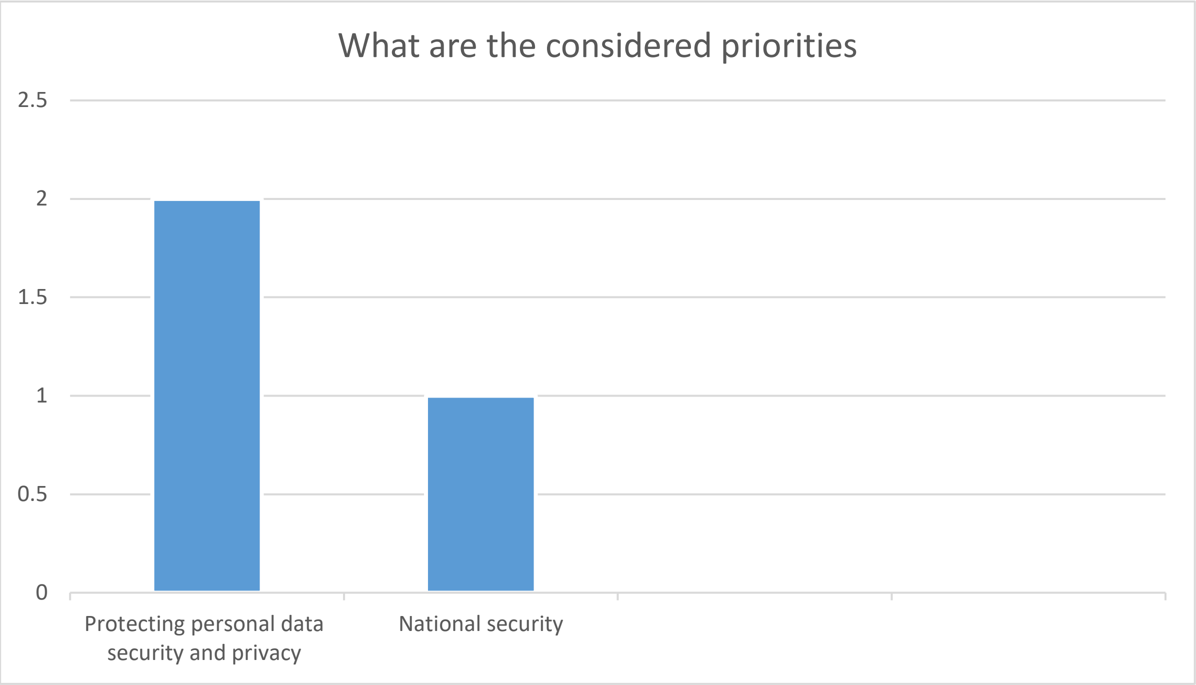


Figure D.533: What are the considered priorities (Public services and administration)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security, which is a significant factor (See figure D.533). However, in an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

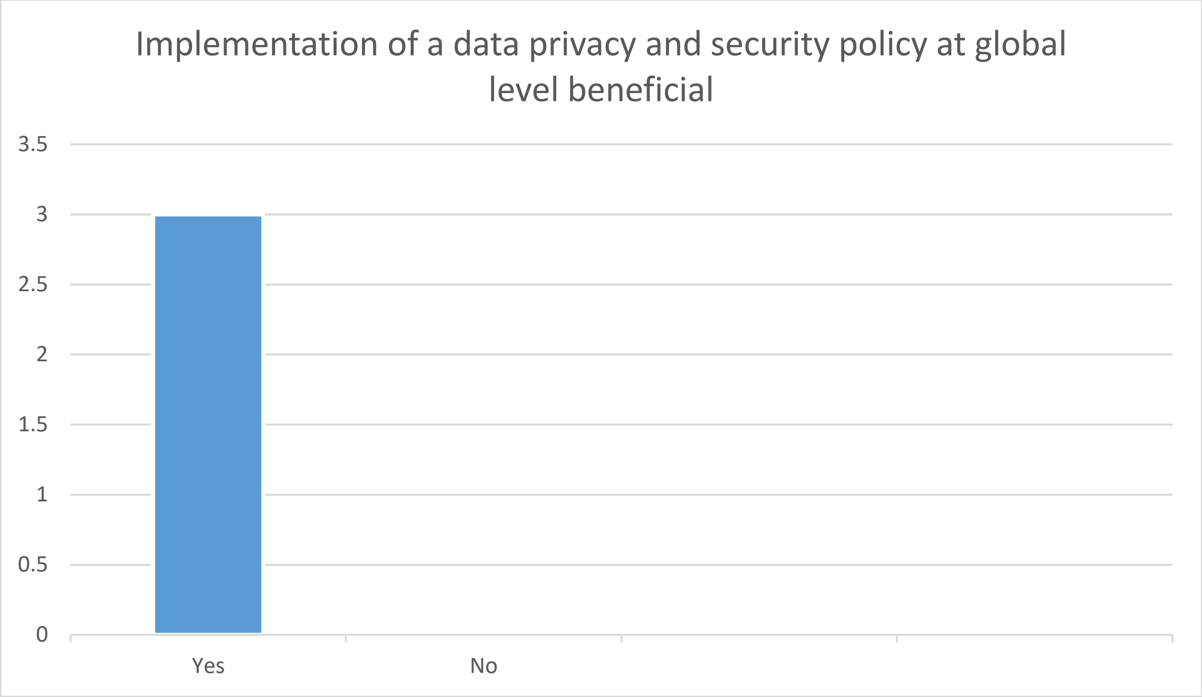


Figure D.534: Implementation of a data privacy and security policy at global level beneficial (Public services and administration)

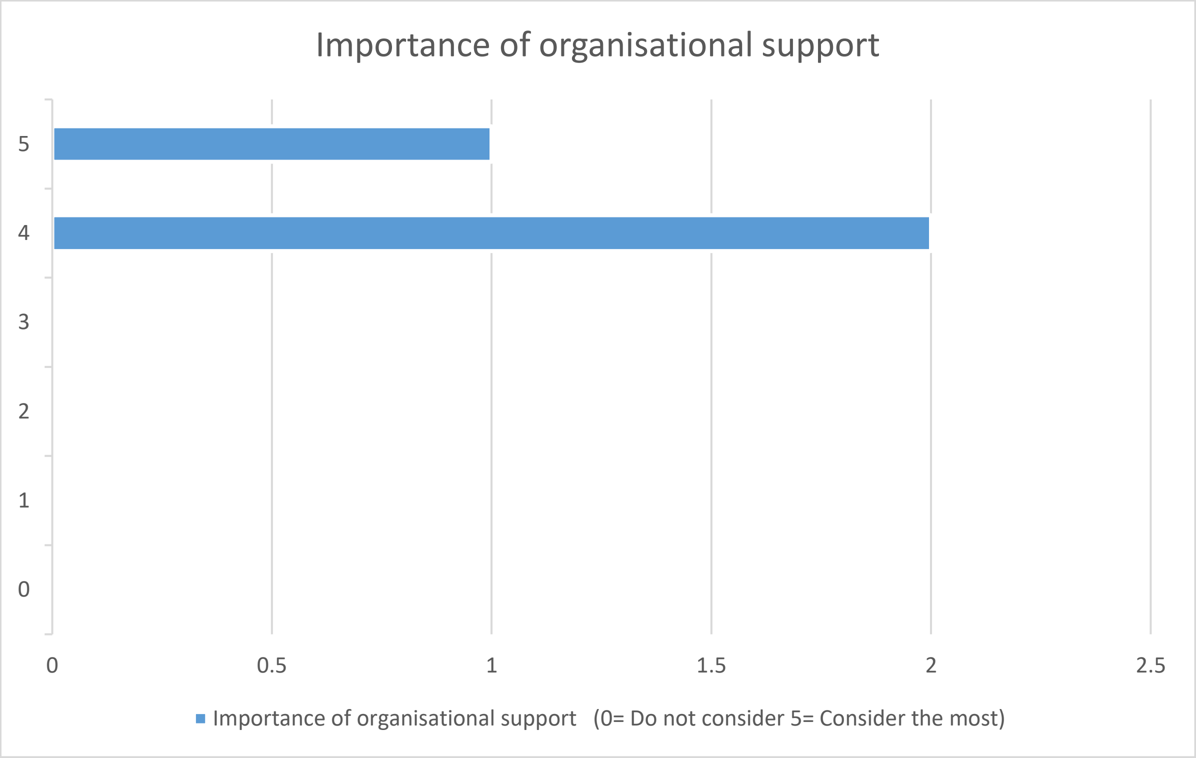


Figure D.535: Importance of organisational support (Public services and administration)

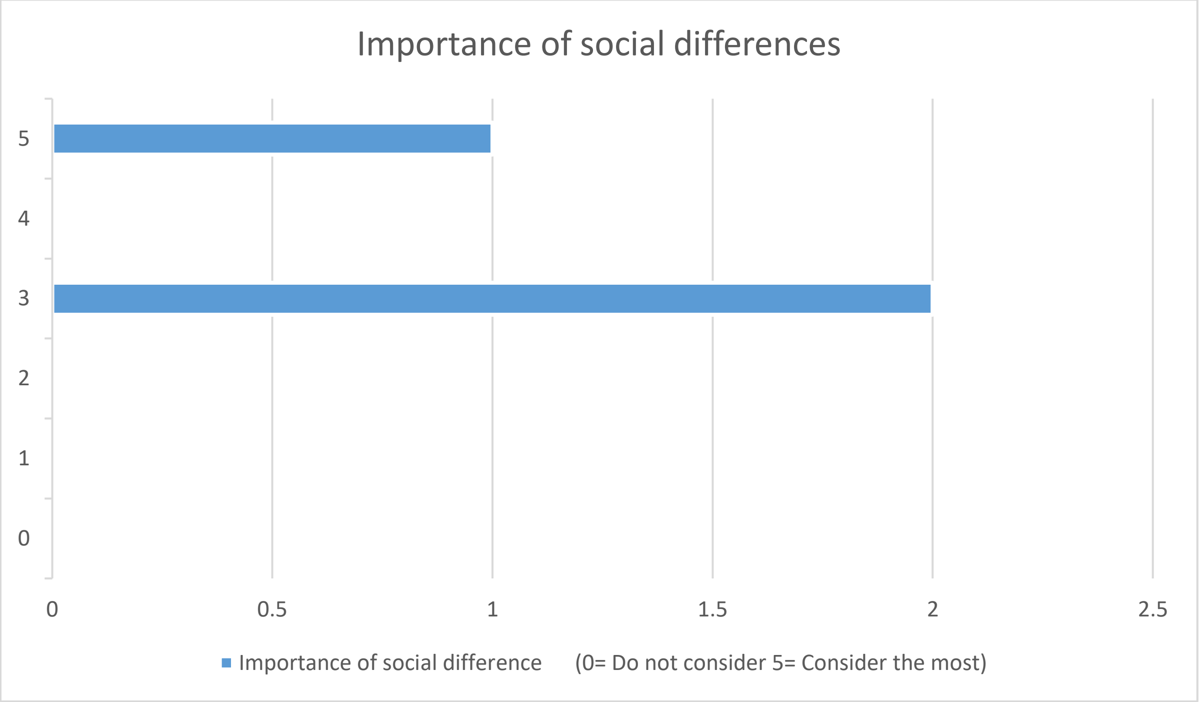


Figure D.536: Importance of social differences (Public services and administration)

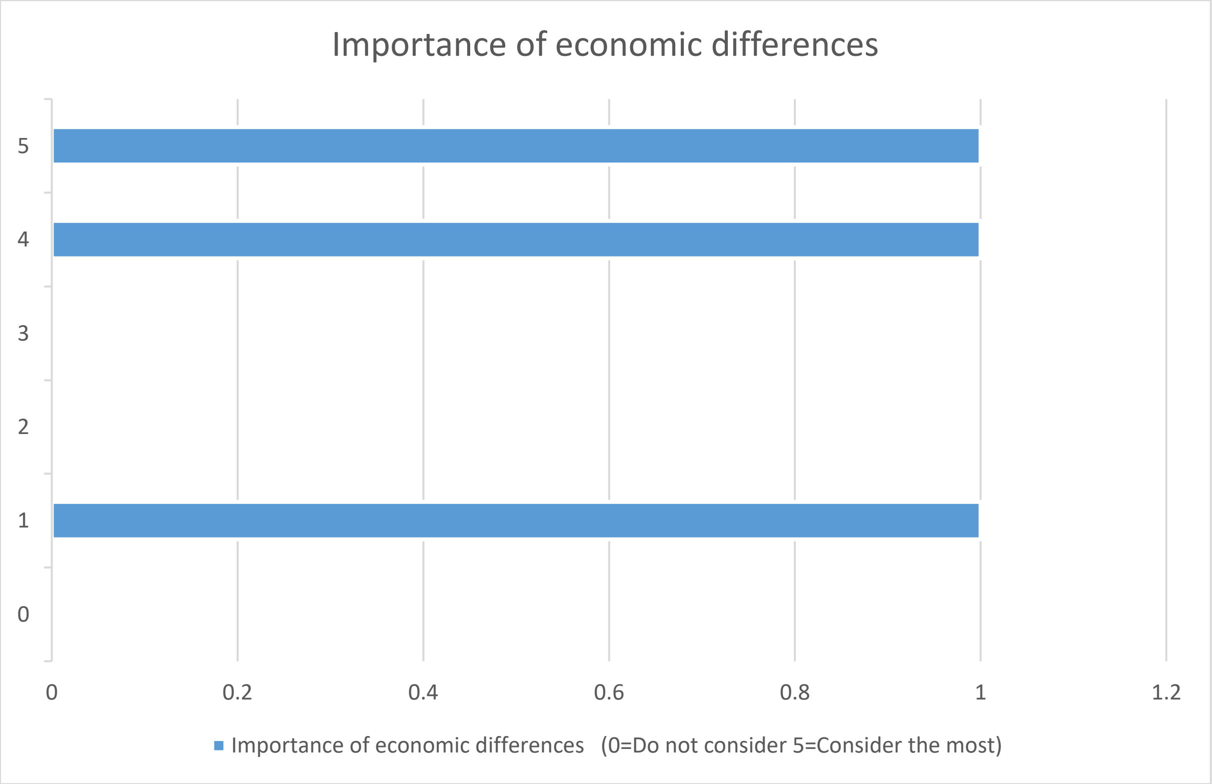


Figure D.537: Importance of economic differences (Public services and administration)

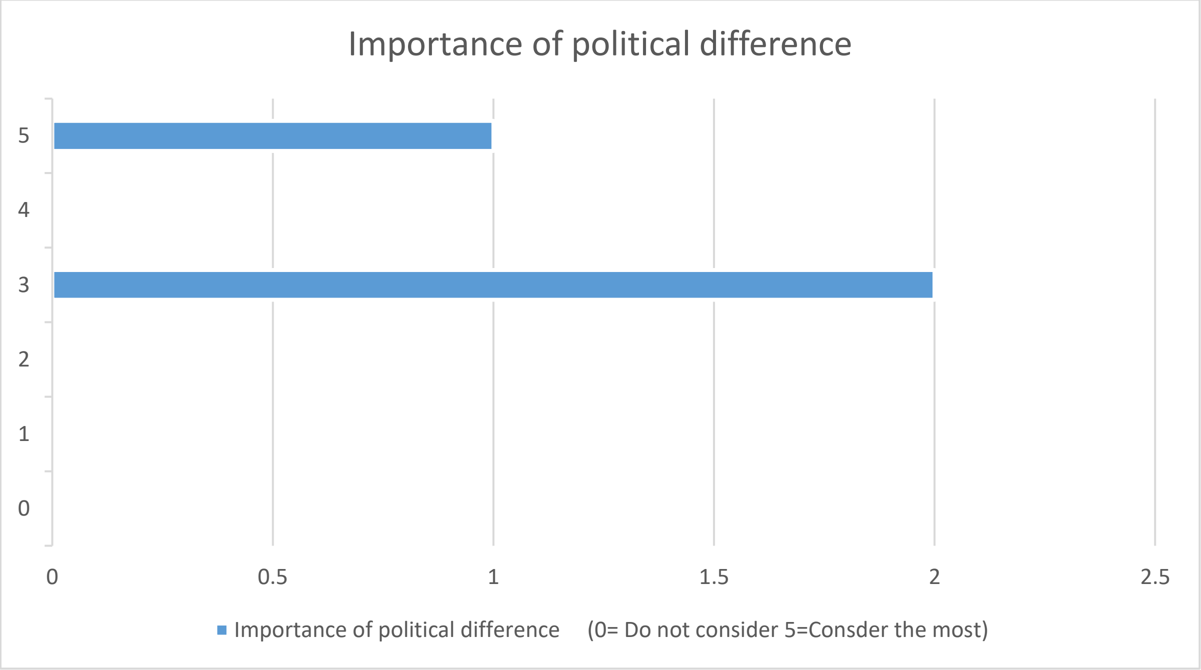


Figure D.538: Importance of political difference (Public services and administration)

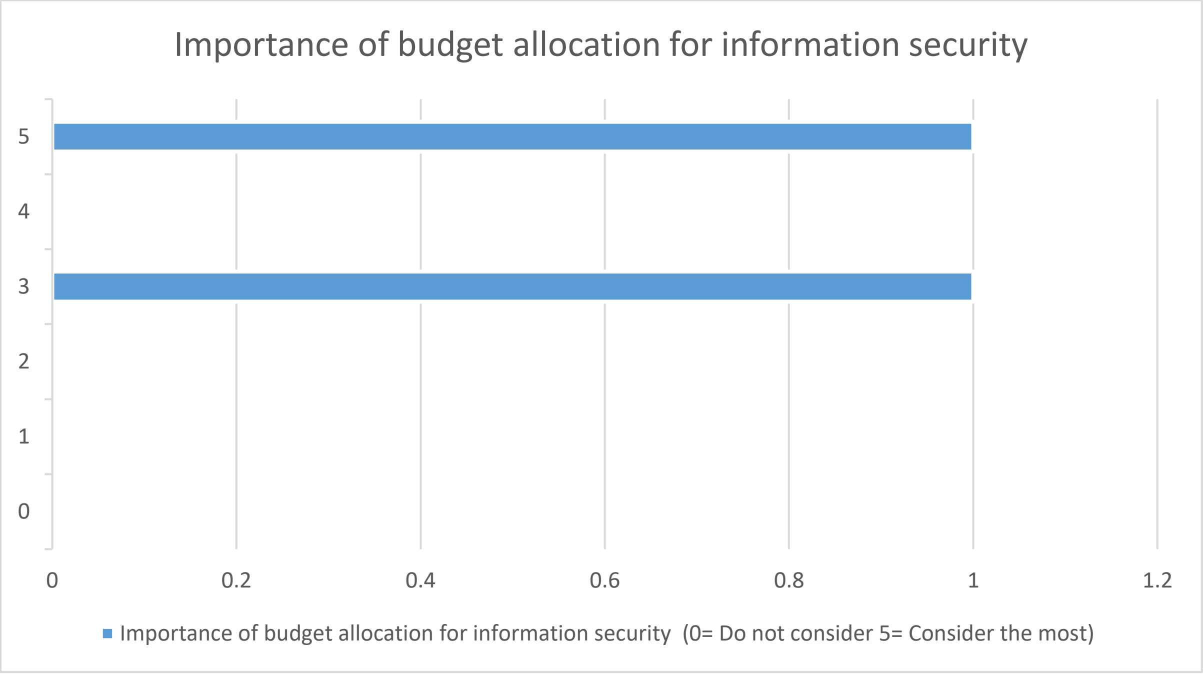


Figure D.539: Importance of budget allocation for information security (Public services and administration)

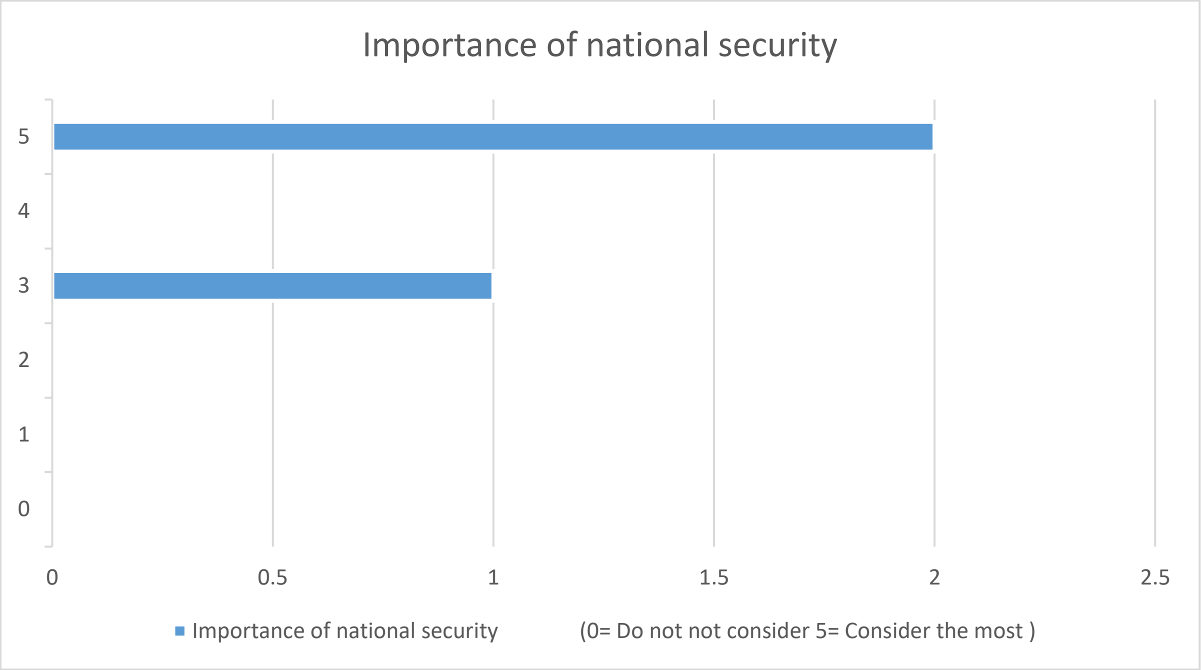


Figure D.540: Importance of national security (Public services and administration)

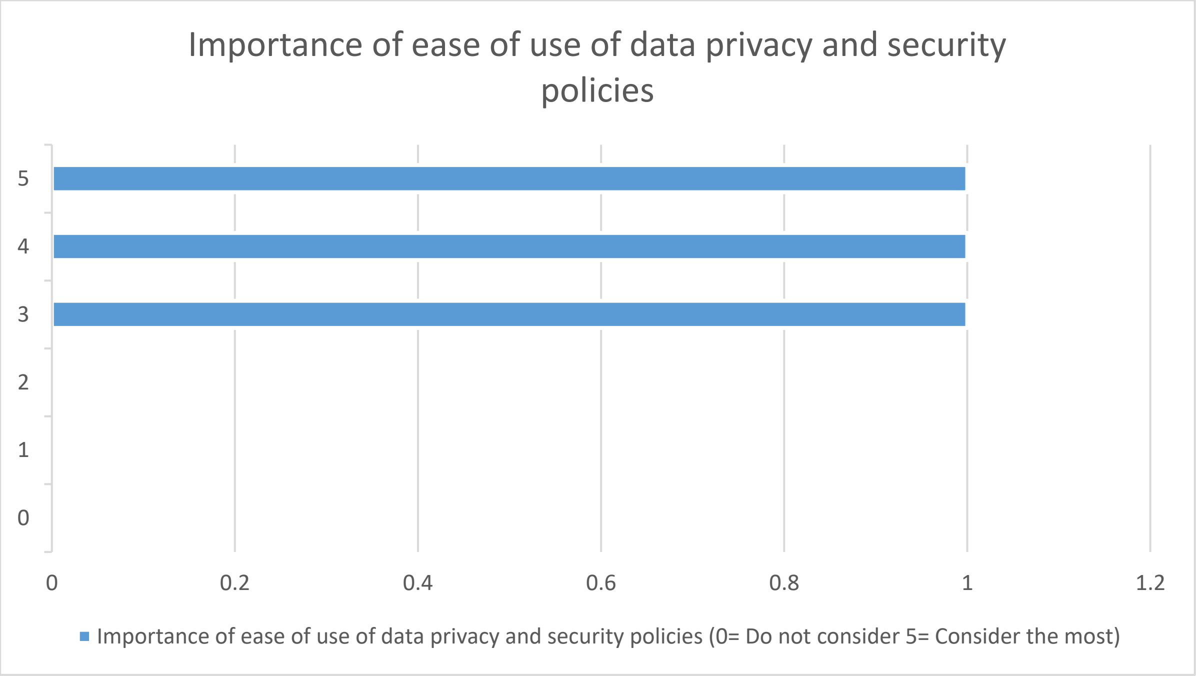


Figure D.541: Importance of ease of use of data privacy and security policies (Public services and administration)

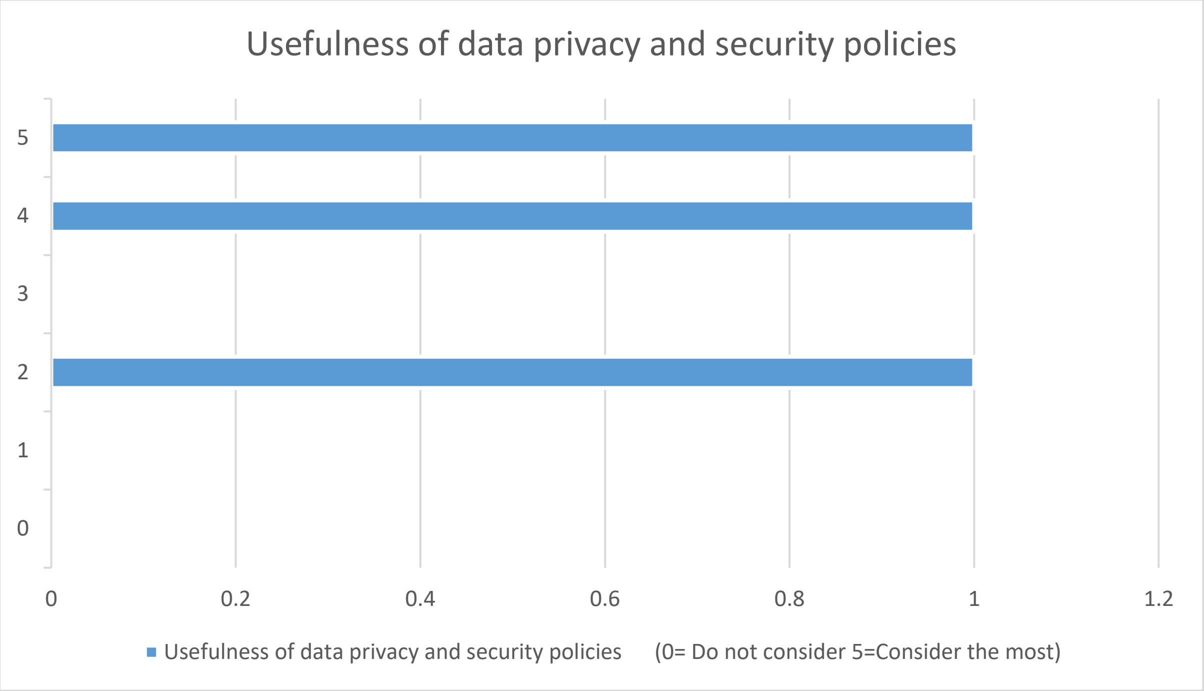


Figure D.542: Usefulness of data privacy and security policies (Public services and administration)

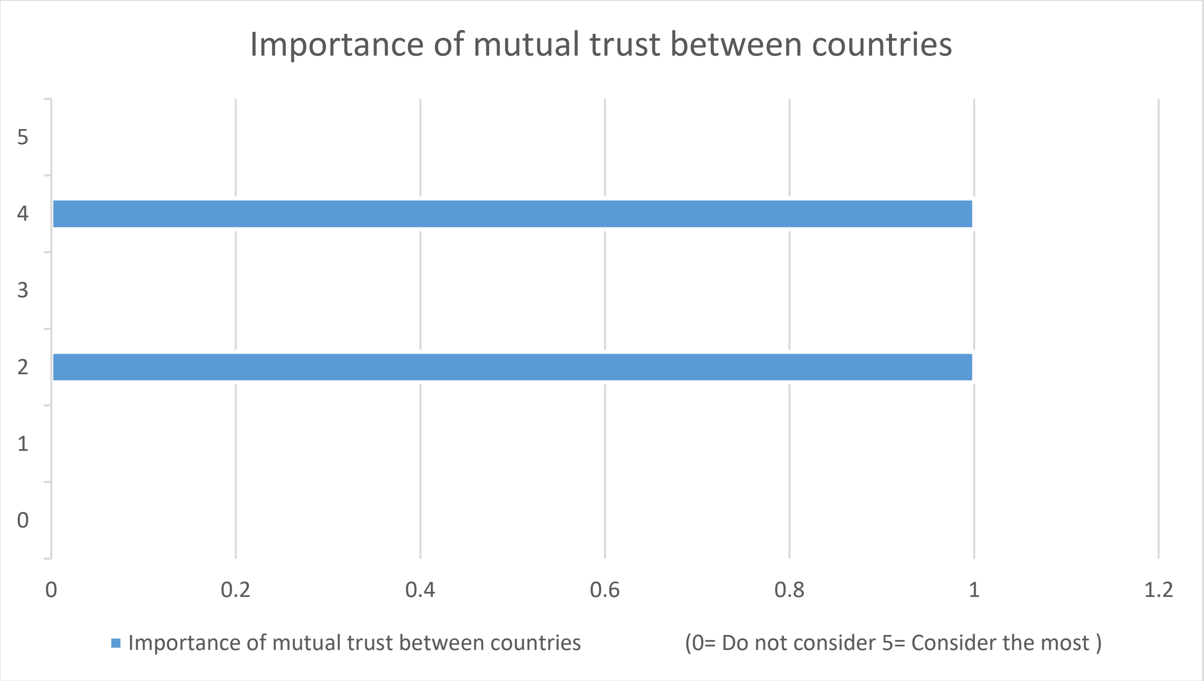


Figure D.543: Importance of mutual trust between countries (Public services and administration)

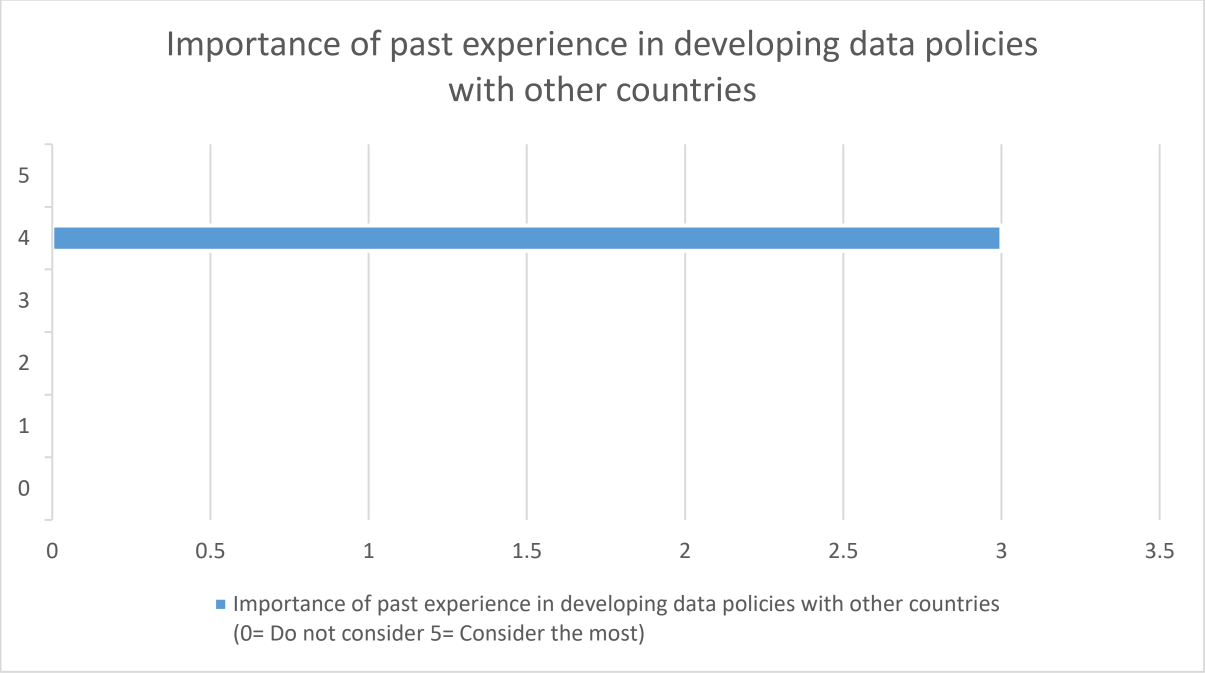


Figure D.544: Importance of past experience in developing data policies with other counties (Public services and administration)

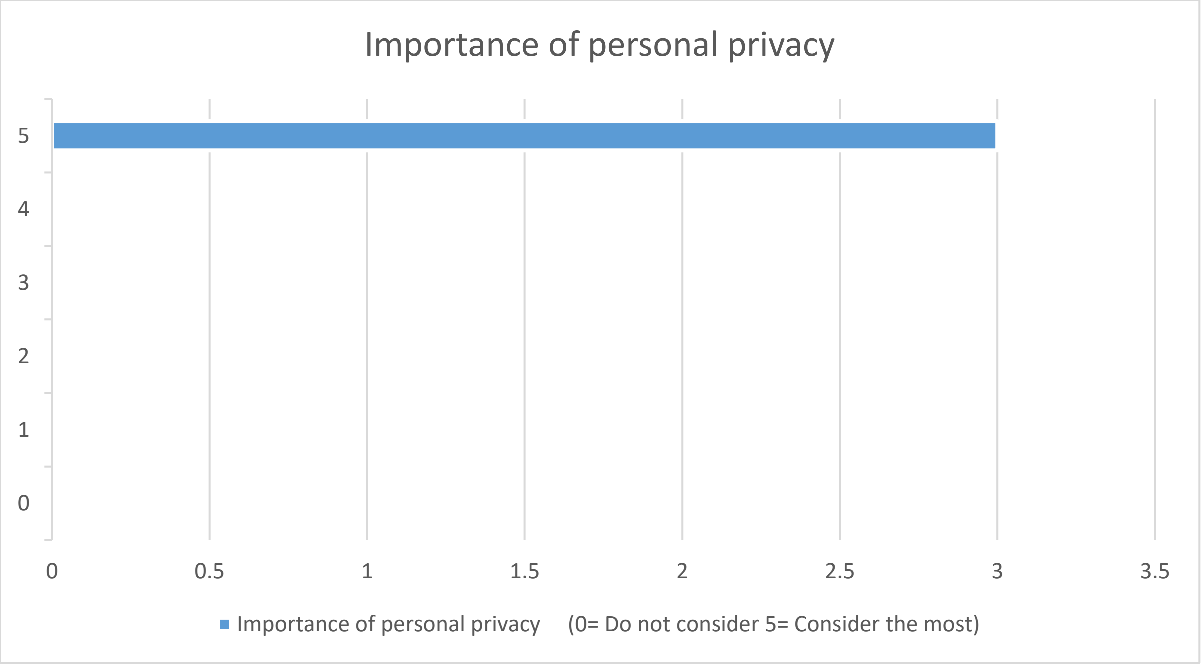


Figure D.545: Importance of personal privacy (Public services and administration)

The message from the respondents is clear. The significance of this survey is there is a need to have a global level data protection mechanism, and this has been endorsed by 100 percent of the participants (See figure D.534). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, political differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies and previous experience with other countries in developing policies (See figure D.523-533) (See figure D.535-545).

Sri Lanka – Tourism

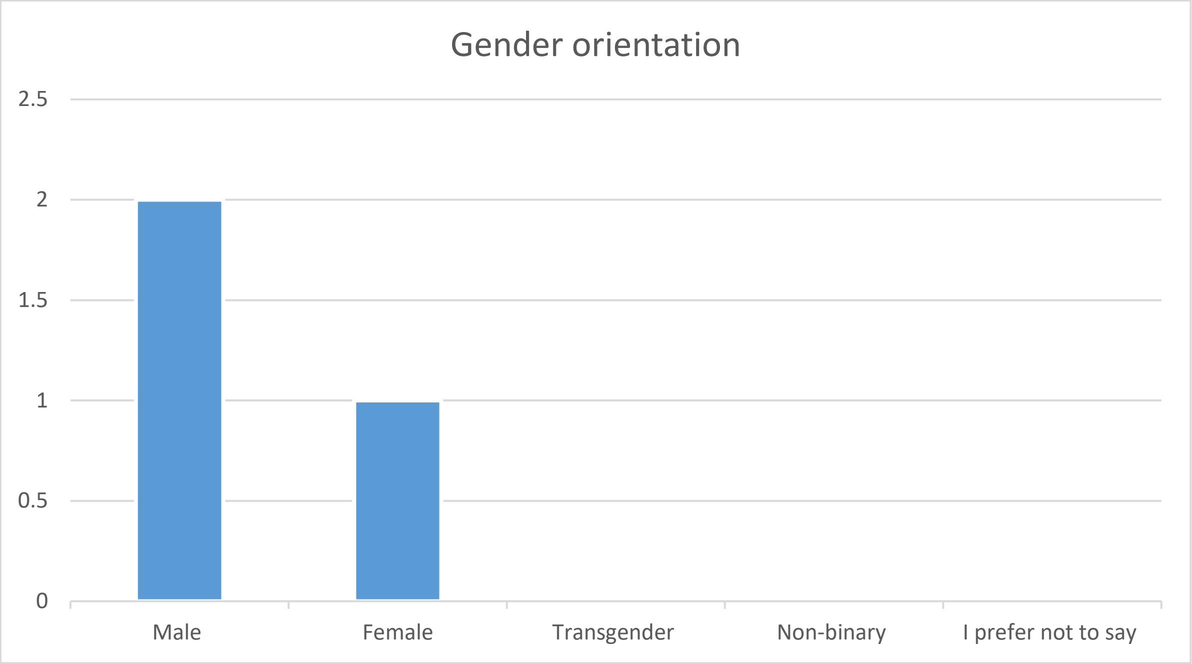


Figure D.546: Gender orientation (Tourism)

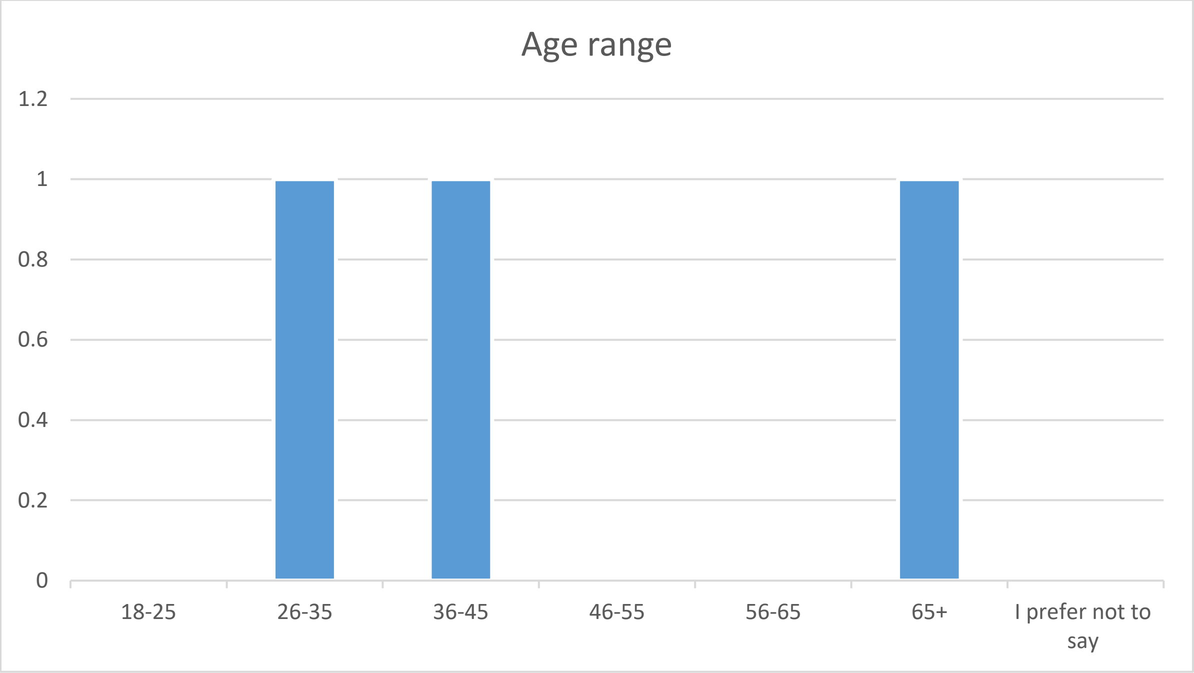


Figure D.547: Age range (Tourism)

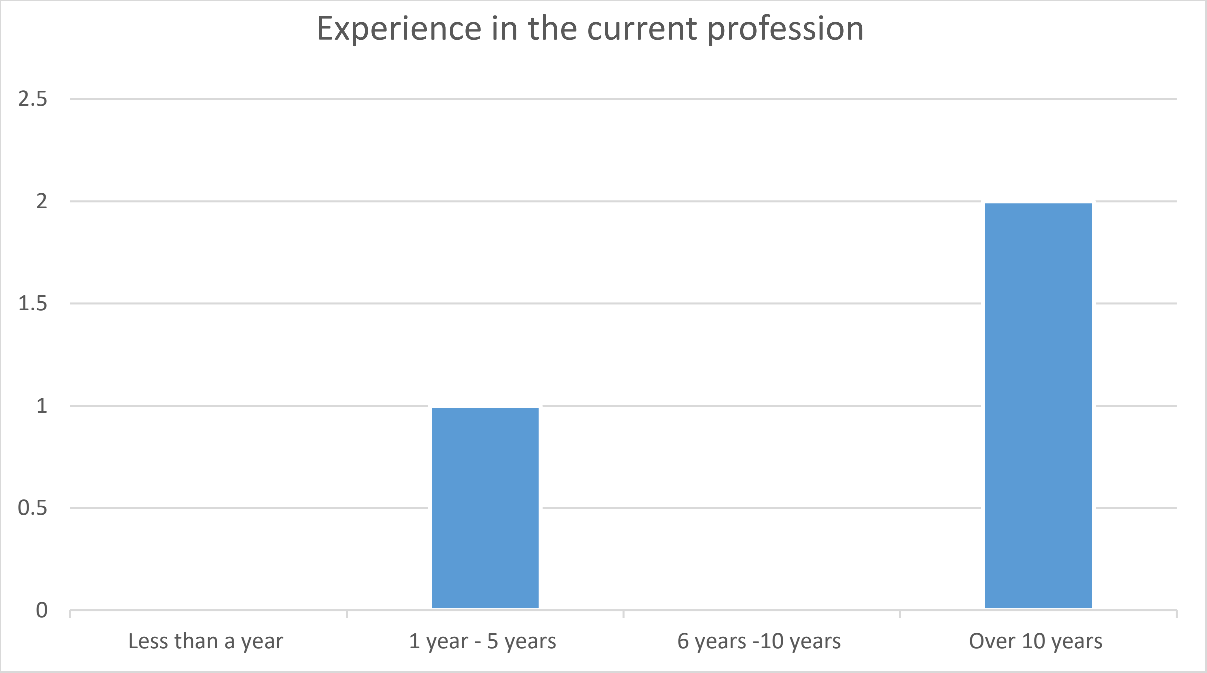


Figure D.548: Experience in current profession (Tourism)

This analysis is based on the responses received from Sri Lankan tourism sector employees. There were 3 participants and 2 out of them were males and 1 female (See figure D.546). They were within 26 and 65 plus age range; 26 – 35 range one; 36-45 range one; 65 plus range one (See figure D.547); also, one employee 1-5 years, and two over 5 years in employment in this sector (See figure D.548).

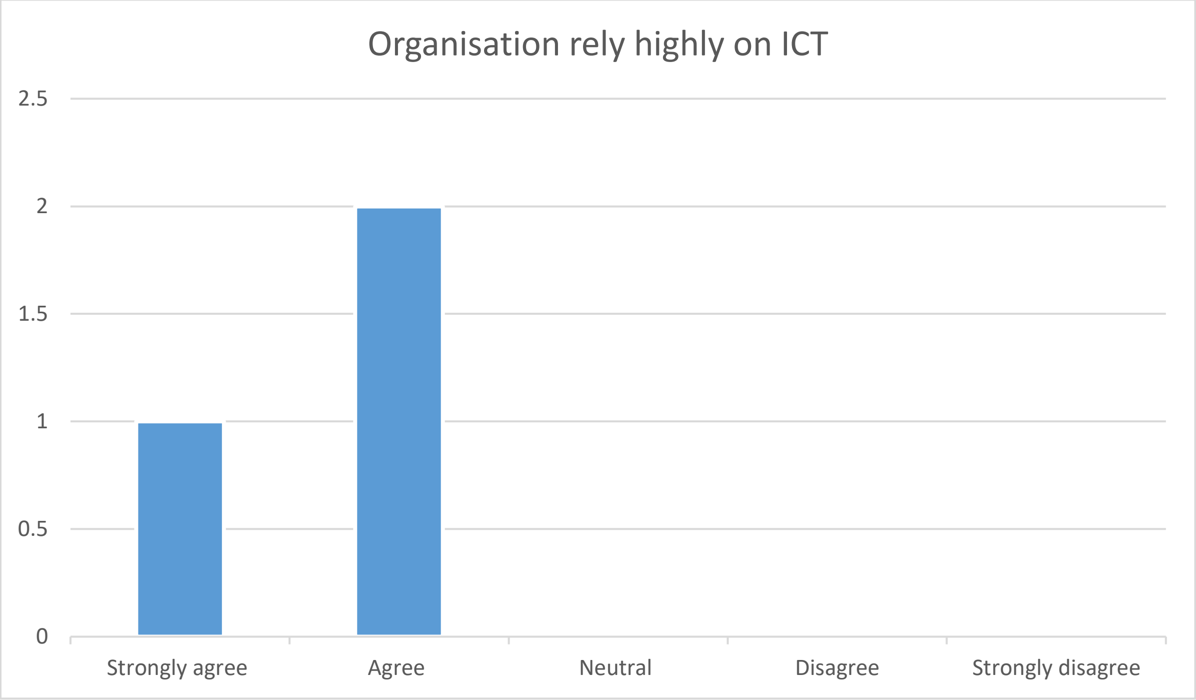


Figure D.549: Organisation rely highly on ICT (Tourism)

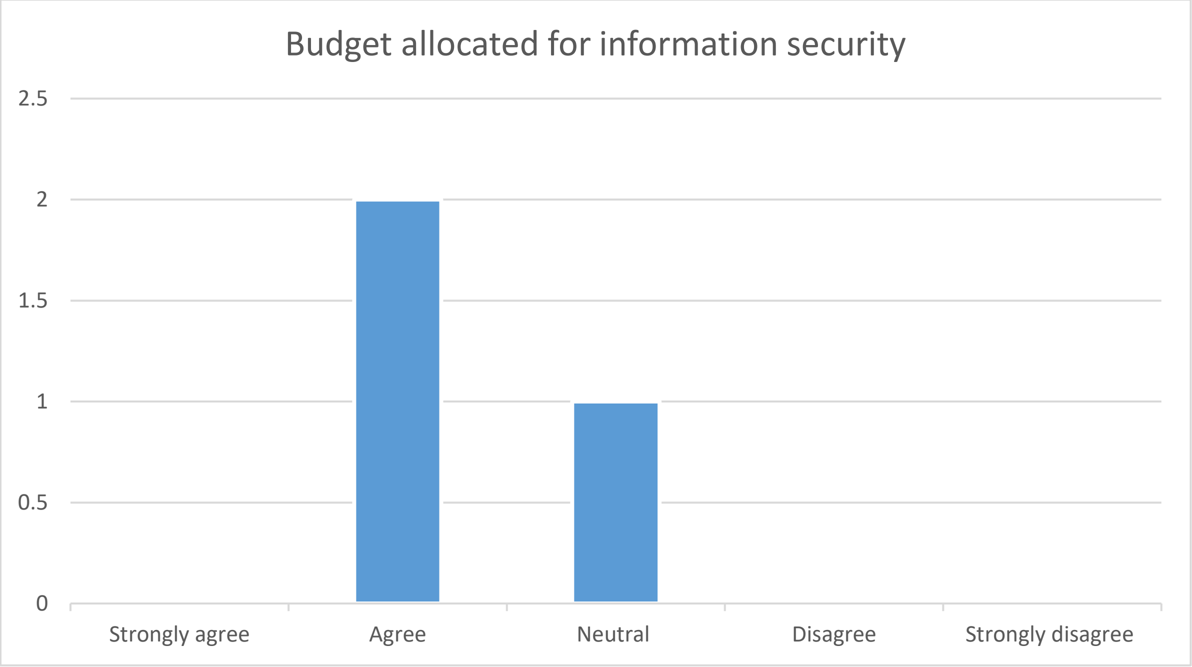


Figure D.550: Budget allocated for information security (Tourism)

In the tourism sector, only received 3 responses to the questionnaire, and all work in a technology reliance working environment (See figure D.549). The organisation had a budget allocation for information security, according to 2, and 1 had not expressed an opinion either way (See figure D.550).

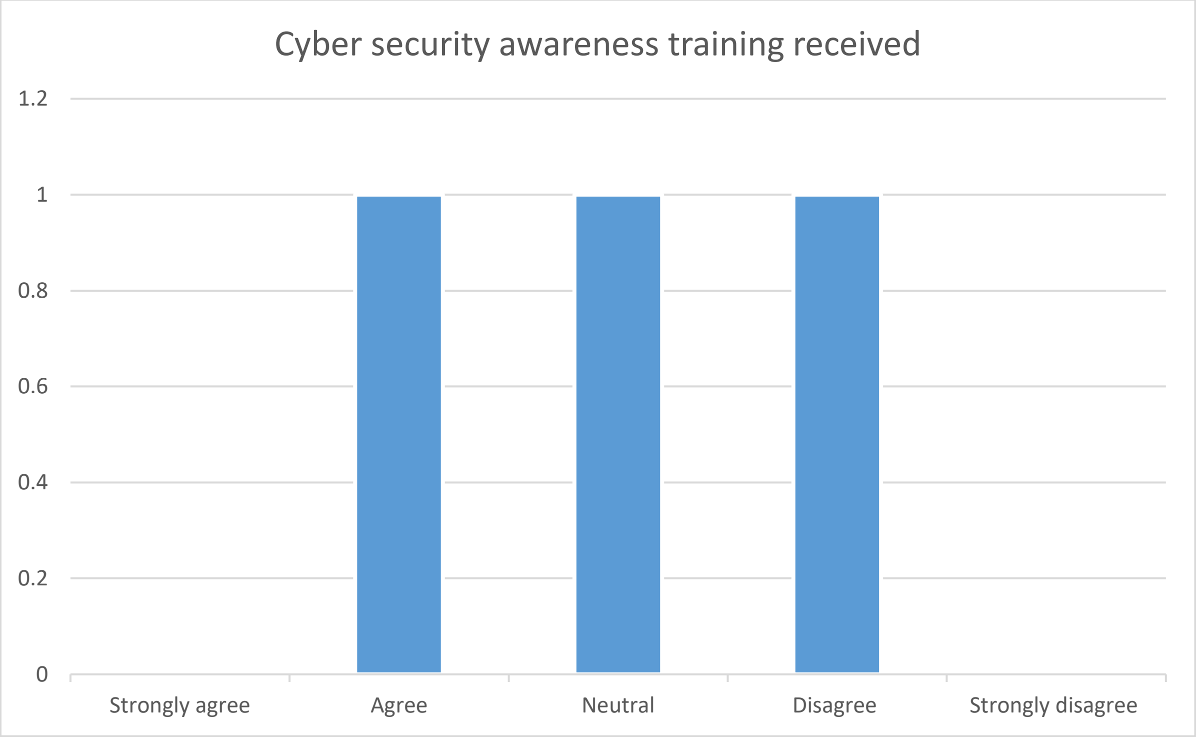


Figure D.551: Cyber security awareness training received (Tourism)

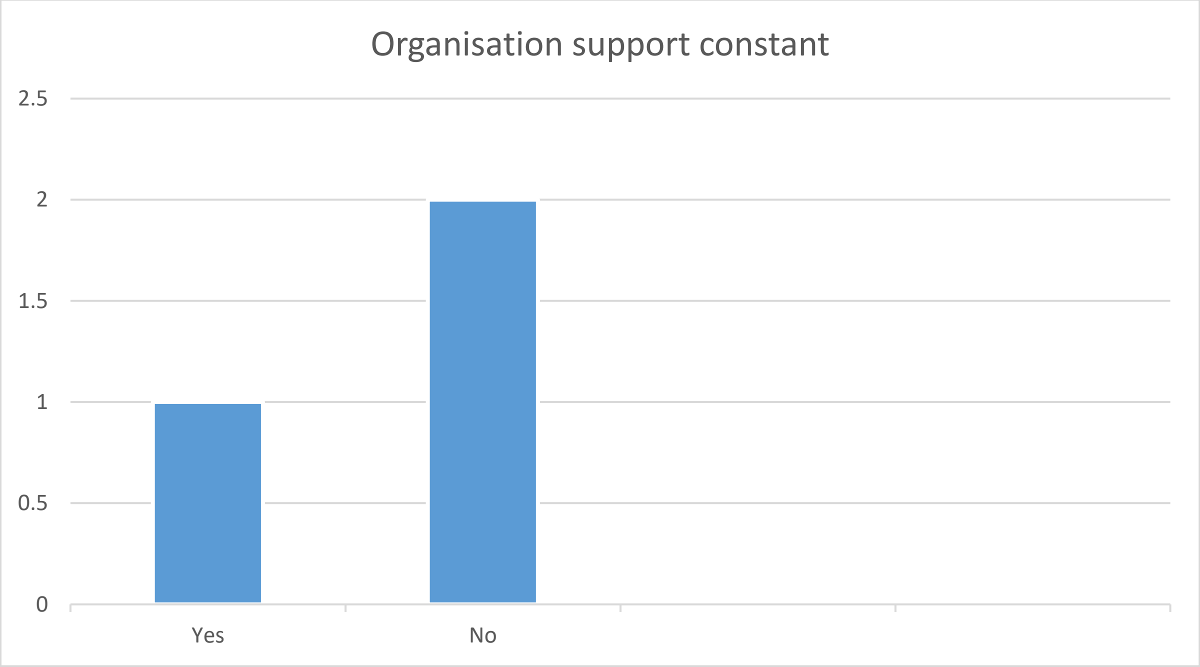


Figure D.552: Organisation support constant (Tourism)

Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 1 participant has received regular cybersecurity awareness training, whilst 1 neither agreed nor disagreed, and 1 participant had not regularly received security awareness training (See figure D.551). In addition, 2 participants had not received support from the organisation to protect personal information, whilst only 1 did (See figure D.552). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

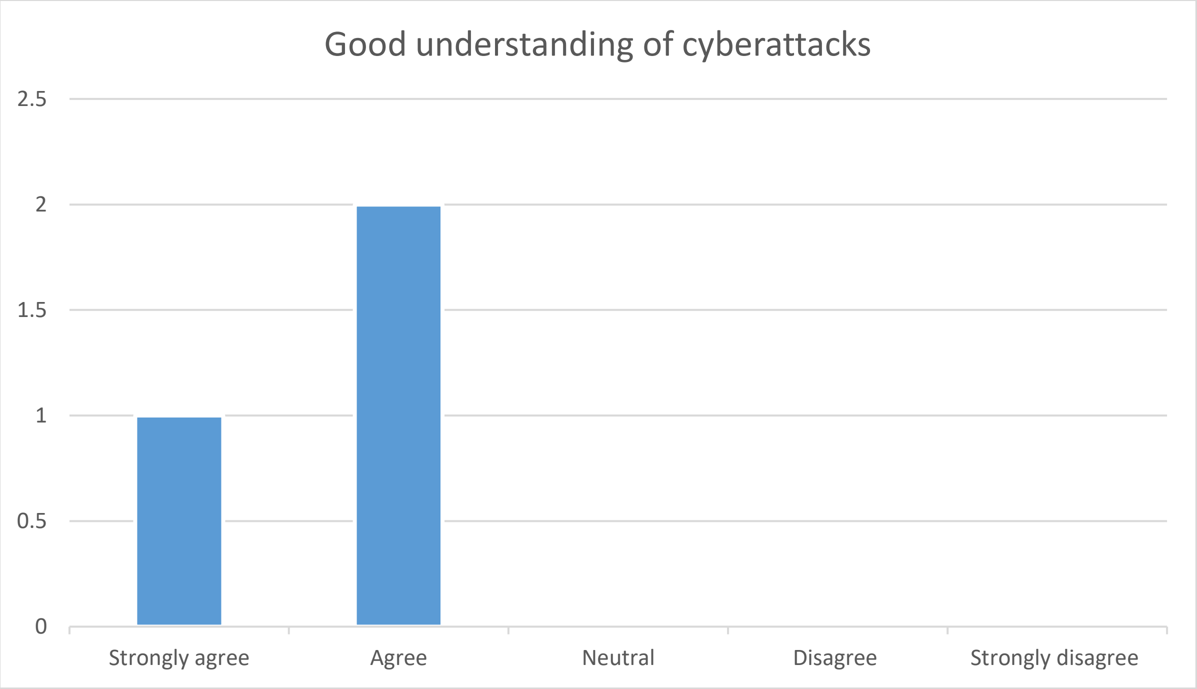


Figure D.553: Good understanding of cyberattacks (Tourism)

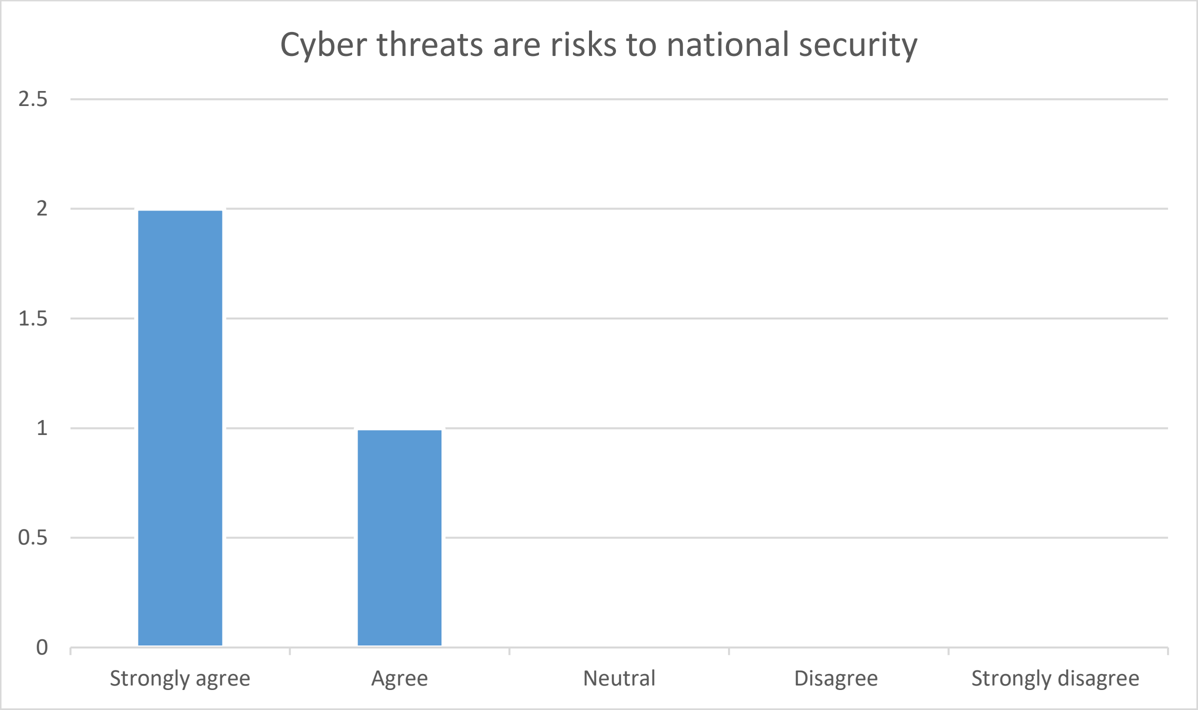


Figure D.554: Cyber threats are risks to national security (Tourism)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. All 3 participants do have (See figure D.553). Furthermore, 100 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure D.554). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

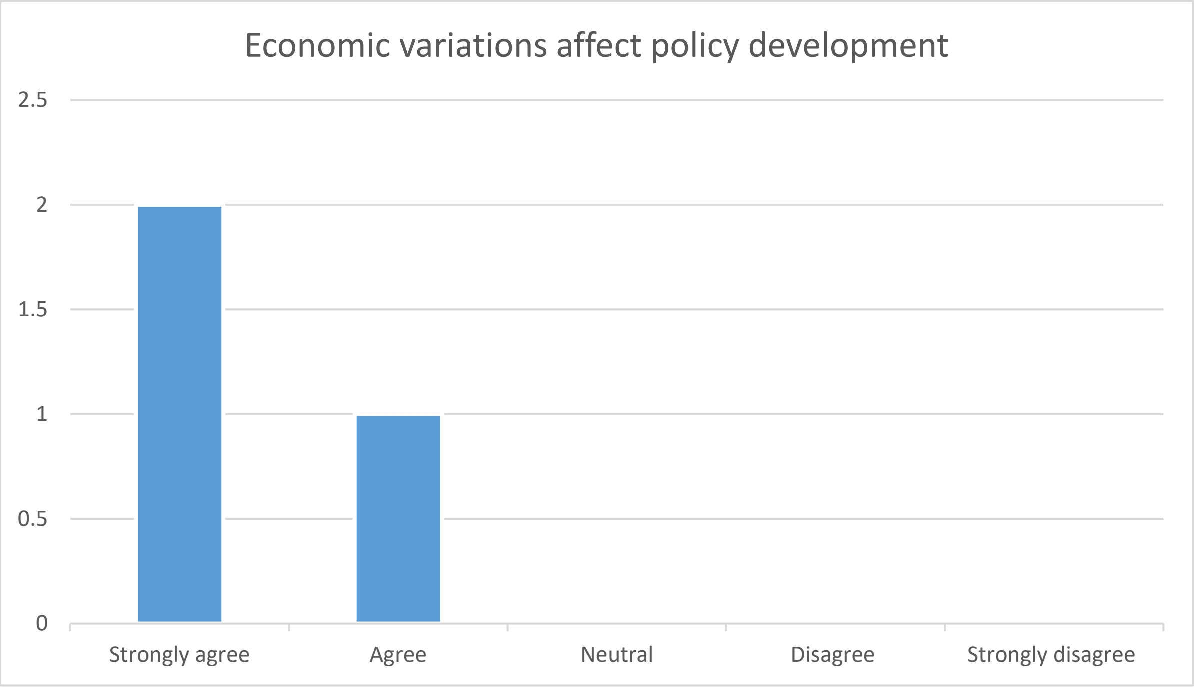


Figure D.555: Economic variations affect policy development (Tourism)

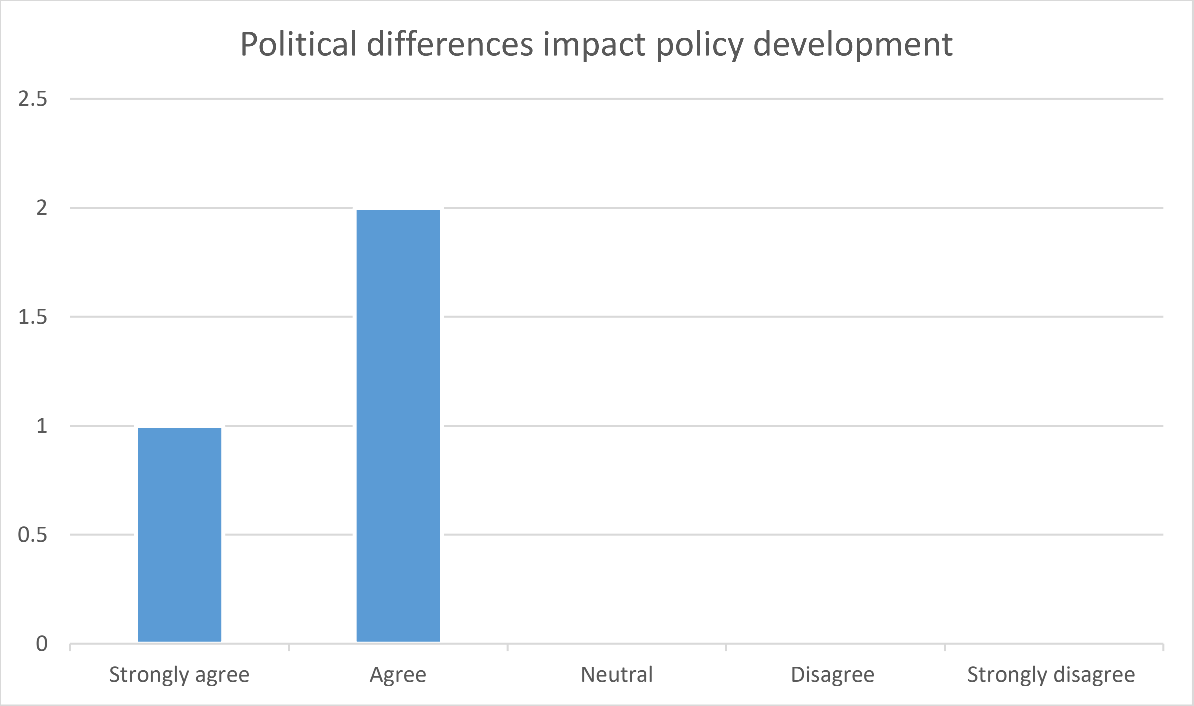


Figure D.556: Political differences impact policy development (Tourism)

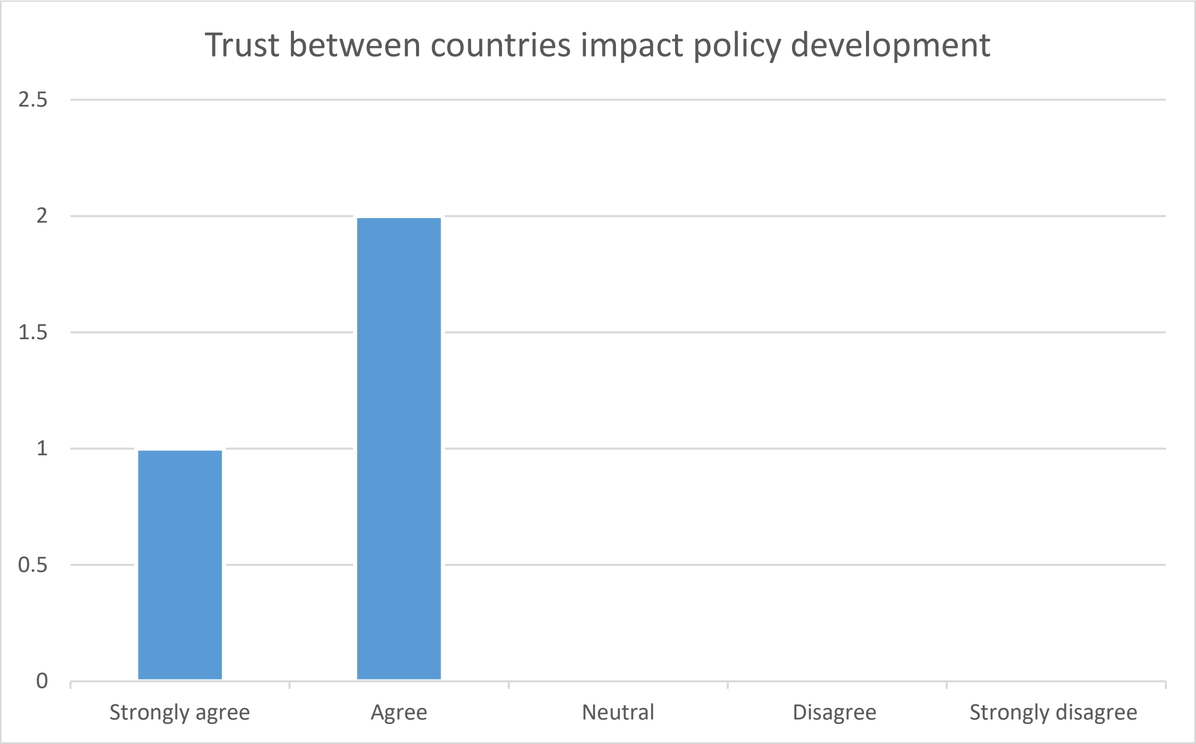


Figure D.557: Trust between countries impact policy development (Tourism)

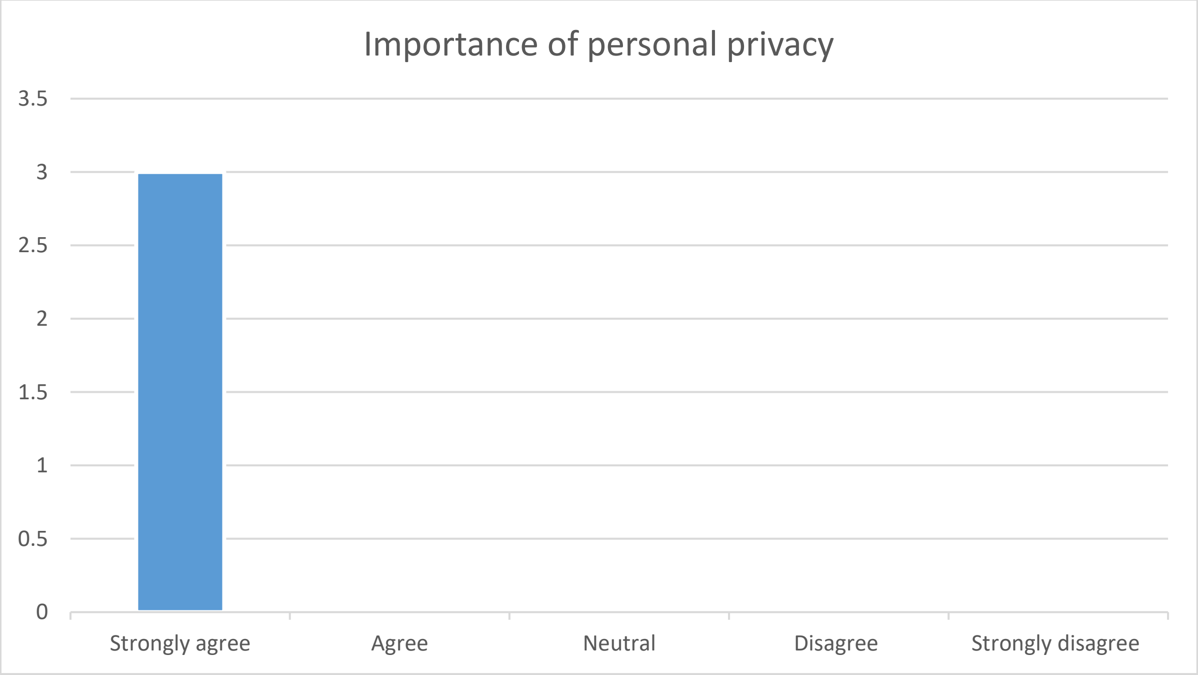


Figure D.558: Importance of personal privacy (Tourism)

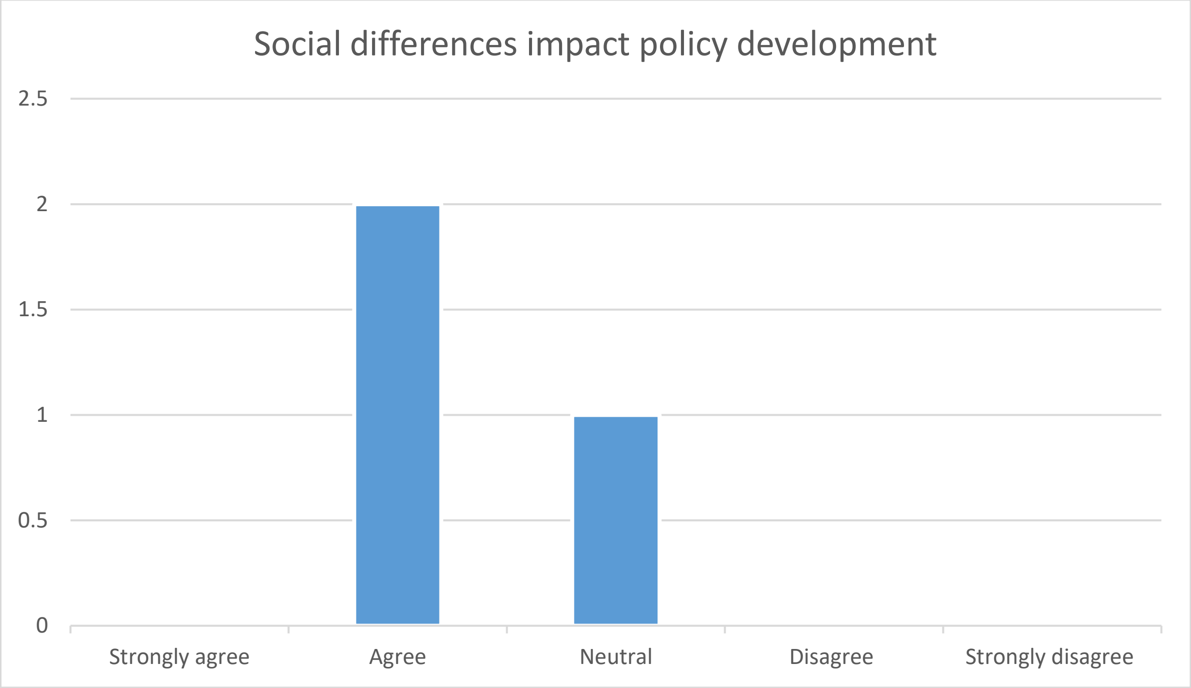


Figure D.559: Social differences impact policy development (Tourism)

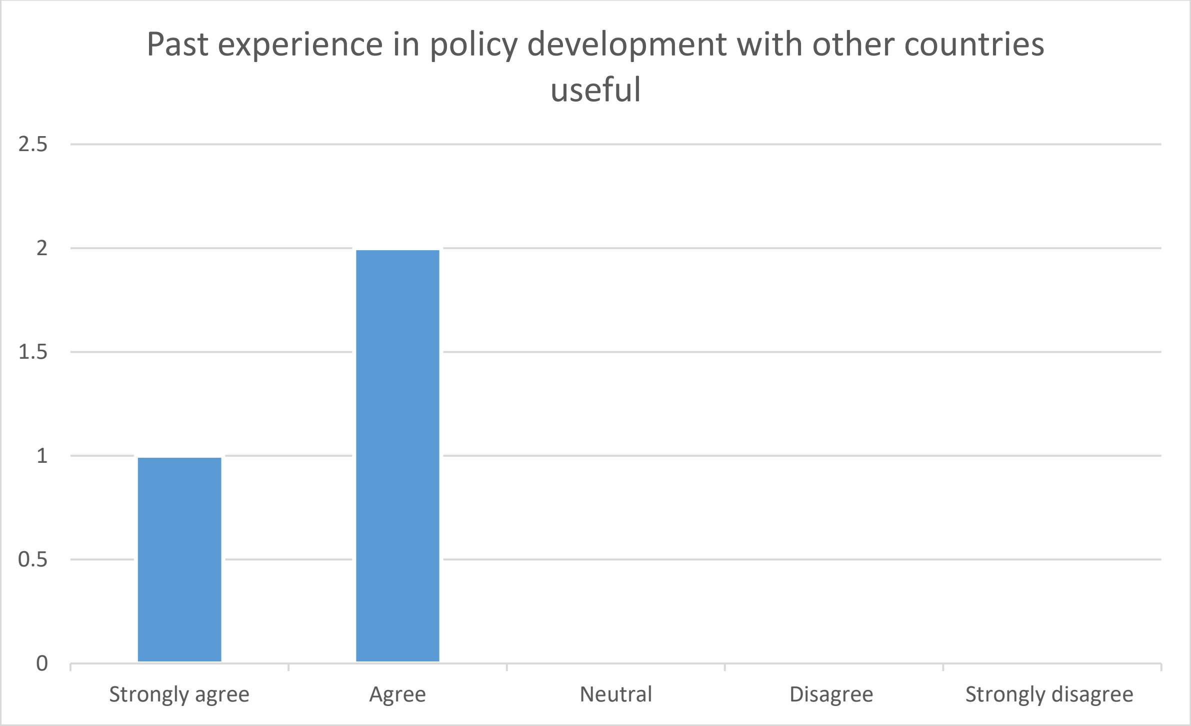


Figure D.560: Past experience in policy development with other countries useful (Tourism)

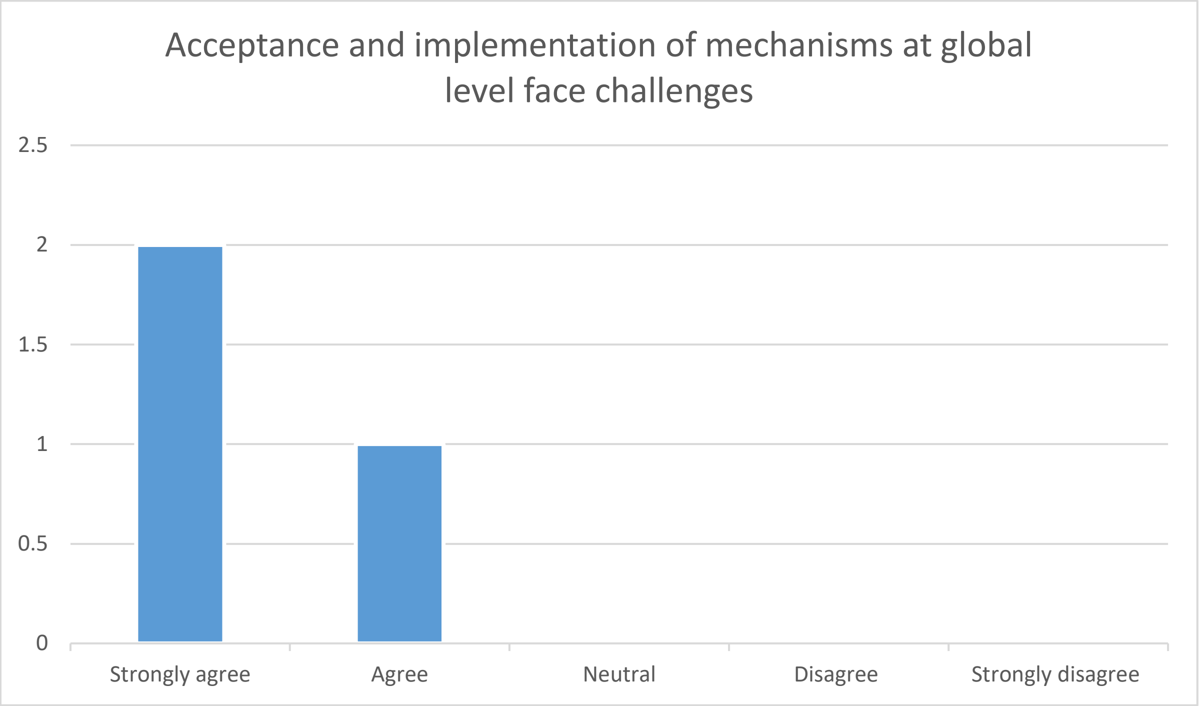


Figure D.561: Acceptance and implementation of mechanisms at global level face challenges (Tourism)

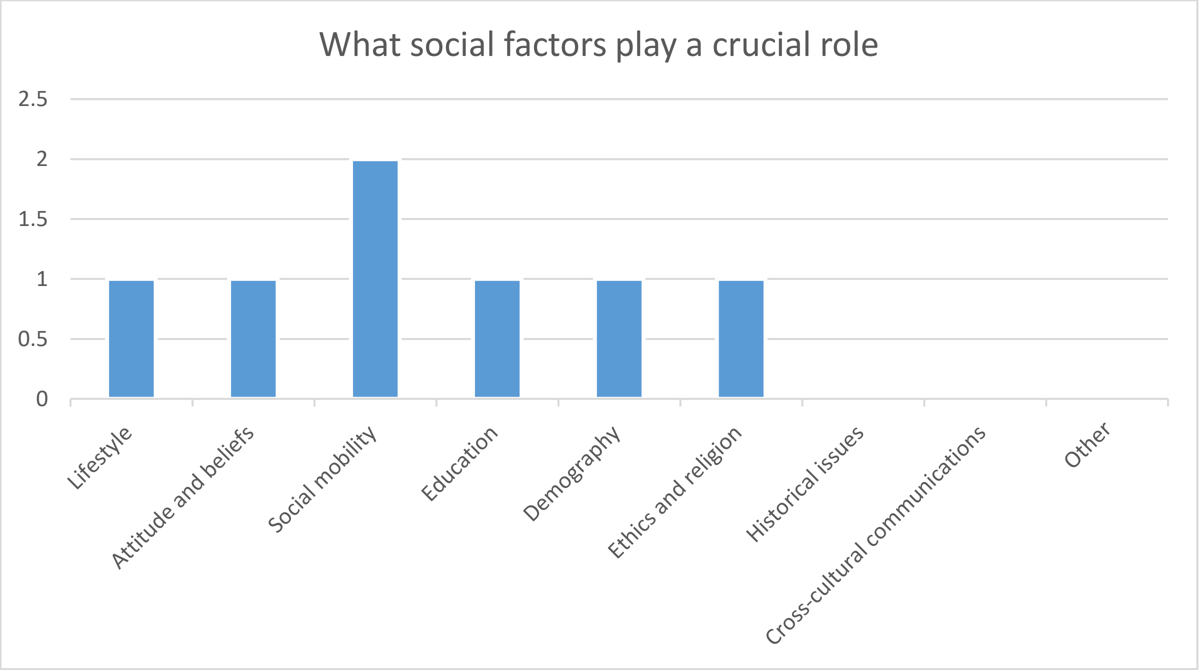


Figure D.562: What social differences play a crucial role (Tourism)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of social mobility (See figure D.562). This is the only sector that have highlighted the importance of social mobility over other factors. It is fair to believe from the experience they gain in dealing with local tourists and foreign tourists the participants may have come to this conclusion.

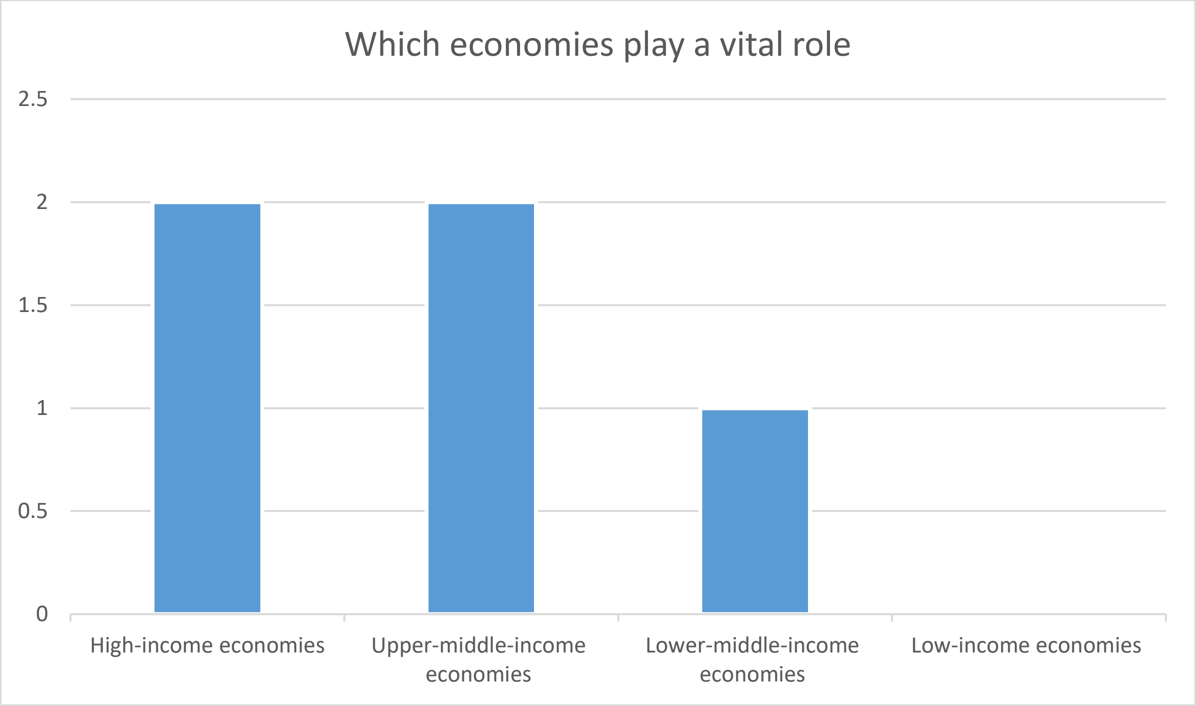


Figure D.563: Which economies play a vital role (Tourism)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure D.563). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

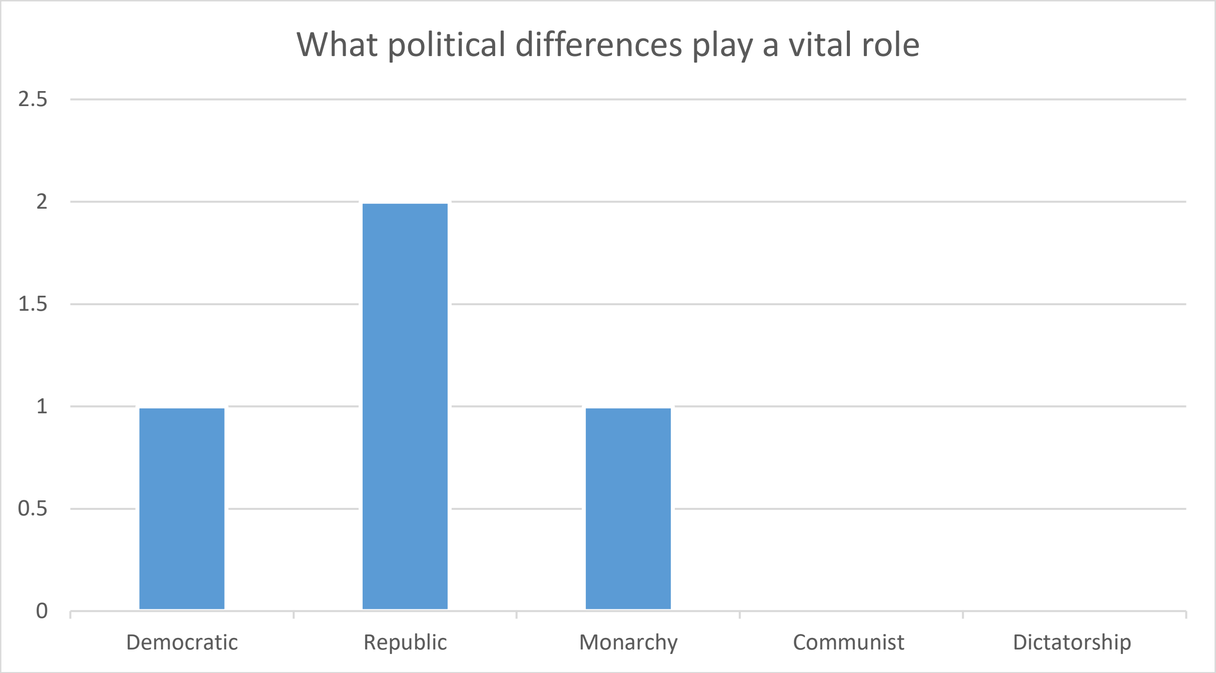


Figure D.564: What political differences play a vital role (Tourism)

Interestingly those who have been in the tourism sector have not voted for a democratic political system (See figure D.564). Unlike in any other political system, in a democratic system, there is a voice for the public as well. In a Republican system, the people and their elected representatives hold the power, and constitutional based decisions are taking. Against that background, it can be assumed that these people presumably looking for legal assurance through the constitutions meaning the governments and the organisations who do collect, share and store personal information cannot compromise people's privacy for any reason. This is particularly important as in this industry they are not only handling information of local residents but also foreigners.

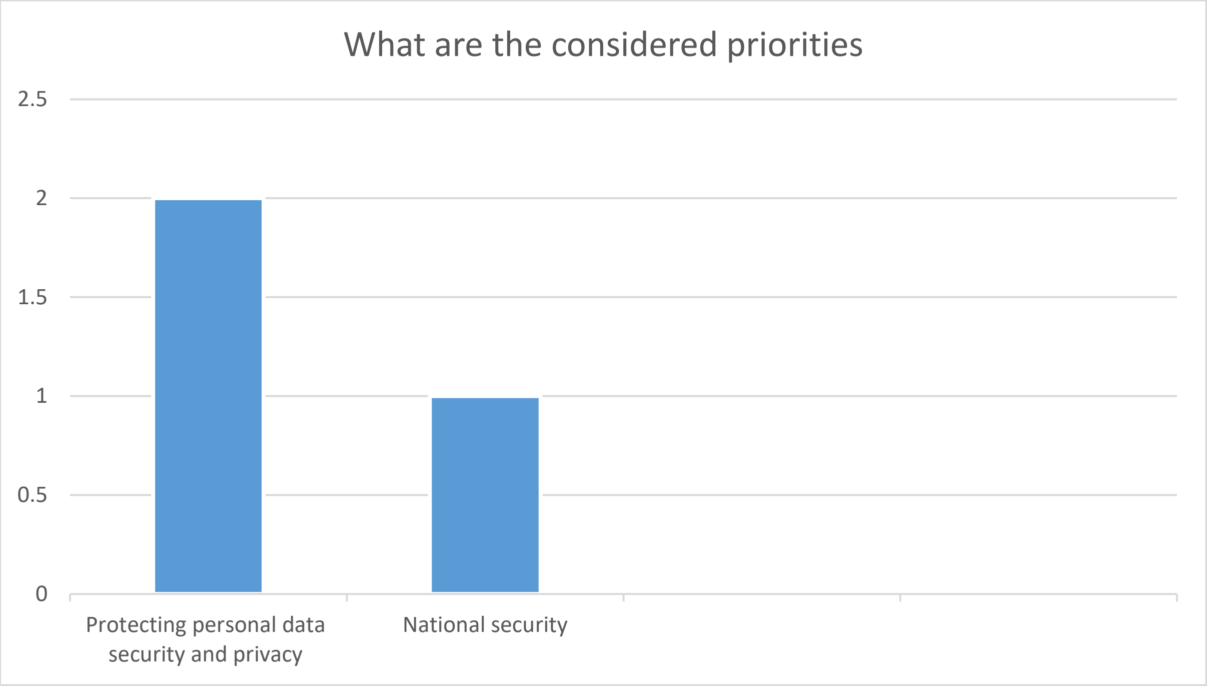


Figure D.565: What are the considered priorities (Tourism)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security (See figure D.565), which is a significant factor. In an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

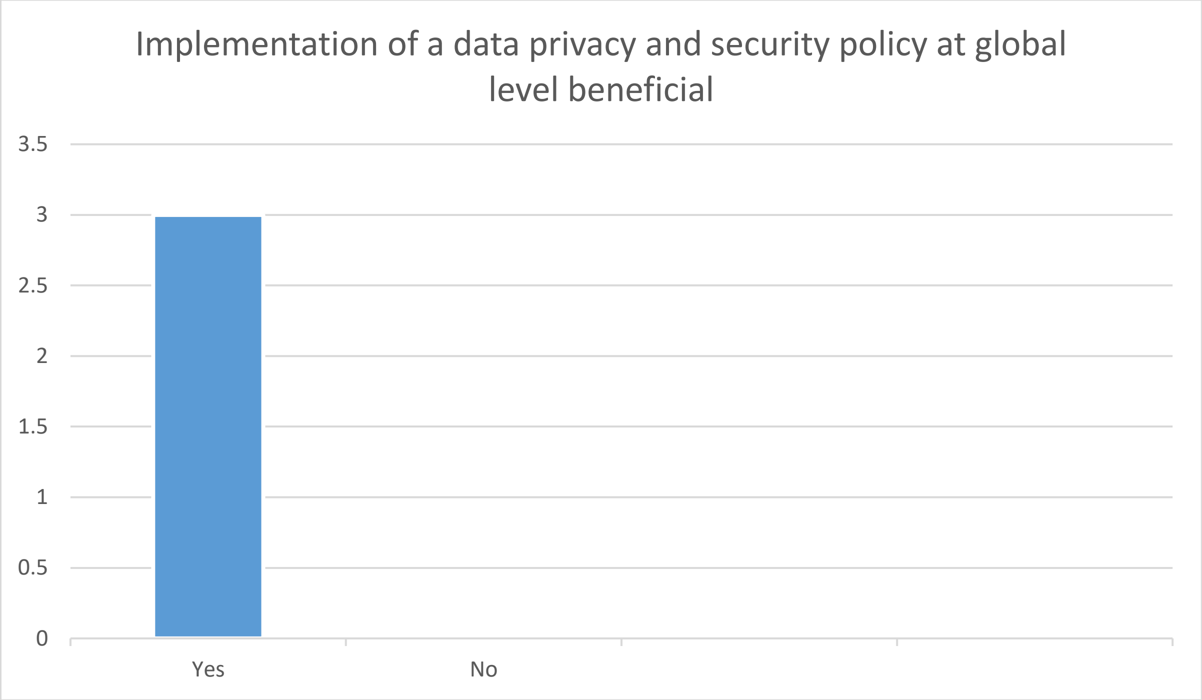


Figure D.566: Implementation of a data privacy and security policy at global level beneficial (Tourism)

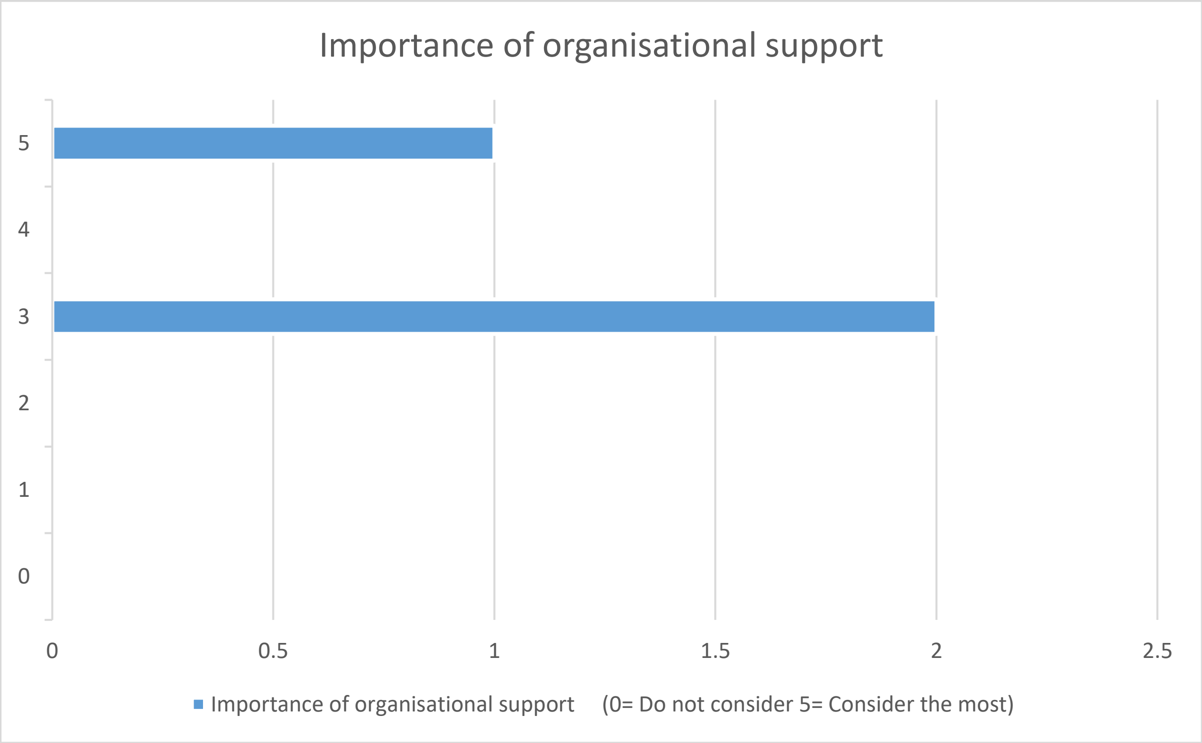


Figure D.567: Importance of organisational support (Tourism)

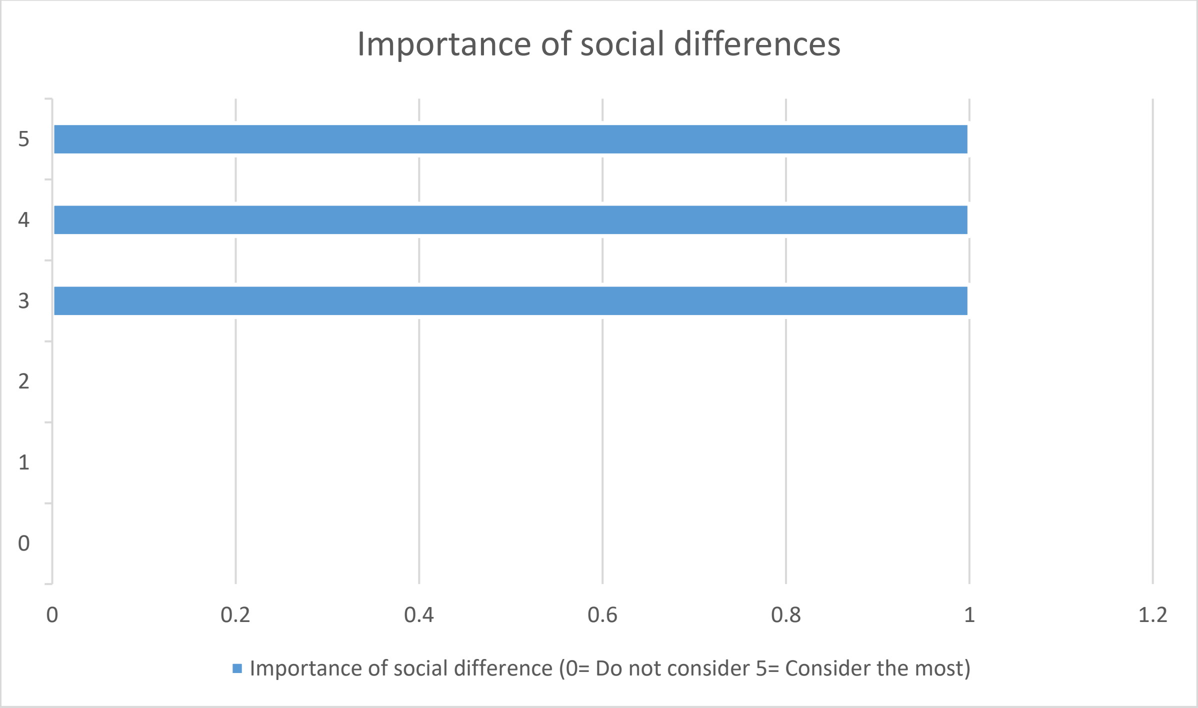


Figure D.568: Importance of social differences (Tourism)

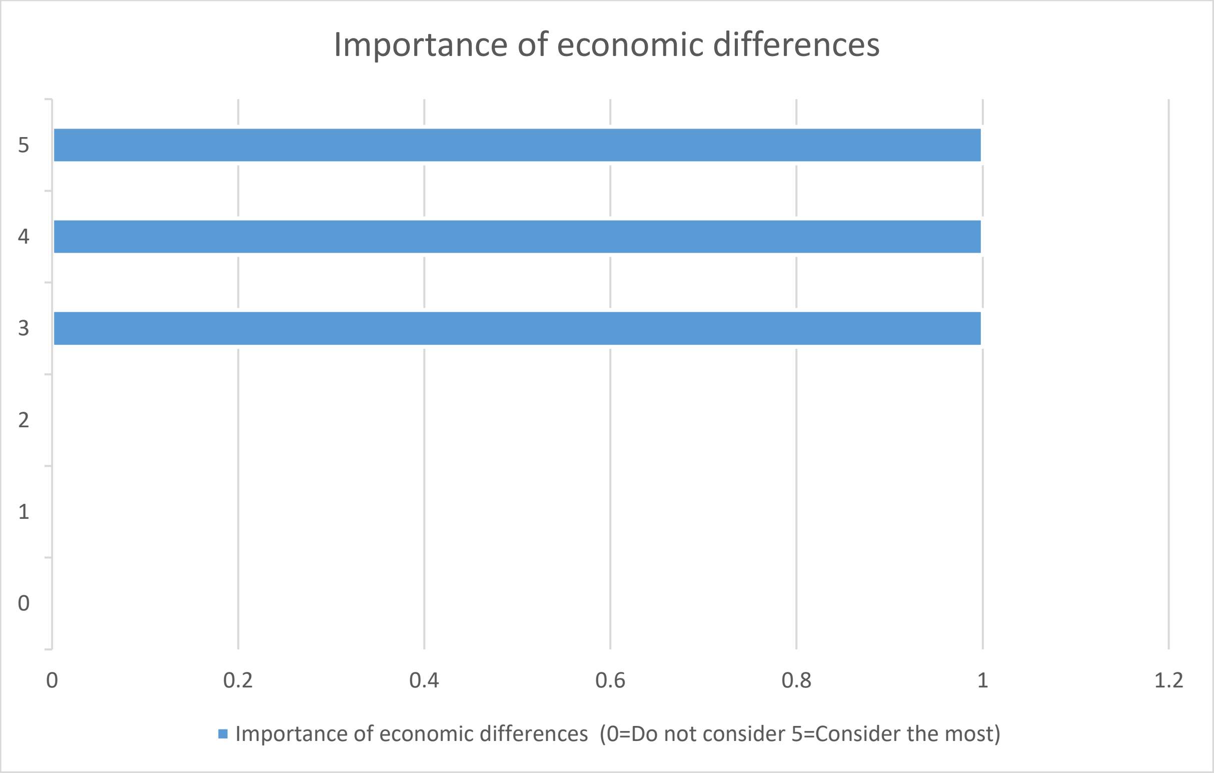


Figure D.569: Importance of economic differences (Tourism)

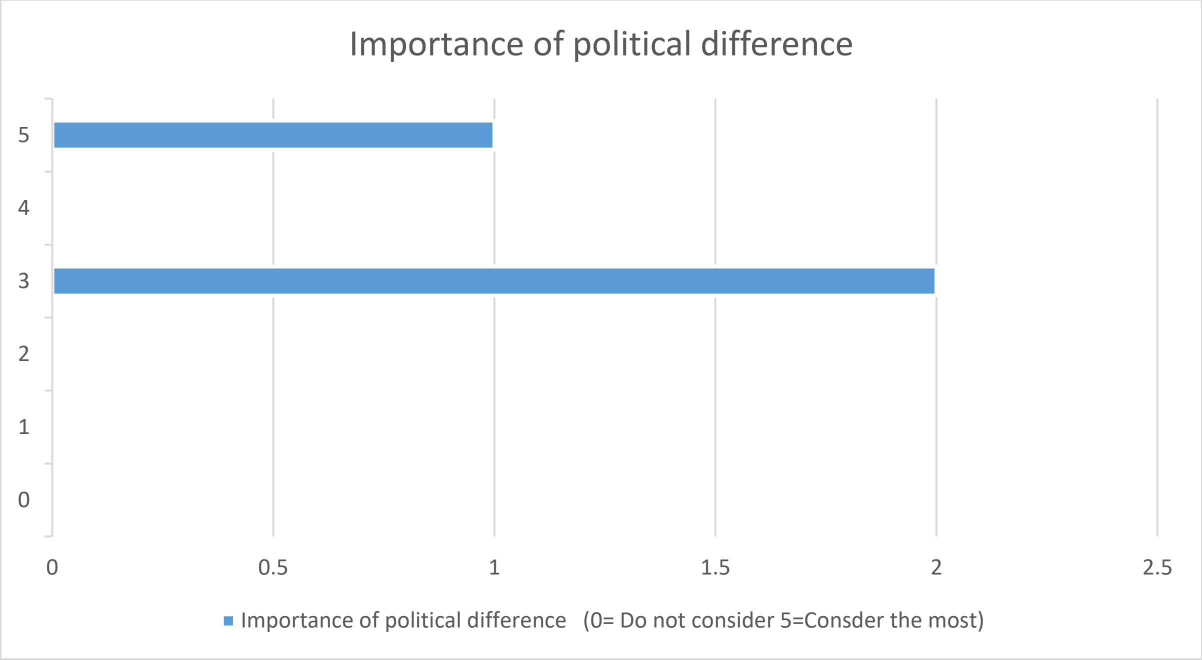


Figure D.570: Importance of political difference (Tourism)

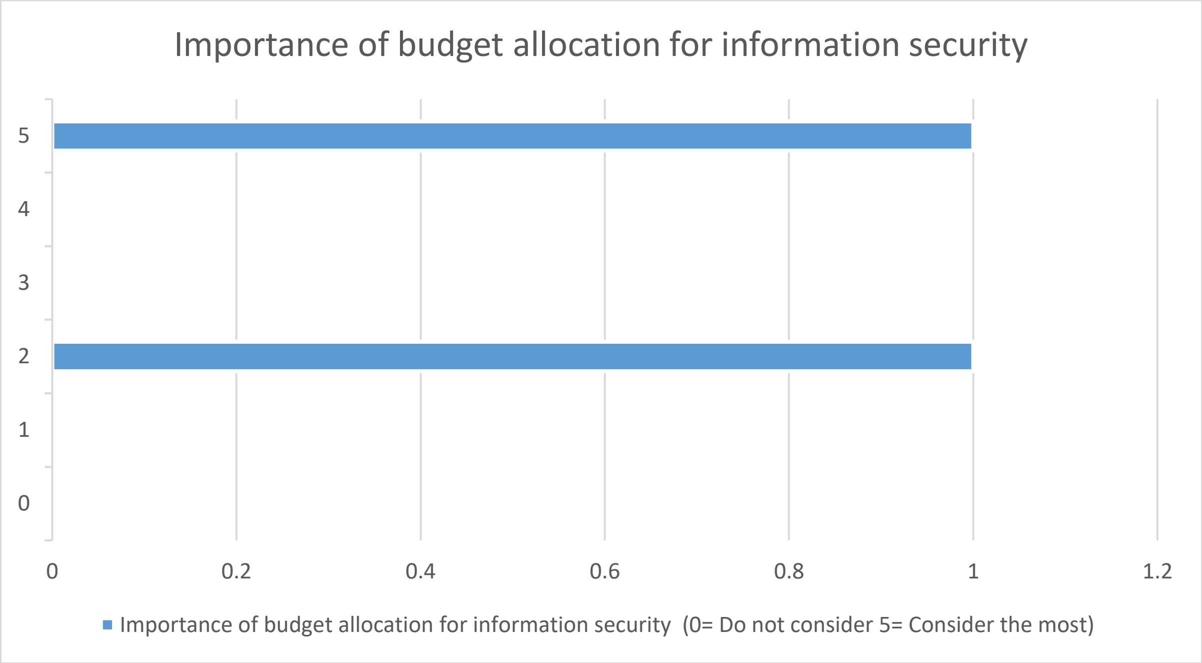


Figure D.571: Importance of budget allocation for information security (Tourism)

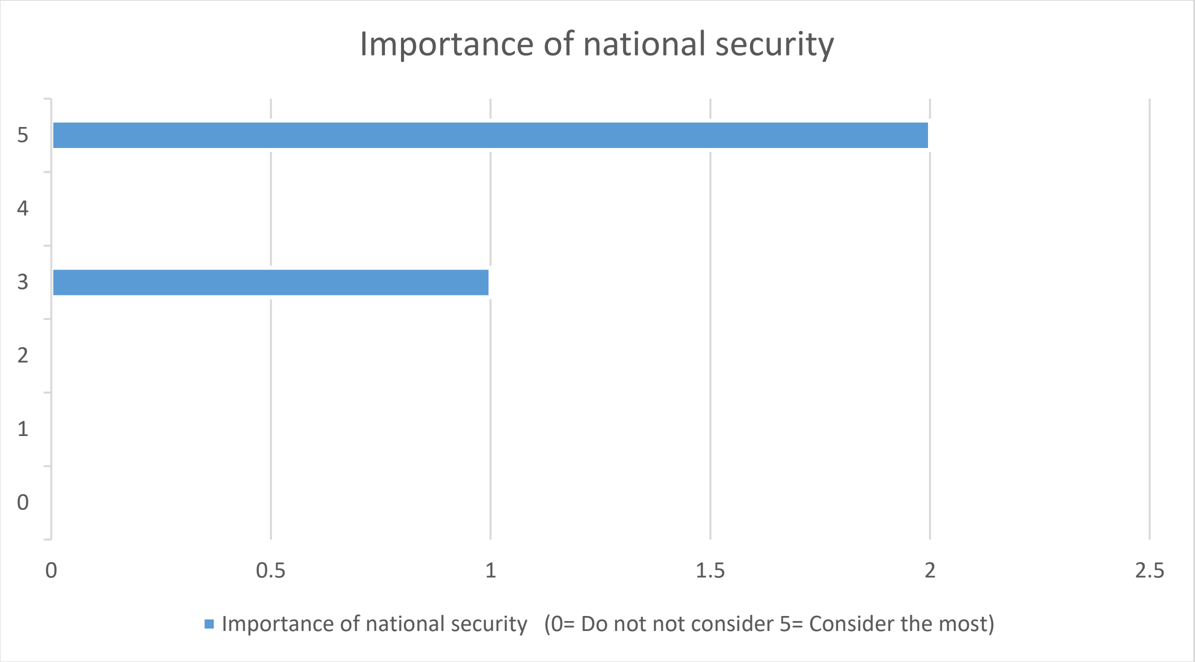


Figure D.572: Importance of national security (Tourism)

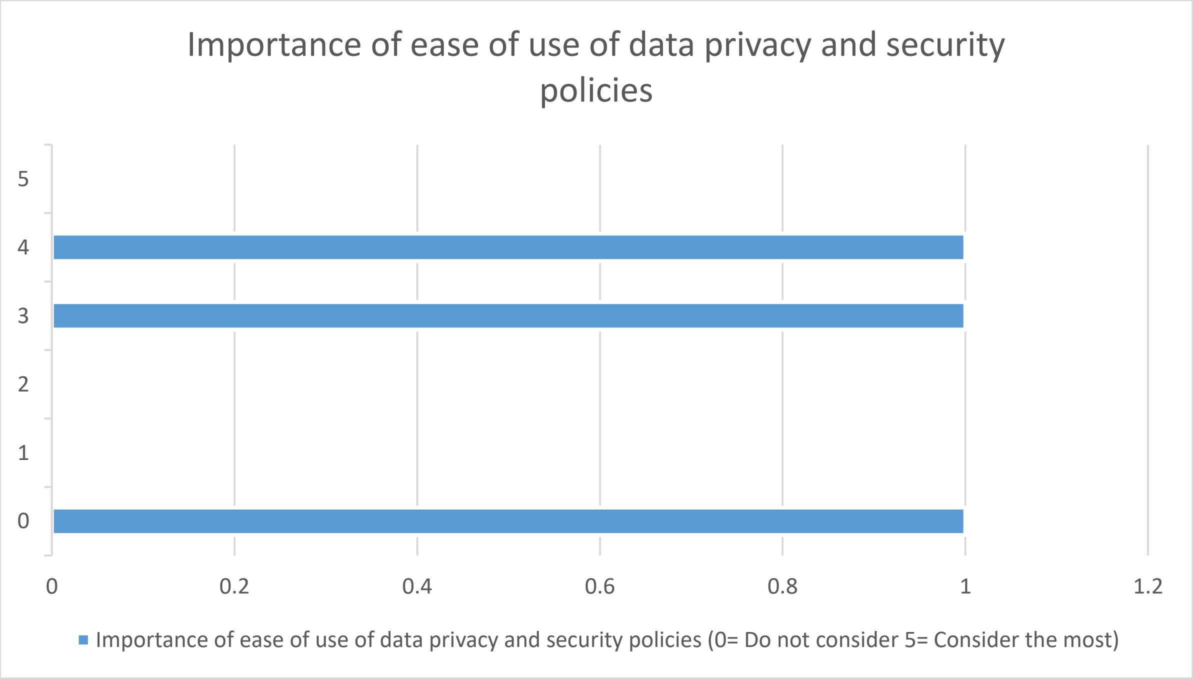


Figure D.573: Importance of ease of use of data privacy and security policies (Tourism)

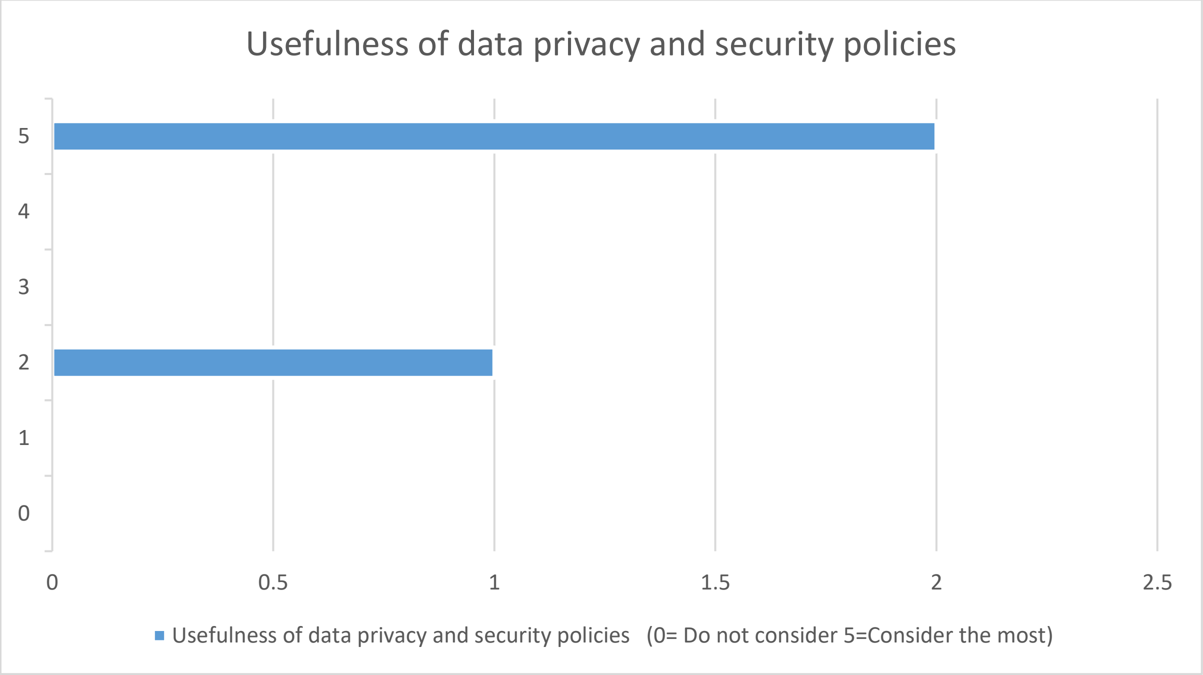


Figure D.574: Usefulness of data privacy and security policies (Tourism)

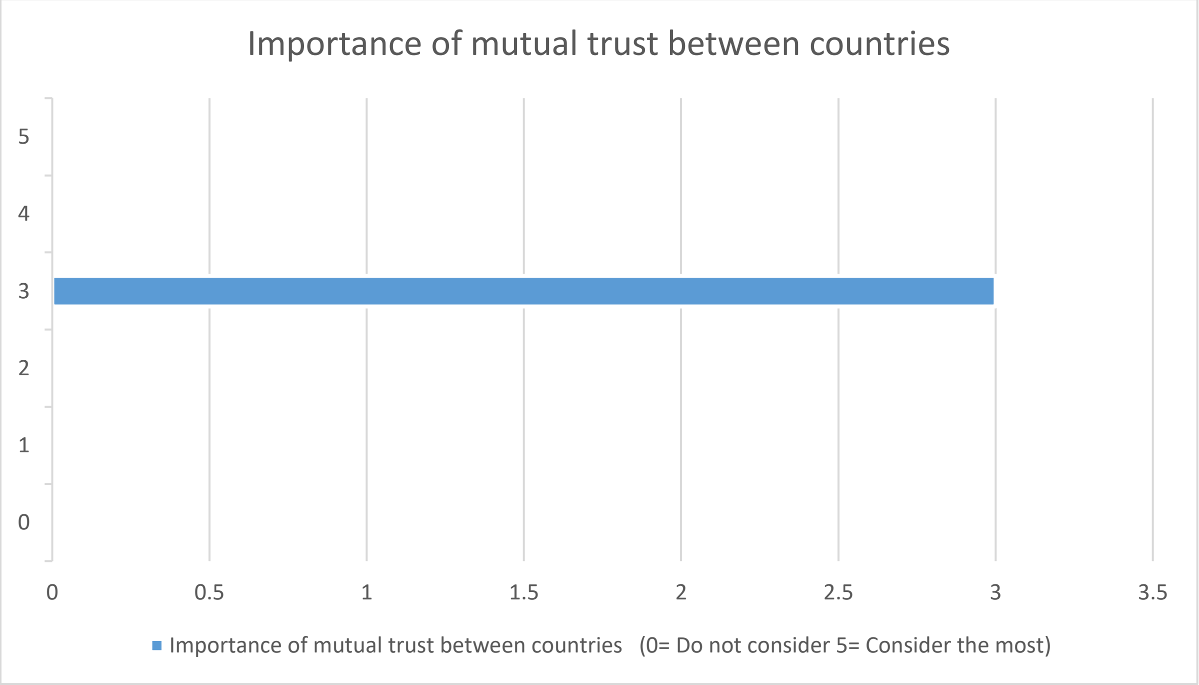


Figure D.575: Importance of mutual trust between countries (Tourism)

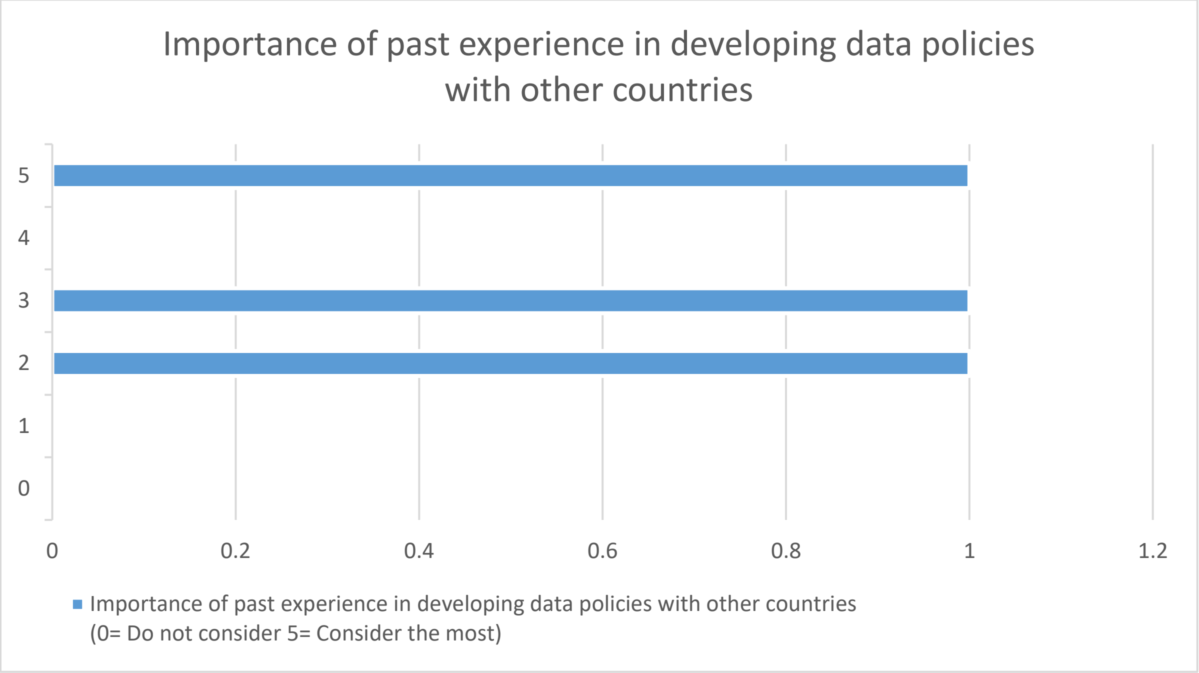


Figure D.576: Importance of past experience in developing data policies with other counties (Tourism)

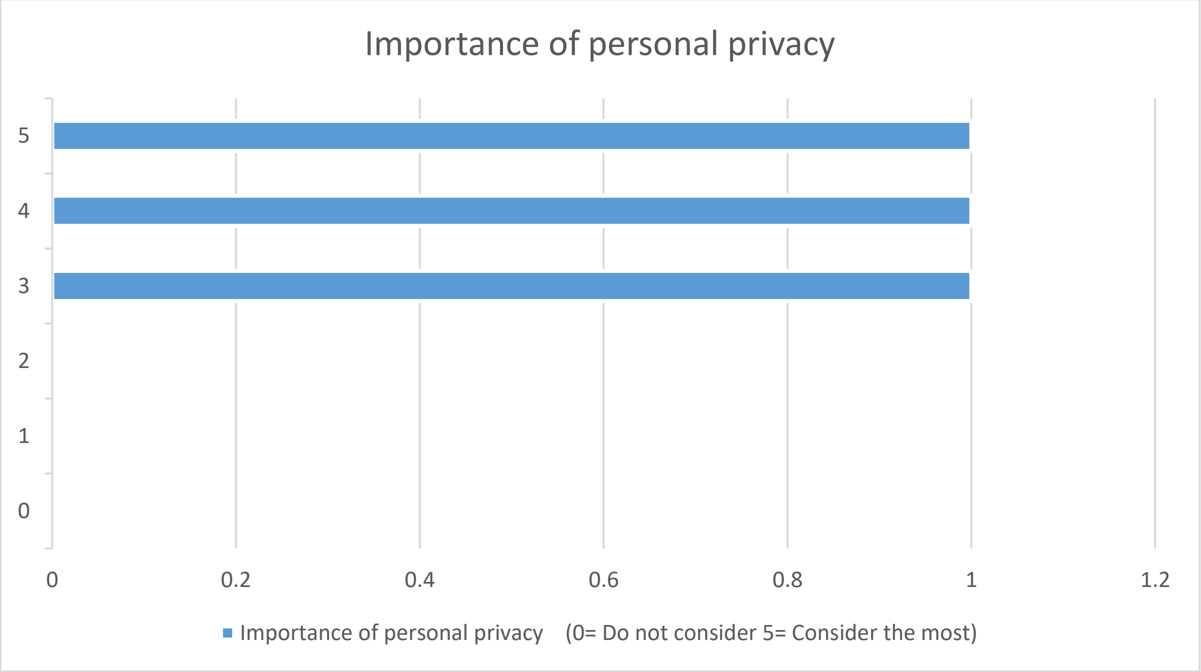


Figure D.577: Importance of personal privacy (Tourism)

The endorsement of the need to have a global level data protection mechanism by full complement of participants is a significant observation (See figure D.566). The other notable factors that have come out of the survey are organisational support, economic differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries, previous experience in developing policies with other countries (See figure D.555-565) (See figure D.567-577). The budget allocation not scored (See figure D.571).

ANNEXURE E

United Kingdom – Male

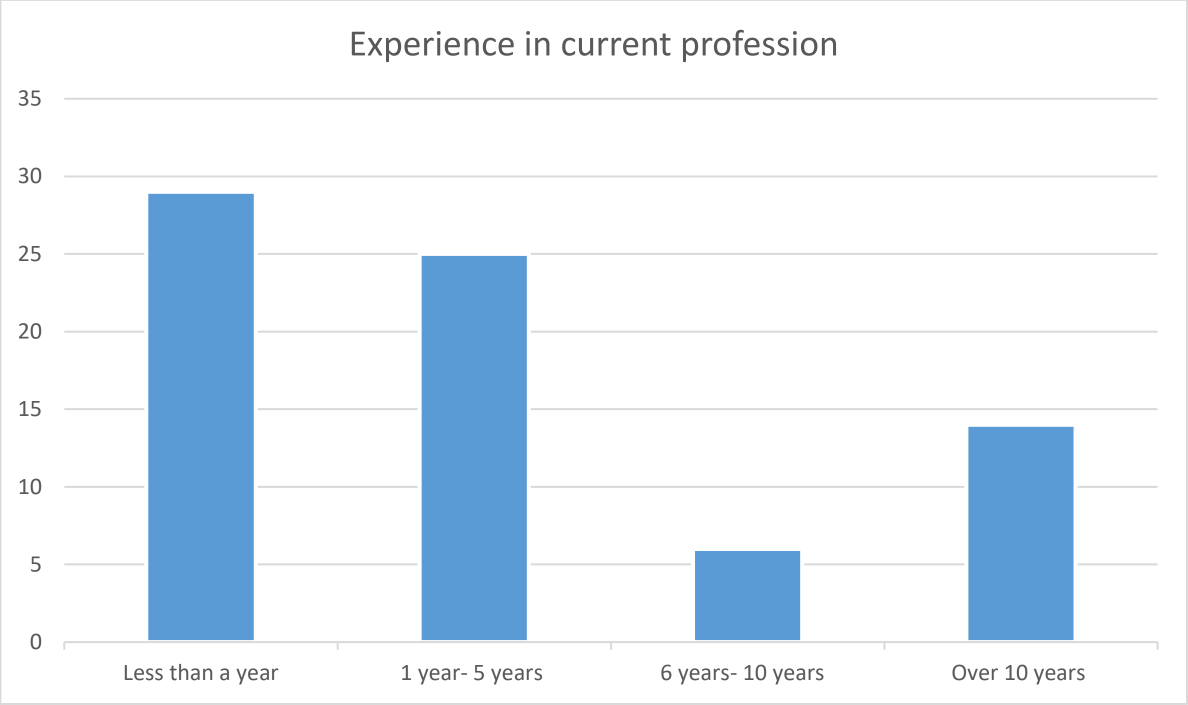


Figure E.1: Experience in current profession (Male-UK)

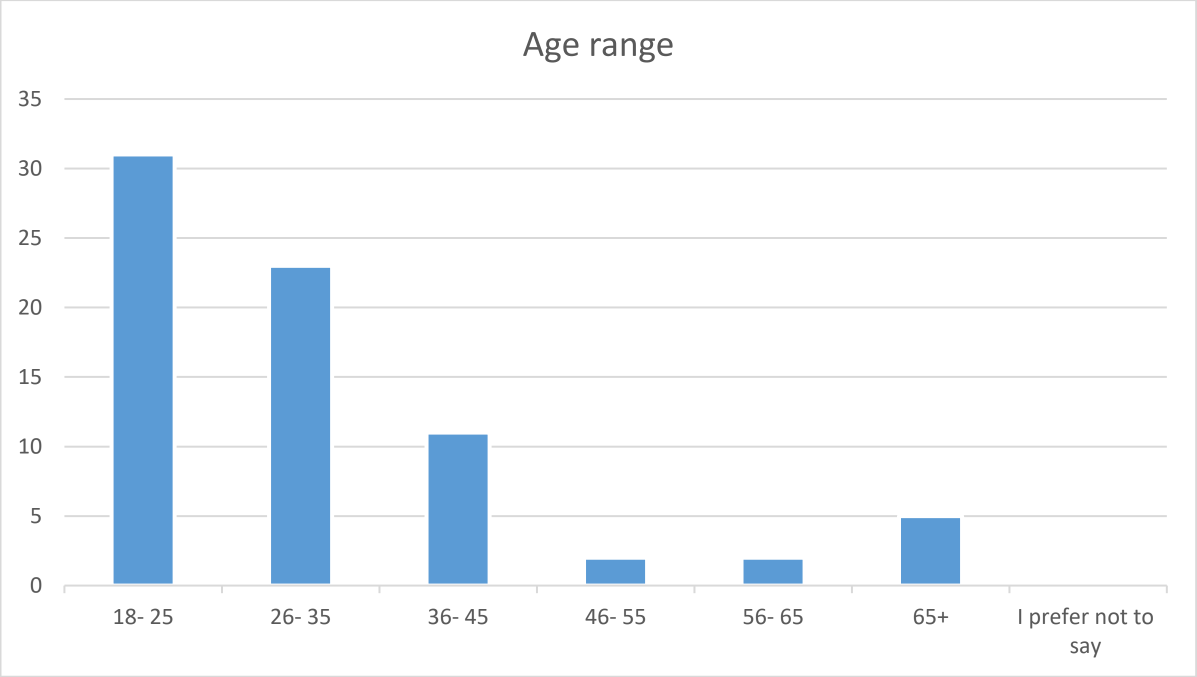


Figure E.2: Age range (Male-UK)

This analysis is based on the responses received from United Kingdom male participants. They were within the 18-65 age range out of which 31 in the 18-25, 23 in the 26-35, and 11 in the 36-45, 2 in the 46-55, and 2 in the 56-65, 5 in the 65+ range (See figure E.2). These participants employed in different industries between less than a year to over 10 years (See figure E.1).

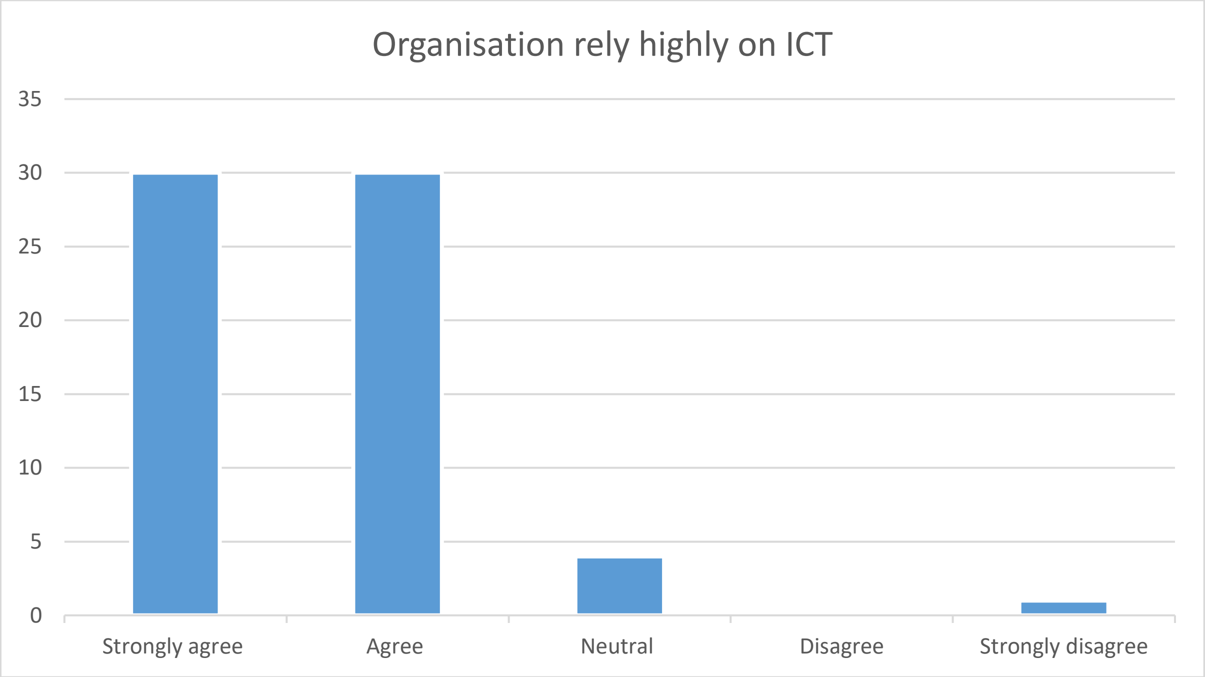


Figure E.3: Organisation rely highly on ICT (Male-UK)

Out of the 74 respondents, 60 have worked in a technology reliance working environment, 4 unaware of reliance on technology because of the nature of the work assigned to them, 1 have marked 'disagree' on ICT (See figure E.3). This indicates a majority of males have had a high reliance on ICT.

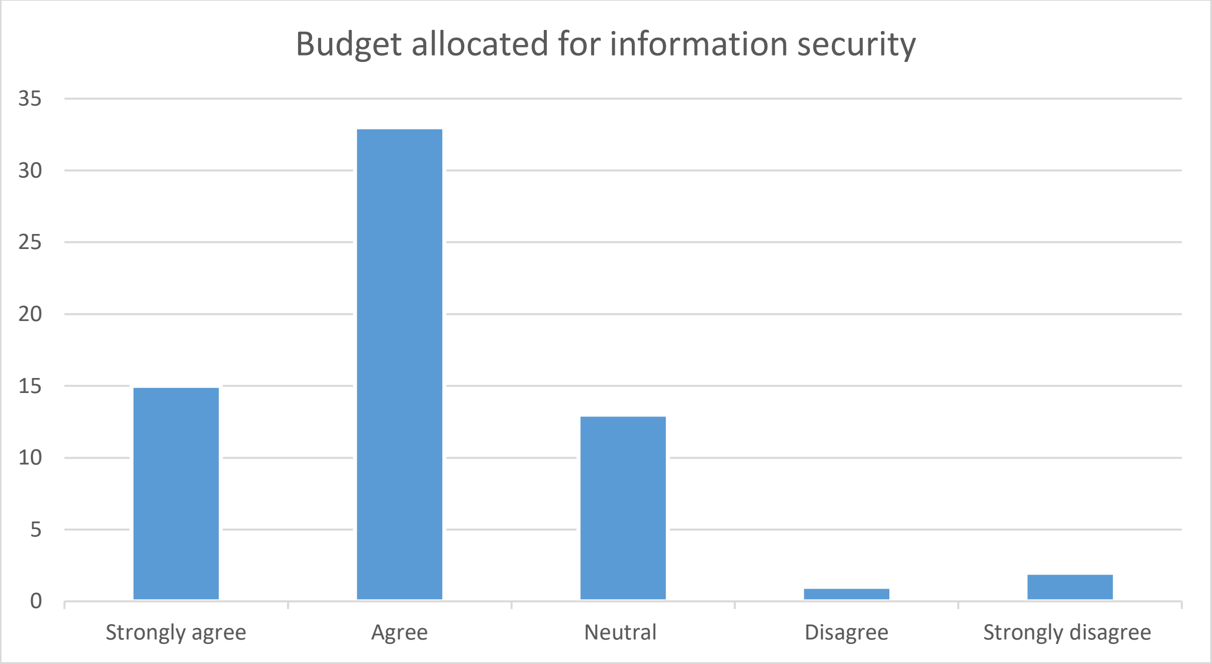


Figure E.4: Budget allocated for information security (Male-UK)

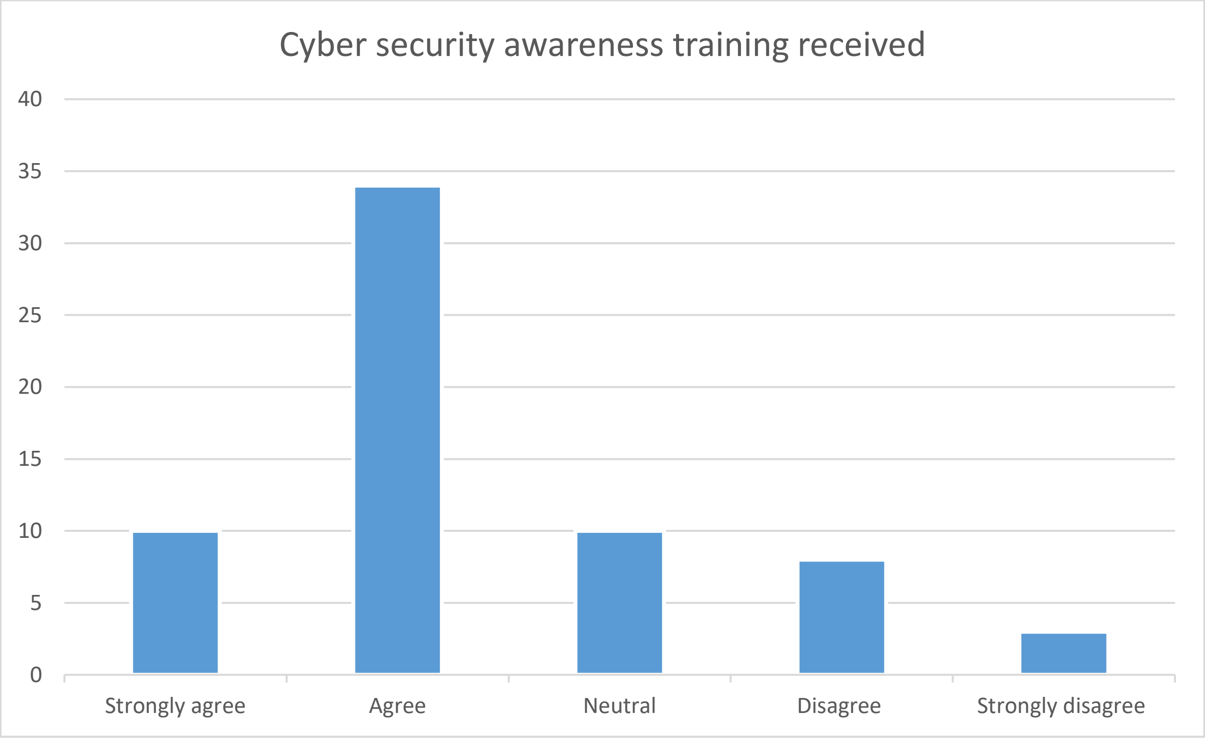


Figure E.5: Cyber security awareness training received (Male-UK)

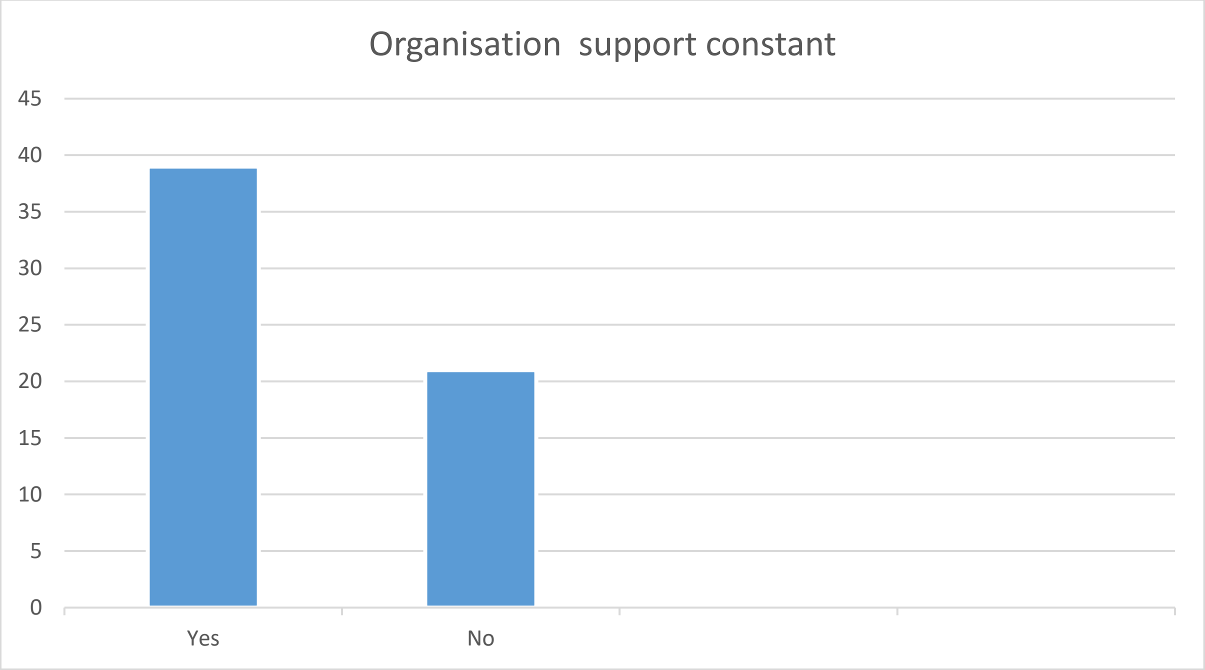


Figure E.6: Organisation support constant (Male-UK)

Funding has been sketchy. 48 out of the 74 have indicated that their organisations had an allocated budget for information security, whilst 13 had not expressed an opinion either way and notably according to the 3 disagreed, their organisations had no budget allocation for information security (See figure E.4). According to some of the participants, regular security awareness training received was adequate despite the satisfactory level of resources allocated for information security. 44 participants have received regular cybersecurity awareness training, whilst 10 neither agreed nor disagreed, and 11 participants had not regularly received security awareness training (See figure E.5). In addition, only 21 participants had not received support from the organisation to protect personal information, whilst 39 did (See figure E.6). This clearly indicates that the organisations have a budget allocation for information security as well as regular security awareness training, and adequate support to protect personal information. This will enable the end user to minimise errors.

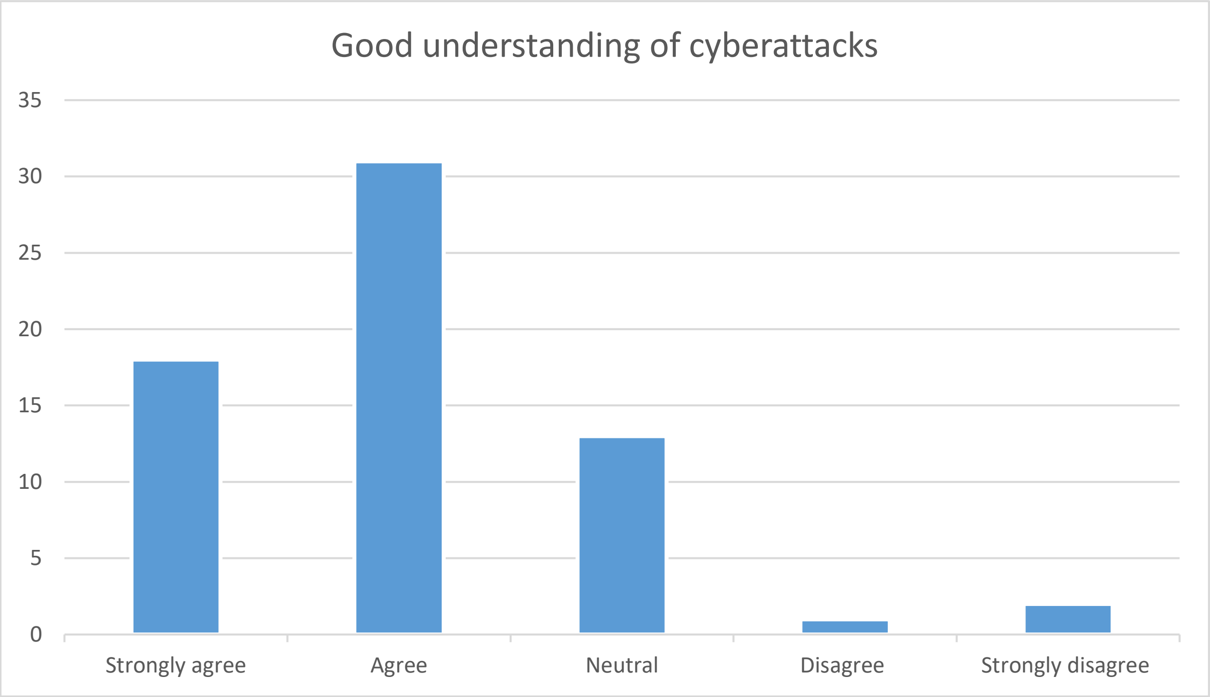


Figure 6.7: Good understanding of cyberattacks (Male- UK)

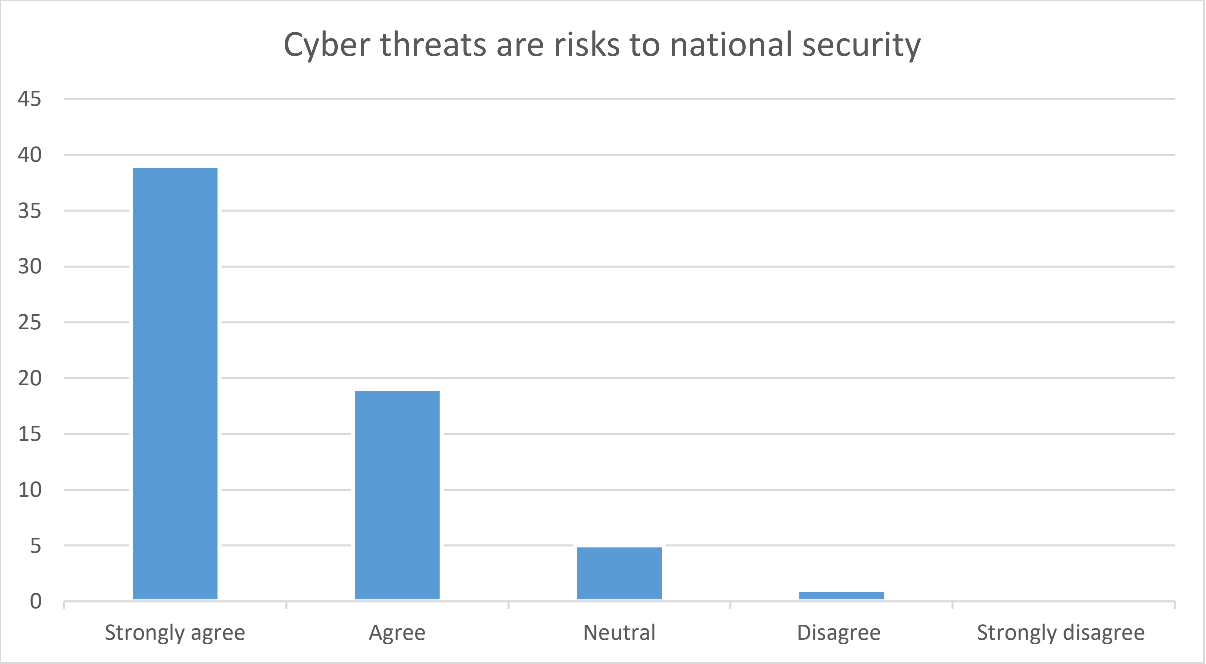


Figure E.8: Cyber threats are risks to national security (Male-UK)

Despite the security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 49 participants do have, 13 have not expressed opinion either way, and only 3 participants had no understanding (See figure E.7). Furthermore, 78 percent of the participants realise the potential threats to national security from cyber-attacks (See figure E.8). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

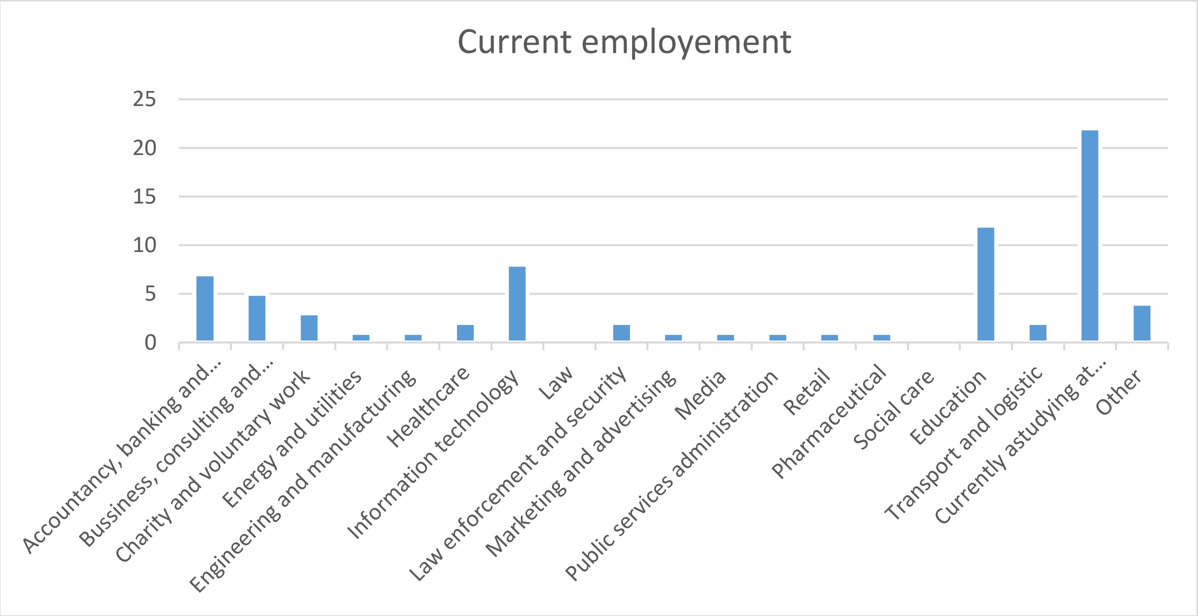


Figure E.9: Current employment (Male-UK)

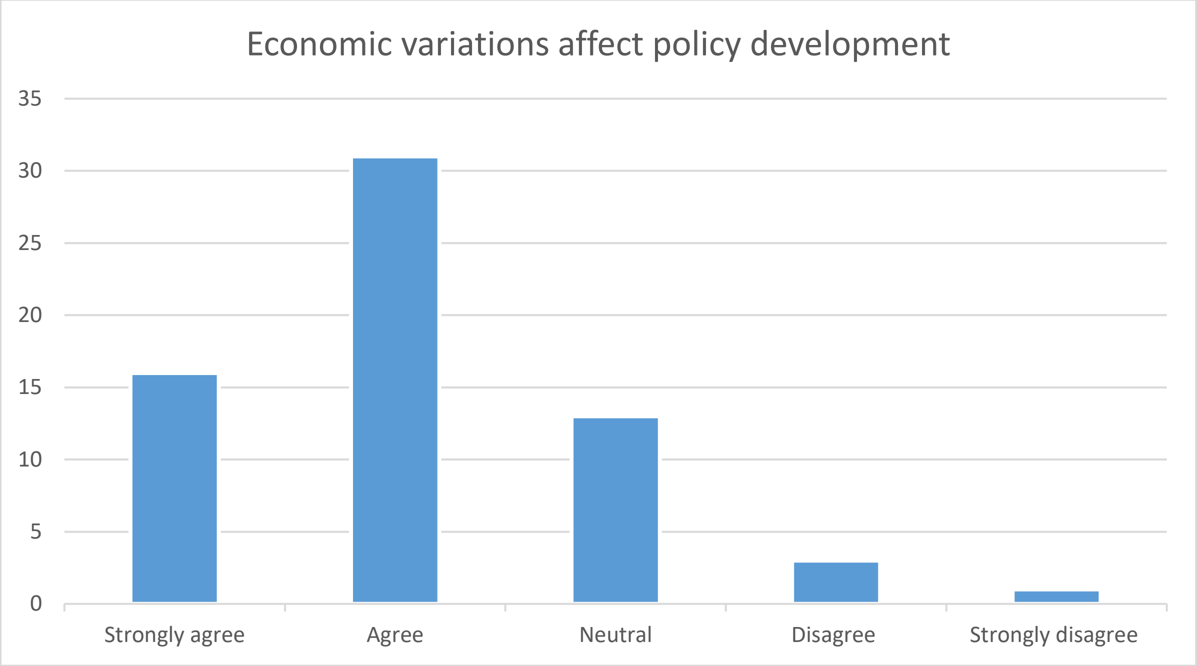


Figure E.10: Economic variations affect policy development (Male-UK)

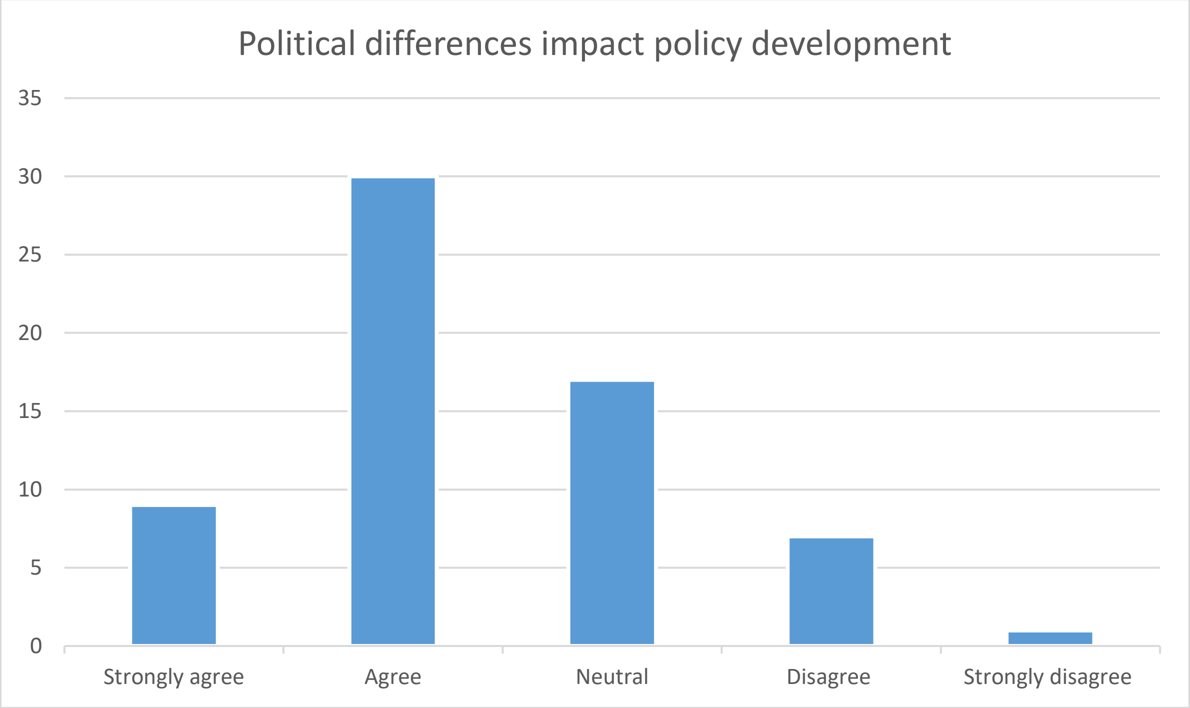


Figure E.11: Political differences impact policy development (Male-UK)

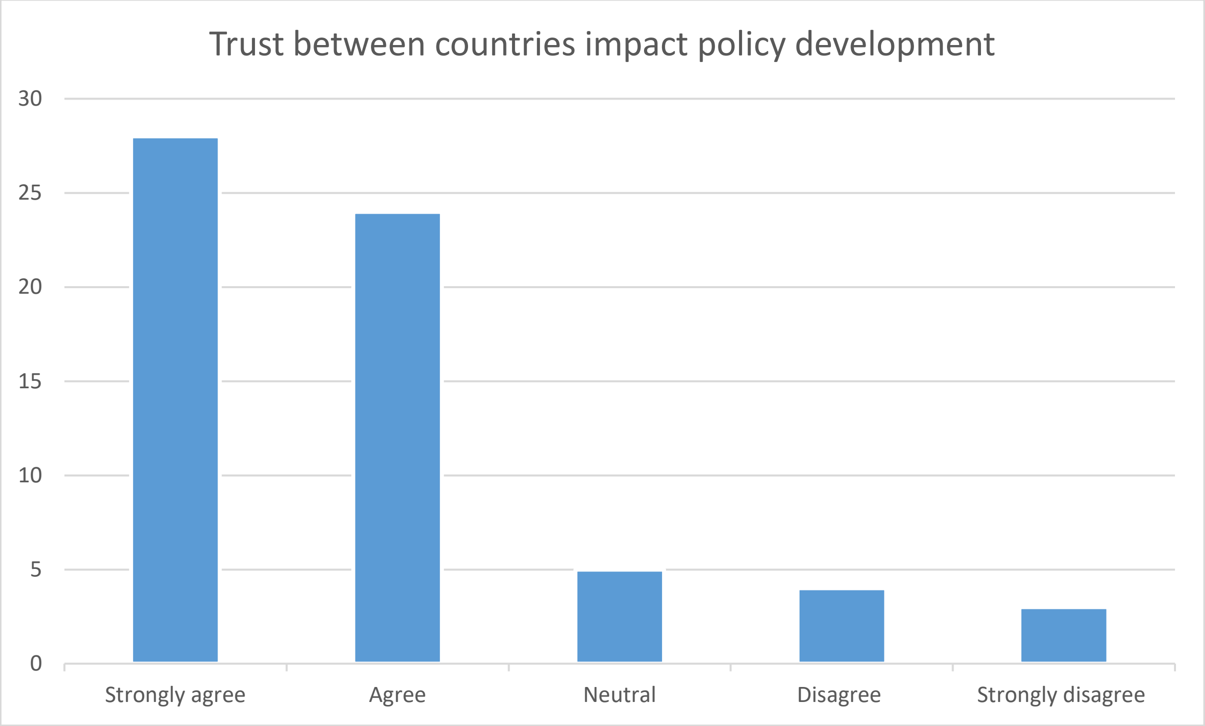


Figure E.12: Trust between countries impact policy development (Male-UK)

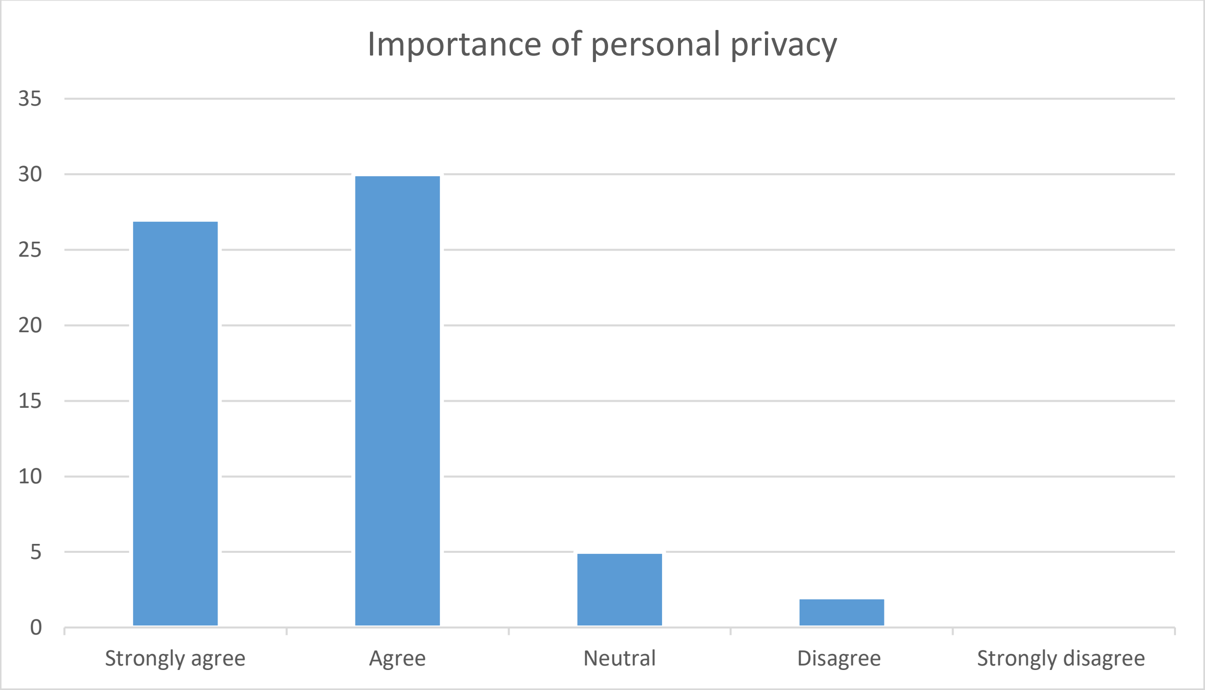


Figure E.13: Importance of personal privacy (Male-UK)

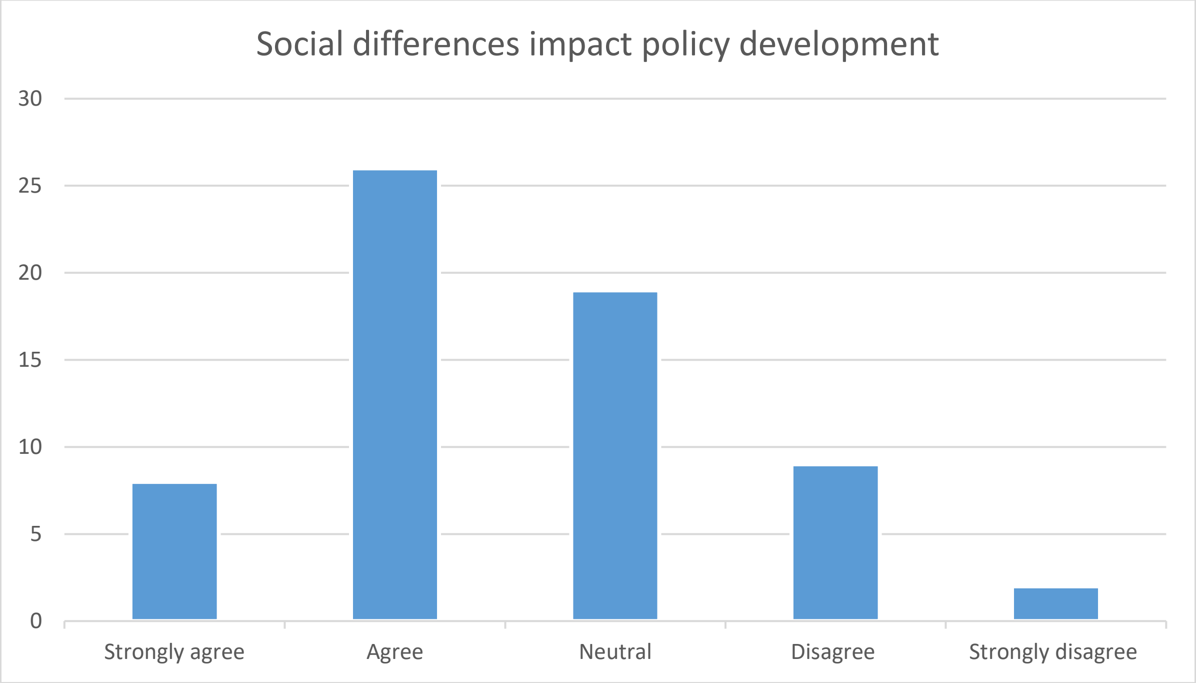


Figure E.14: Social differences impact policy development (Male-UK)

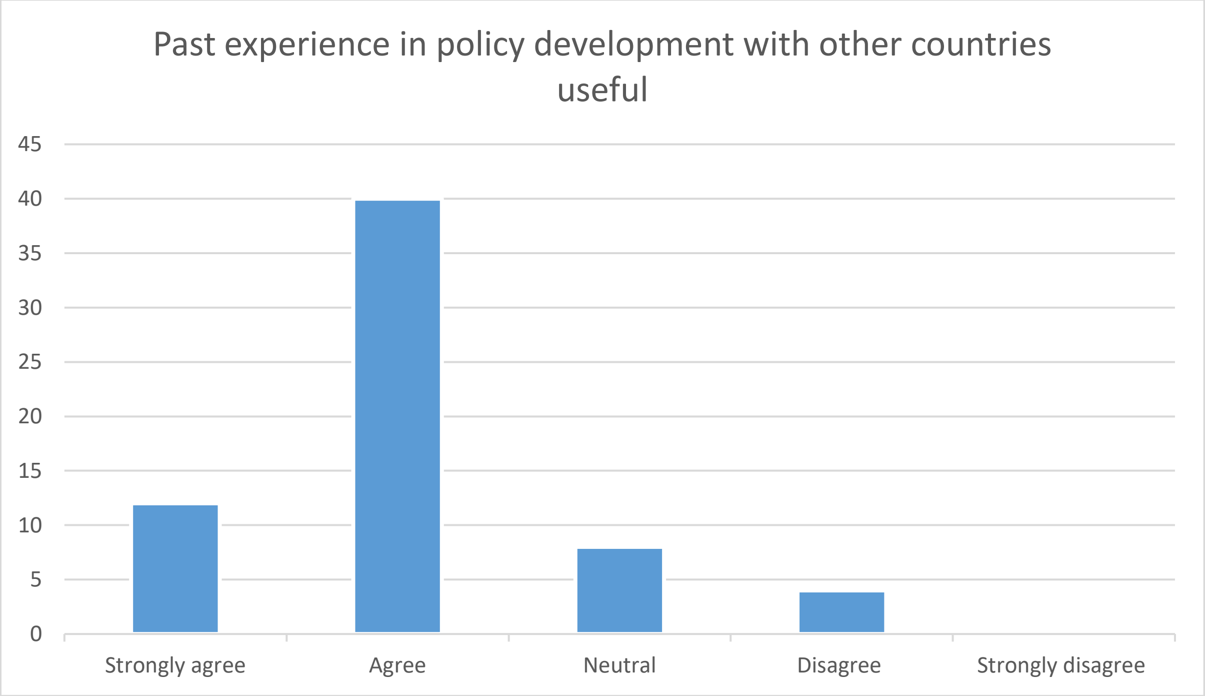


Figure E.15: Past experience in policy development with other countries useful (Male-UK)

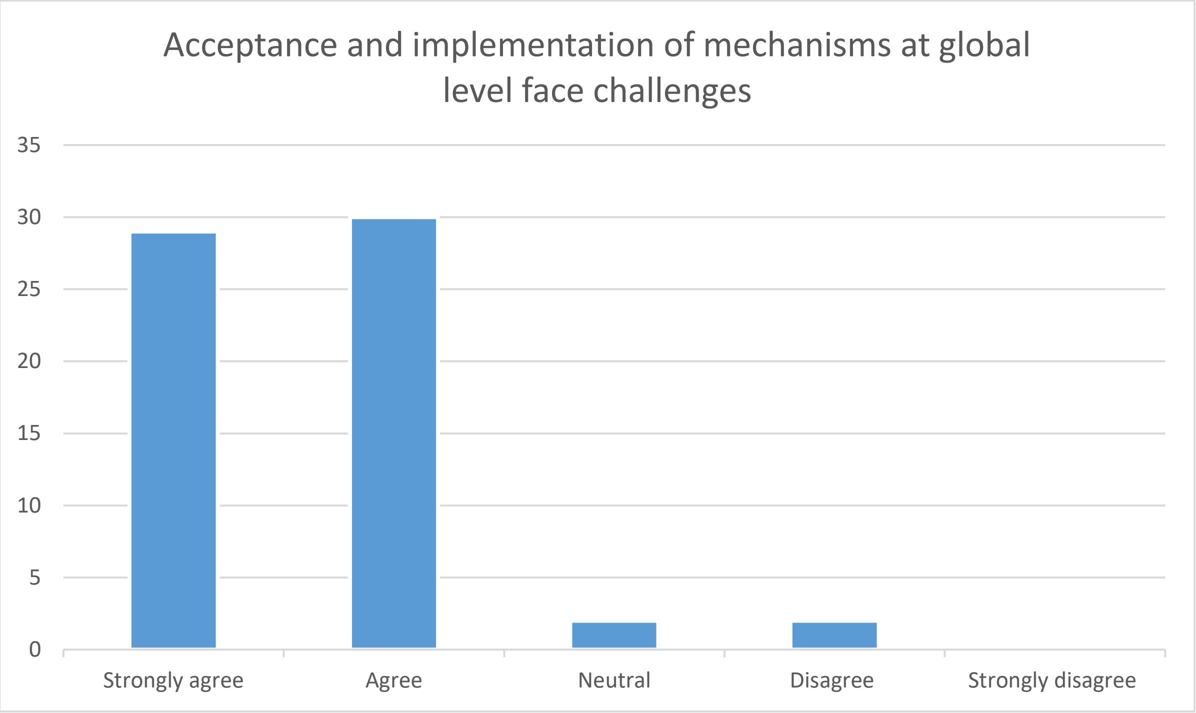


Figure E.16: Acceptance and implementation of mechanisms at global level face challenges (Male-UK)

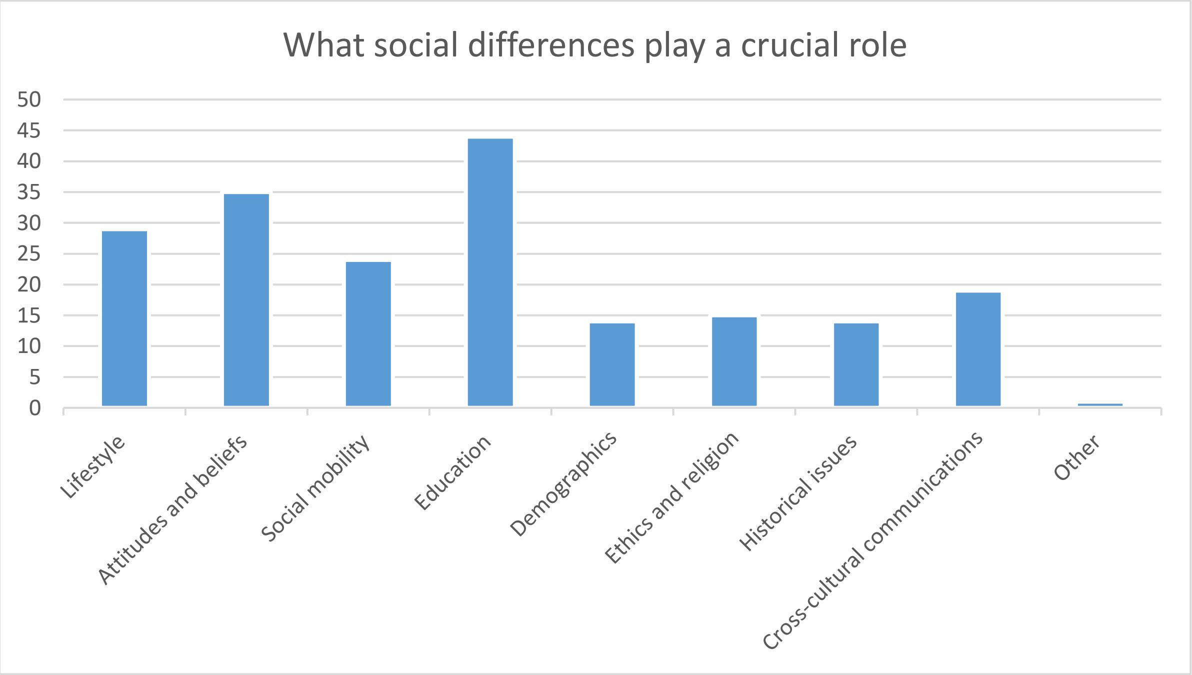


Figure E.17: What social differences play a crucial role (Male-UK)

The response to the social differences listed in the questionnaire, majority has highlighted the importance of education (See figure E.17). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level.

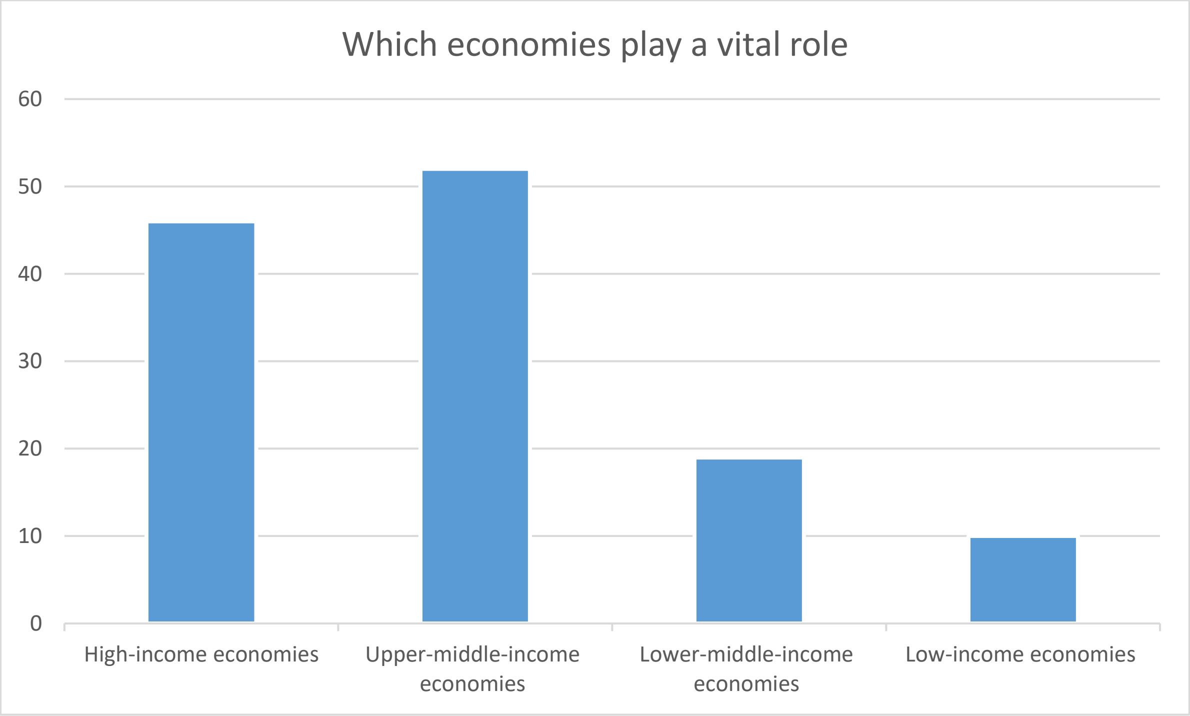


Figure E.18: Which economies play a vital role (Male-UK)

In the questionnaire majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.18). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

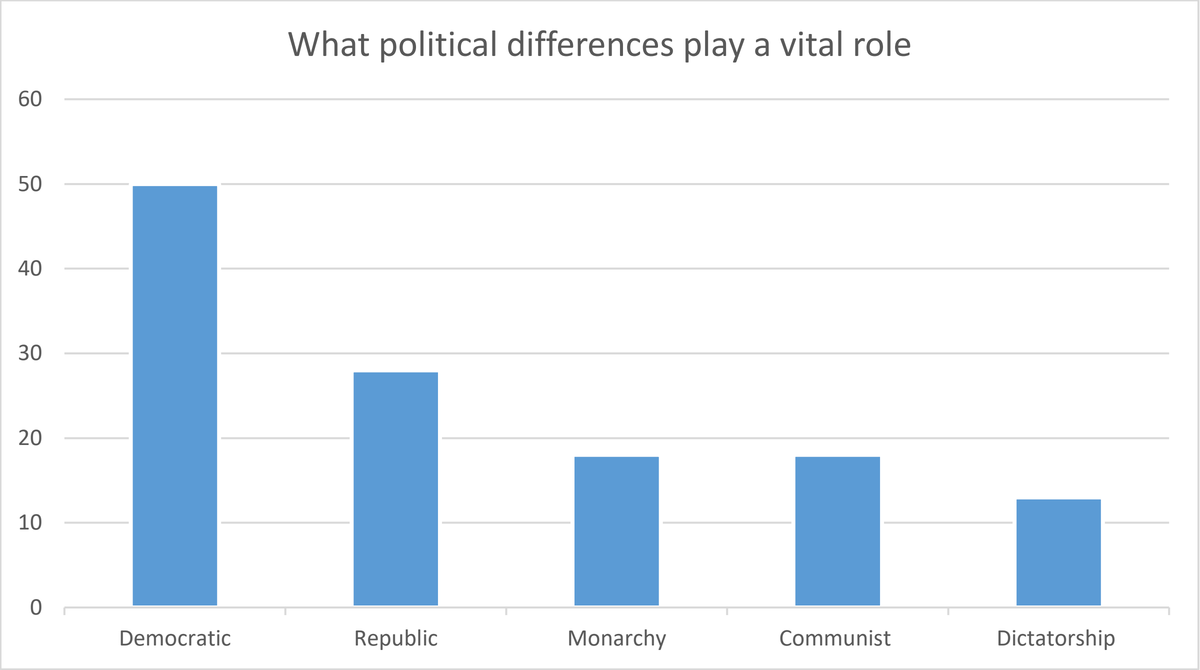


Figure E.19: What political differences play a vital role (Male-UK)

The majority have chosen democratic political system (See figure E.19), in preference to others as because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

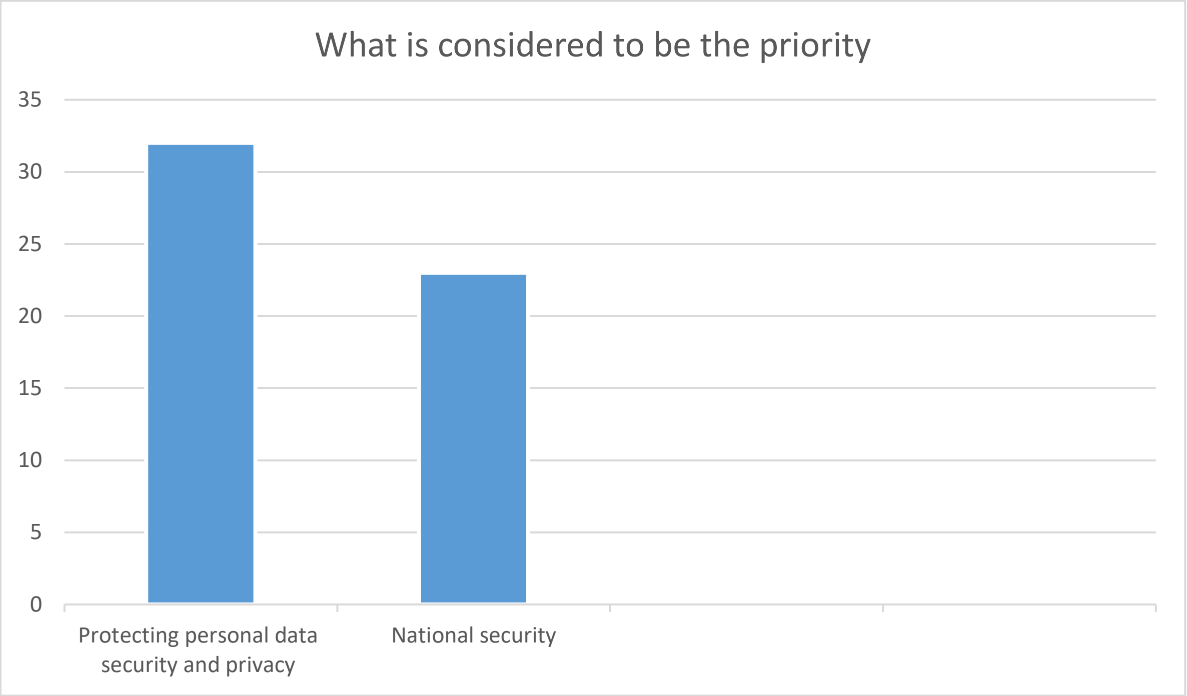


Figure E.20: What are the considered priorities (Male-UK)

The majority not considered either the importance of protection of personal data security and privacy or protection of national security, in accepting and implementing a global data privacy and security policies (See figure E.20). However, in an incident of a personal data breach, there will potentially be a knock-on effect on both personal data security and privacy, and national security, and it will also be felt right across the groups as well as the community alike.

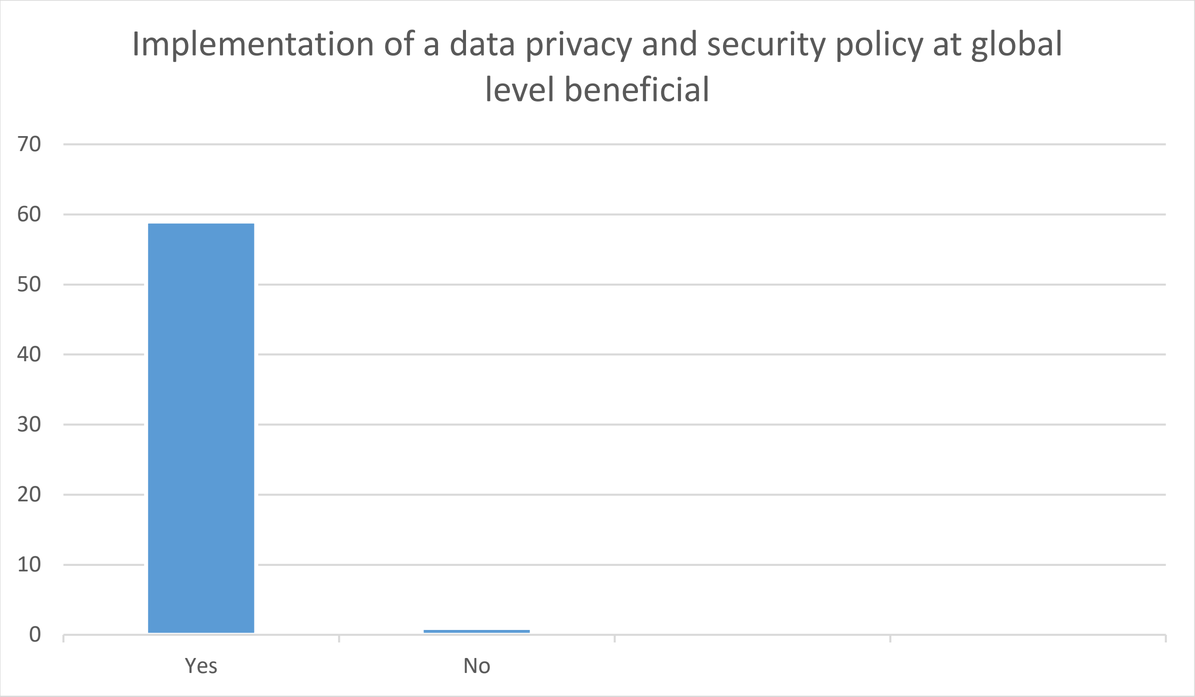


Figure E.21: Implementation of a data privacy and security policy at global level beneficial (Male-UK)

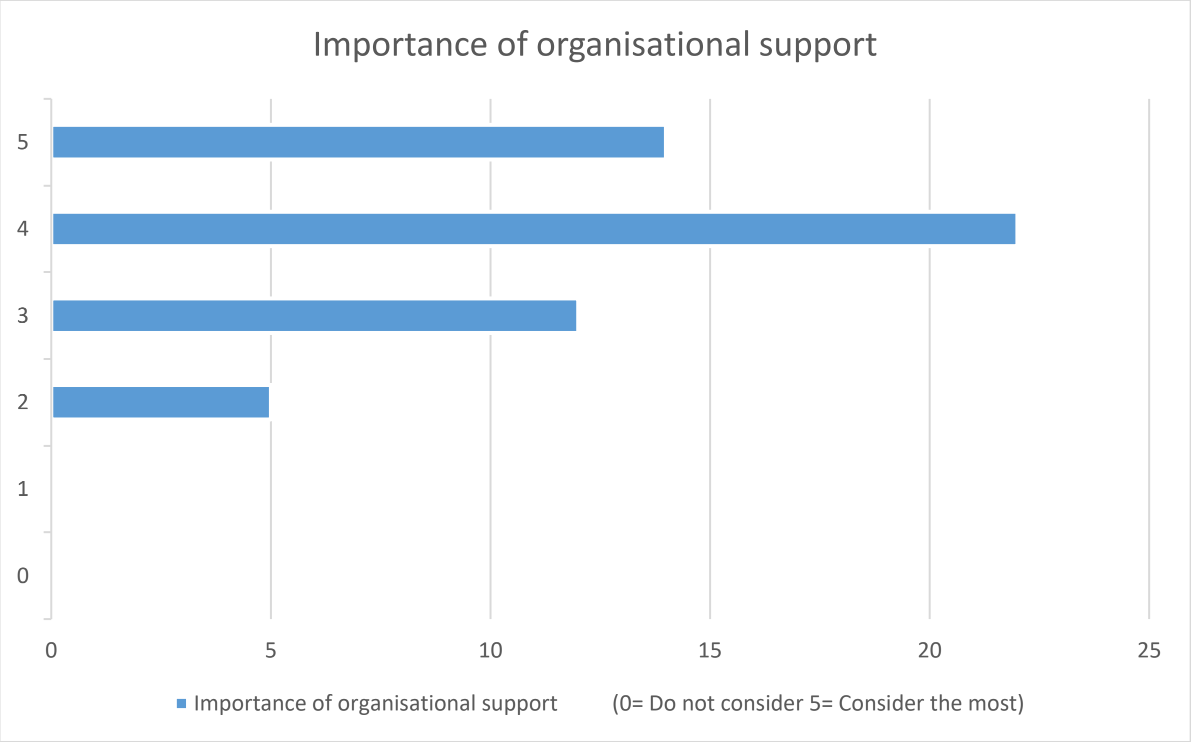


Figure E.22: Importance of organisational support (Male-UK)

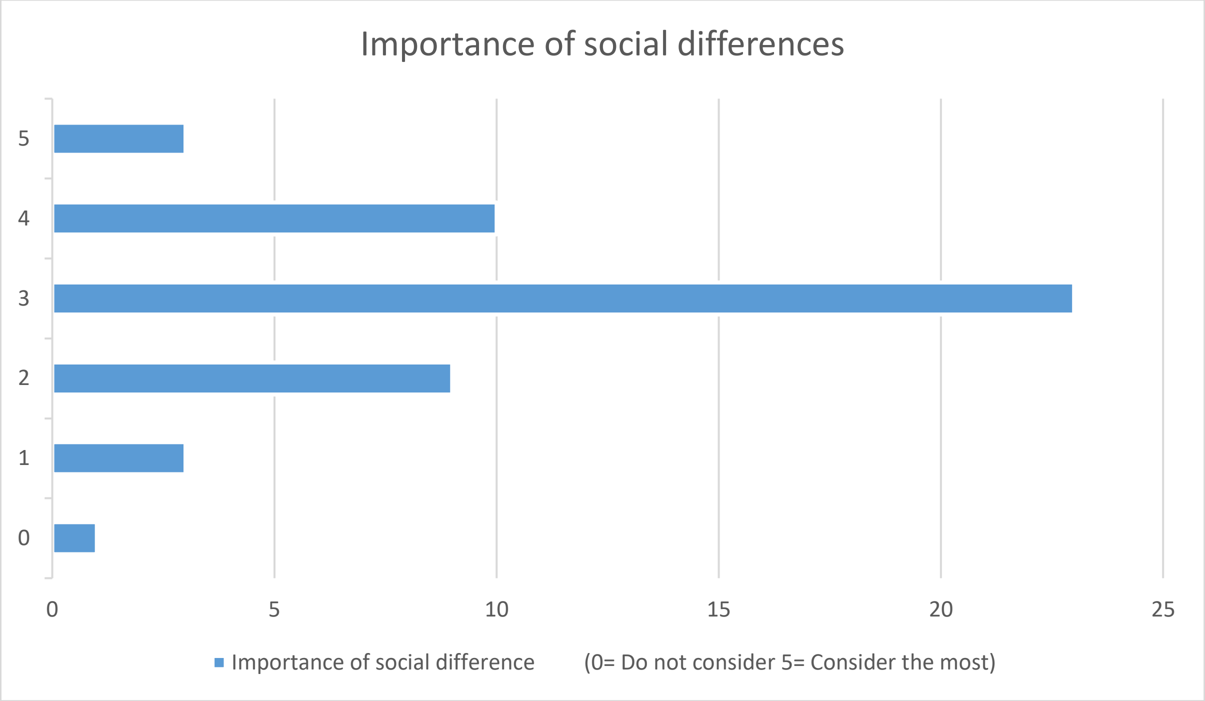


Figure E.23: Importance of social differences (Male-UK)

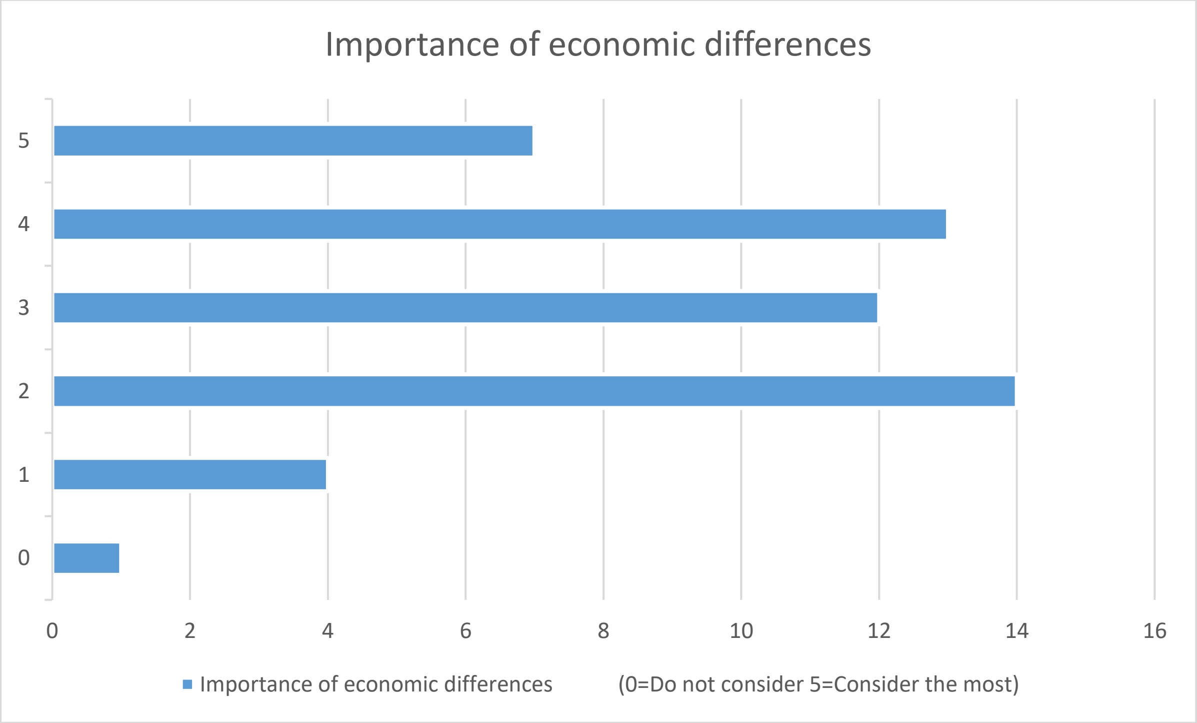


Figure E.24: Importance of economic differences (Male-UK)

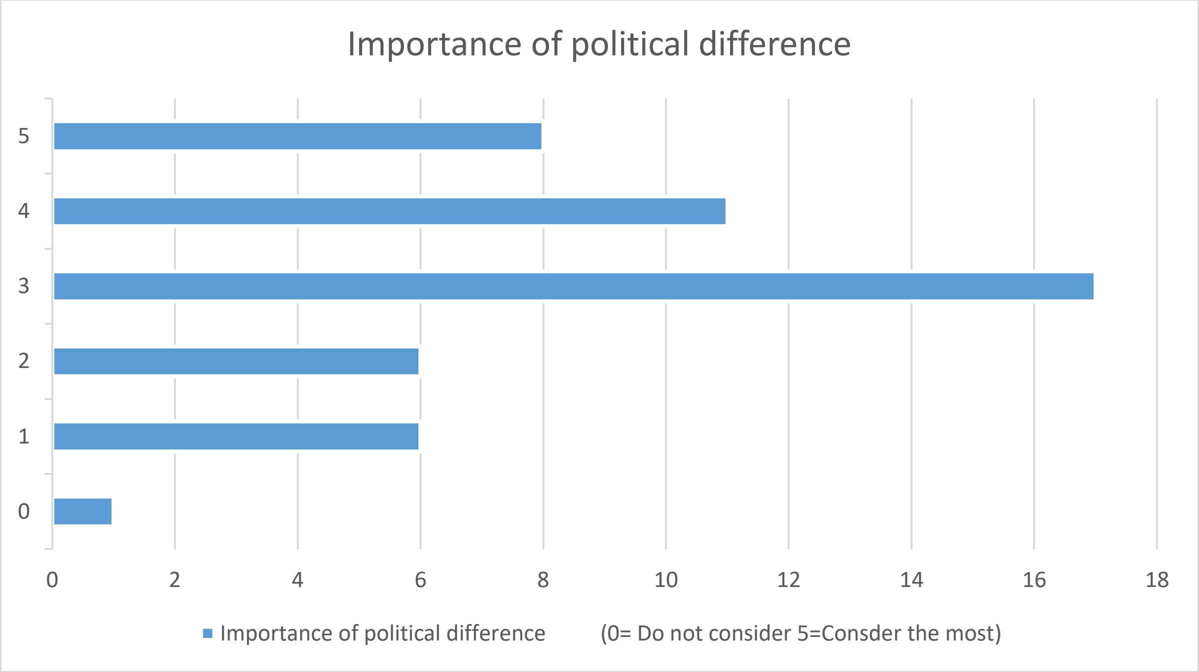


Figure E.25: Importance of political difference (Male-UK)

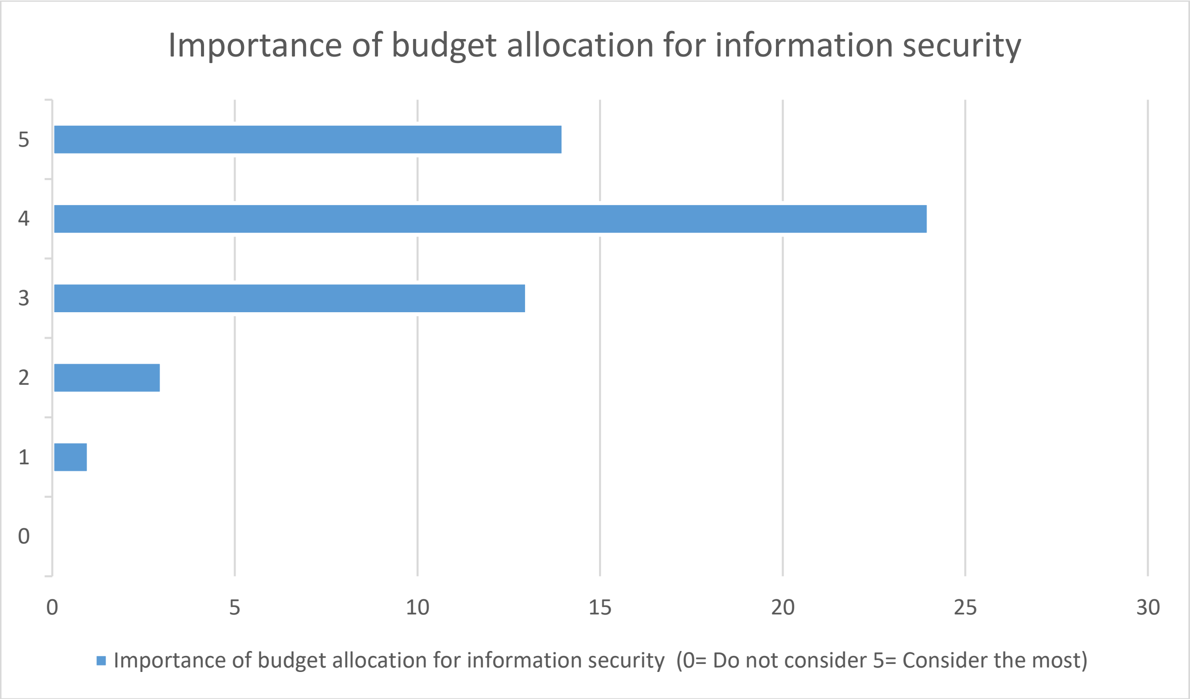


Figure E.26: Importance of budget allocation for information security (Male-UK)

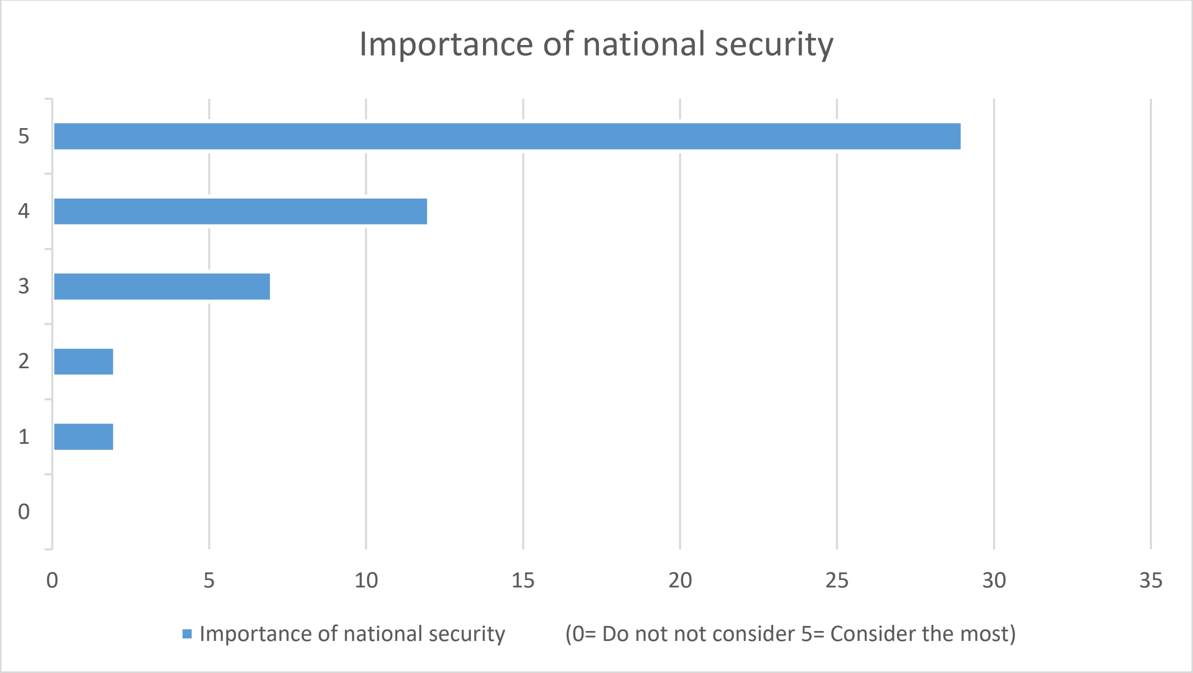


Figure E.27: Importance of national security (Male-UK)

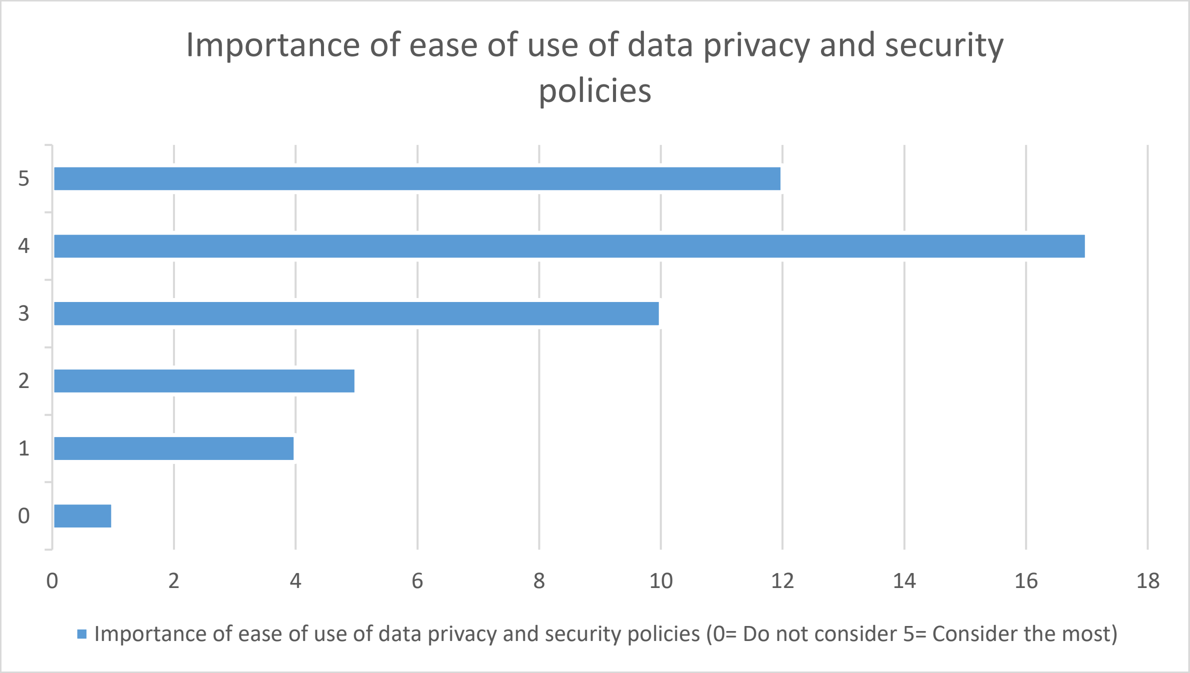


Figure E.28: Importance of ease of use of data privacy and security policies (Male-UK)

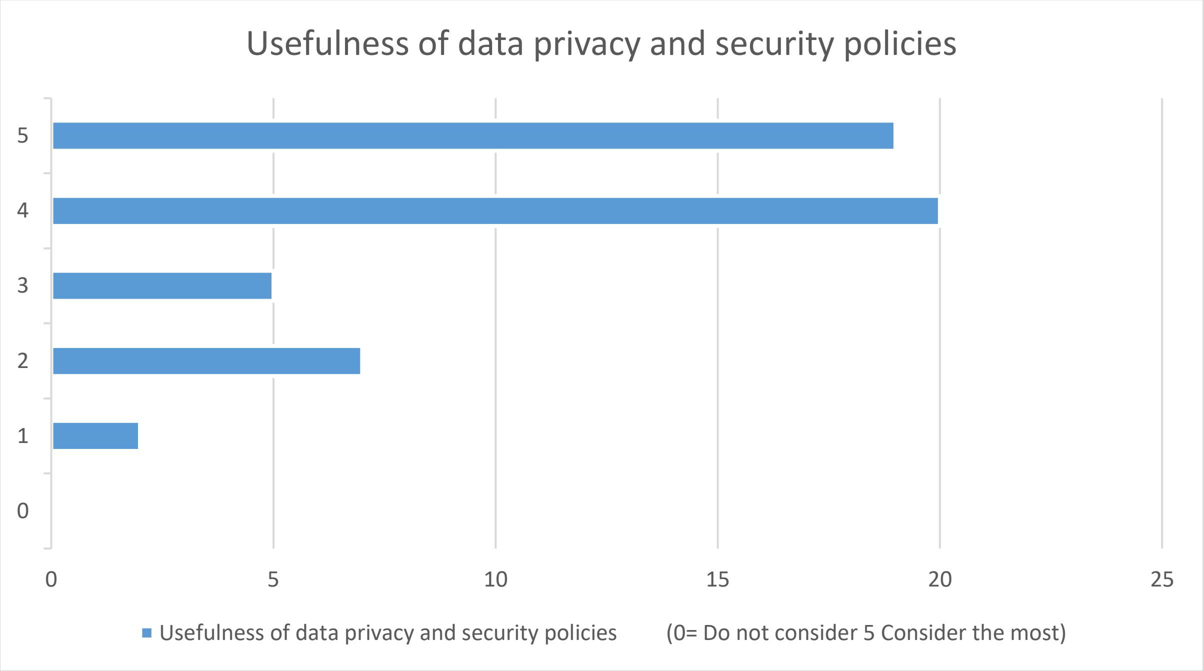


Figure 4.29: Usefulness of data privacy and security policies (Male-UK)

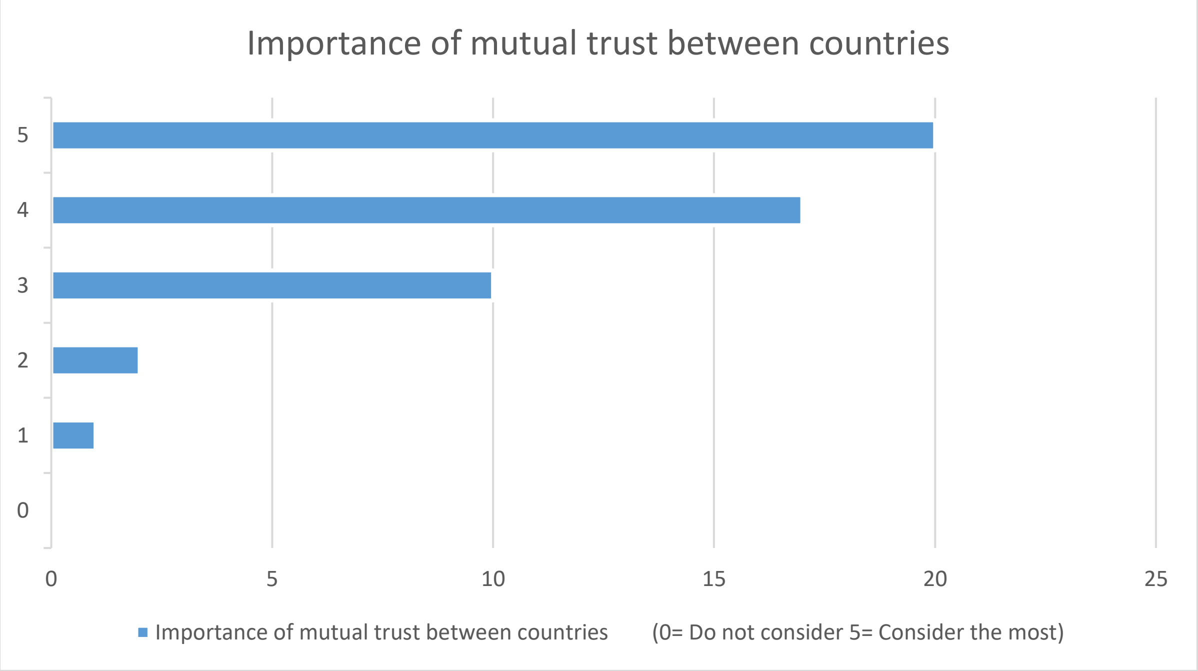


Figure E.30: Importance of mutual trust between countries (Male-UK)

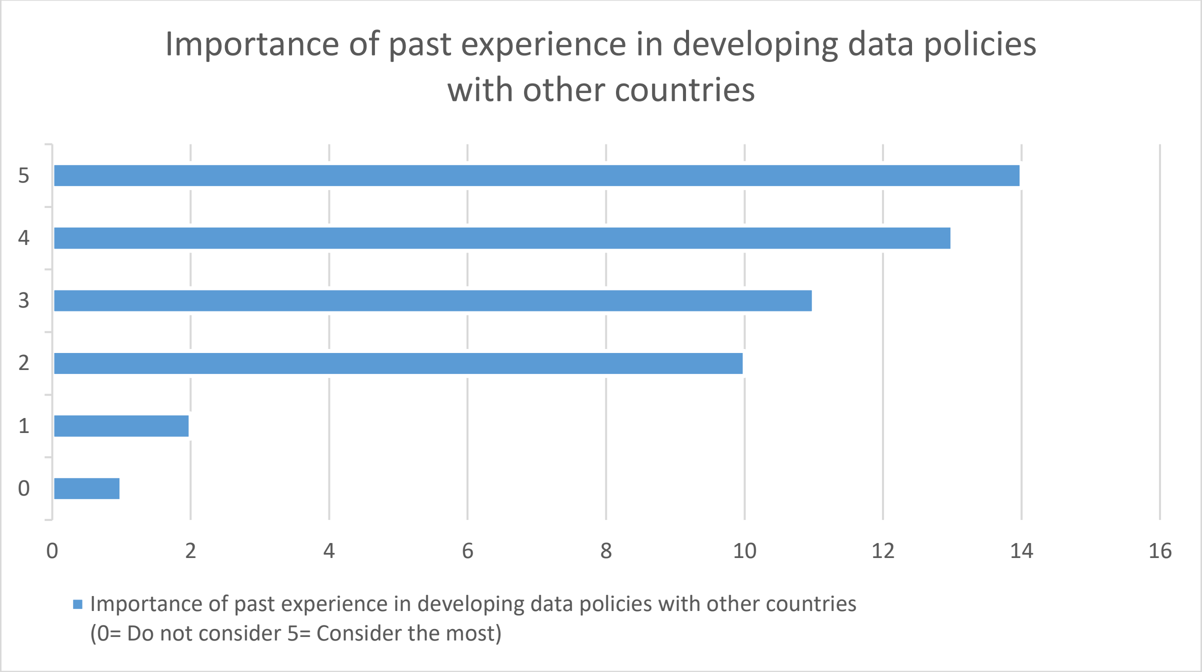


Figure E.31: Importance of past experience in developing data policies with other counties (Male- UK)

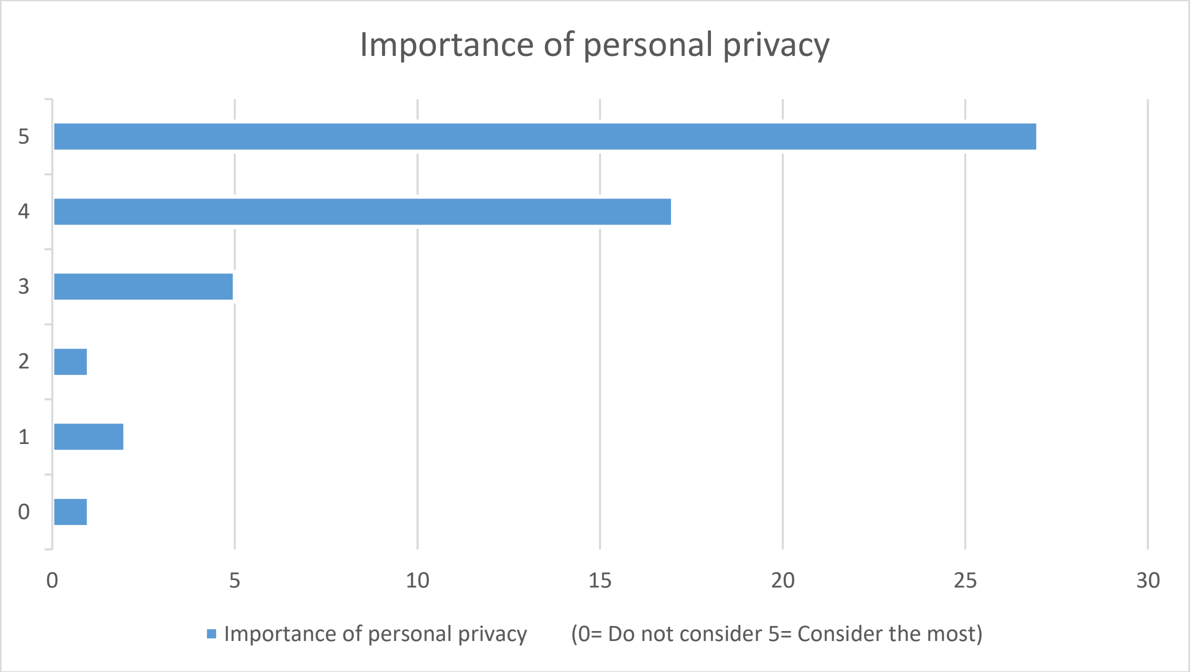


Figure E.32: Importance of personal privacy (Male-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 80 percent of the respondents have endorsed (See figure E.21). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure E.10-20) (See figure E.22-32)

United Kingdom - Female

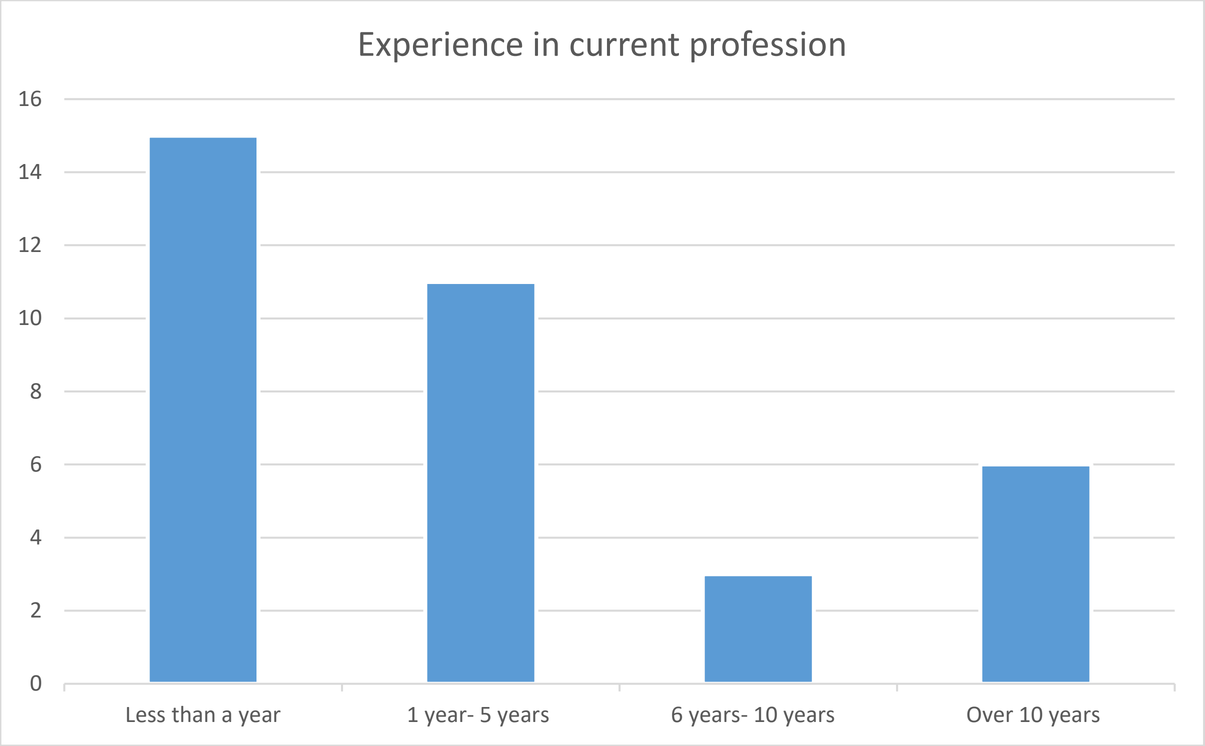


Figure E.33: Experience in current profession (Female-UK)

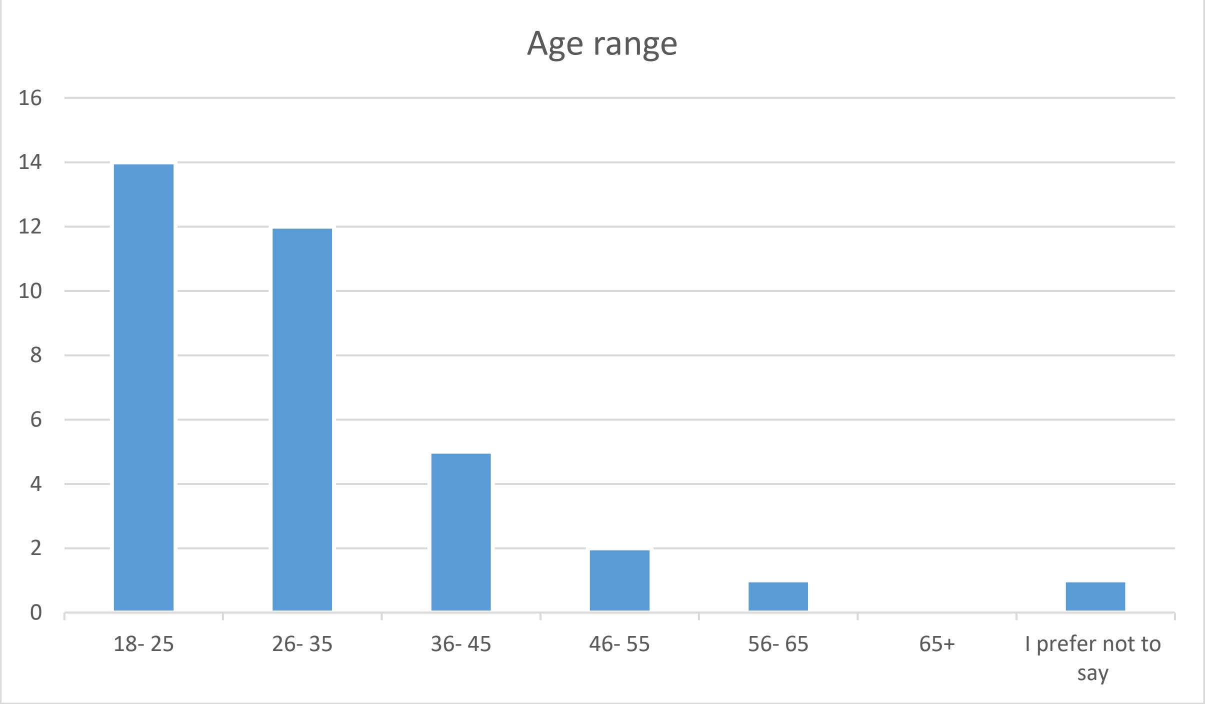


Figure E.34: Age range (Female-UK)

This analysis is based on the responses received from United Kingdom female participants. They were within the 18-65 age range out of which 14 in the 18-25, 12 in the 26-35, and 5 in the 36-45, 2 in the 46-55, and 1 in the 56-65 range (See figure E.34). The participants employed in industry between less than a year and over 10 years (See figure E.33).

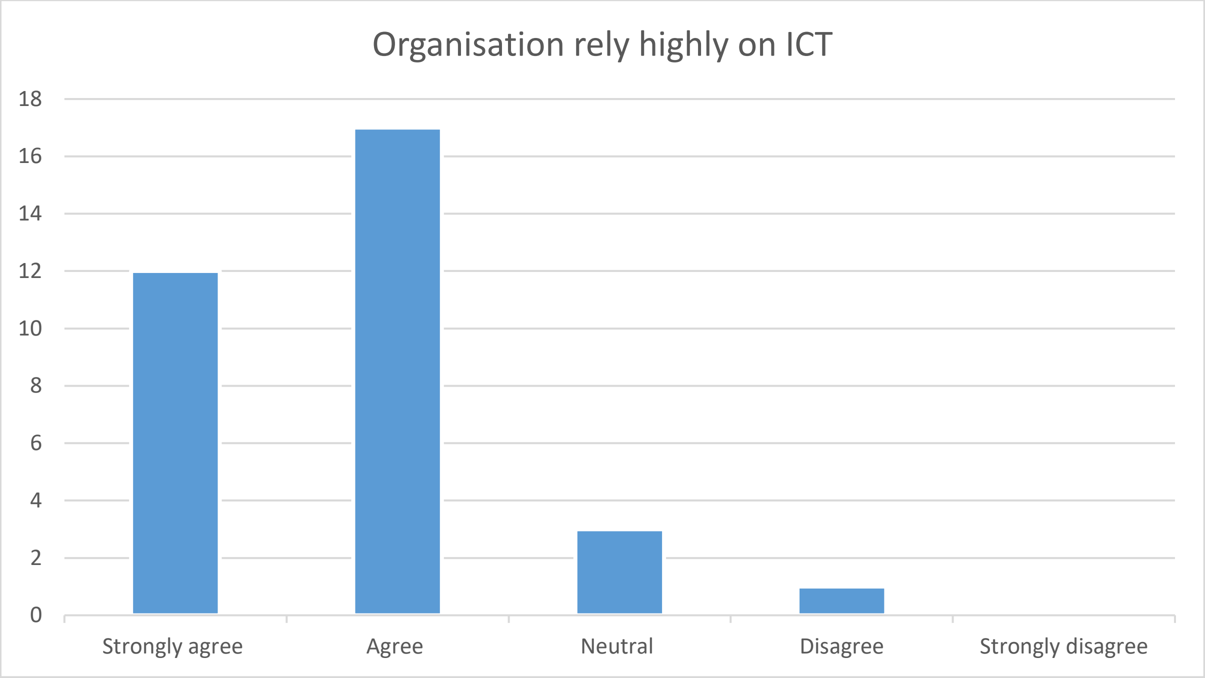


Figure E.35: Organisation rely highly on ICT (Female-UK)

Out of the 35 respondents, 29 have worked in a technology reliance working environment, 3 unaware of reliance on technology because of the nature of the work assigned to them, 1 have marked ‘disagree’ on ICT (See figure E.34). This indicates a majority of females have had a high reliance on ICT.

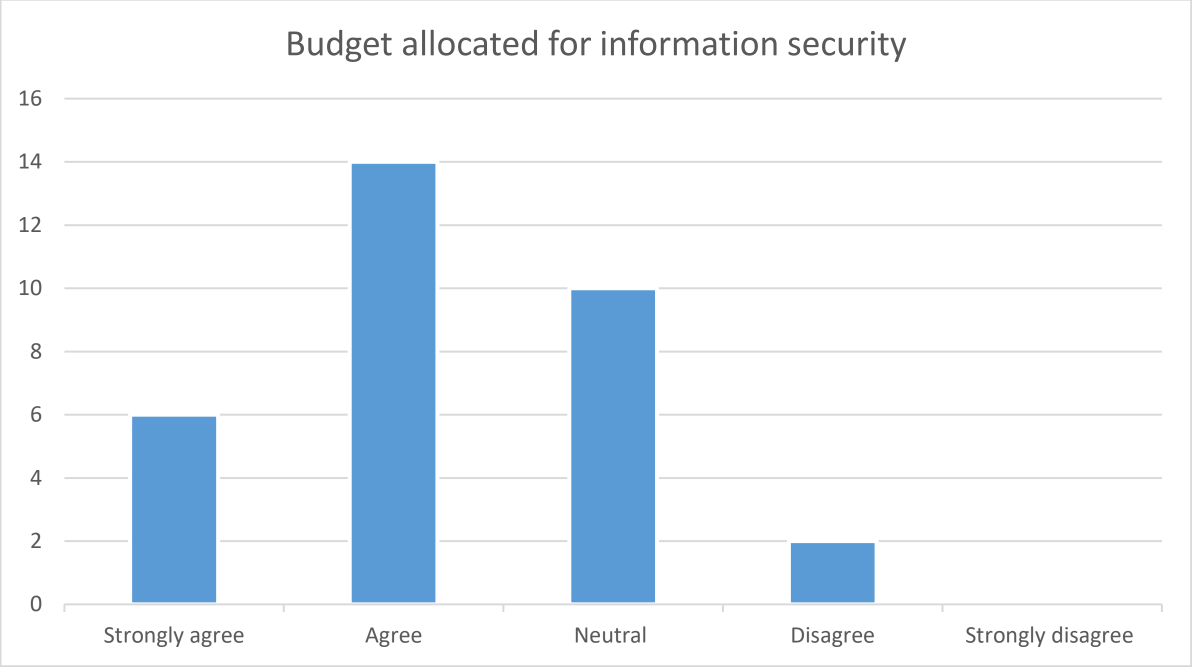


Figure E.36: Budget allocated for information security (Female-UK)

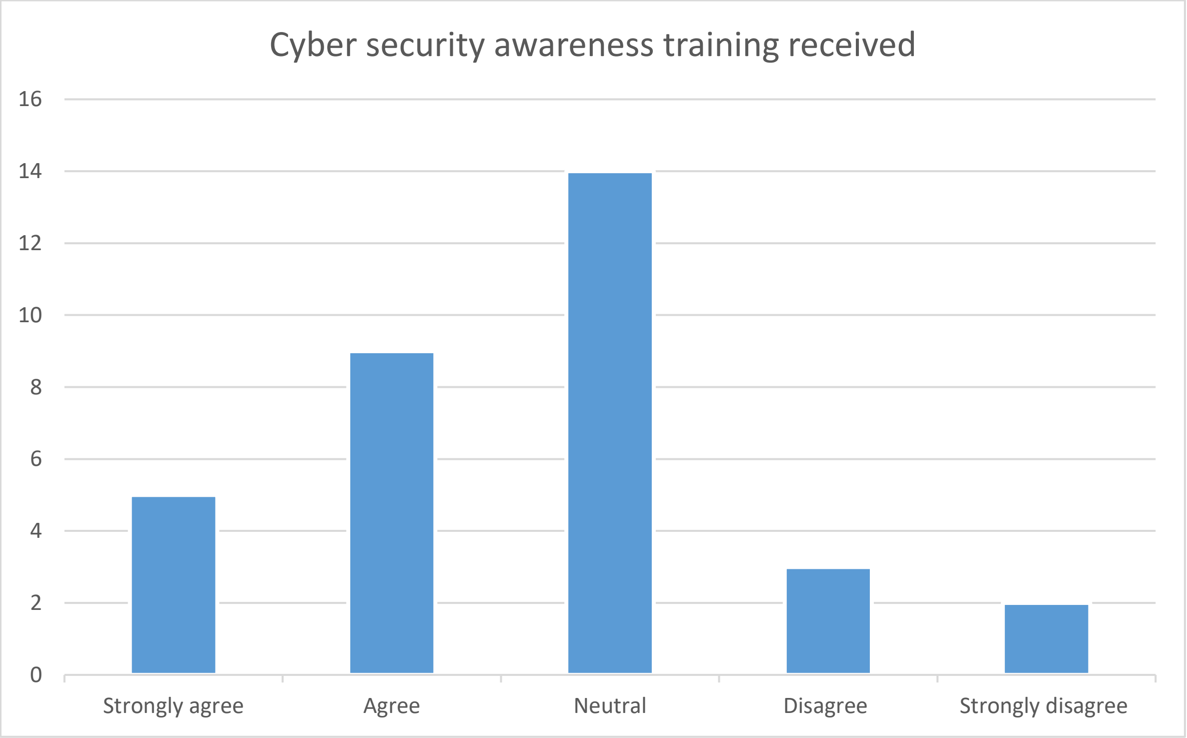


Figure E.37: Cyber security awareness training received (Female-UK)

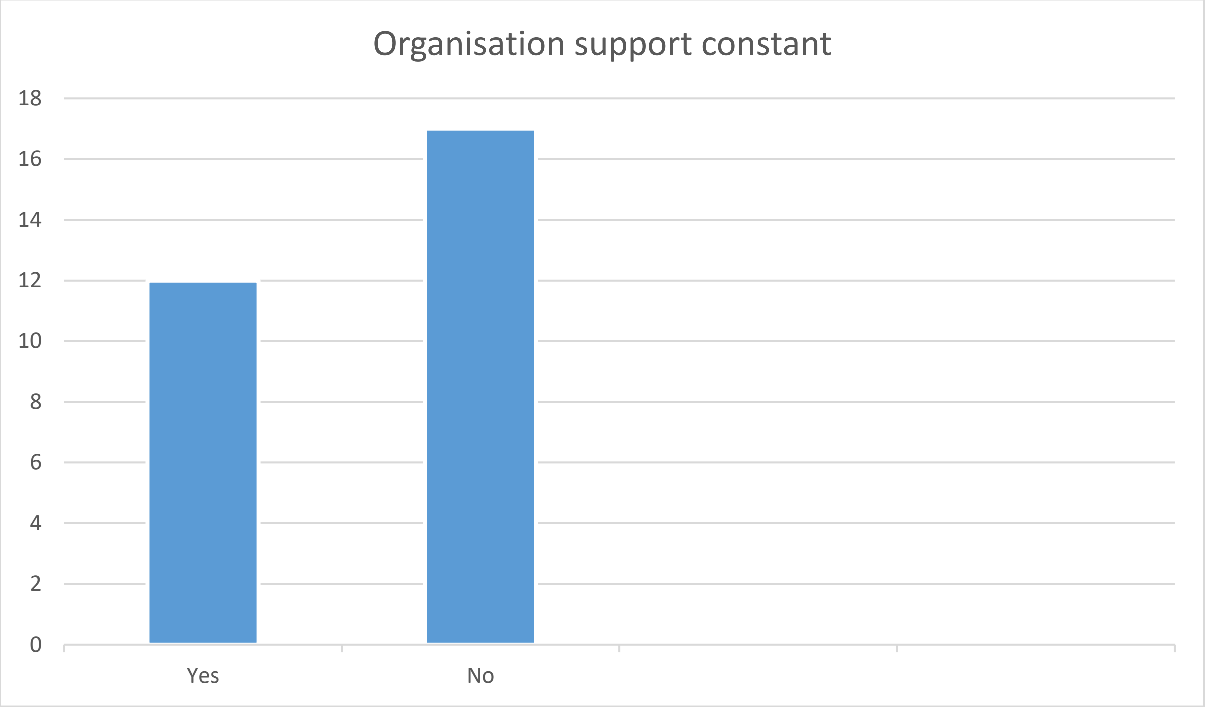


Figure E.38: Organisation support constant (Female-UK)

Funding has been sketchy. 20 out of the 35 have indicated that their organisations had an allocated budget for information security, whilst 10 had not expressed an opinion either way and notably according to the 2 disagreed, their organisations had no budget allocation for information security (See figure E.36). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 14 participants have received regular cybersecurity awareness training, whilst 14 neither agreed nor disagreed, and 5 participants had not regularly received security awareness training (See figure E.37). In addition, 17 participants had not received support from the organisation to protect personal information, whilst only 12 did (See figure E.38). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

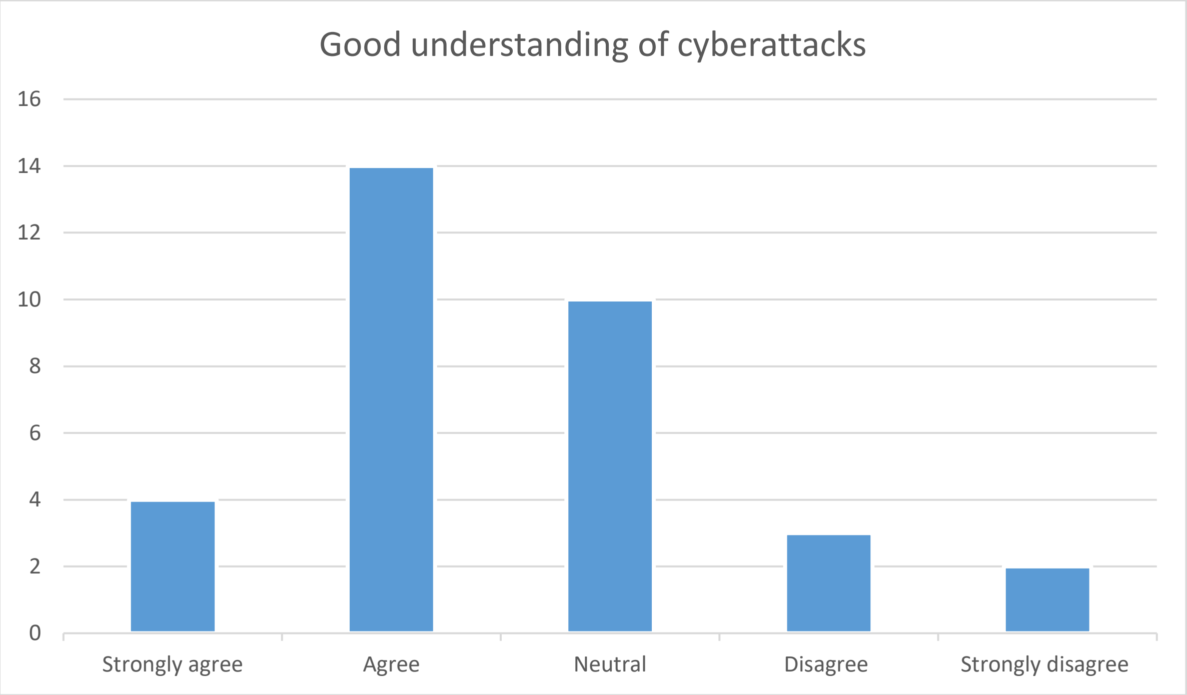


Figure E.39: Good understanding of cyberattacks (Female-UK)

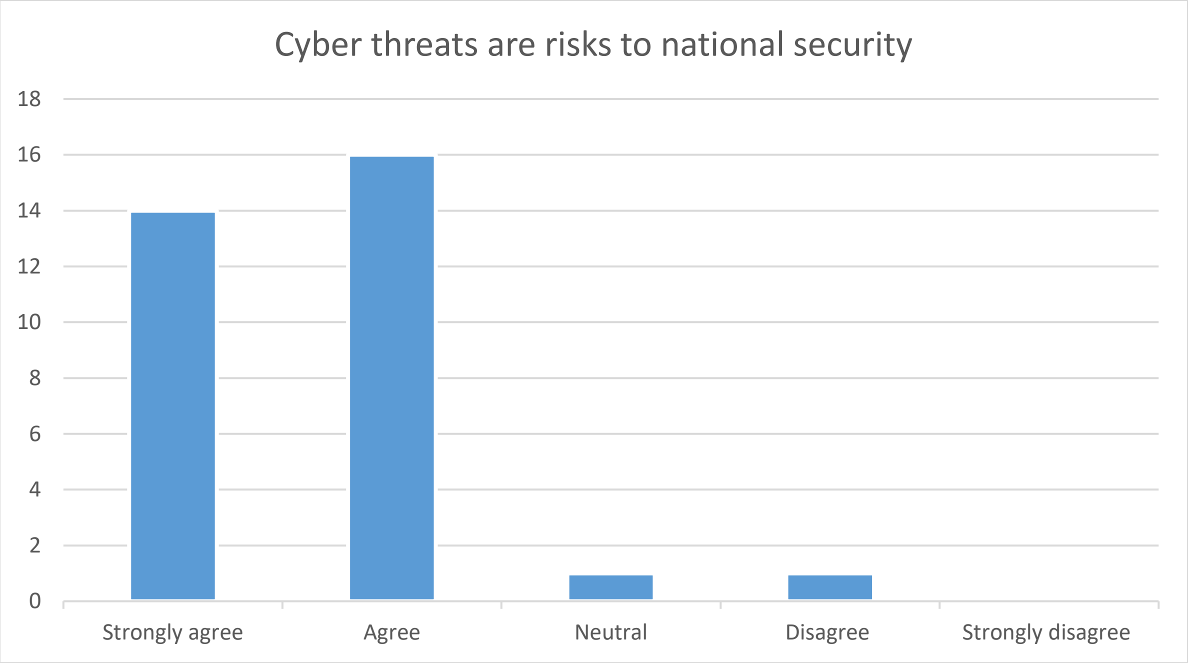


Figure E.40: Cyber threats are risks to national security (Female-UK)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 18 participants do have, 10 have not expressed opinion either way, and only 5 participants had no understanding (See figure E.39). Furthermore, 86 percent of the participants realises the potential threats to national security from cyber-attacks (See figure E.40). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

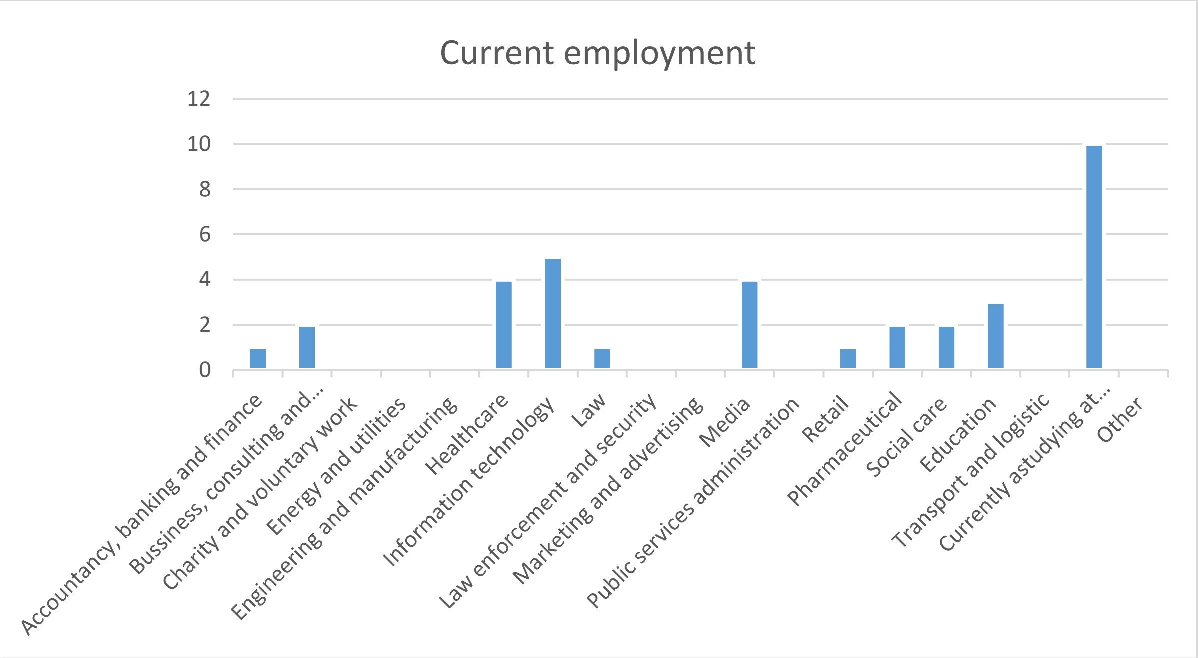


Figure E.41: Current employment (Female-UK)

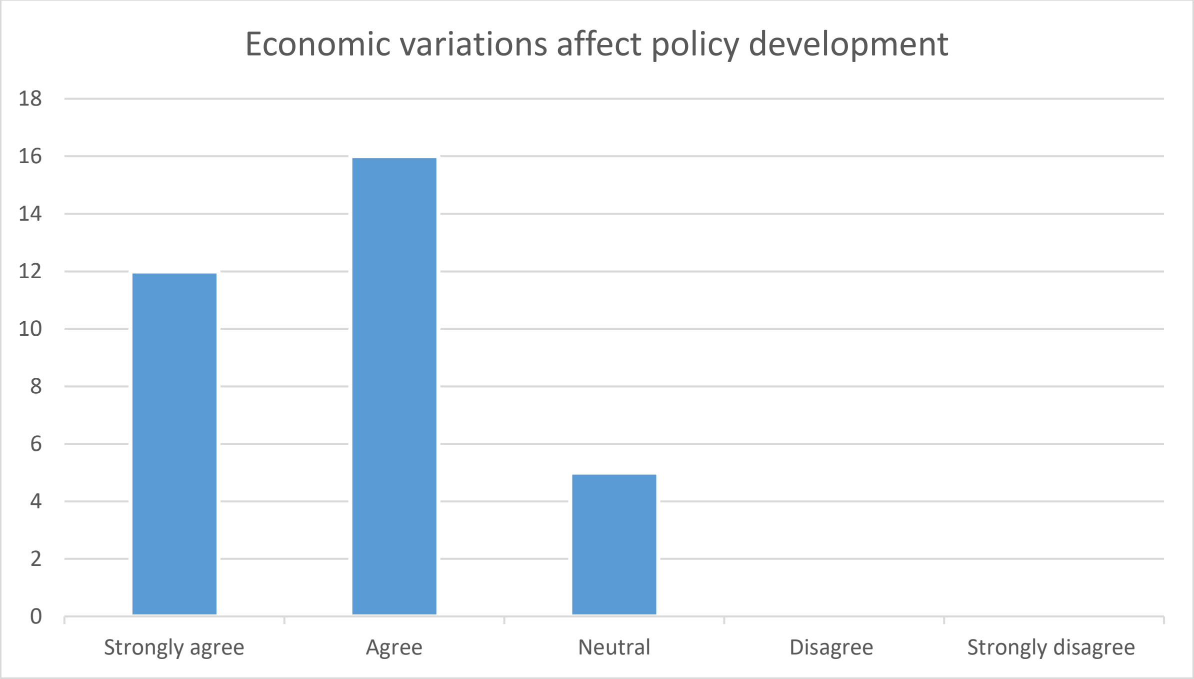


Figure E.42: Economic variations affect policy development (Female-UK)

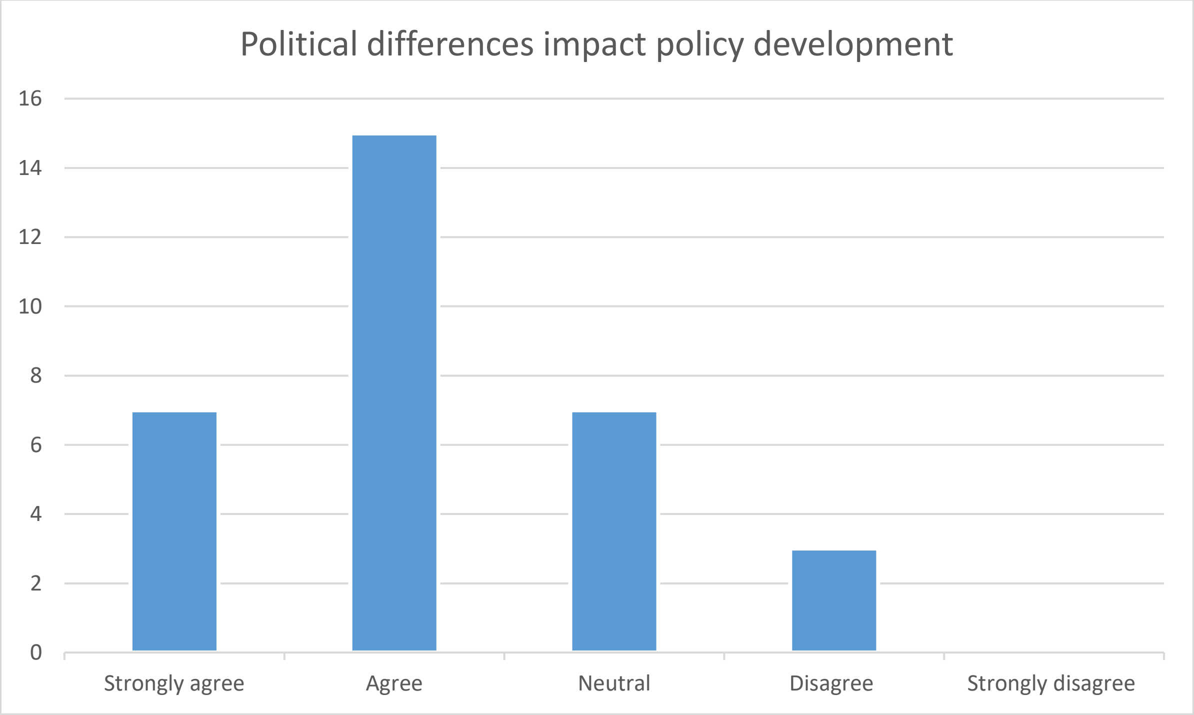


Figure E.43: Political differences impact policy development (Female-UK)

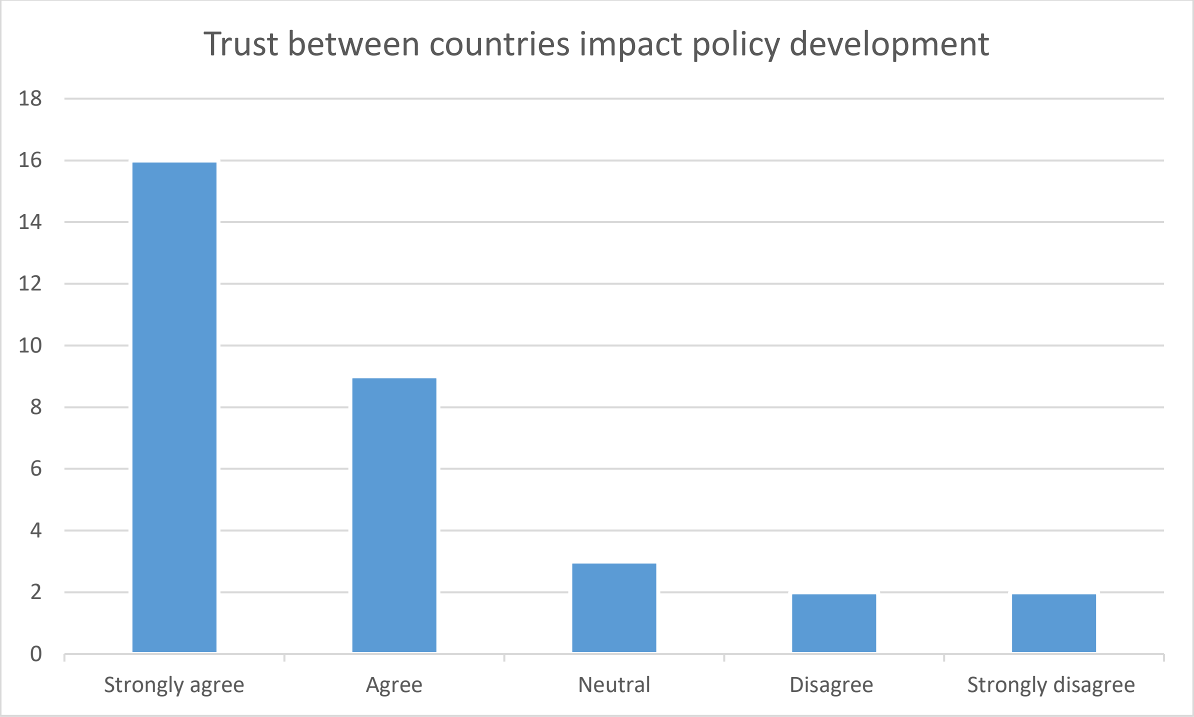


Figure E.44: Trust between countries impact policy development (Female-UK)

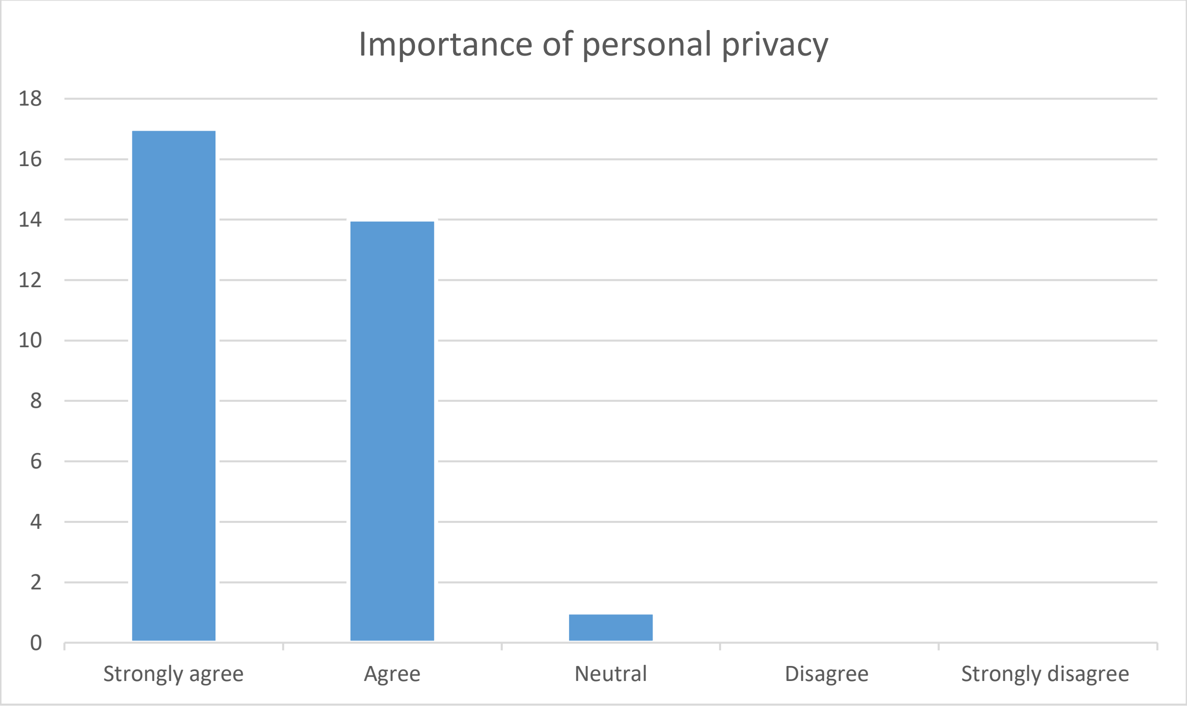


Figure E.45: Importance of personal privacy (Female-UK)

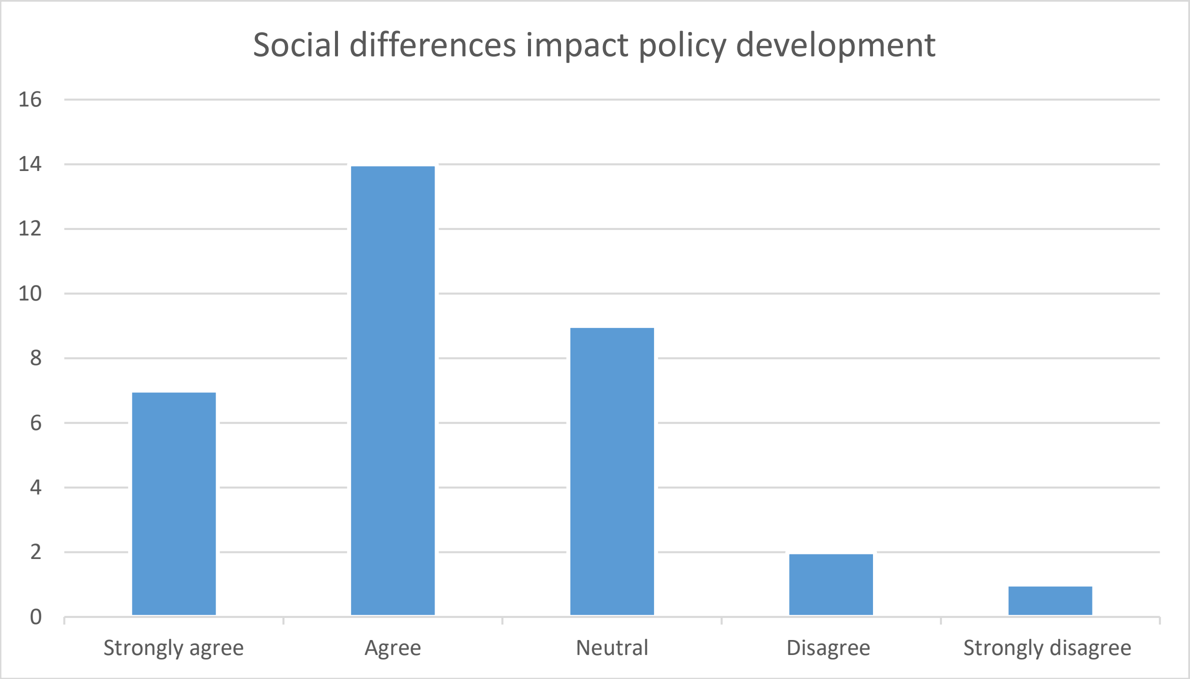


Figure E.46: Social differences impact policy development (Female-UK)

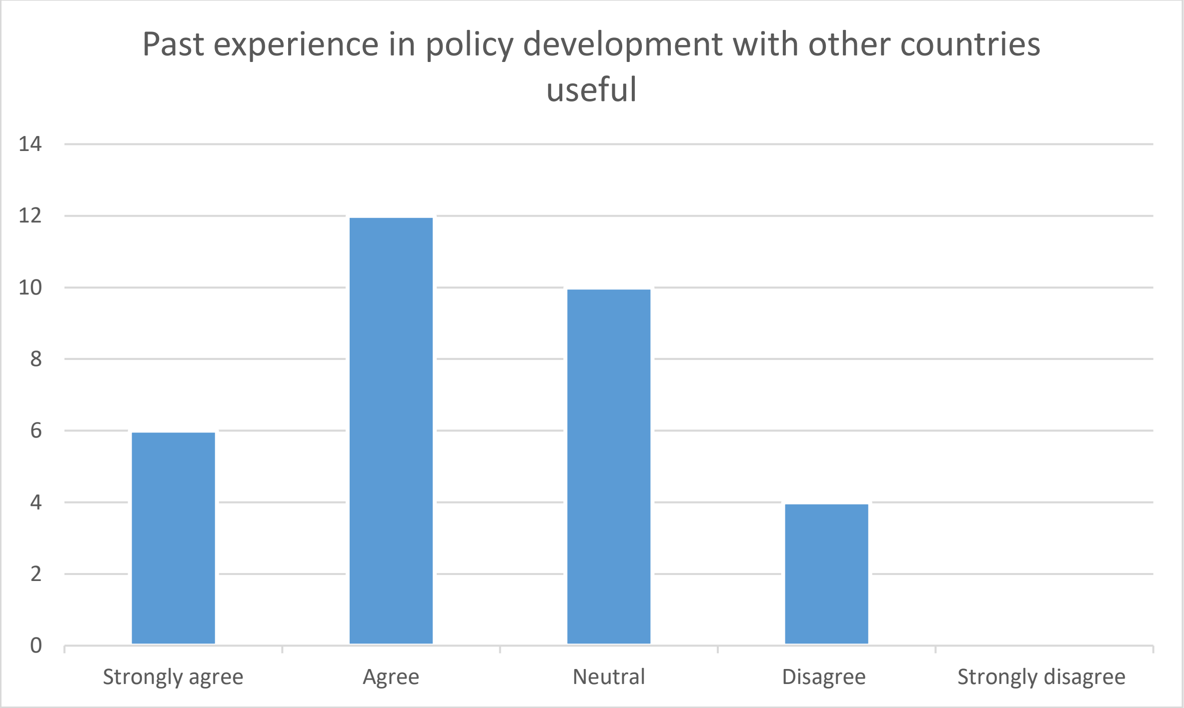


Figure E.47: Past experience in policy development with other countries useful (Female-UK)

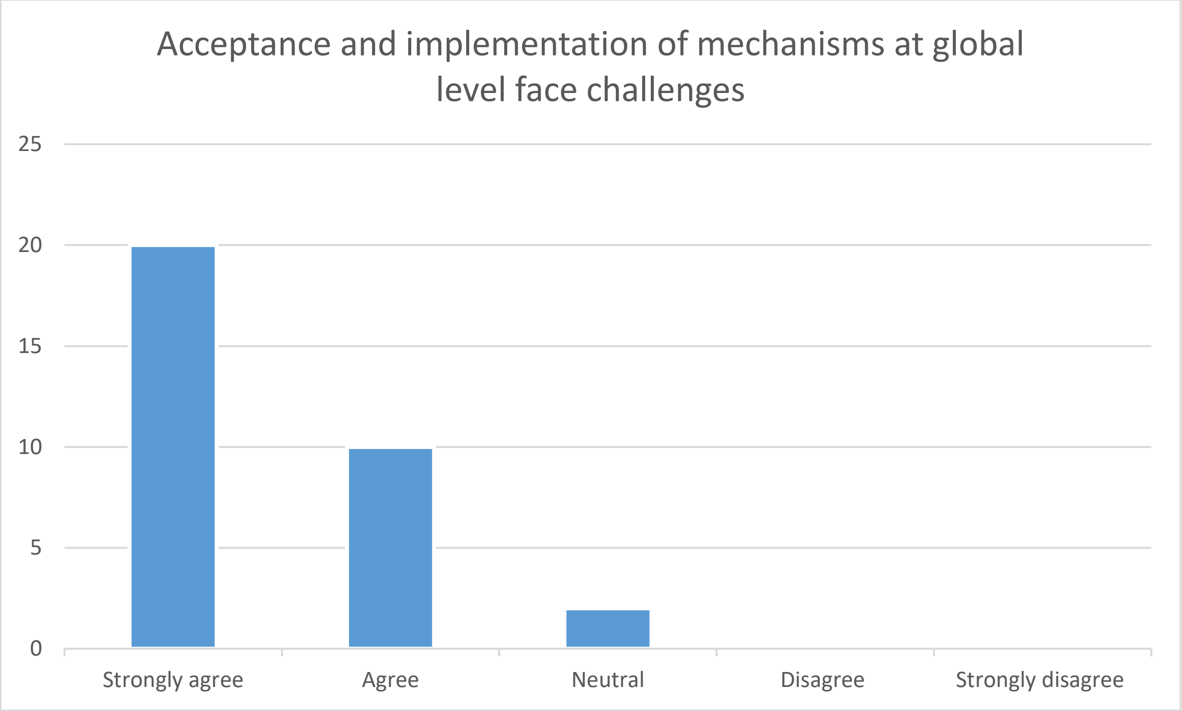


Figure E.48: Acceptance and implementation of mechanisms at global level face challenges (Female-UK)

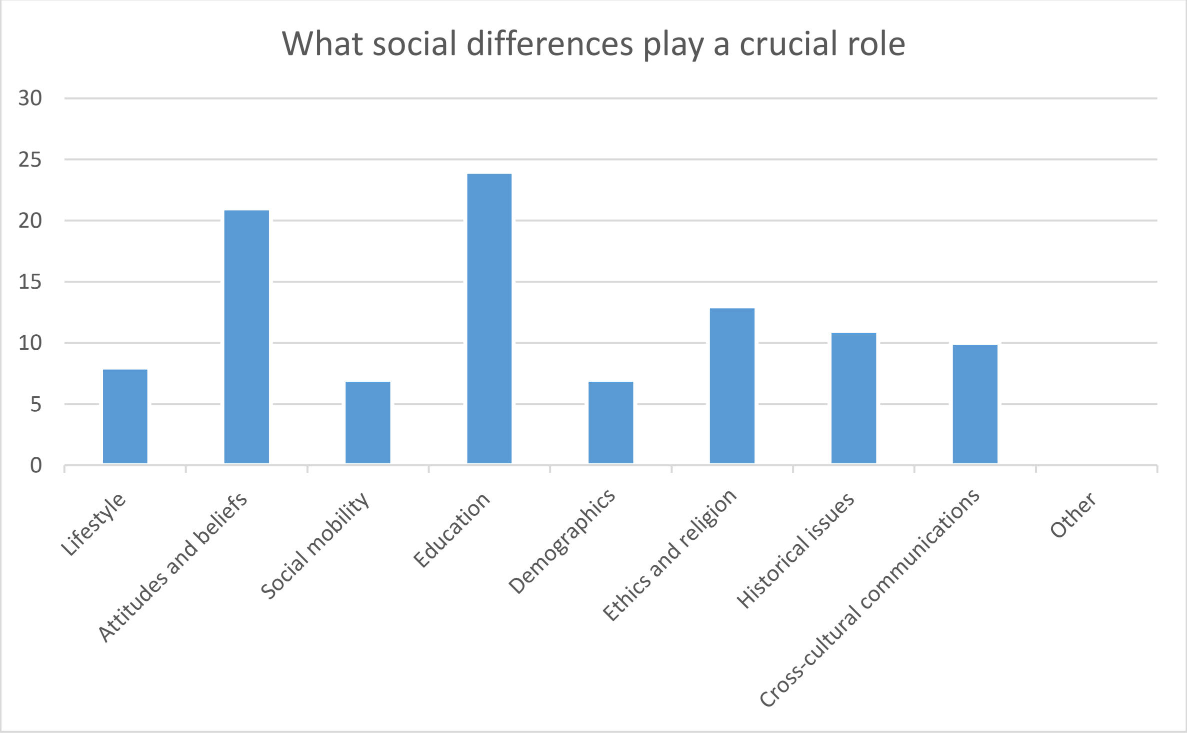


Figure E.49: What social differences play a crucial role (Female-UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure E.49). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

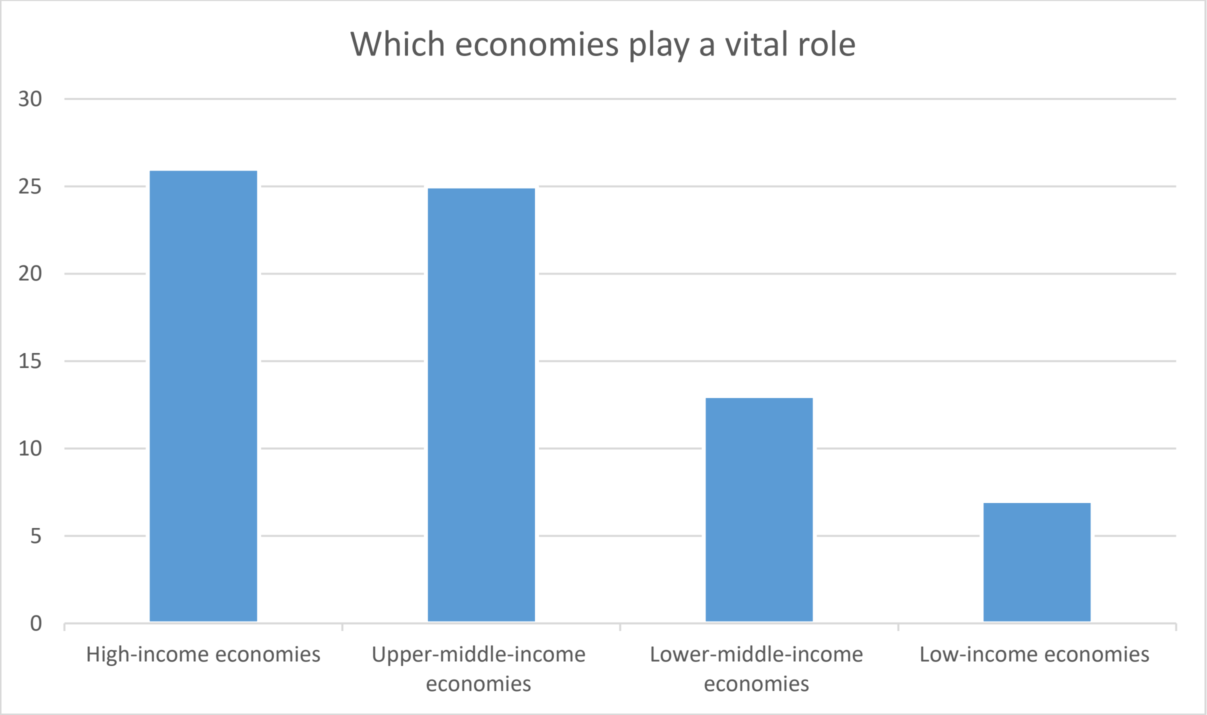


Figure E.50: Which economies play a vital role (Female-UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.50). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

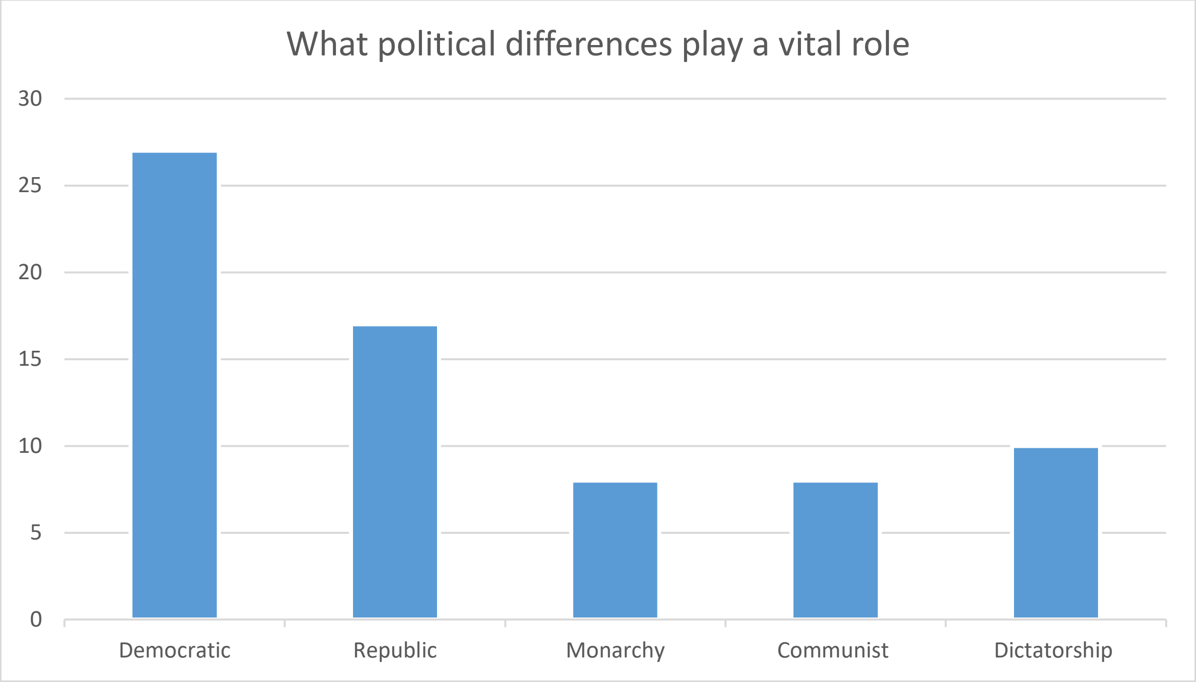


Figure 4.651: What political differences play a vital role (Female-UK)

The majority have chosen a democratic political system (See figure E.51), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

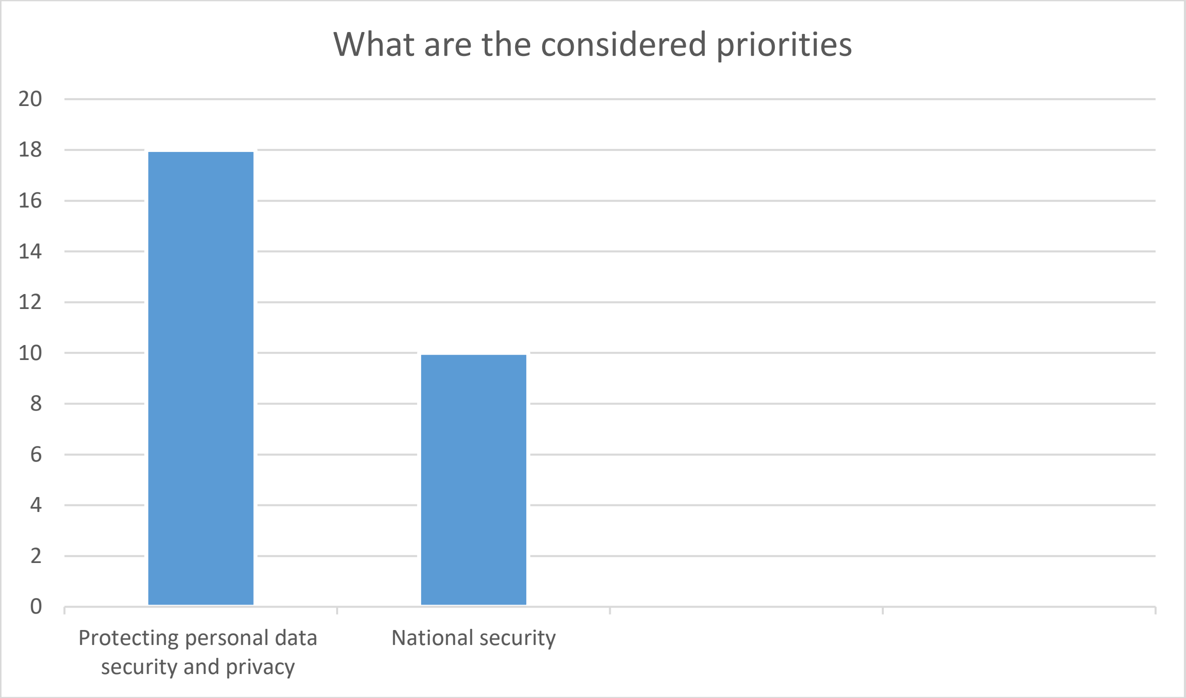


Figure E.52: What are the considered priorities (Female- UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security (See figure E.52), which is a significant factor. In an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

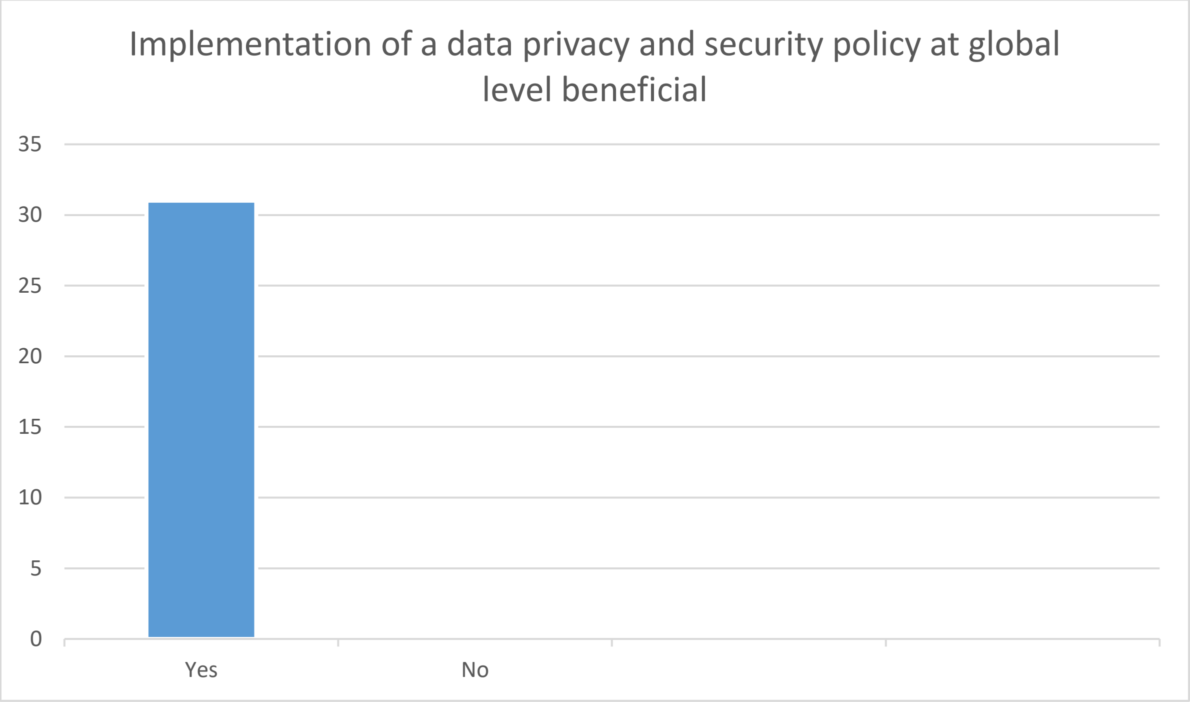


Figure E.53: Implementation of a data privacy and security policy at global level beneficial (Female-UK)

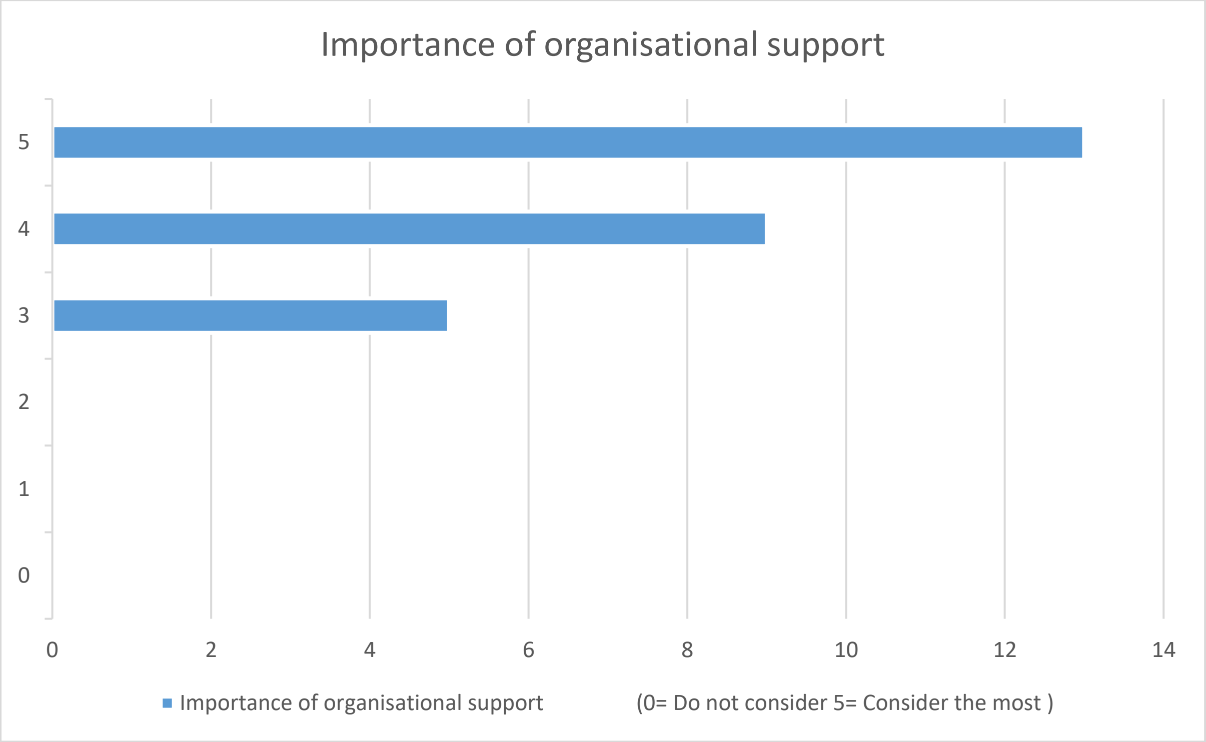


Figure E.54: Importance of organisational support (Female-UK)

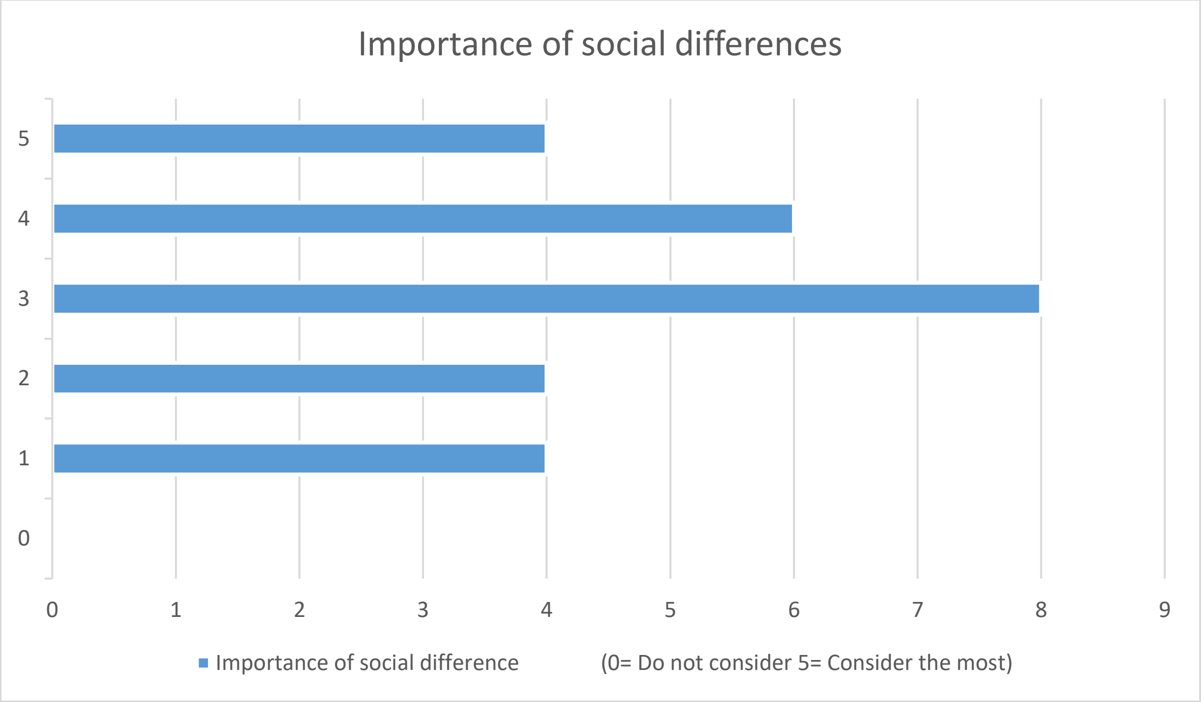


Figure E.55: Importance of social differences (Female-UK)

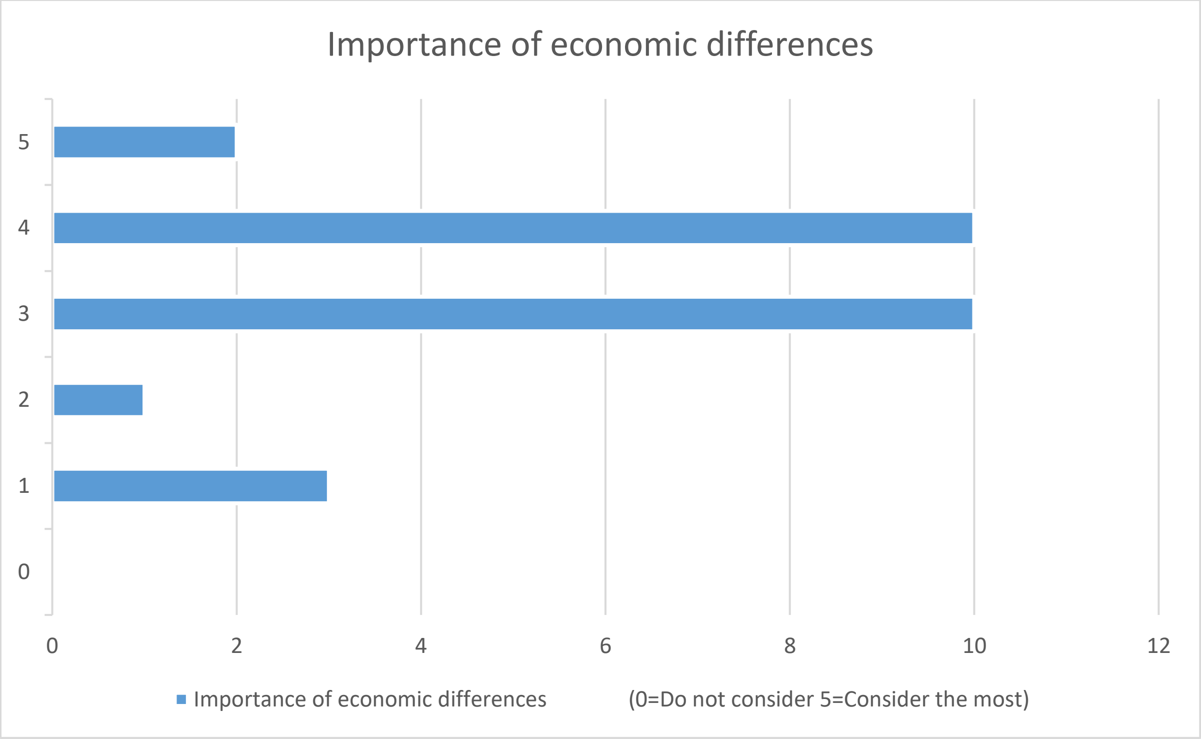


Figure E.56: Importance of economic differences (Female-UK)

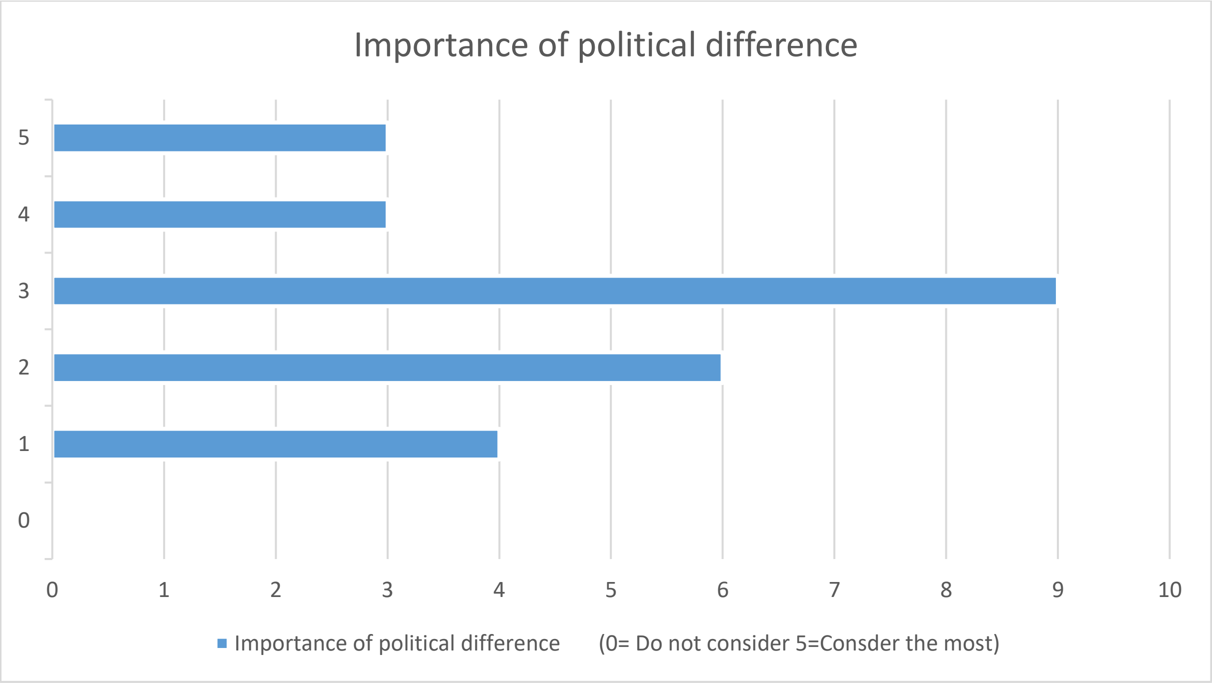


Figure E.57: Importance of political difference (Female-UK)

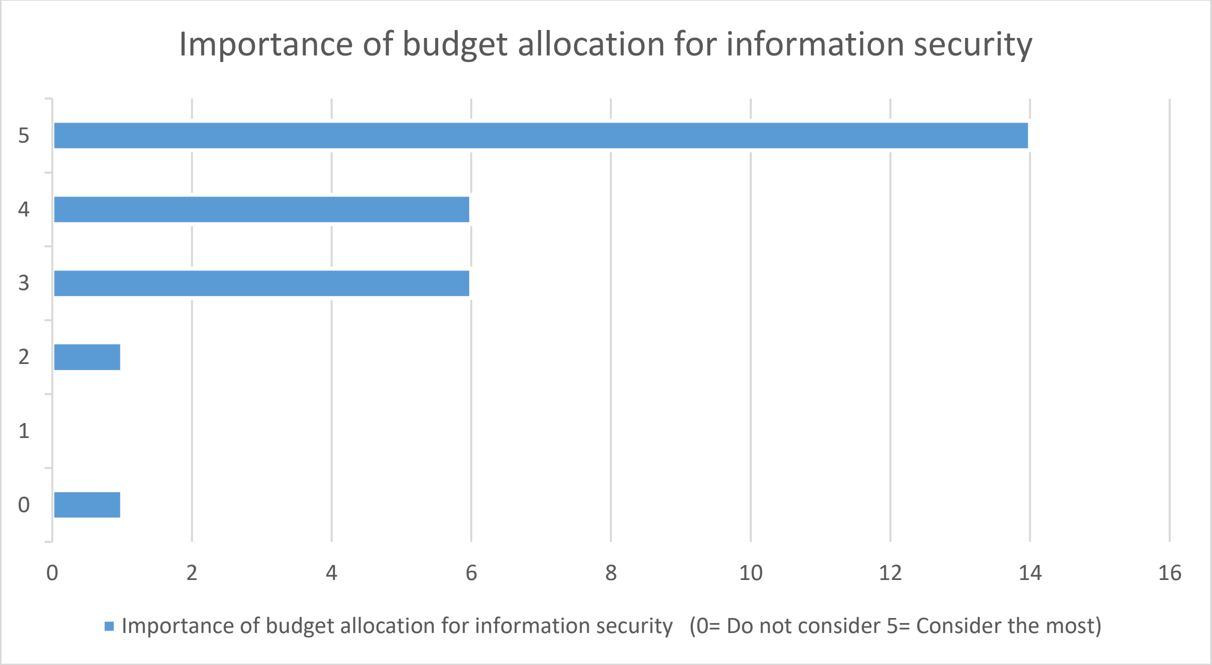


Figure E.58 Importance of budget allocation for information security (Female-UK)

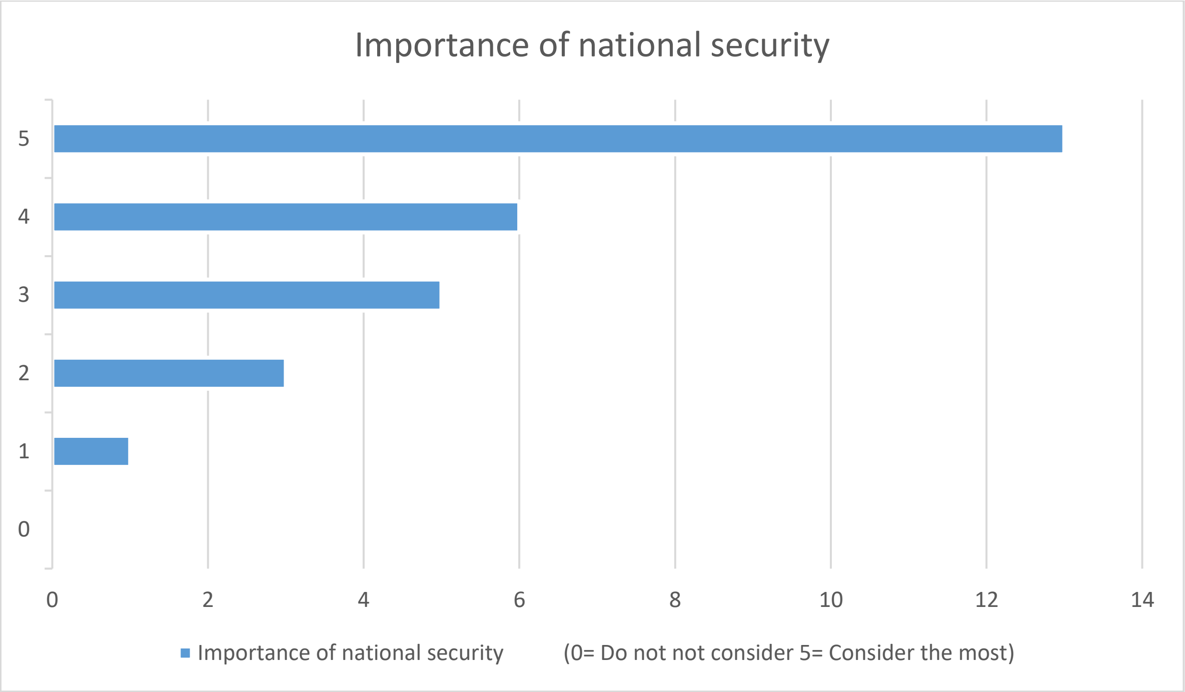


Figure E.59: Importance of national security (Female-UK)

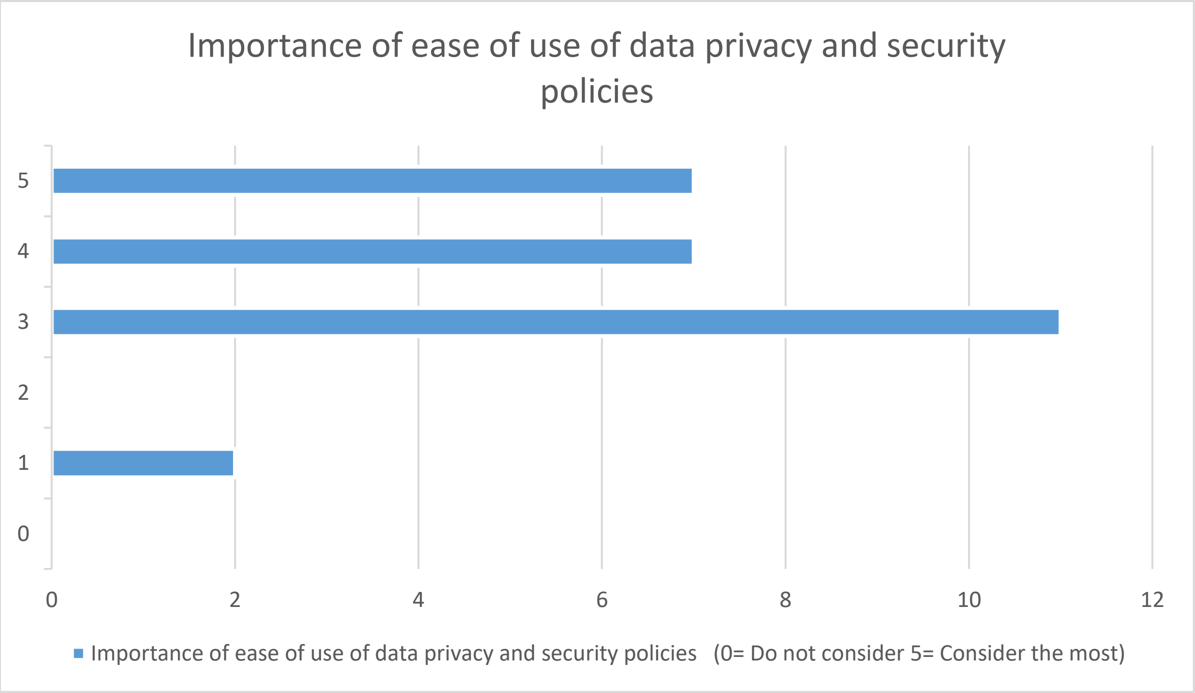


Figure E.60: Importance of ease of use of data privacy and security policies (Female-UK)

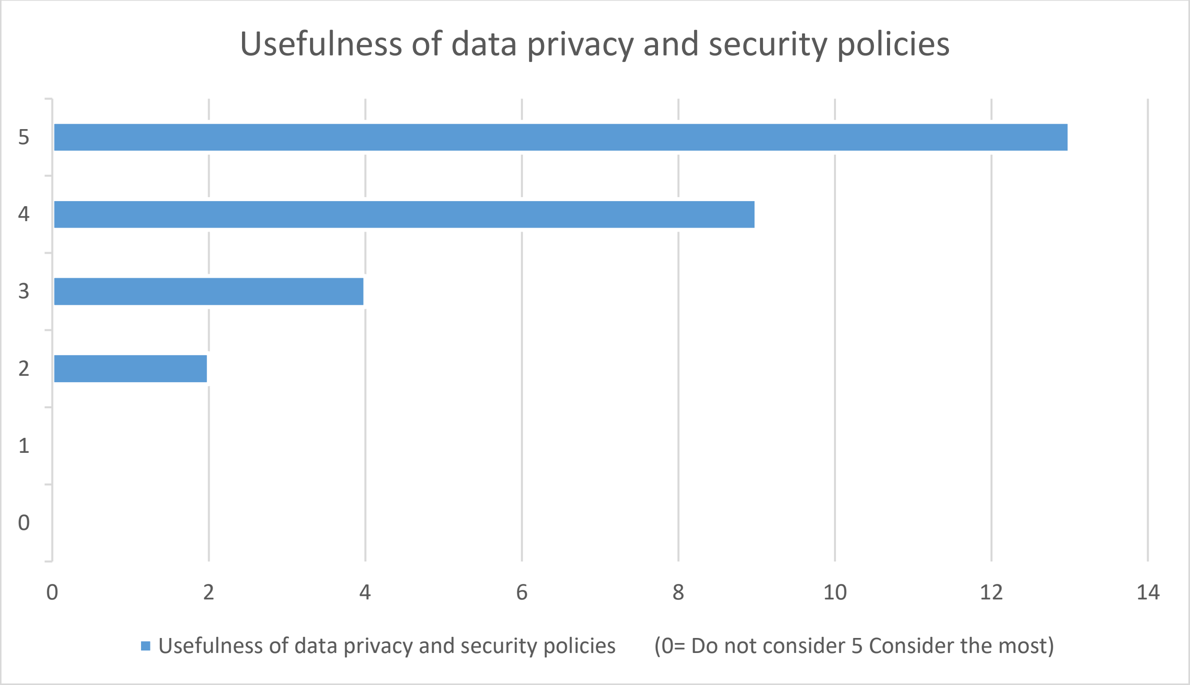


Figure E.61: Usefulness of data privacy and security policies (Female-UK)

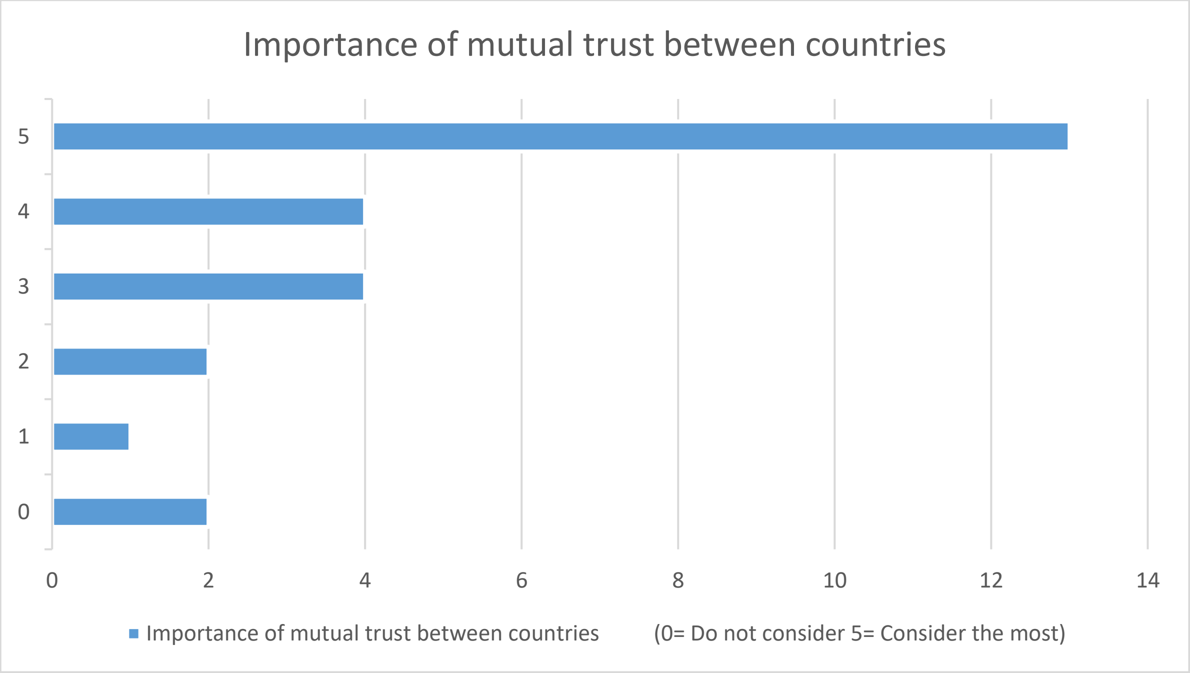


Figure E.62: Importance of mutual trust between countries (Female-UK)

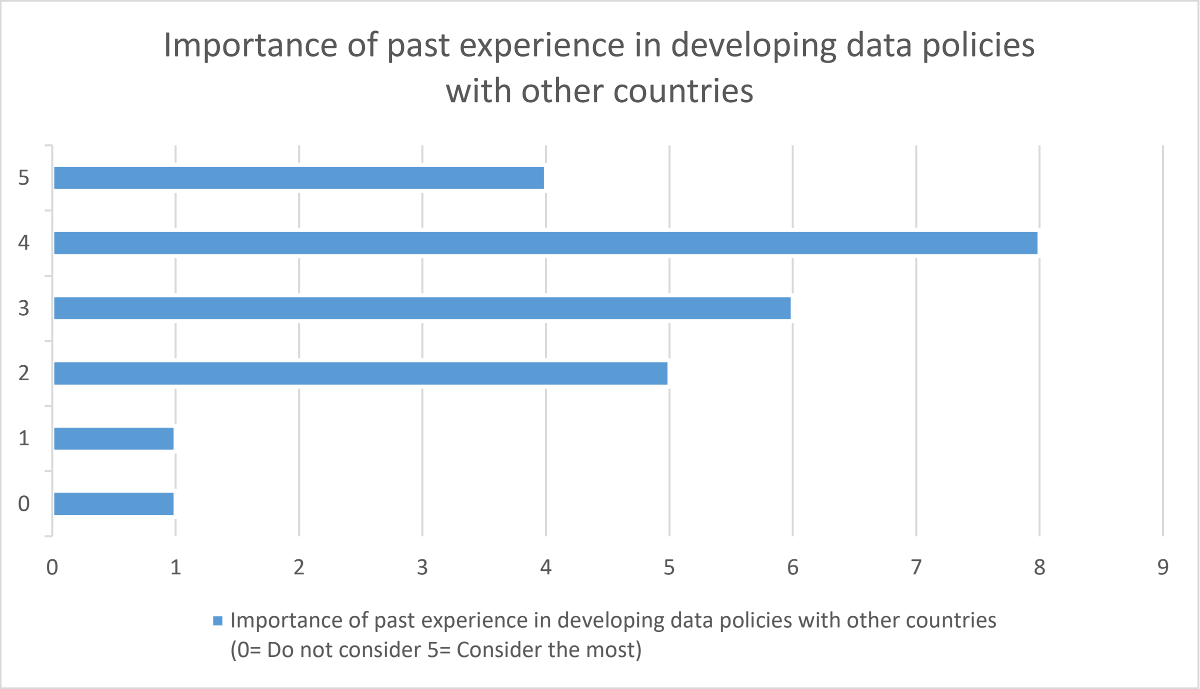


Figure E.63: Importance of past experience in developing data policies with other counties (Female-UK)

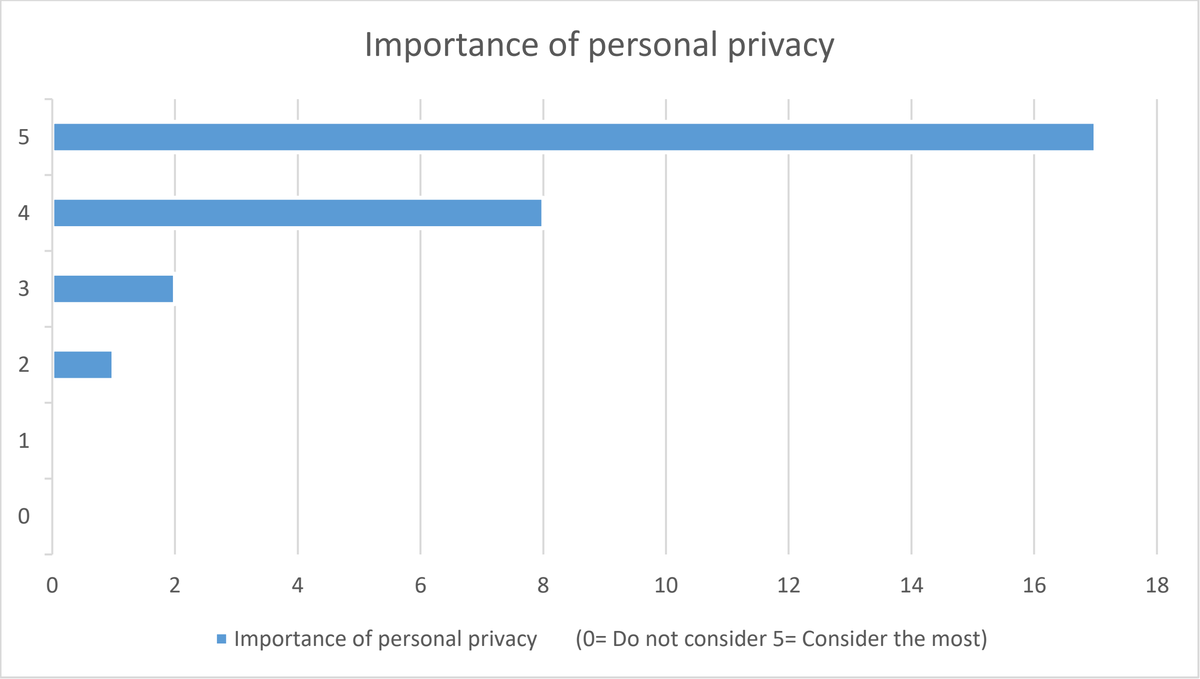


Figure E.64: Importance of personal privacy (Female-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 89 percent of the respondents have endorsed (See figure E.53). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure E.42-52) (See figure E.54-64).

United Kingdom – 18-25

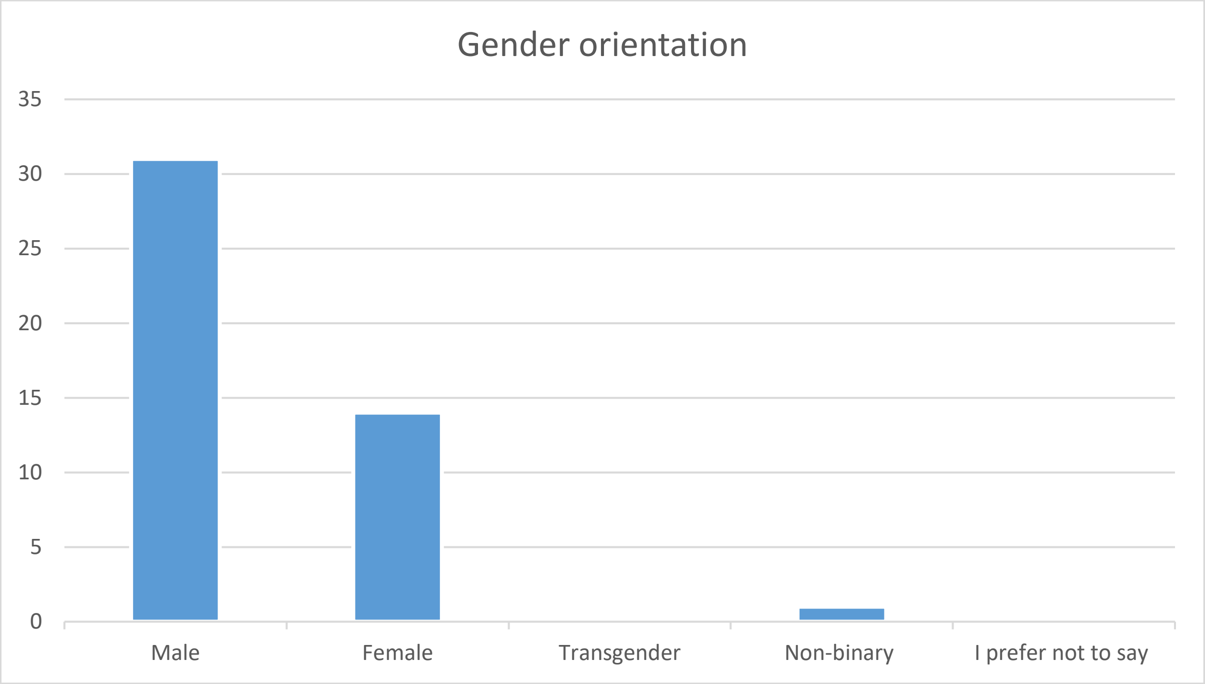


Figure E.65: Gender orientation (18-25-UK)

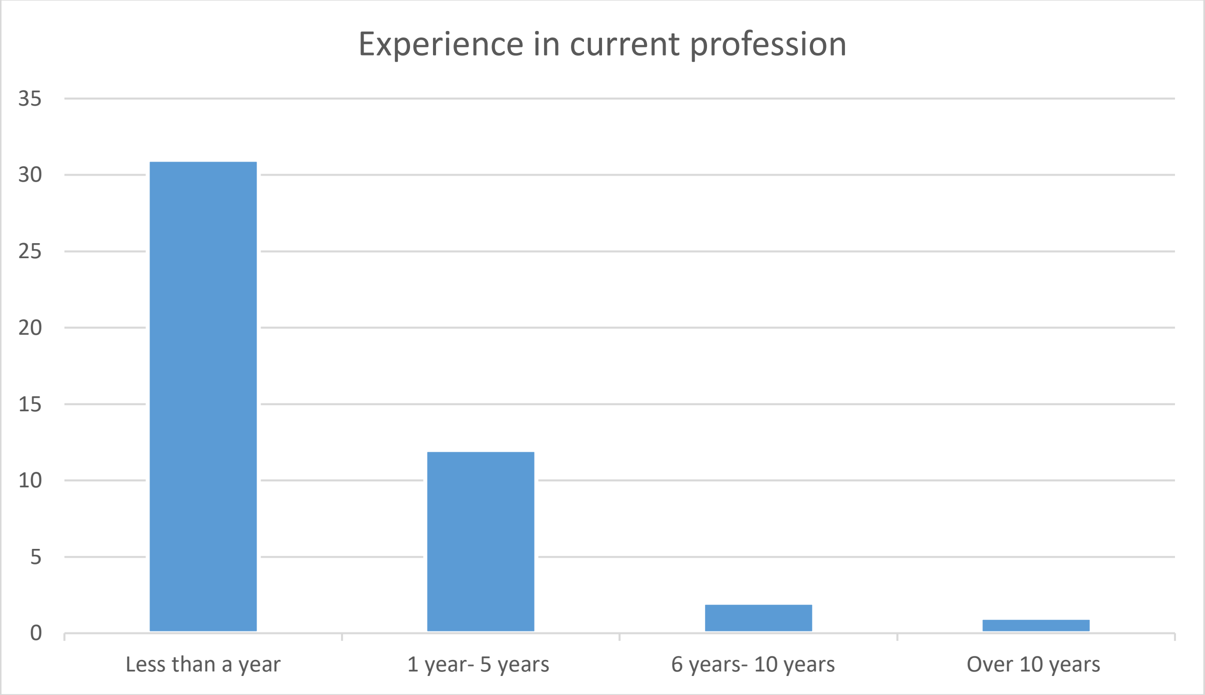


Figure E.66: Experience in current profession (18-25-UK)

This analysis is based on the responses received from United Kingdom participants aged between 18-25. There were 46 participants and 31 out of them were males and 14 females (See figure E.65), all of them have been in employment for less than a year to over 10 years (See figure E.66).

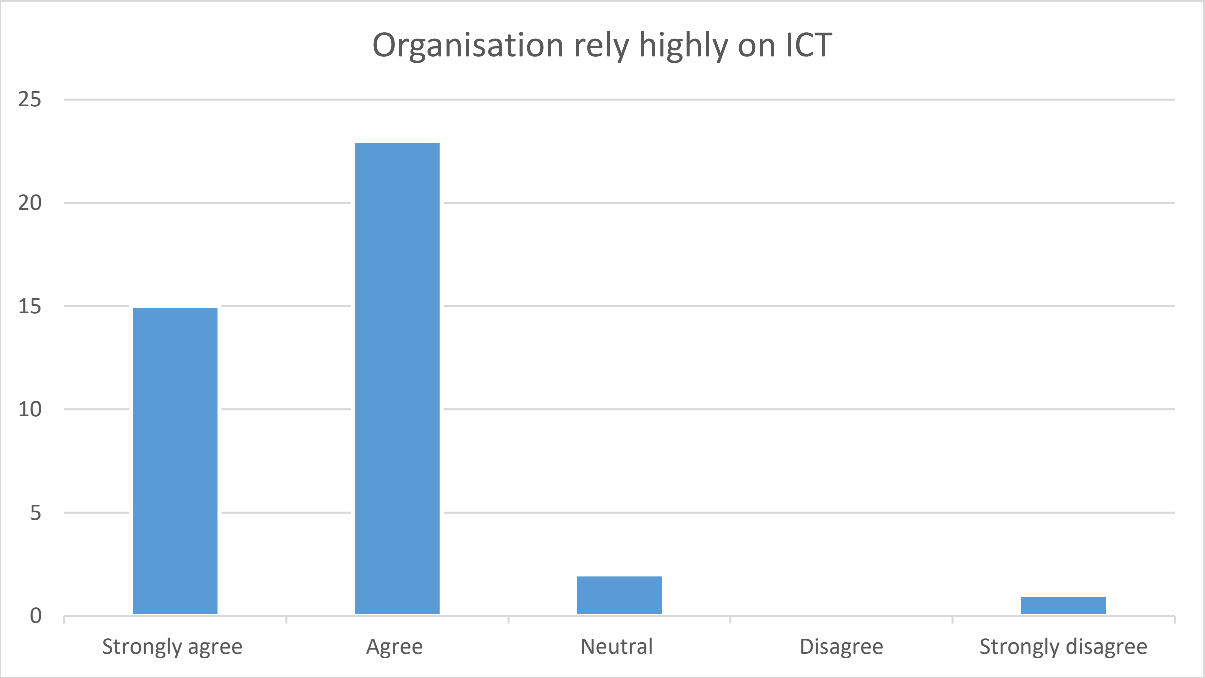


Figure E.67: Organisation rely highly on ICT (18-25-UK)

Out of the 46 respondents, 38 have worked in a technology reliance working environment, 2 unaware of reliance on technology because of the nature of the work assigned to them, 1 has marked 'disagree' on ICT (See figure E.67). The majority of the employees within the 18-25 age range have a high reliance on ICT.

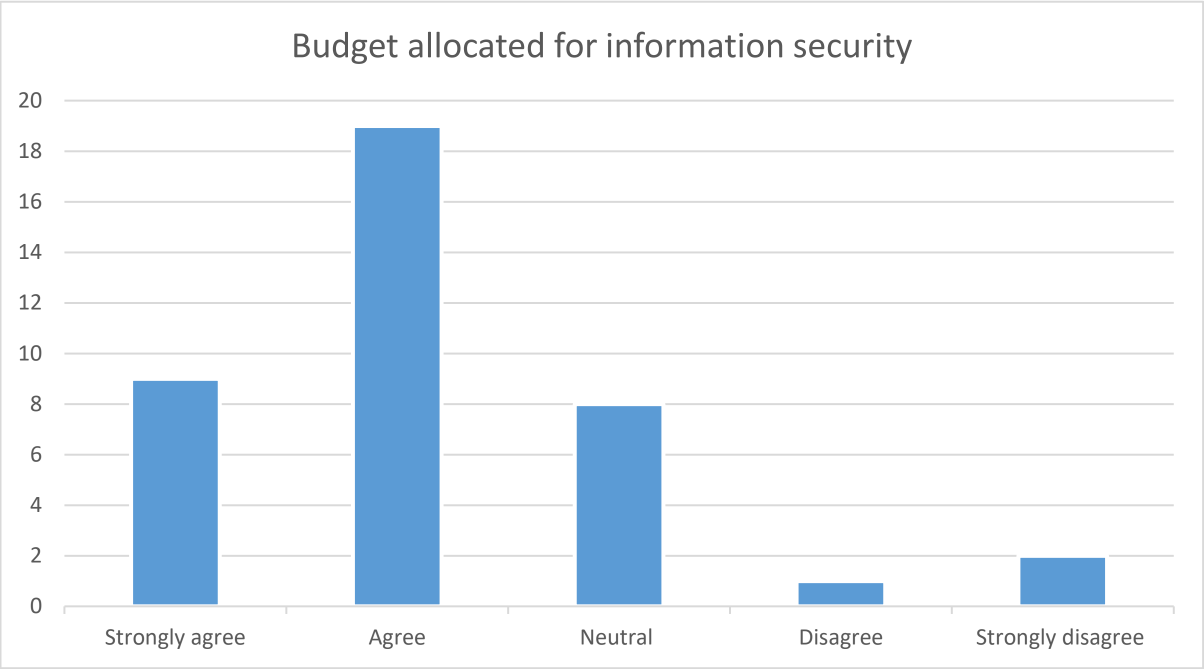


Figure E.68: Budget allocated for information security (18-25-UK)

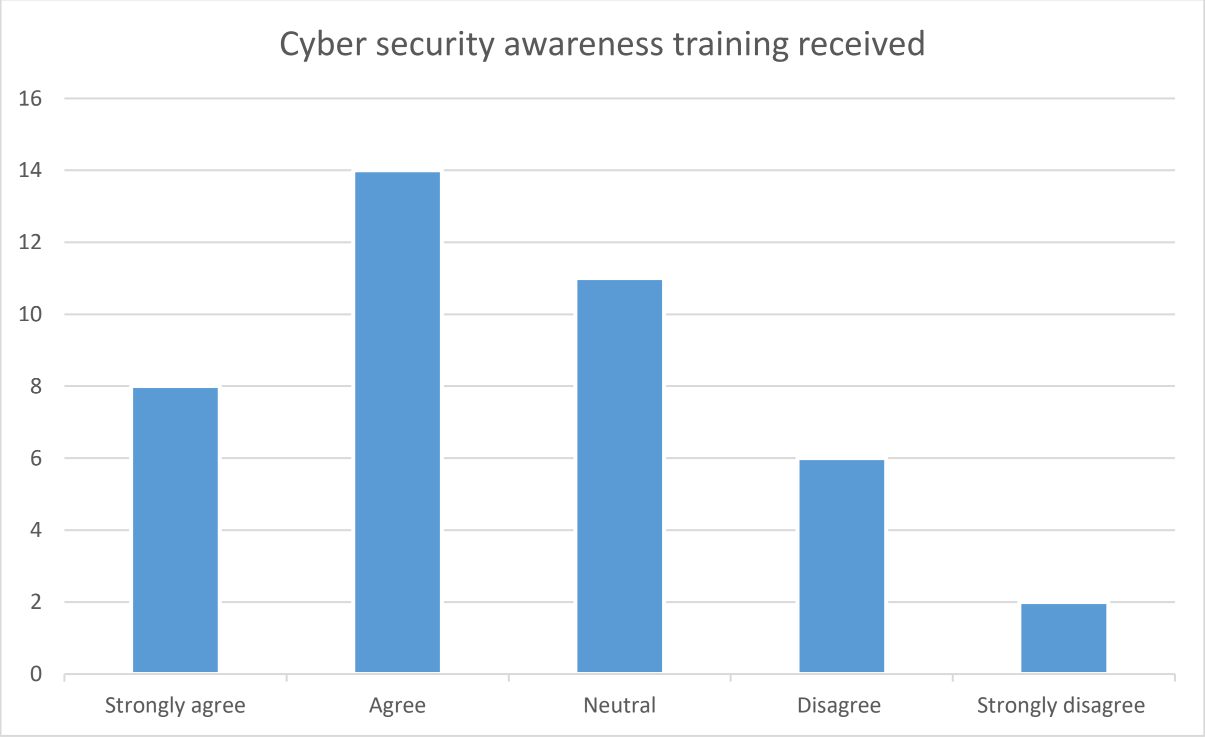


Figure E.69: Cyber security awareness training received (18-25-UK)

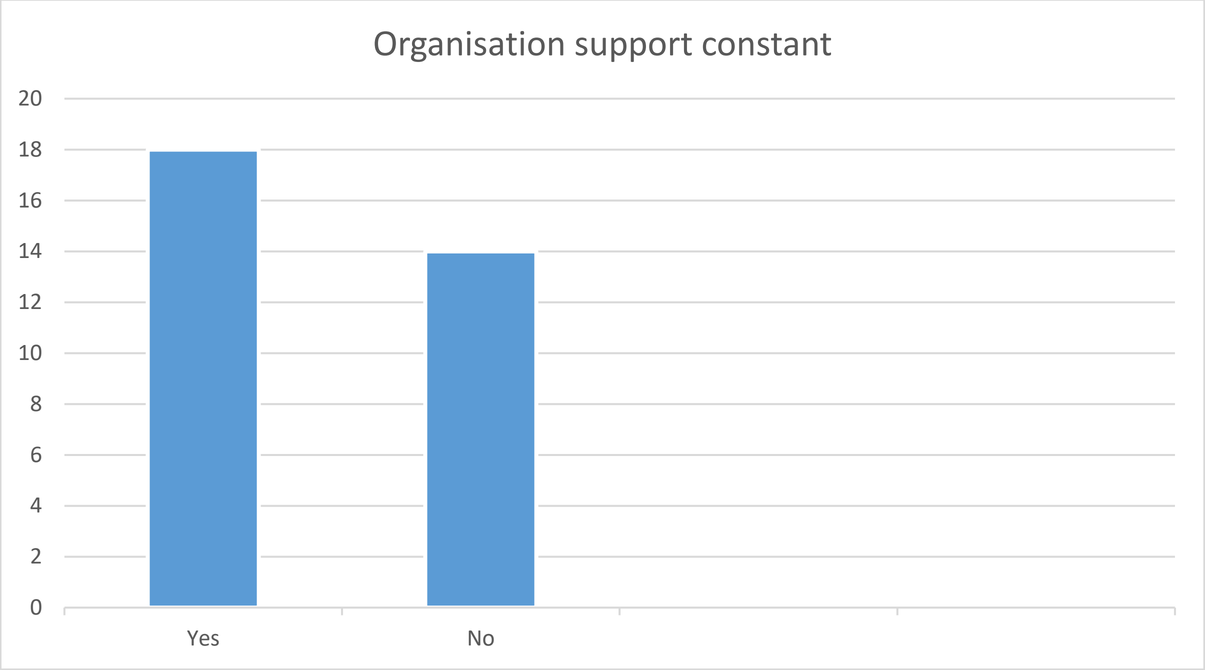


Figure E.70: Organisation support constant (18-25-UK)

Funding has been sketchy. 28 out of the 46 have indicated that their organisations had an allocated budget for information security, whilst 8 had not expressed an opinion either way and notably according to the 3 disagreed, their organisations had no budget allocation for information security (See figure E.68). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 22 participants have received regular cybersecurity awareness training, whilst 11 participants neither agreed nor disagreed, and 8 participants had not regularly received security awareness training (See figure E.69). In addition, 14 participants had not received support from the organisation to protect personal information, whilst only 18 did (See figure E.70). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

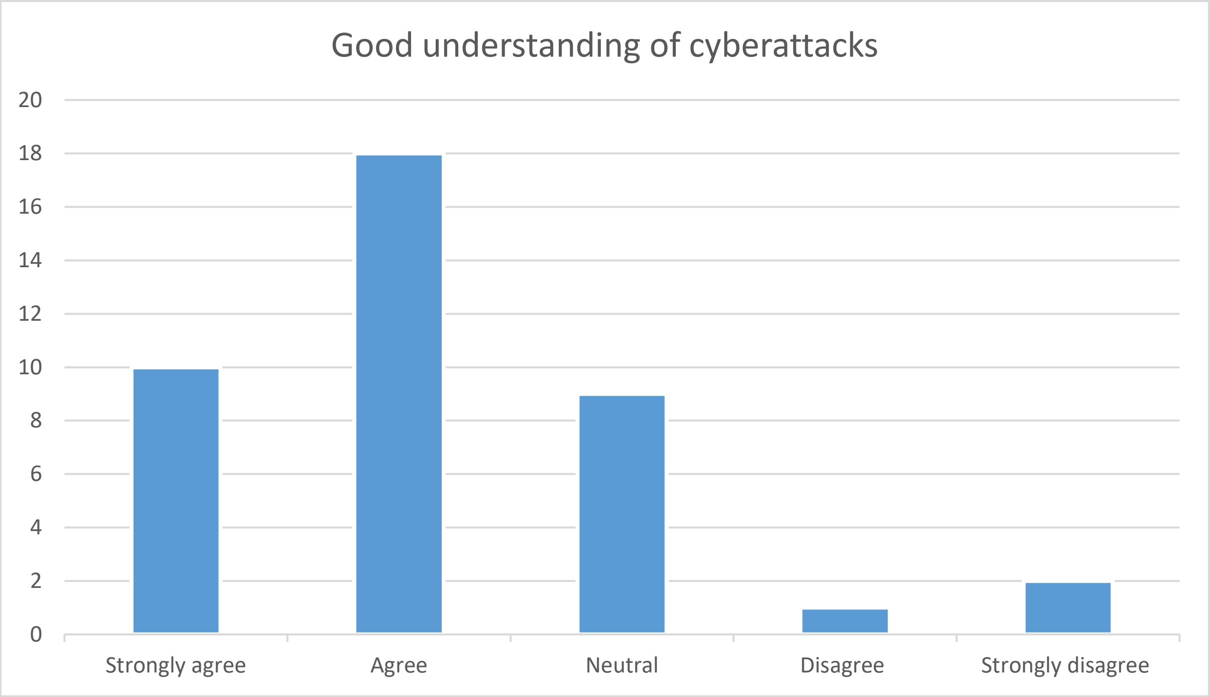


Figure E.71: Good understanding of cyberattacks (18-25-UK)

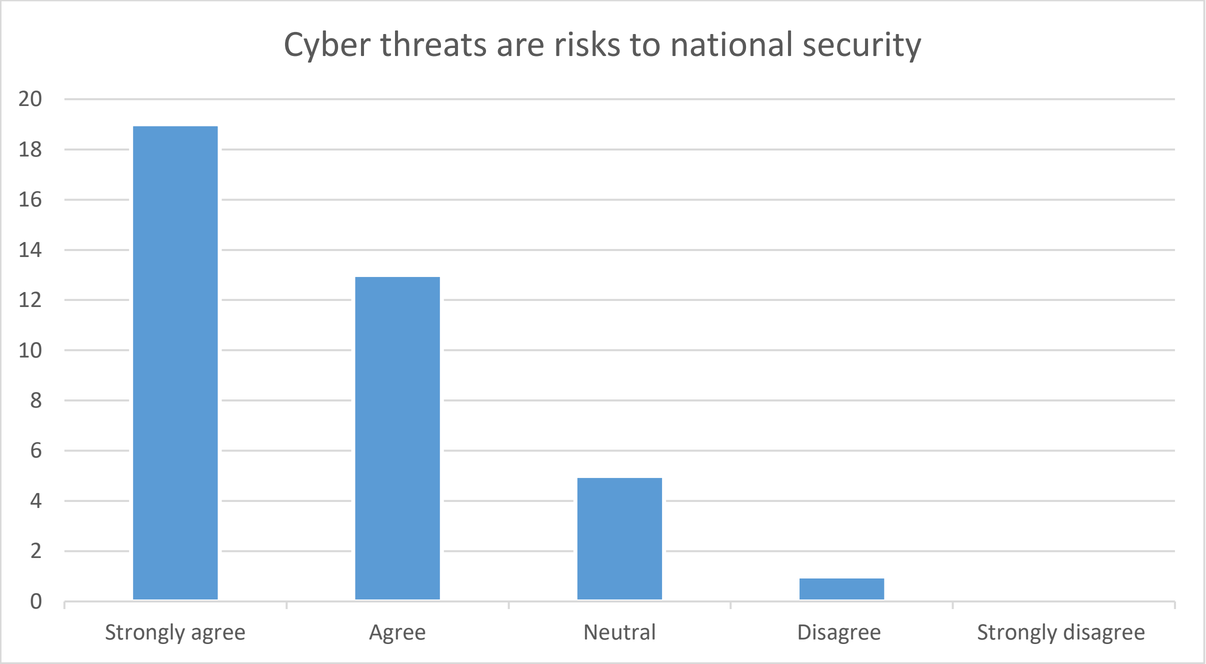


Figure E.72: Cyber threats are risks to national security (18-25-UK)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 28 participants do have, 9 have not expressed opinion either way, and only 3 participants had no understanding (See figure E.71). Furthermore, 70 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure E.72). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

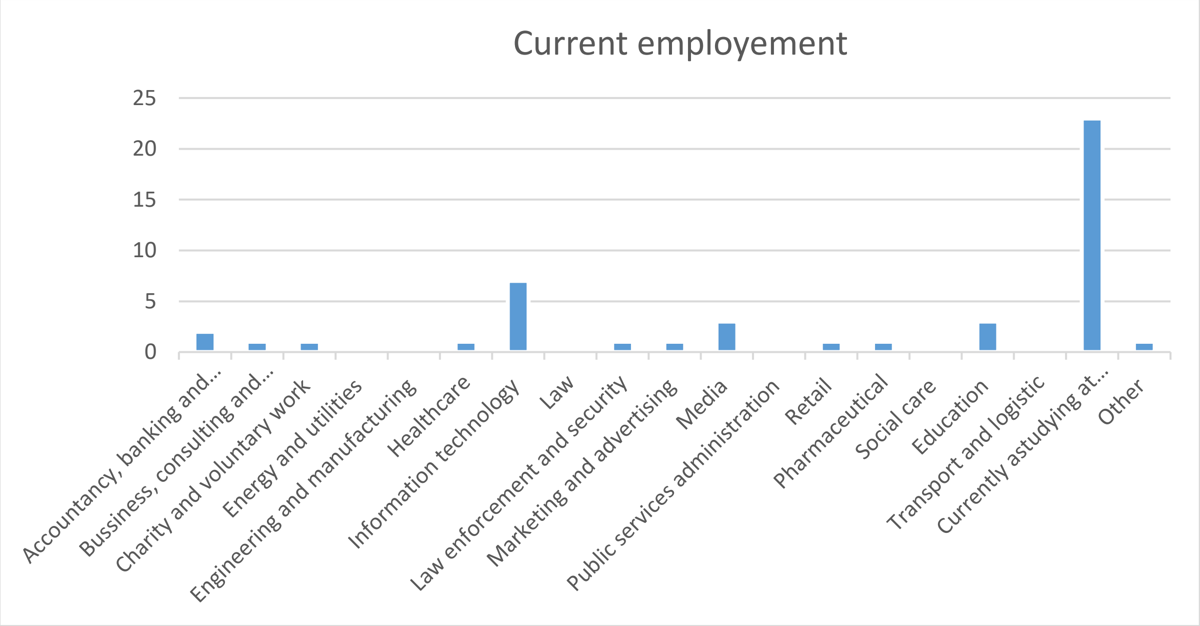


Figure E.73: Current employment (18-25-UK)

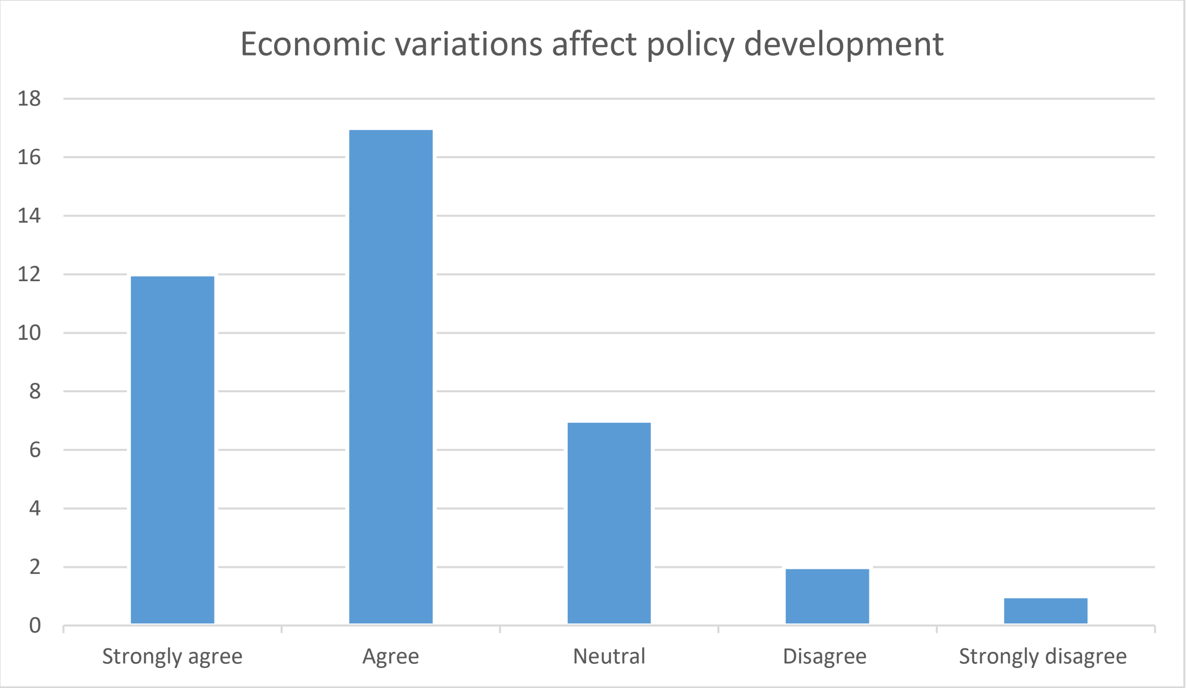


Figure E.74: Economic variations affect policy development (18-25-UK)

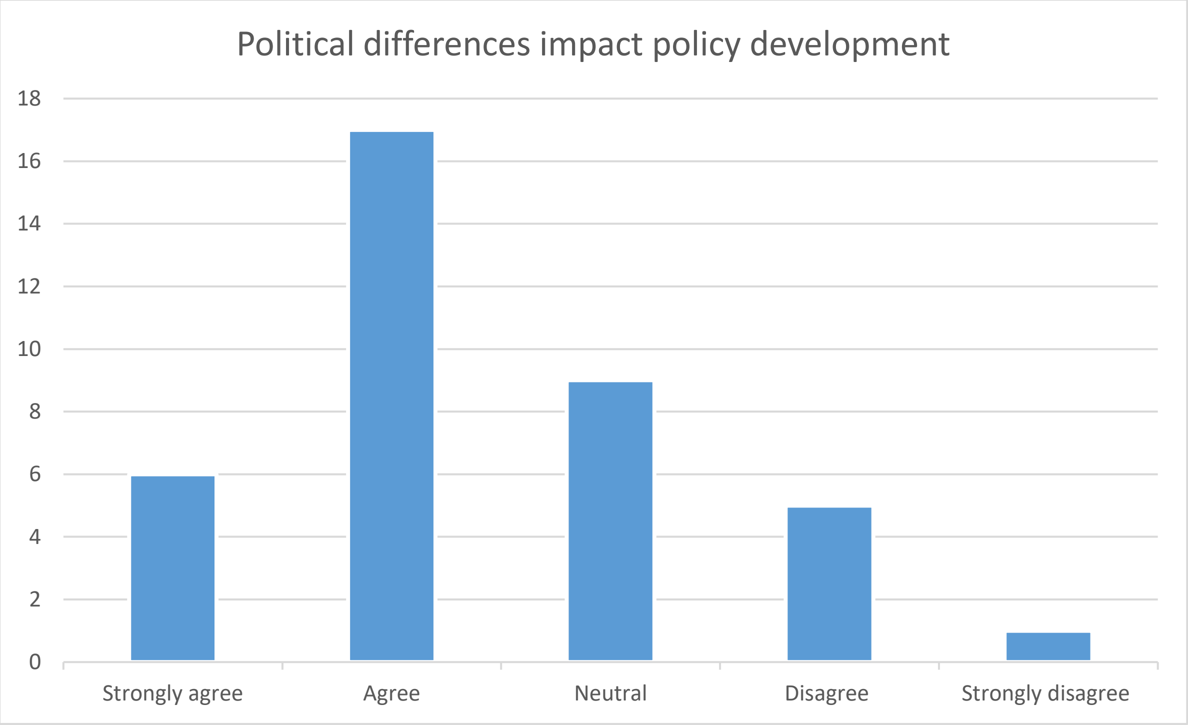


Figure E.75: Political differences impact policy development (18-25-UK)

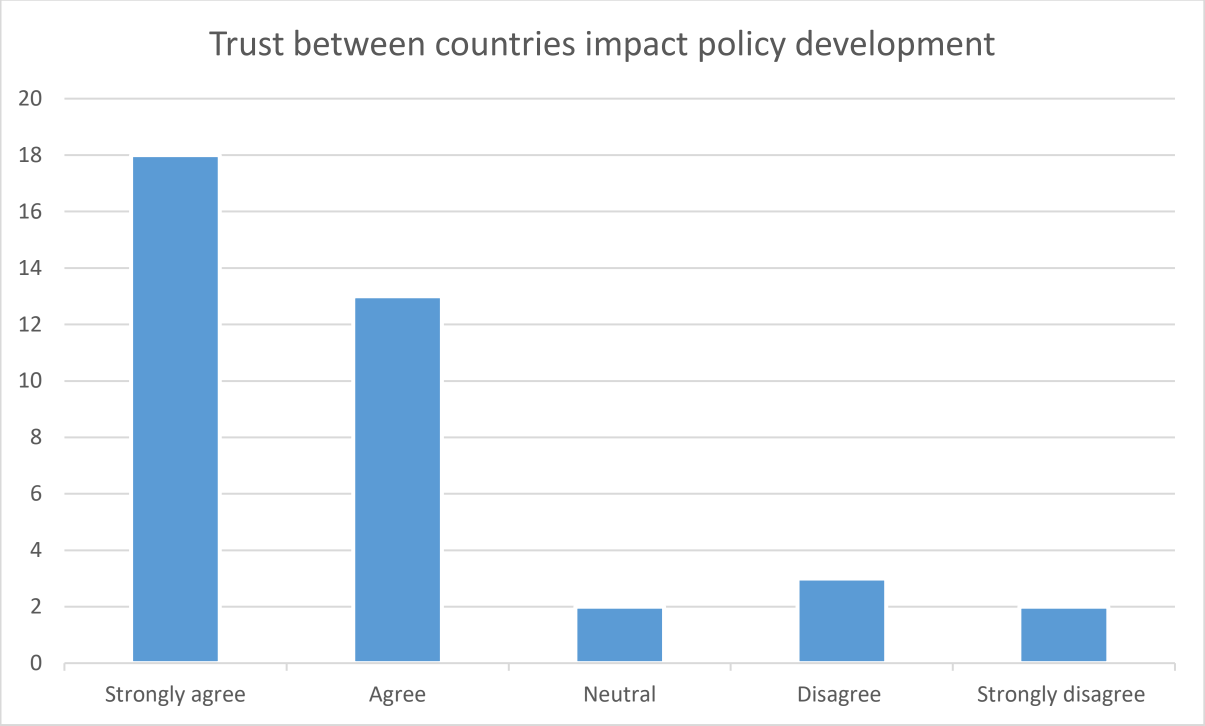


Figure E.76: Trust between countries impact policy development (18-25-UK)

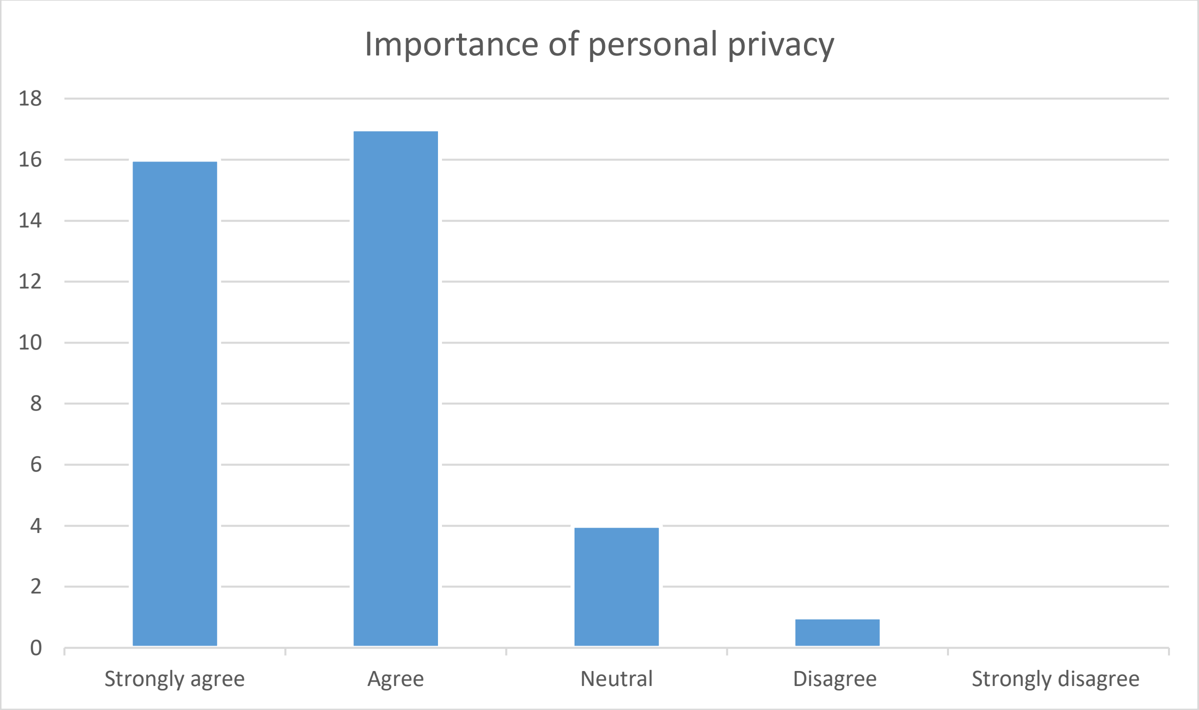


Figure E.77: Importance of personal privacy (18-25-UK)

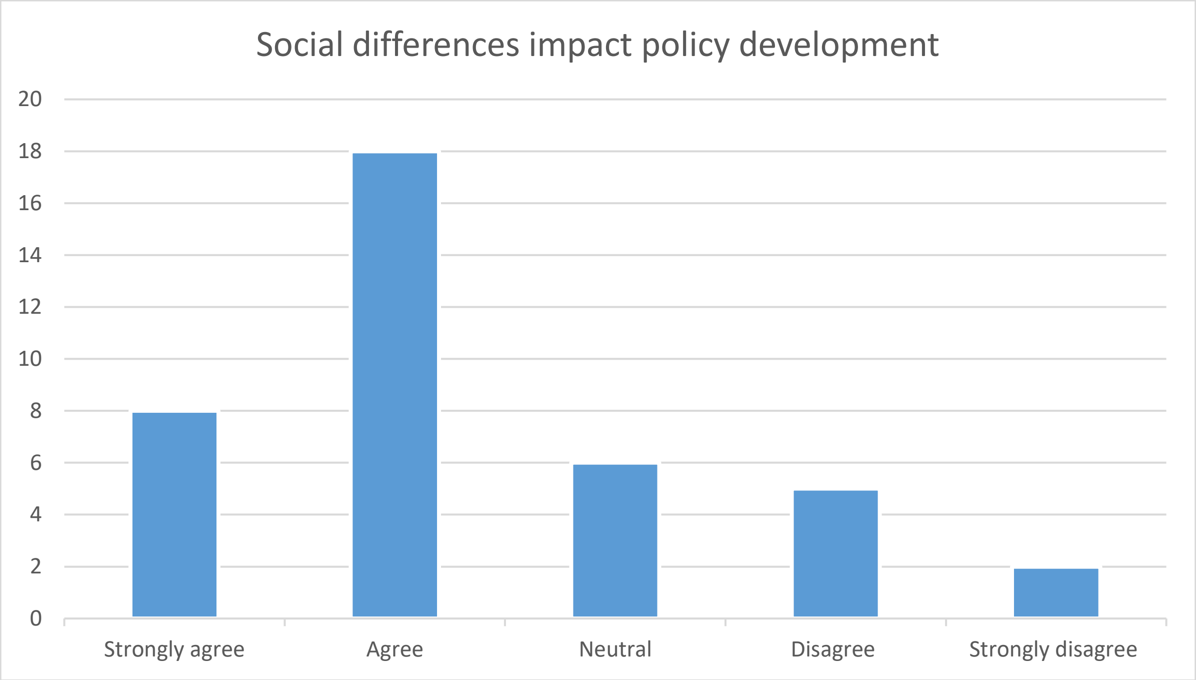


Figure E.78: Social differences impact policy development (18-25-UK)

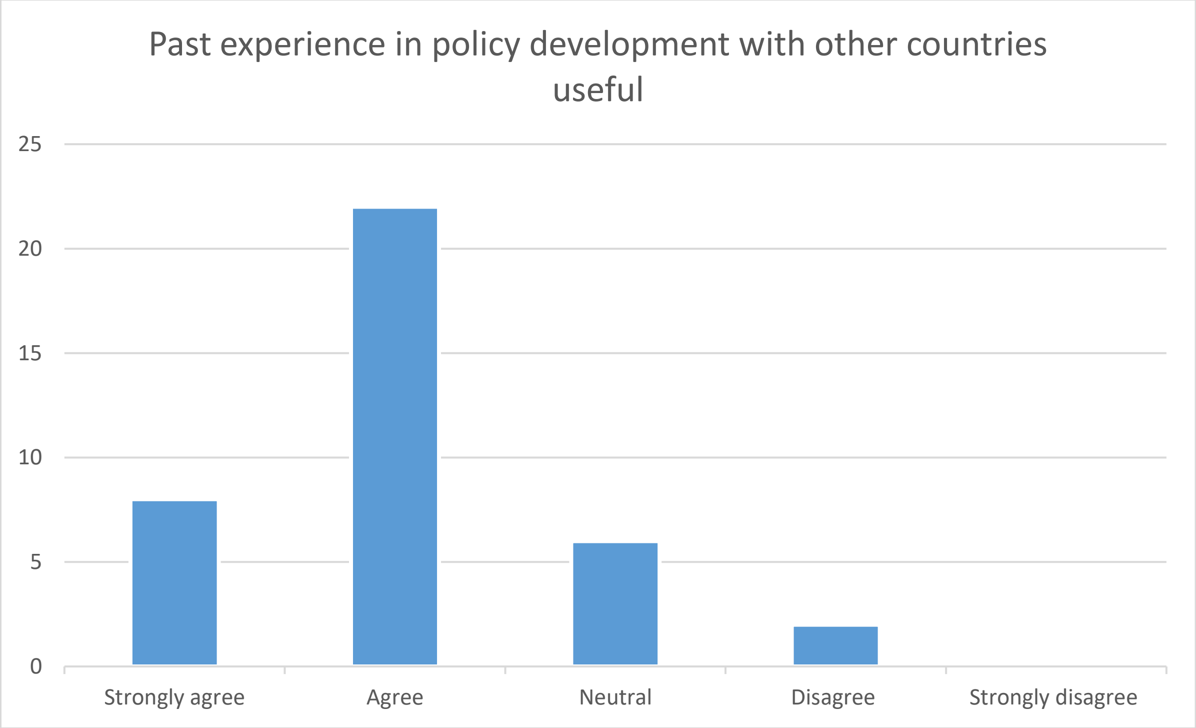


Figure E.79: Past experience in policy development with other countries useful (18-25-UK)

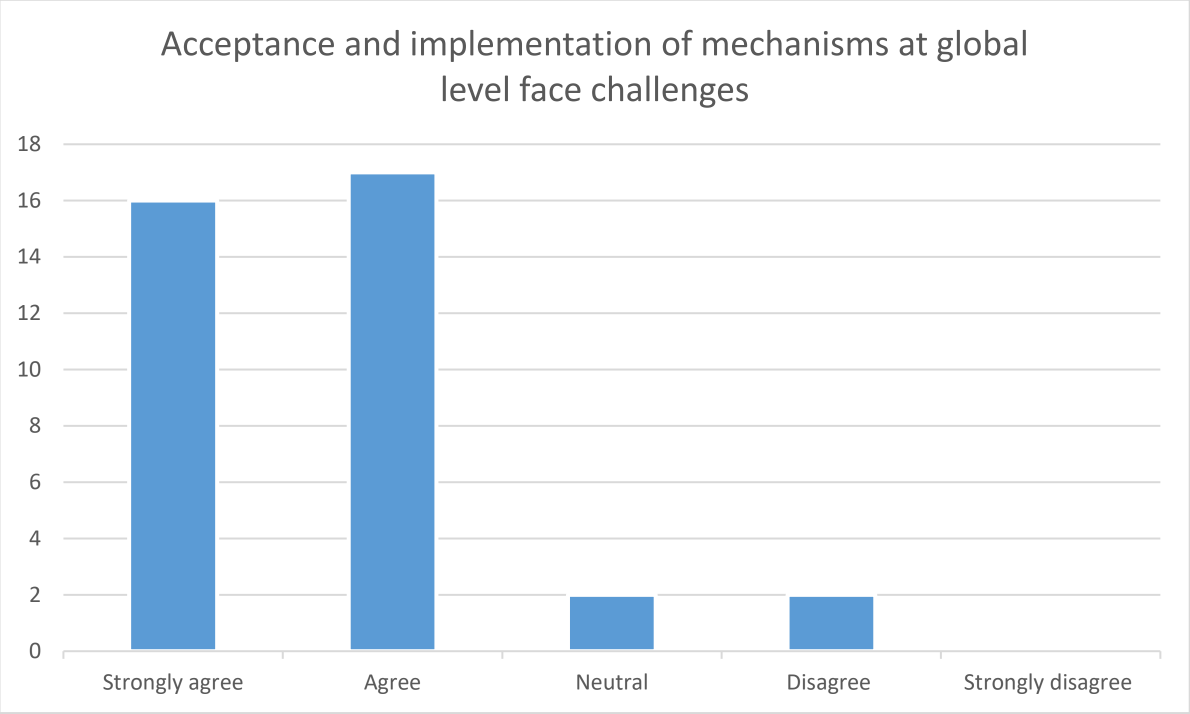


Figure E.80: Acceptance and implementation of mechanisms at global level face challenges (18-25-UK)

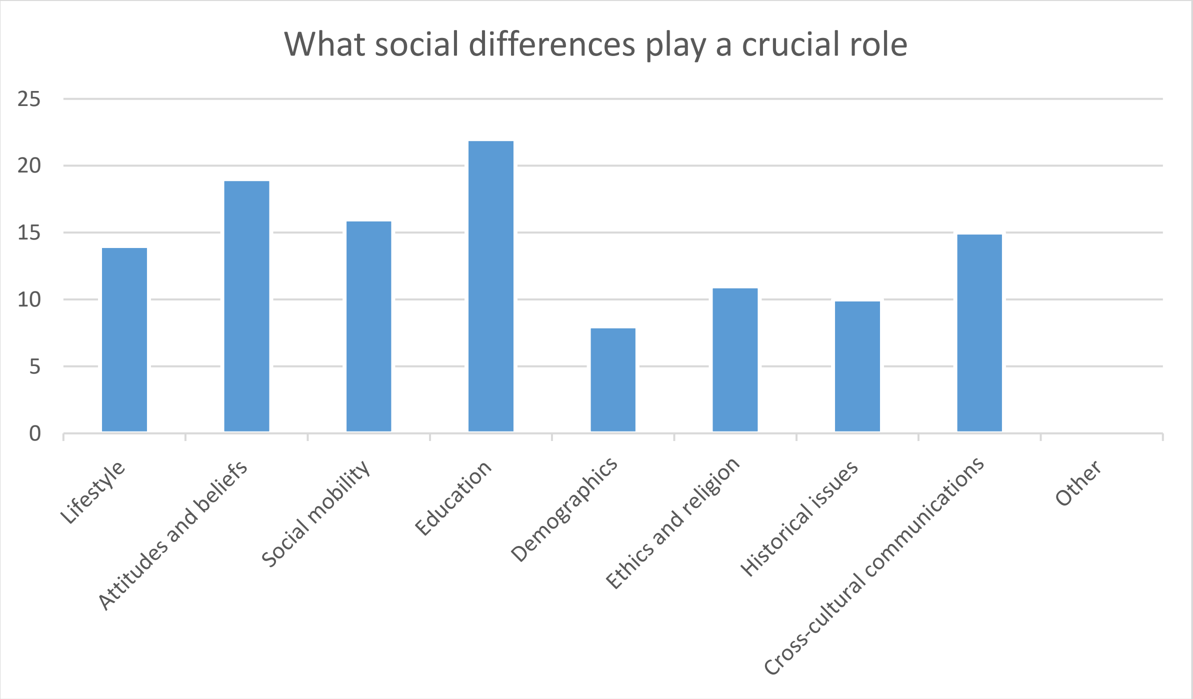


Figure E.81: What social differences play a crucial role (18-25-UK)

Interestingly, majority of the participants in 18-25 age range does not specify a particular social difference category (See figure E.81). There are two possible explanations for this, either the participants do not have an understanding of the social differences, and their impact on policy acceptance and implementation, or they do not believe social differences matter.

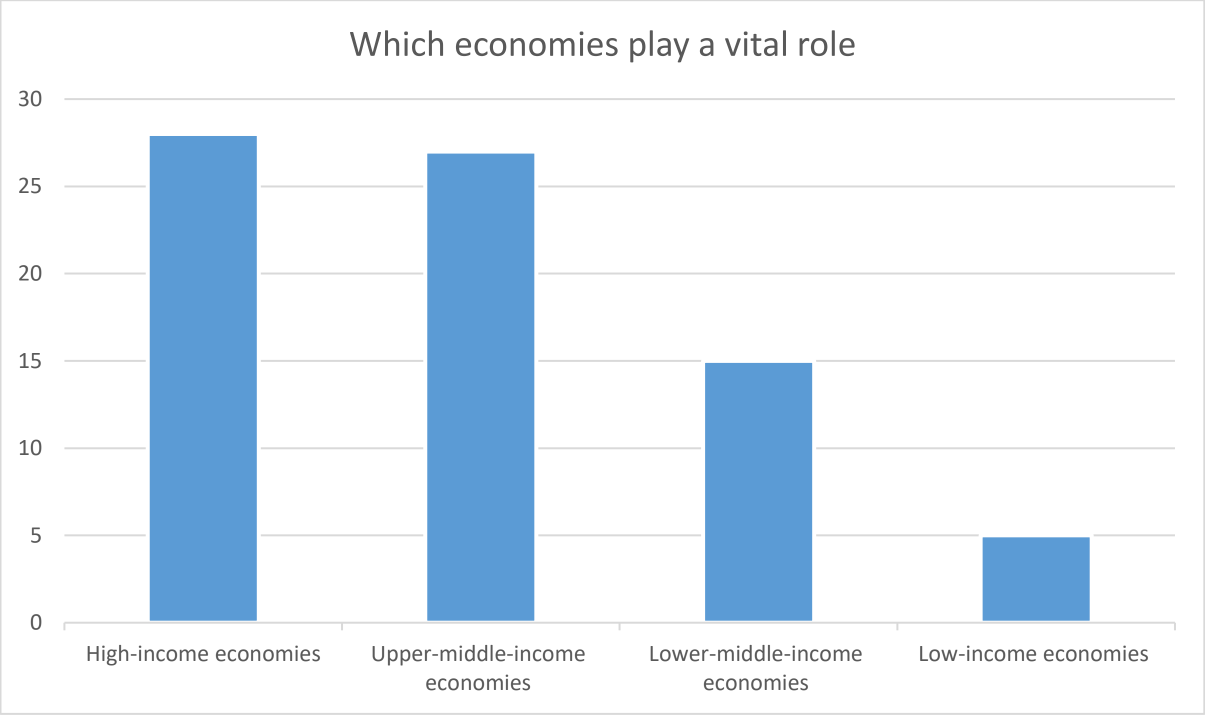


Figure E.82: Which economies play a vital role (18-25-UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.82). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

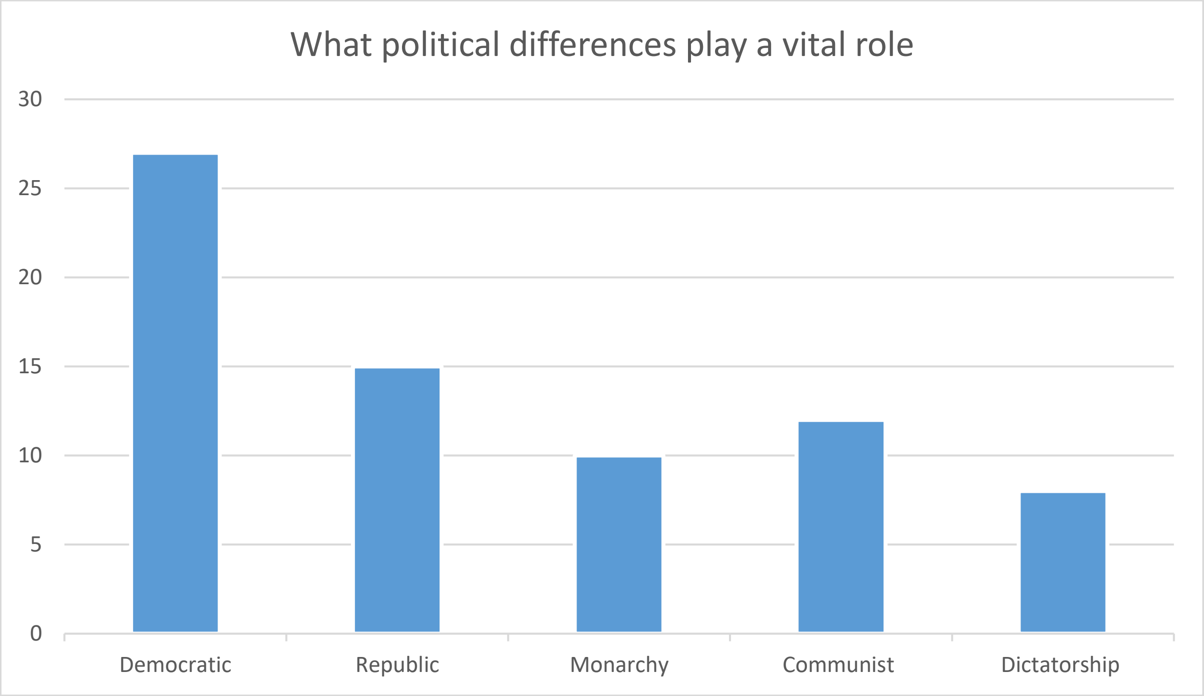


Figure E.83: What political differences play a vital role (18-25-UK)

The majority have chosen a democratic political system (See figure E.83), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

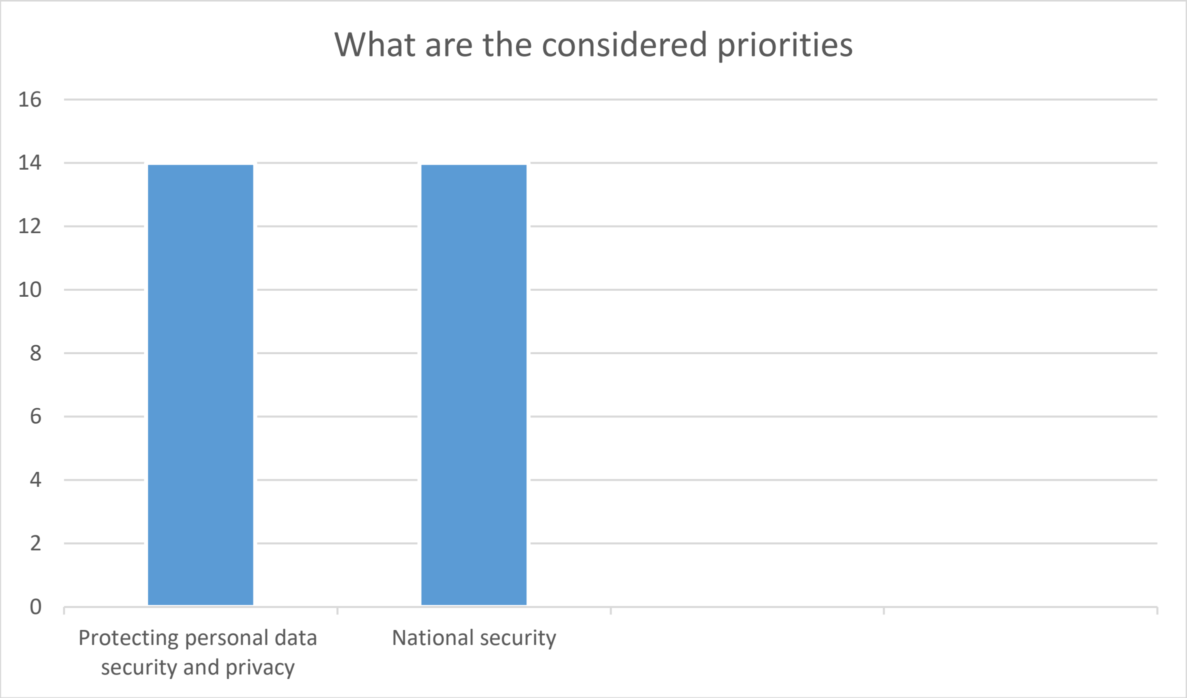


Figure E.84: What are the considered priorities (18-25-UK)

In accepting and implementing a global framework of data privacy and security policies, the participants have not highlighted the importance of protecting personal data security and privacy, and national security to a satisfactory level (See figure E.84). However, in an incident of personal data breach, there will potentially be a knock-on effect on both personal data security and privacy, and national security, and it will also be felt right across the groups as well as the community alike.

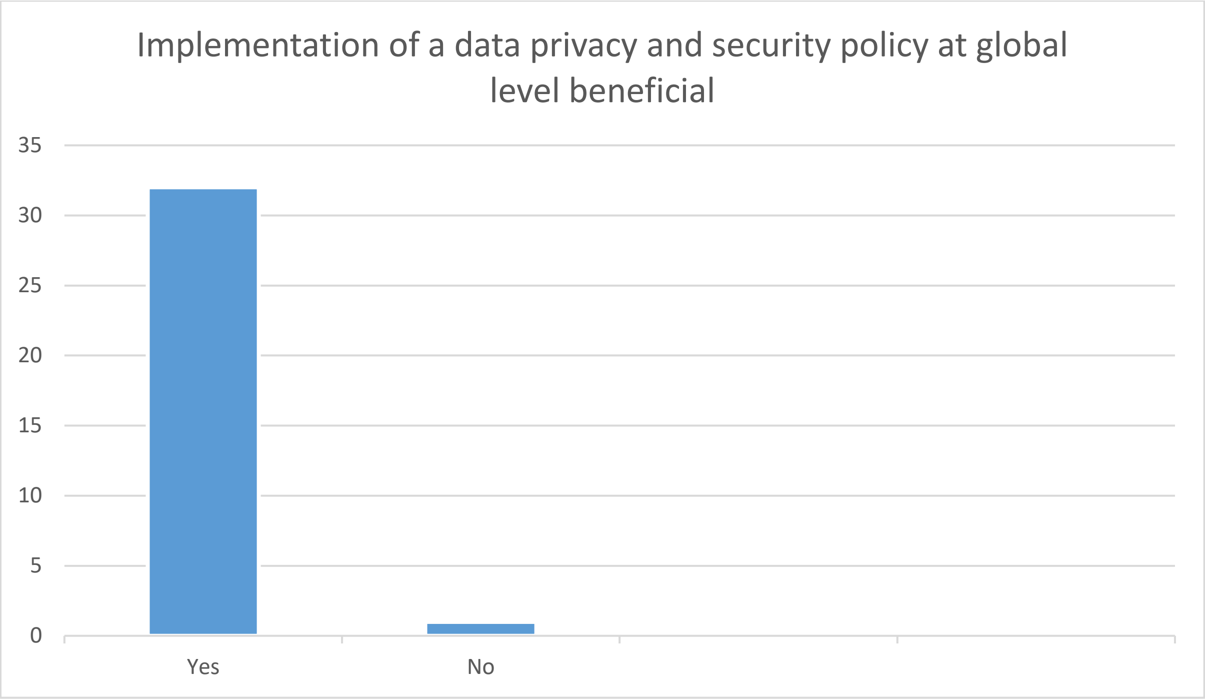


Figure E.85: Implementation of a data privacy and security policy at global level beneficial (18-25-UK)

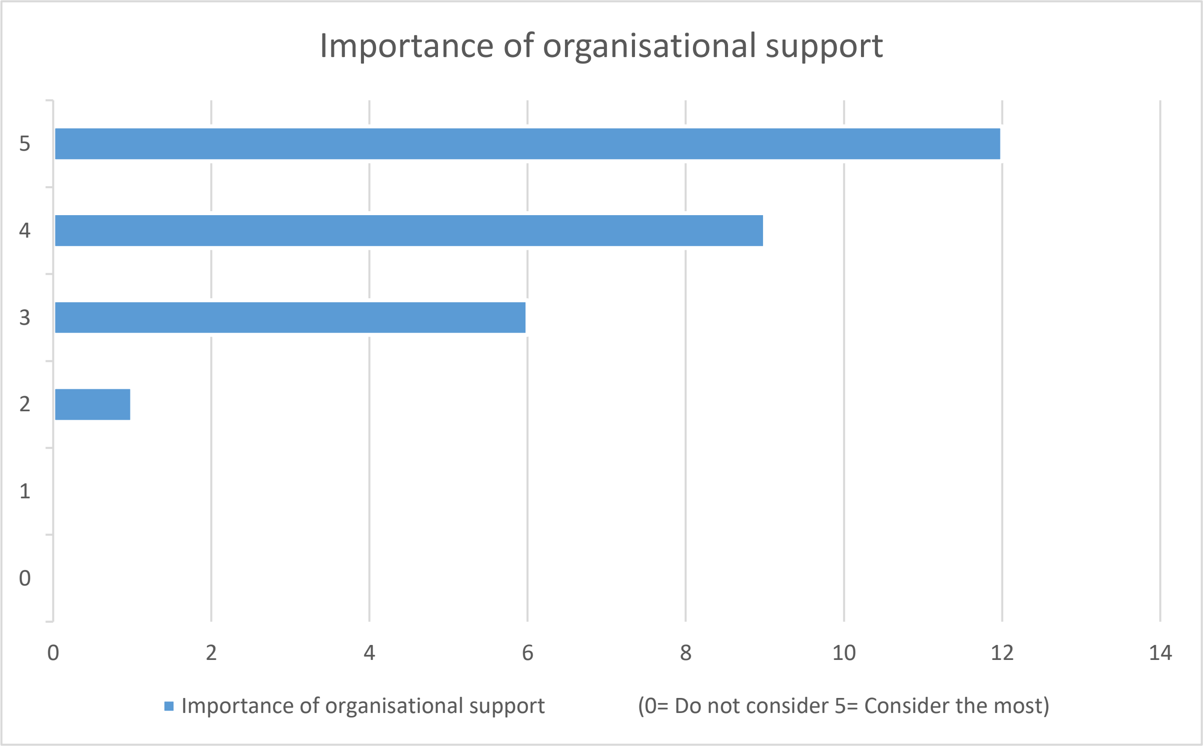


Figure E.86: Importance of organisational support (18-25-UK)

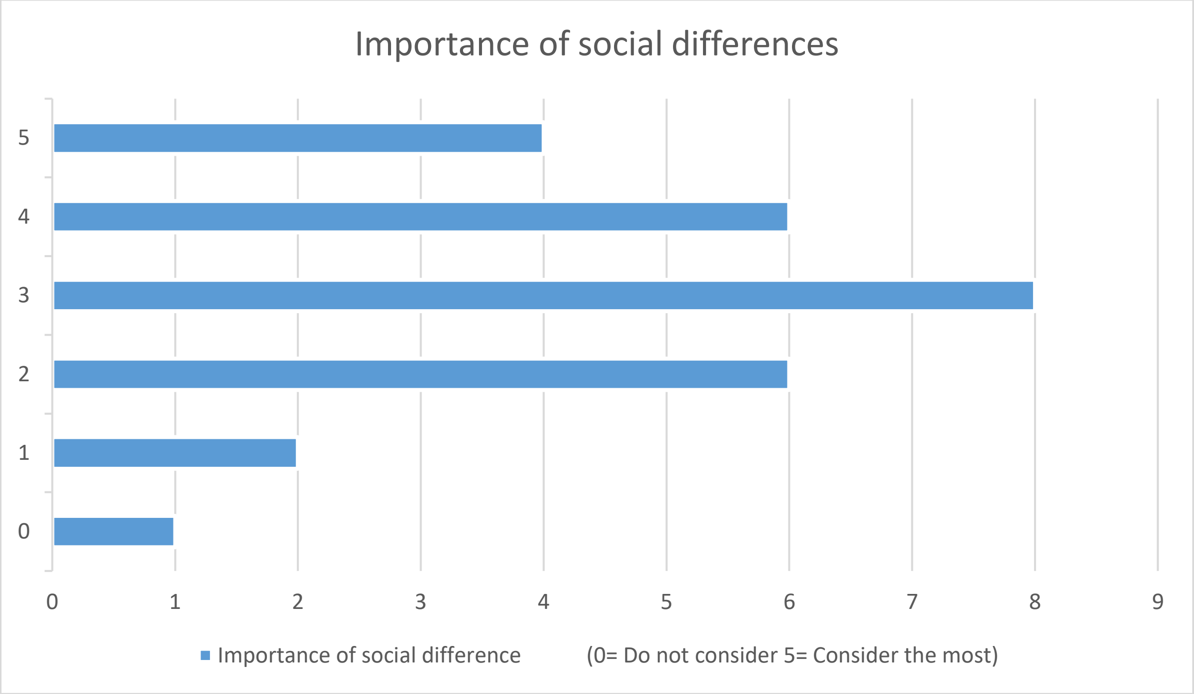


Figure E.87: Importance of social differences (18-25-UK)

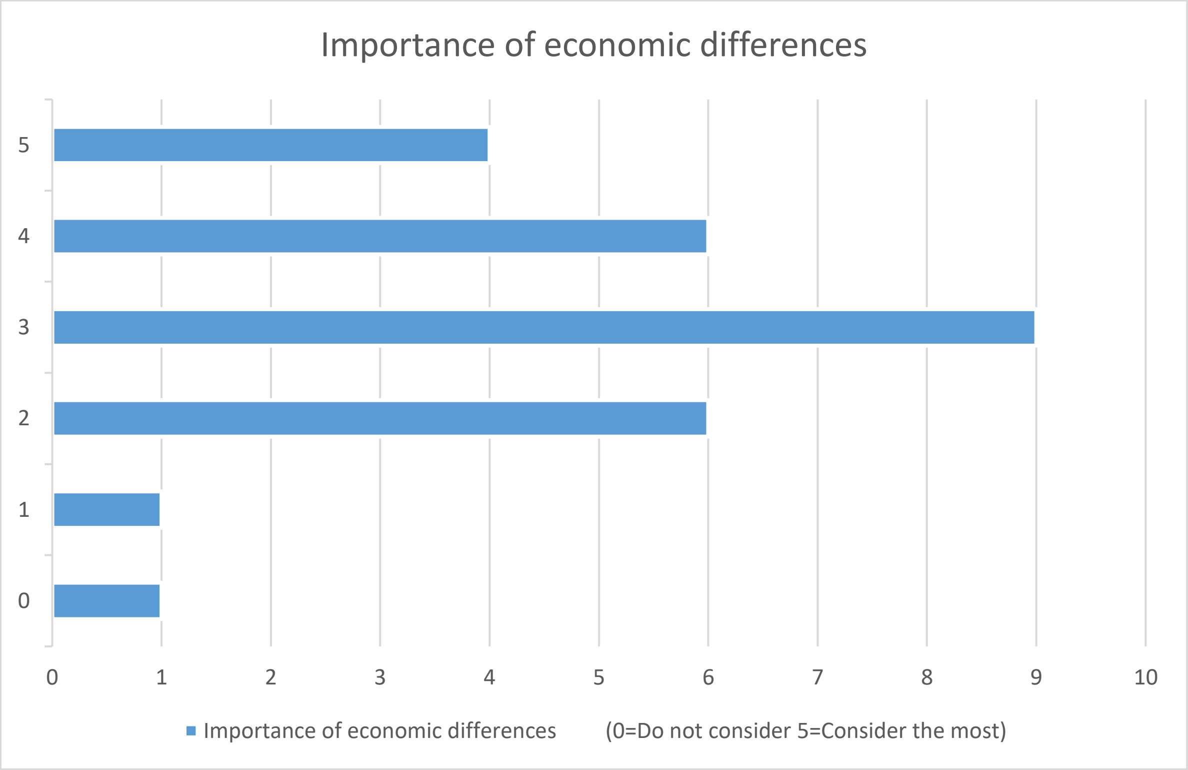


Figure E.88: Importance of economic differences (18-25-UK)

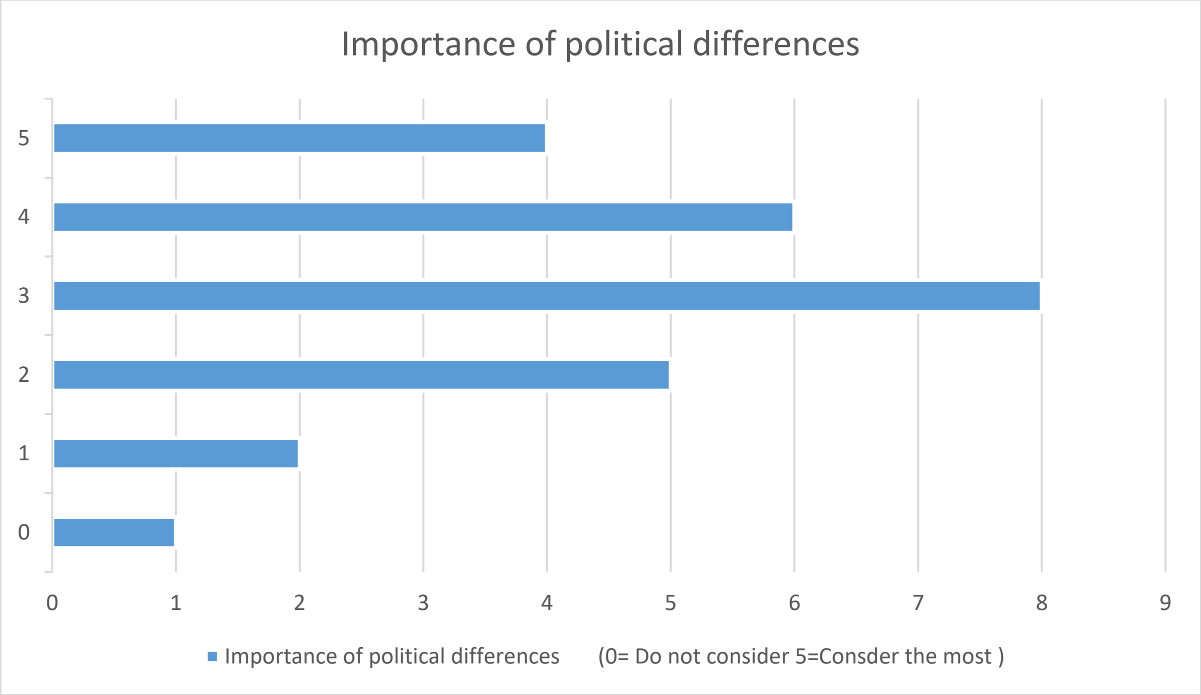


Figure E.89: Importance of political difference (18-25-UK)

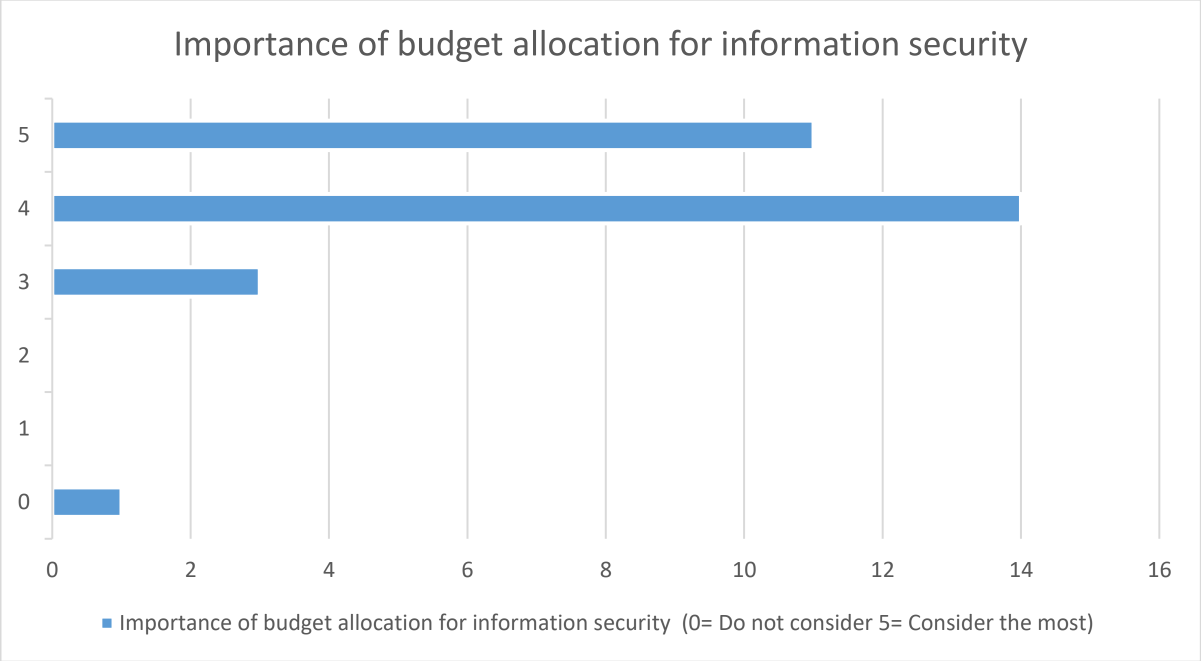


Figure E.90: Importance of budget allocation for information security (18-25-UK)

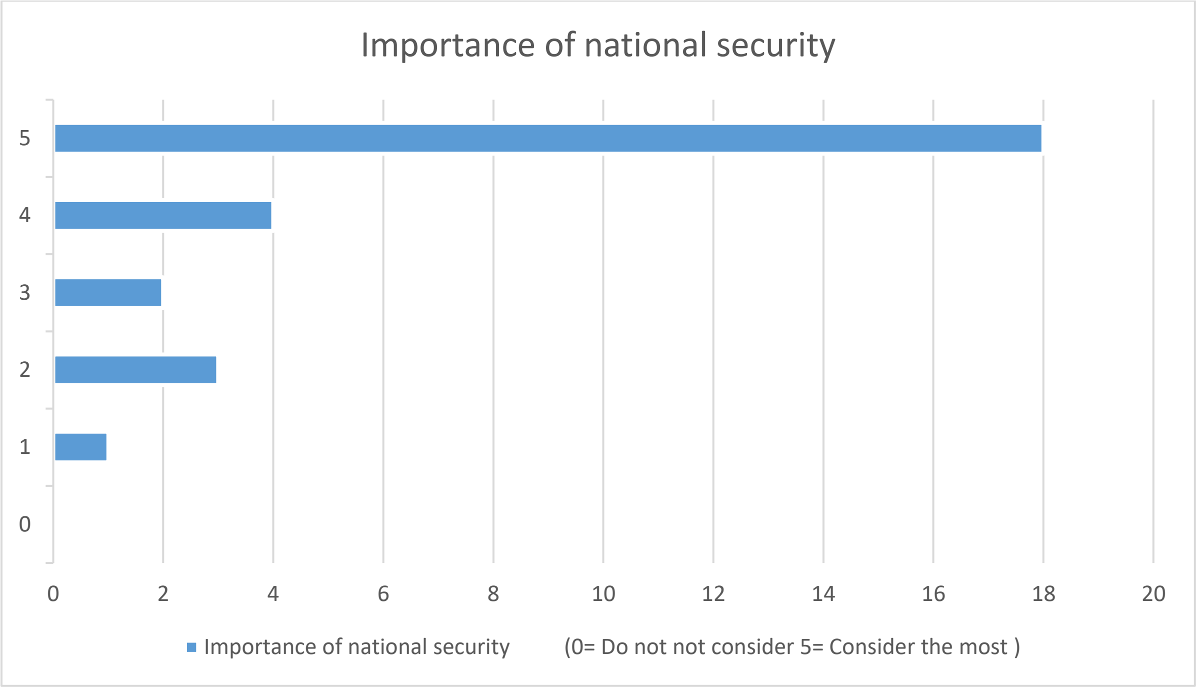


Figure E.91: Importance of national security (18-25-UK)

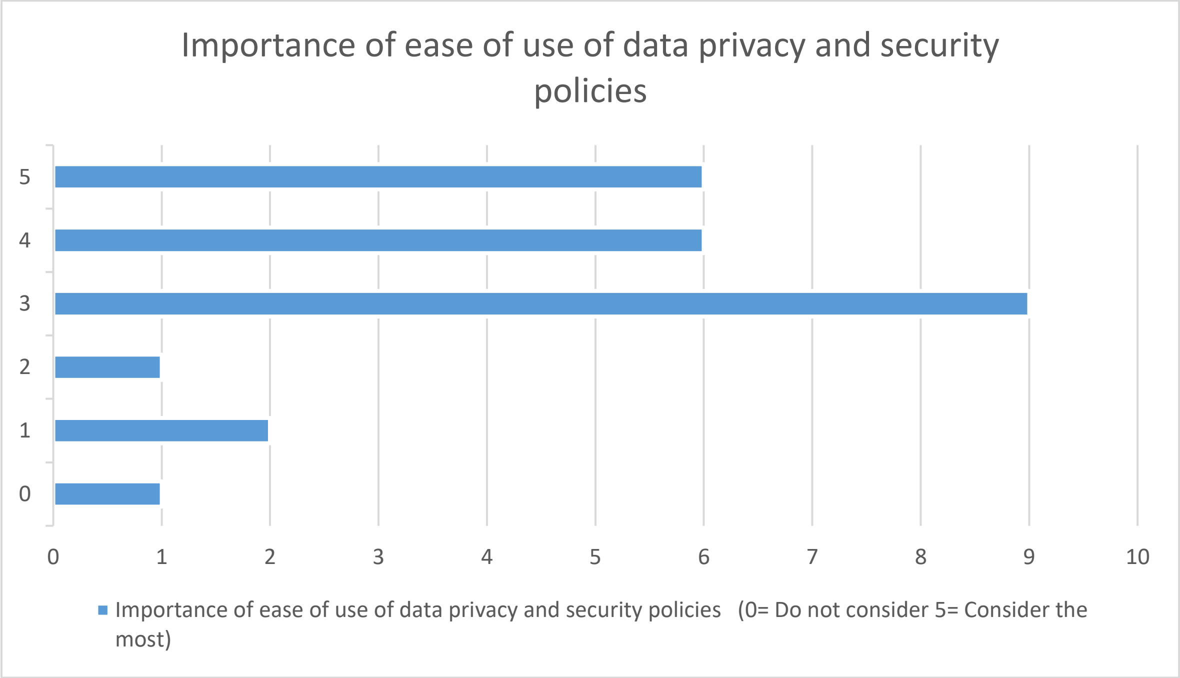


Figure E.92: Importance of ease of use of data privacy and security policies (18-25-UK)

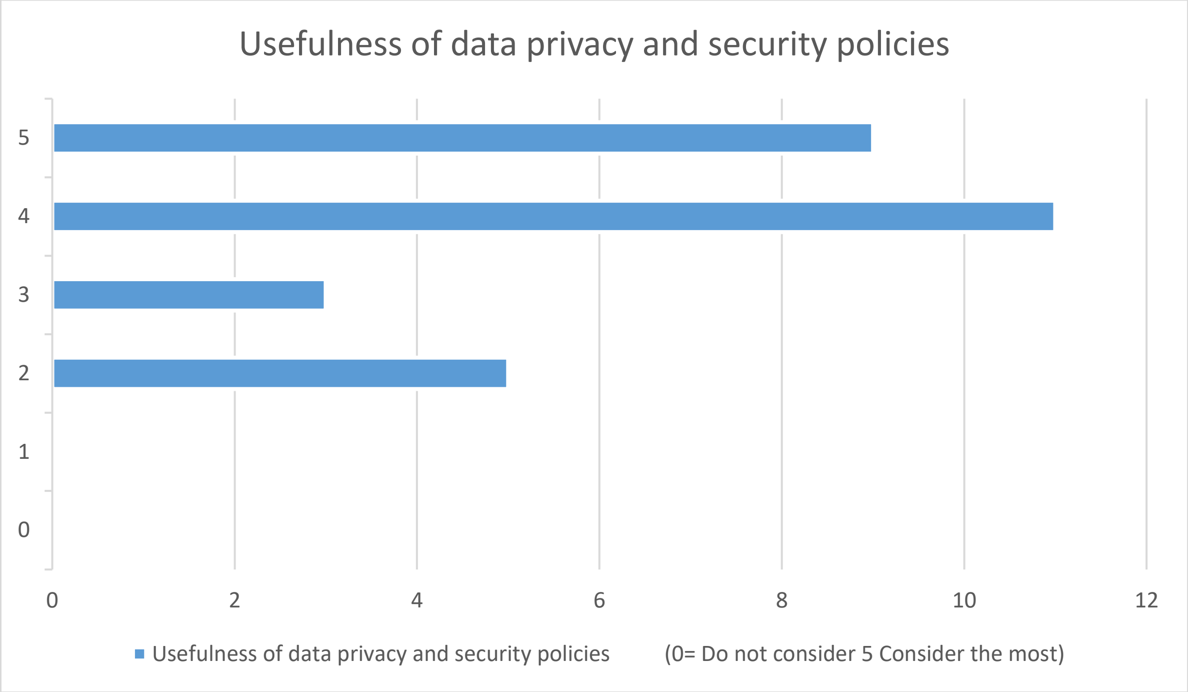


Figure E.93: Usefulness of data privacy and security policies (18-25-UK)

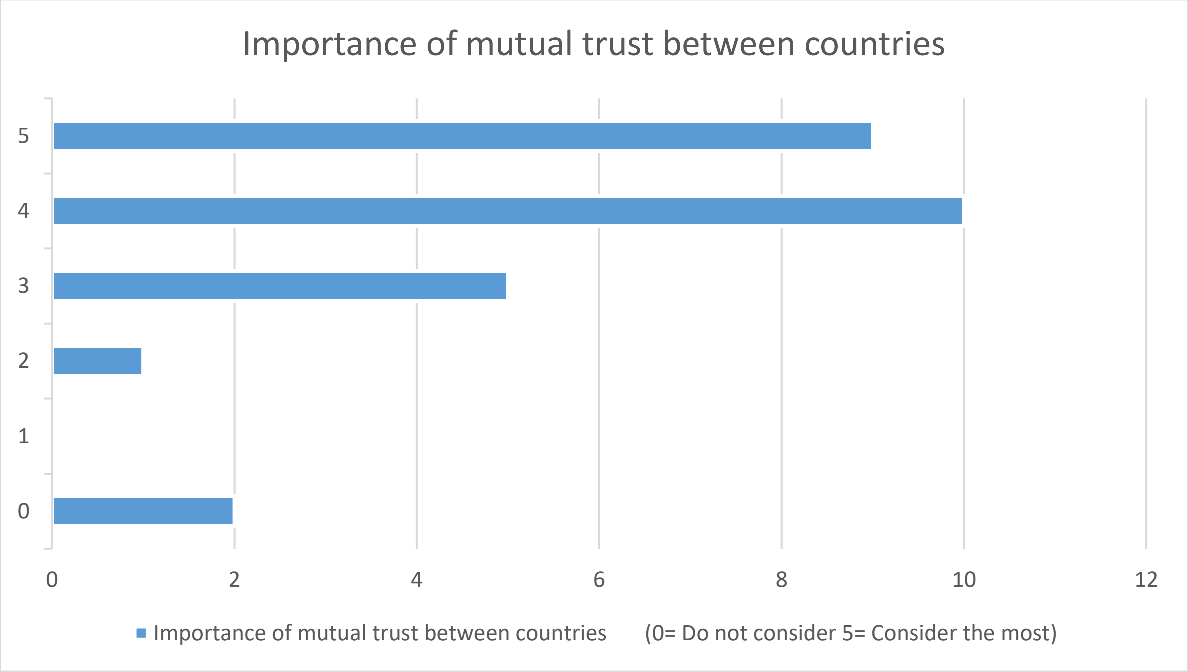


Figure E.94: Importance of mutual trust between countries (18-25-UK)

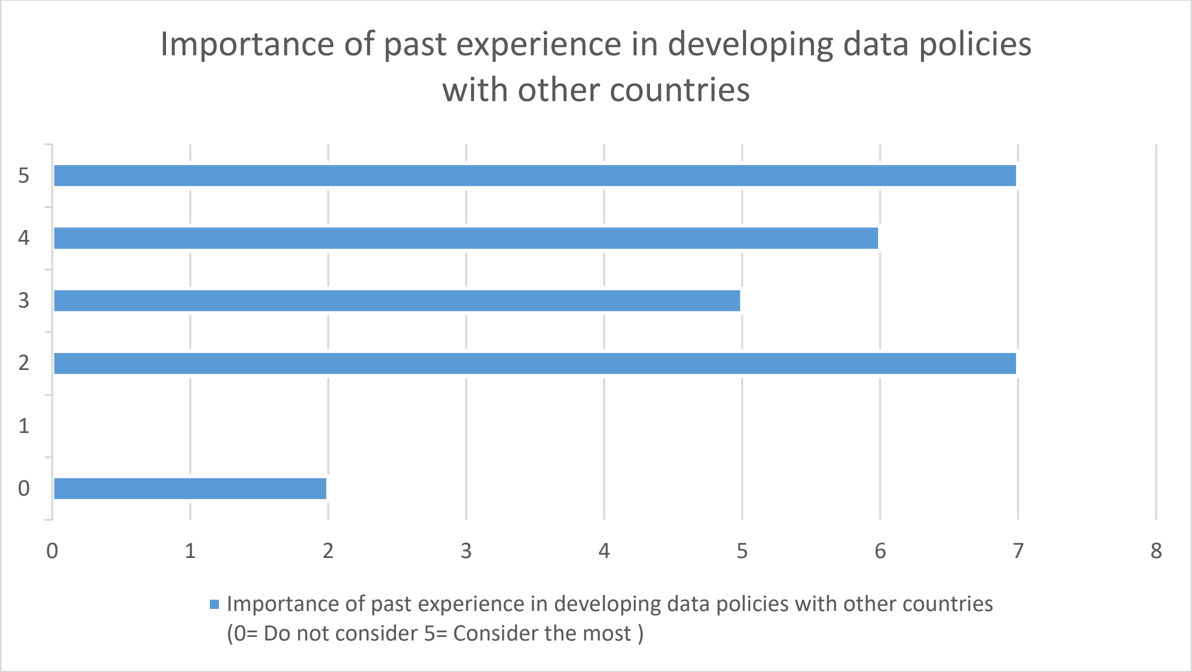


Figure E.95: Importance of past experience in developing data policies with other counties (18-25-UK)

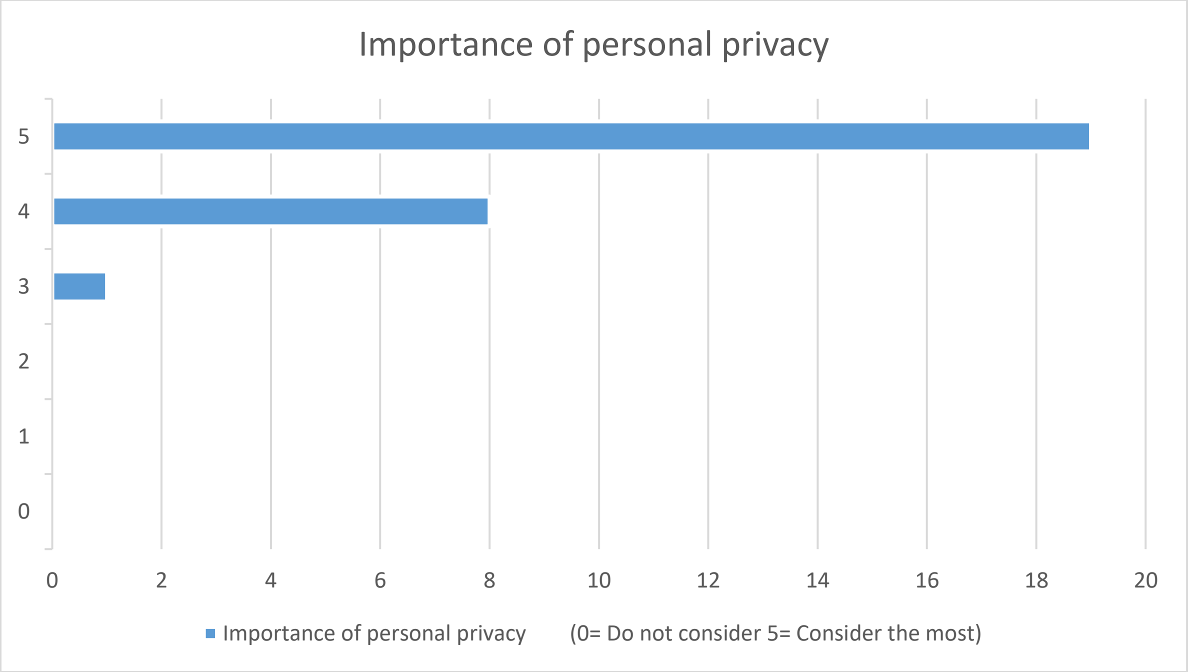


Figure E.96: Importance of personal privacy (18-25-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 70 percent of the respondents have endorsed (See figure E.85). The other notable factors that have come out of the survey are organisational support, budget allocation, personal privacy, national security, the usefulness of data privacy and security policies and mutual trust between countries (See figure E.74-84) (See figure E.86-96).

United Kingdom – 26-35

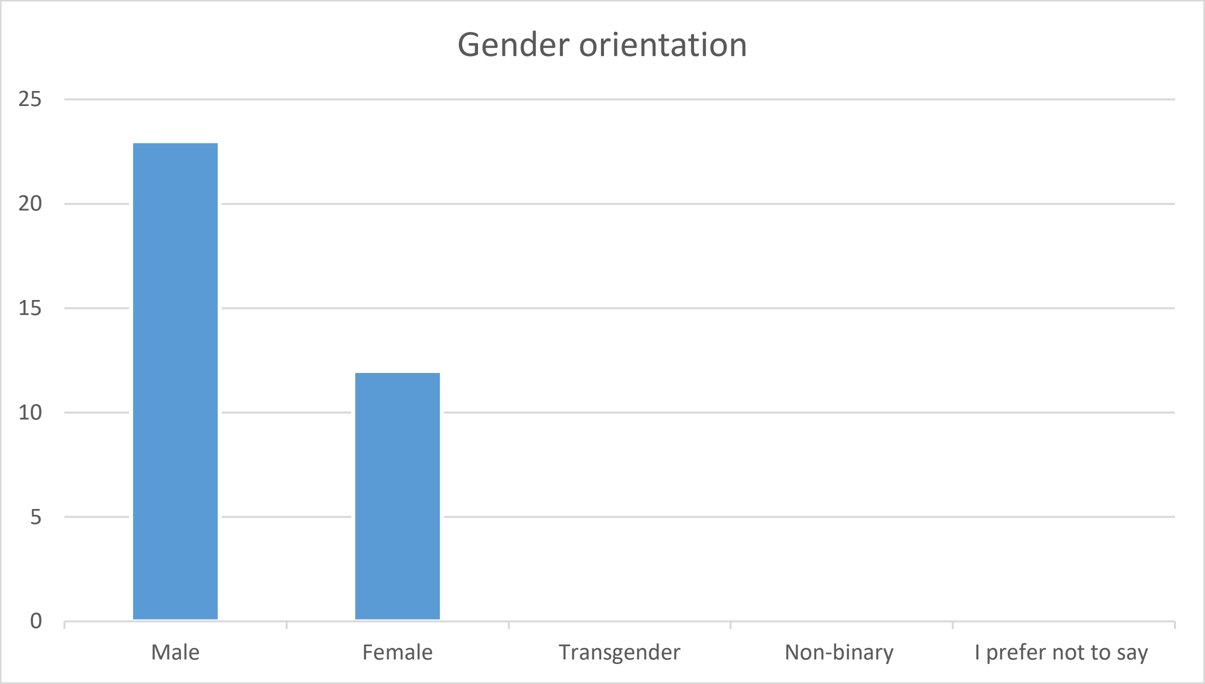


Figure E.97: Gender orientation (26-35-UK)

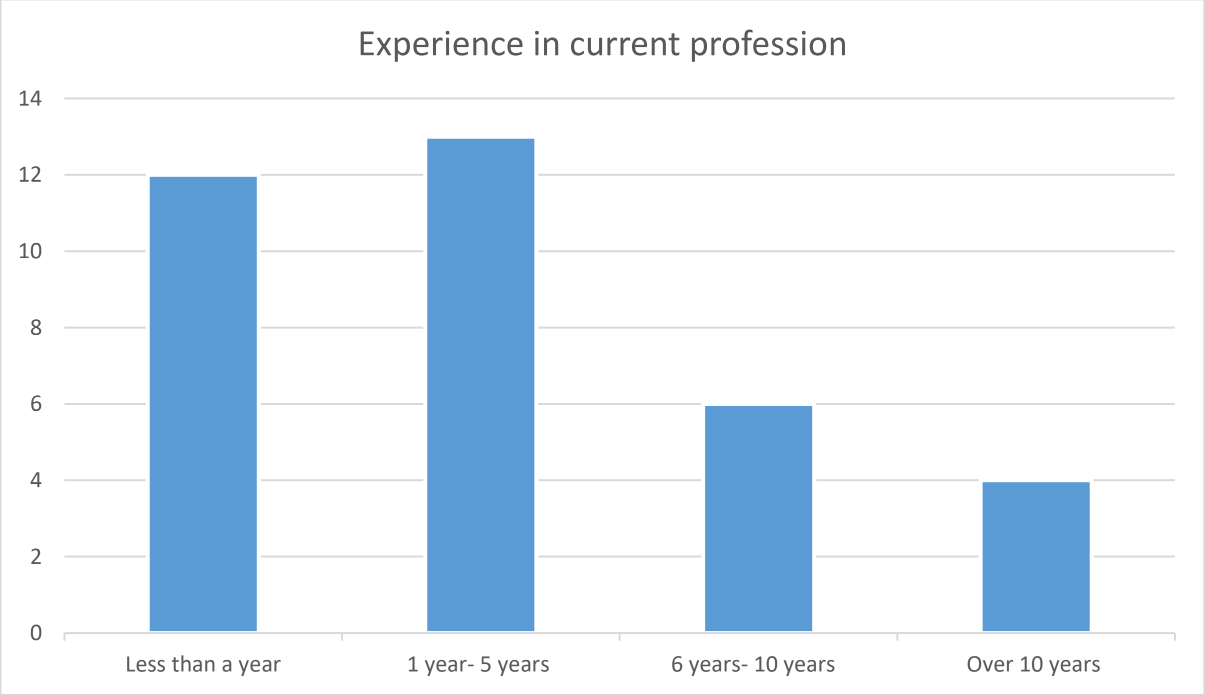


Figure E.98: Experience in current profession (26-35-UK)

This analysis is based on the responses received from United Kingdom participants aged between 26-35. There were 35 participants and 23 out of them were males and 12 females (See figure E.97). The participants have been in employment for less than a year to over 10 years (See figure E.98).

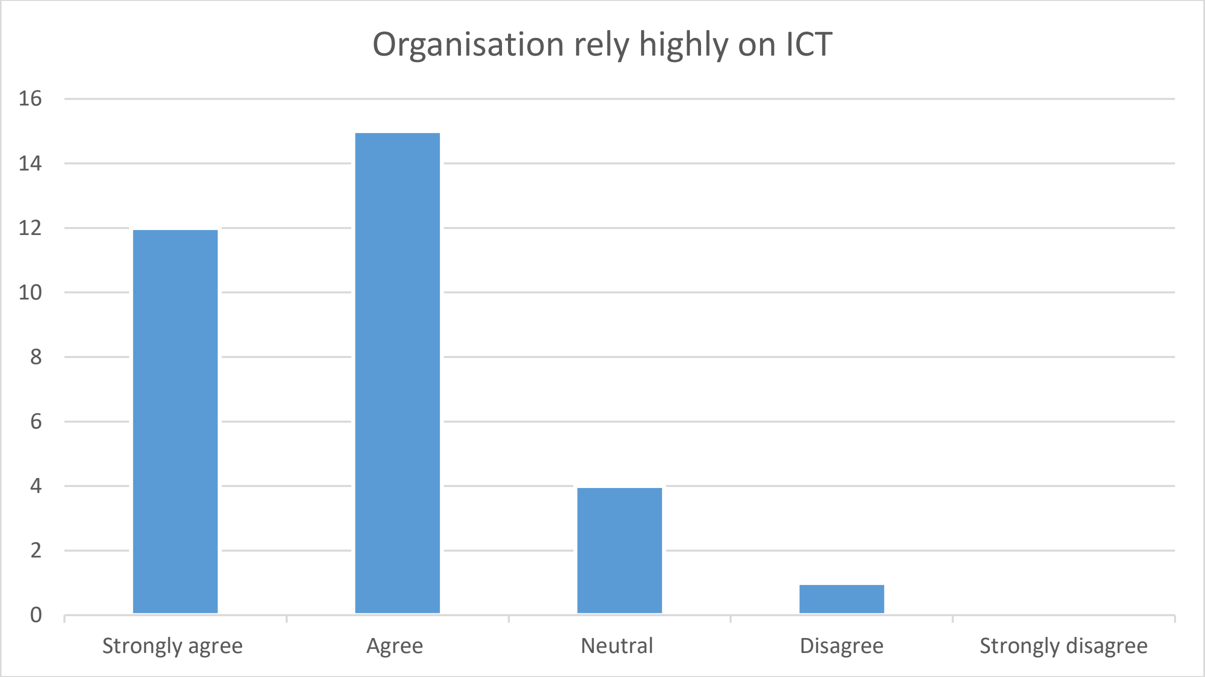


Figure E.99: Organisation rely highly on ICT (26-35-UK)

Out of the 35 respondents, 27 have worked in a technology reliance working environment, 4 unaware of reliance on technology because of the nature of the work assigned to them, 1 have marked 'disagree' on ICT (See figure E.99). The majority of the employees within the 26-35 age range have a high reliance on ICT.

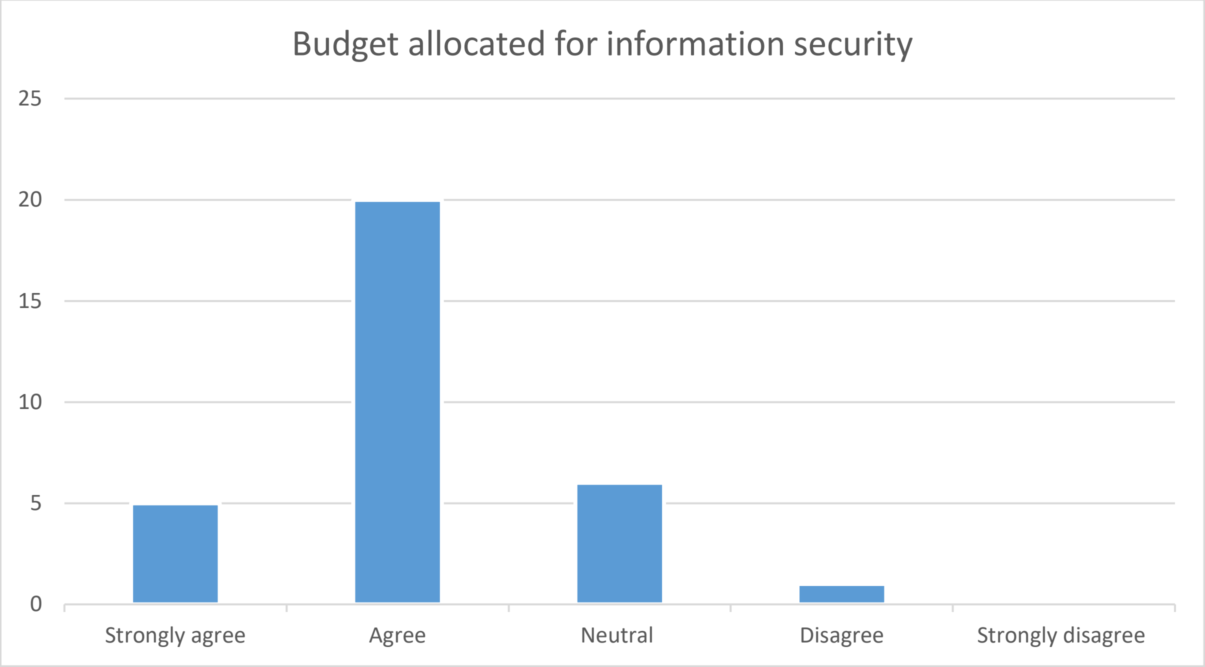


Figure E.100: Budget allocated for information security (26-35-UK)

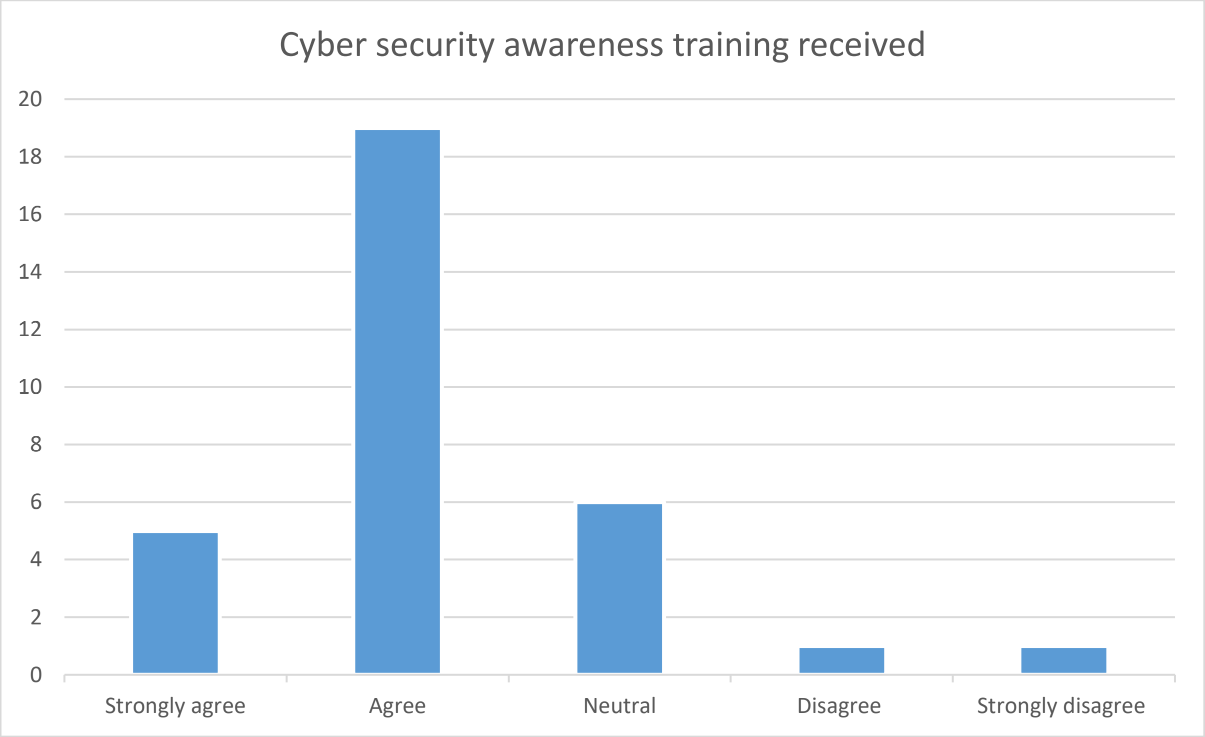


Figure E.101: Cyber security awareness training received (26-35-UK)

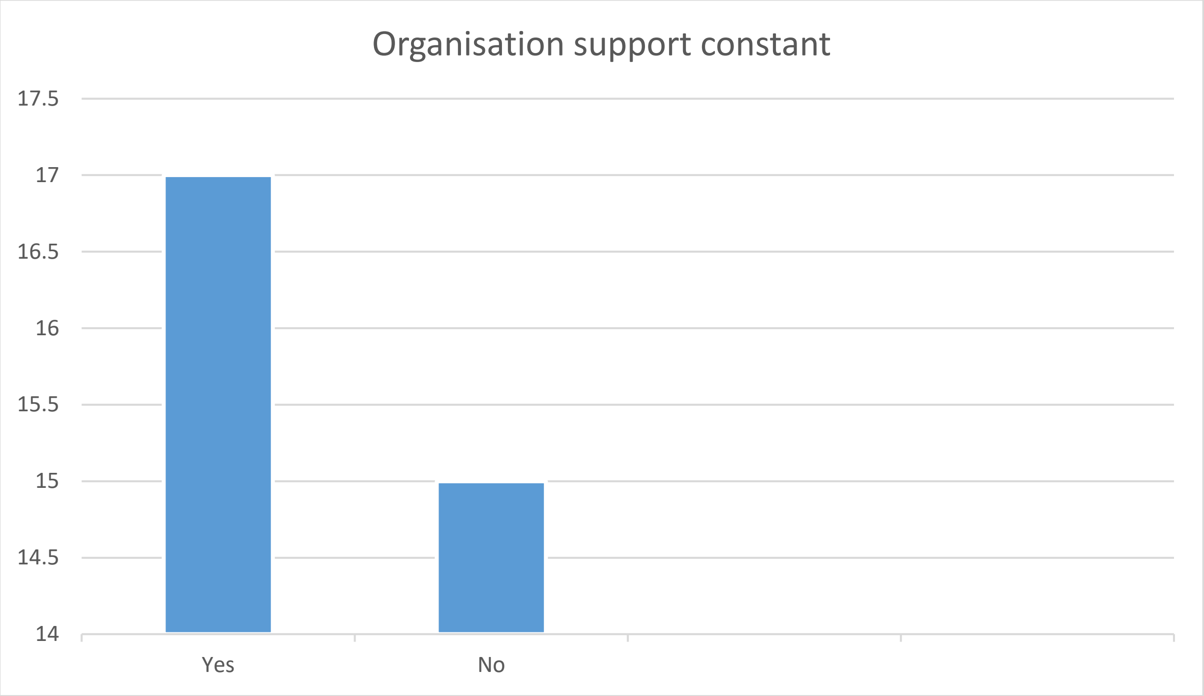


Figure E.102: Organisation support constant (26-35-UK)

Funding has been sketchy. 25 out of the 35 have indicated that their organisations had an allocated budget for information security, whilst 6 had not expressed an opinion either way and notably according to the 1 disagreed, their organisations had no budget allocation for information security (See figure E.100). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was also adequate. 24 participants have received regular cybersecurity awareness training, whilst 6 neither agreed nor disagreed, and 2 participants had not regularly received security awareness training (See figure E.101). In addition, 15 participants had not received support from the organisation to protect personal information, whilst 17 did. (See figure E.102). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

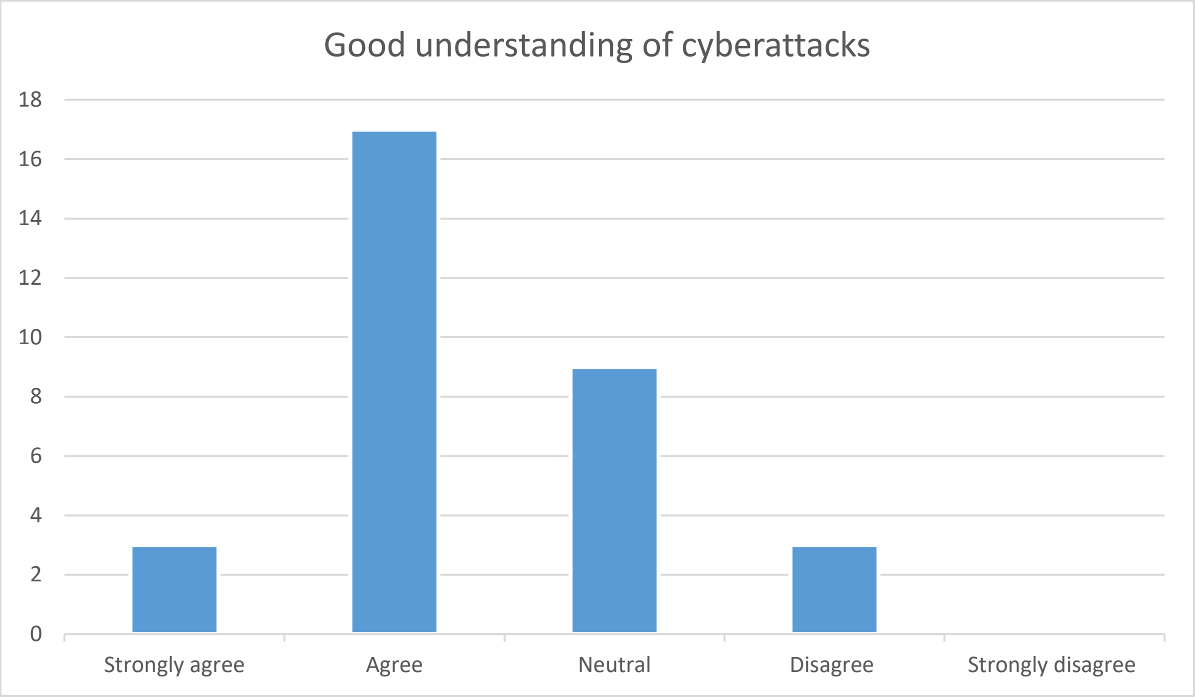


Figure E.103: Good understanding of cyberattacks (26-35-UK)

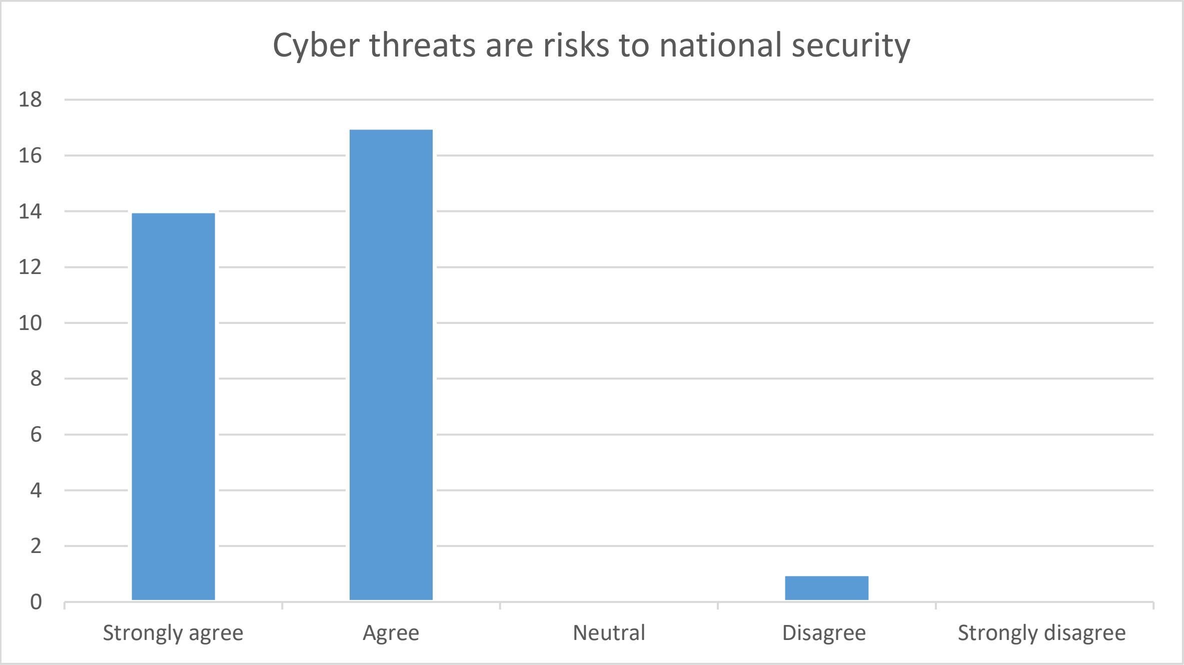


Figure E.104: Cyber threats are risks to national security (26-35-UK)

Despite the security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 20 participants do have, 9 have not expressed opinion either way, and only 3 participants had no understanding (See figure E.103). Furthermore, 67 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure E.104). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

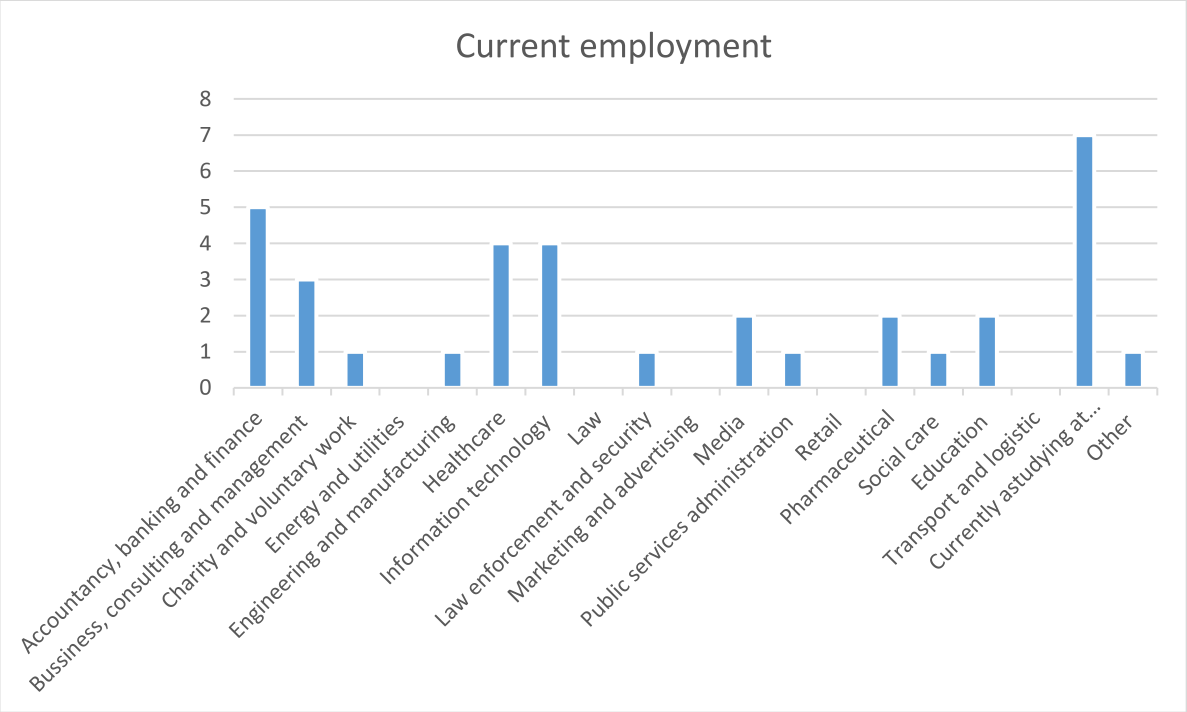


Figure E.105: Current employment (26-35-UK)

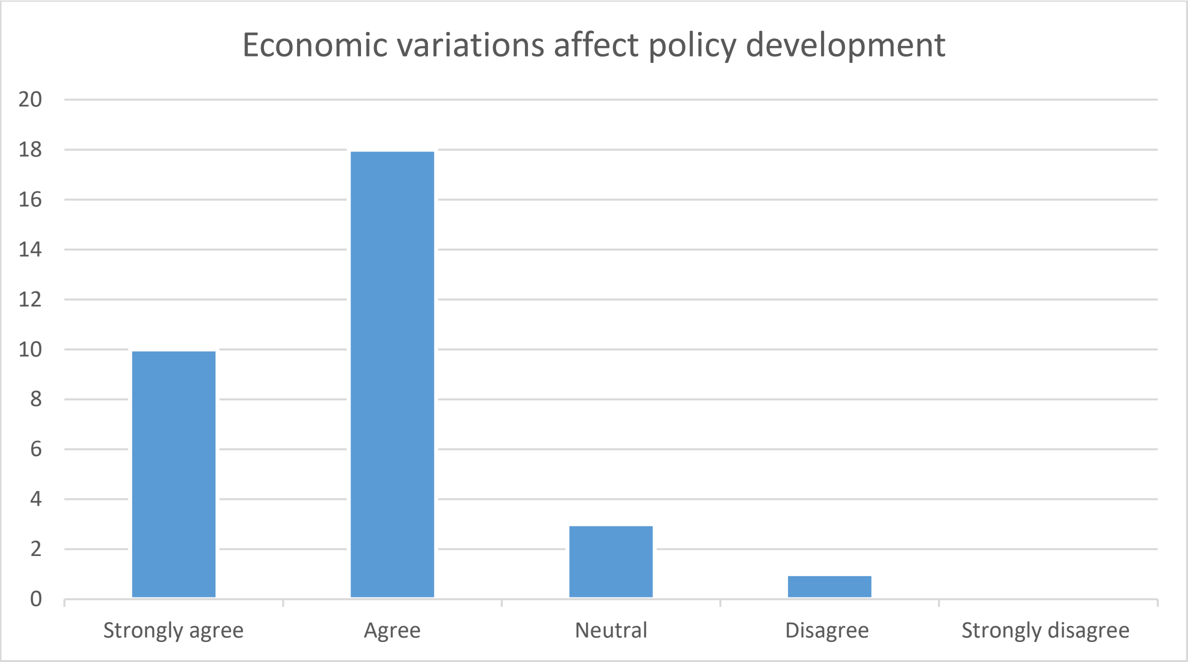


Figure E.106: Economic variations affect policy development (26-35-UK)

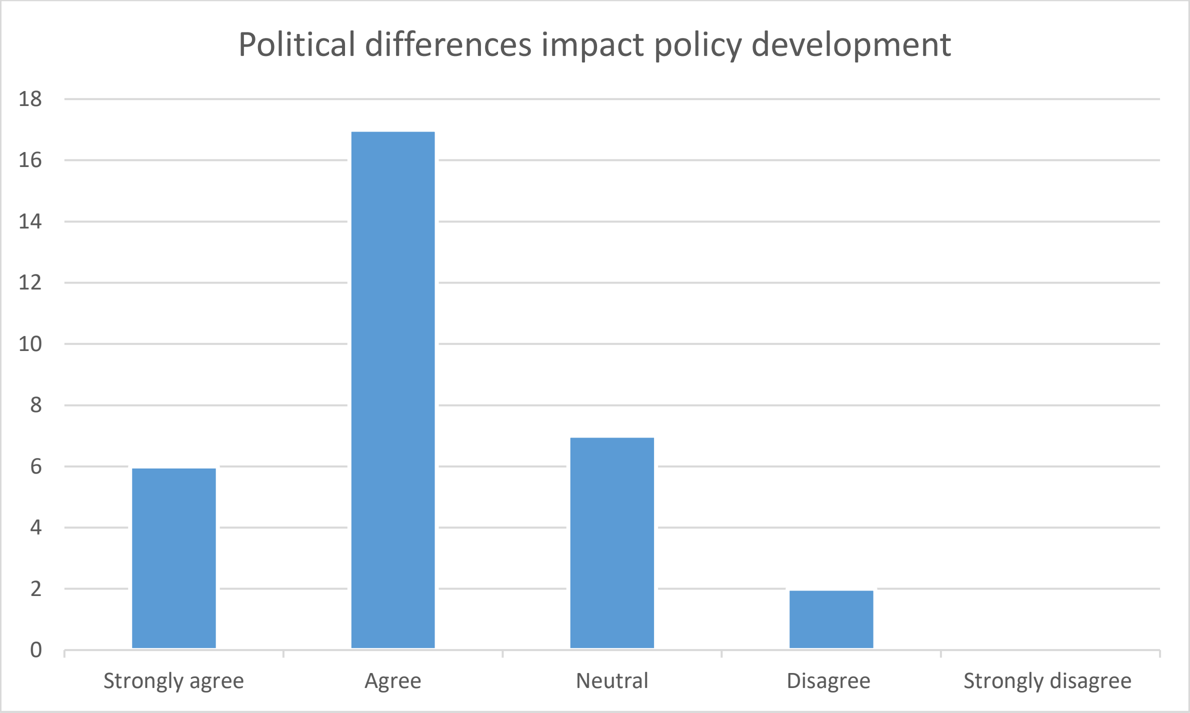


Figure E.107: Political differences impact policy development (26-35-UK)

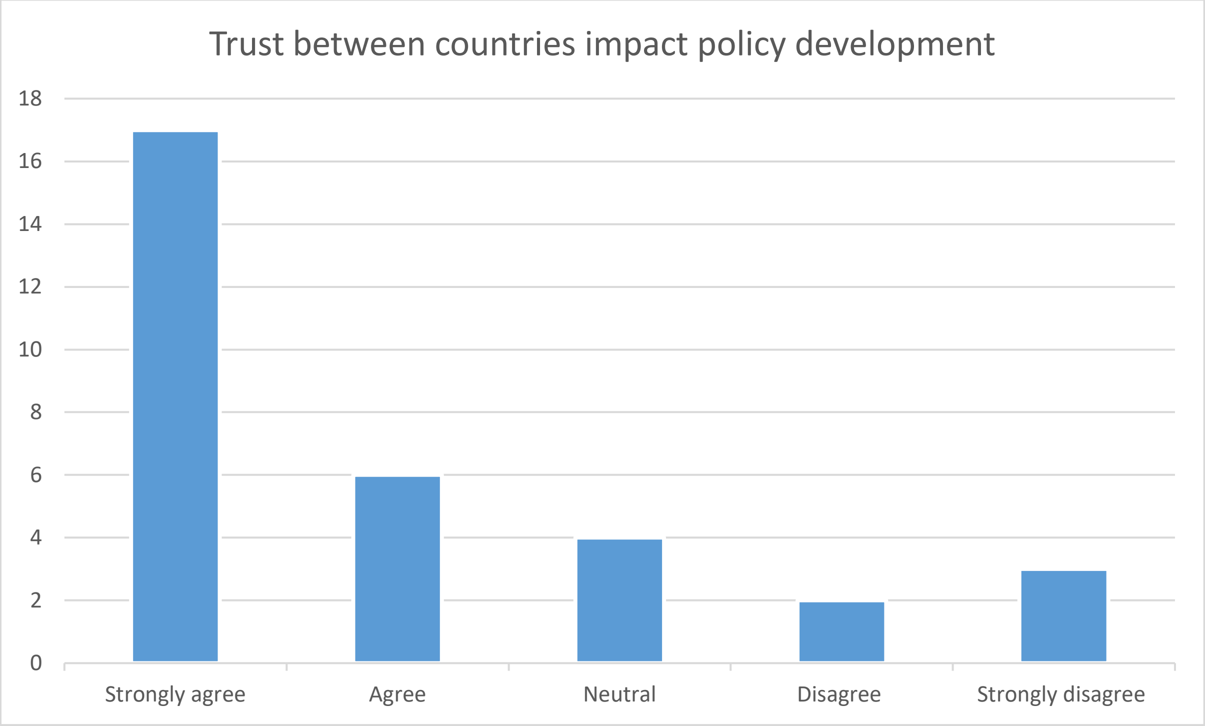


Figure E.108: Trust between countries impact policy development (26-35-UK)

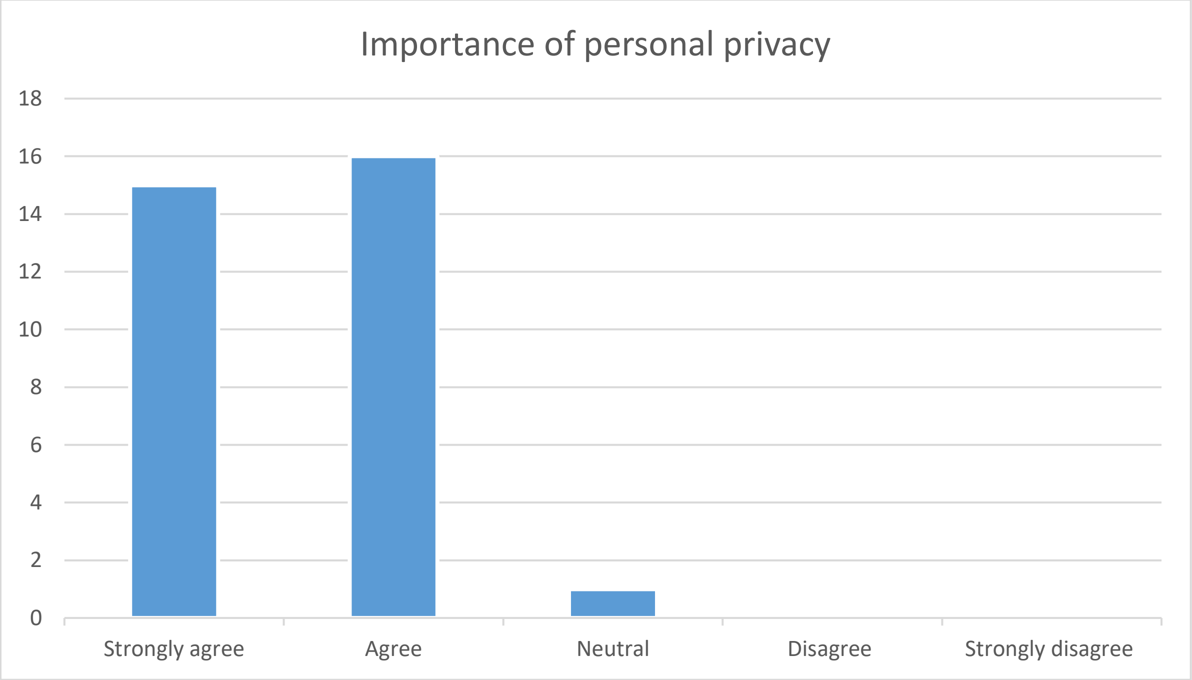


Figure E.109: Importance of personal privacy (26-35-UK)

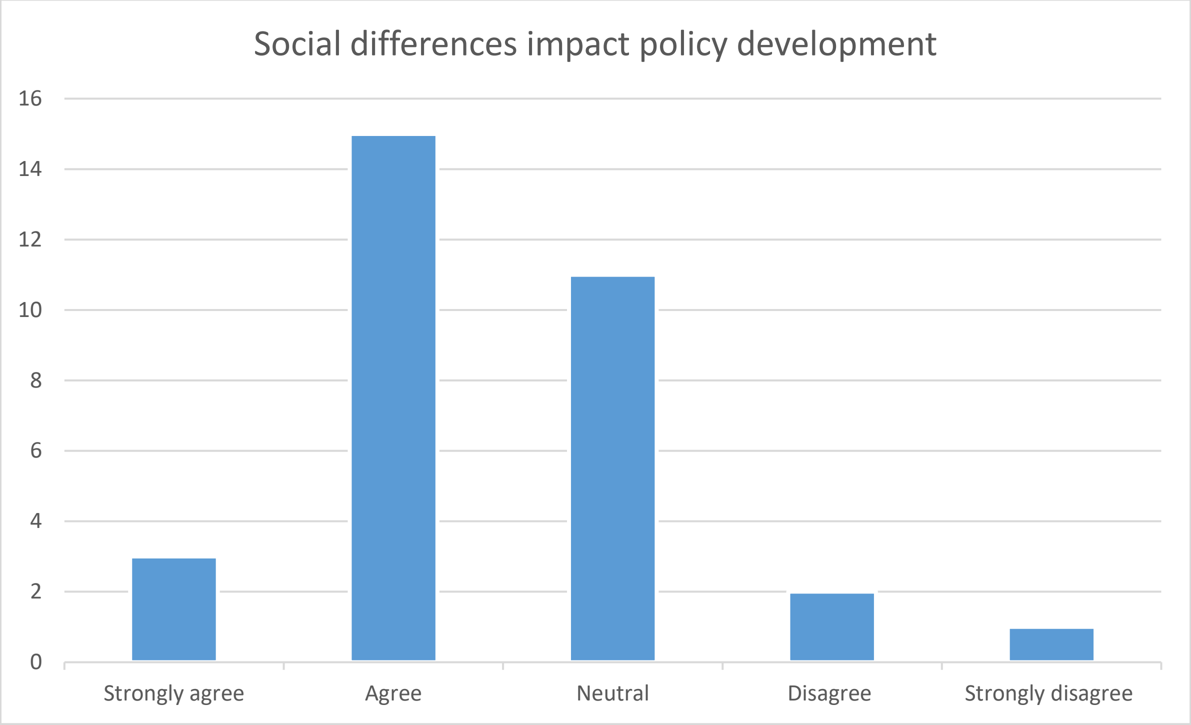


Figure E.110: Social differences impact policy development (26-35-UK)

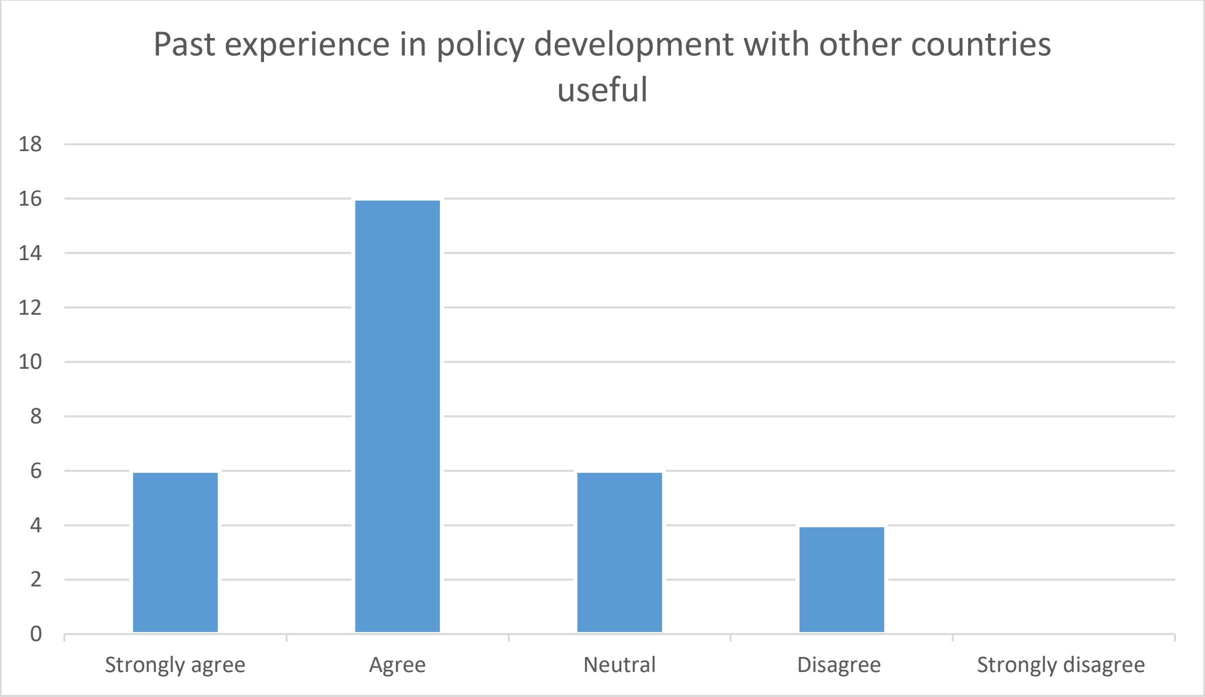


Figure E.111: Past experience in policy development with other countries useful (26-35-UK)

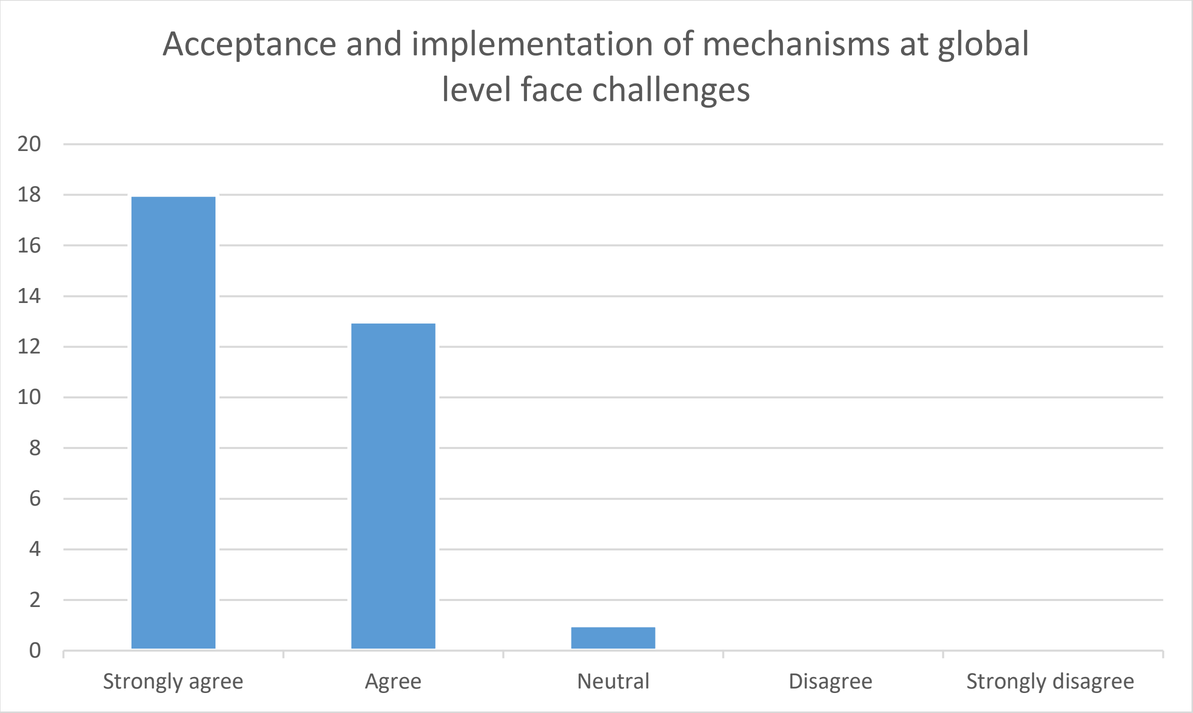


Figure E.112: Acceptance and implementation of mechanisms at global level face challenges (26-35-UK)

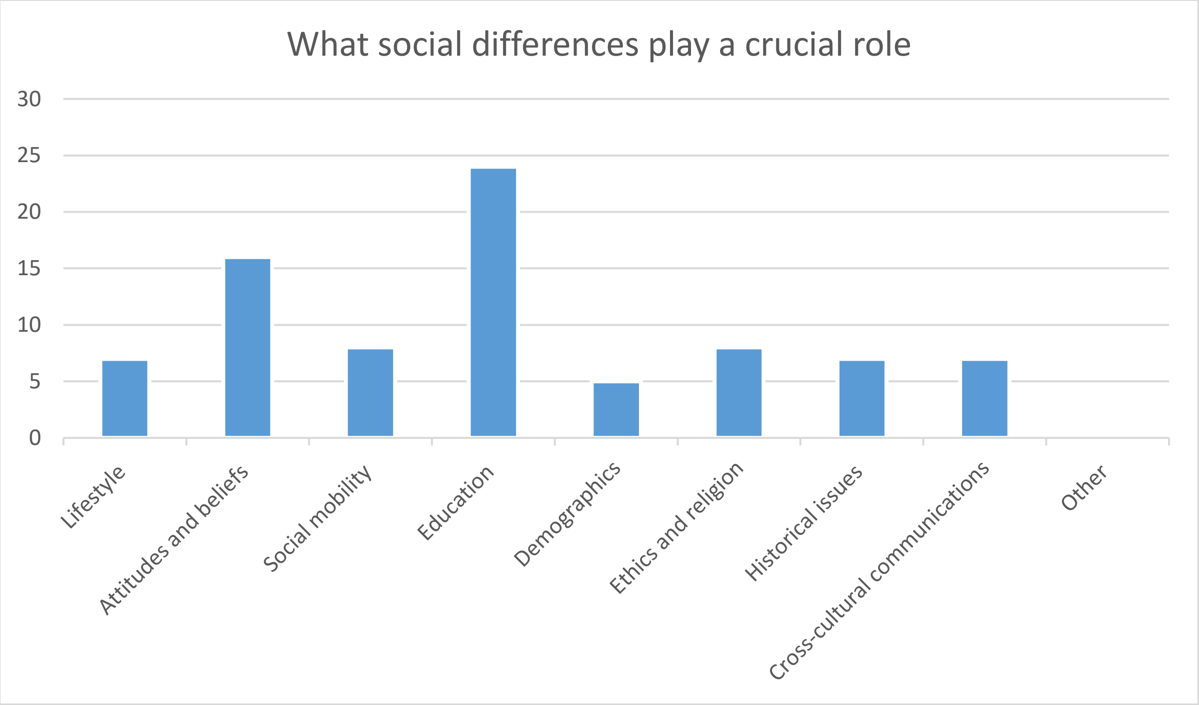


Figure E.113: What social differences play a crucial role (26-35-UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education (See figure E.113). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level.

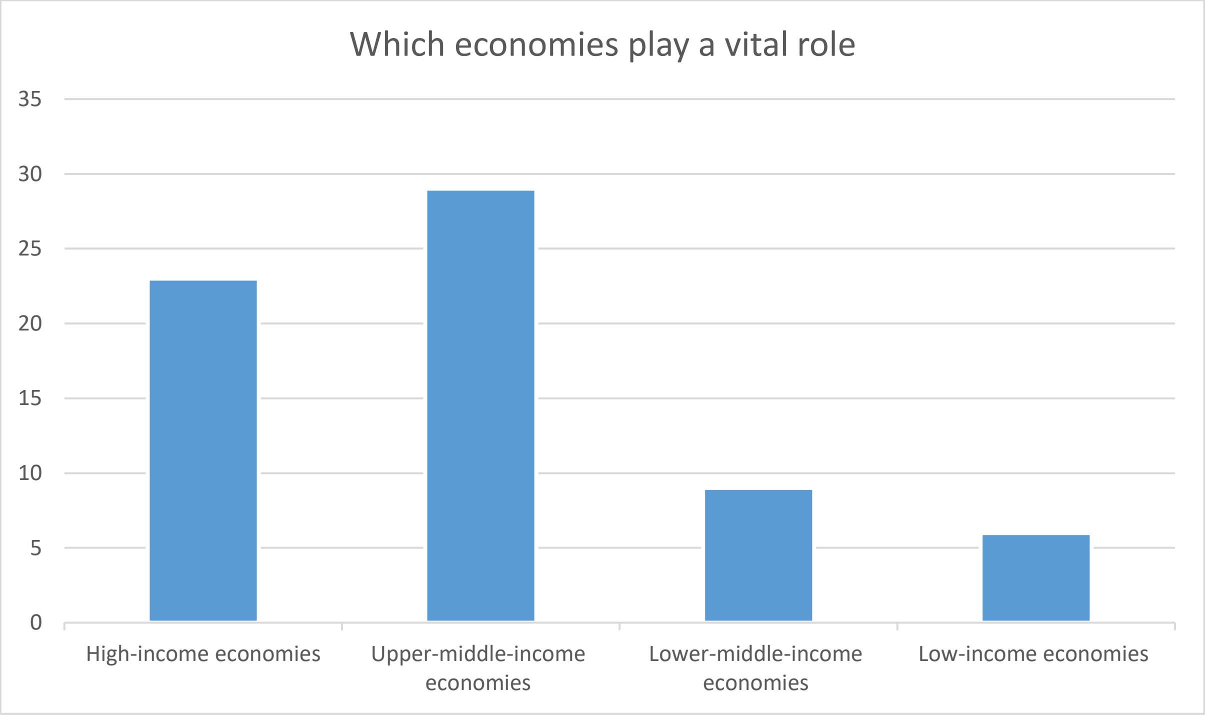


Figure E.114: Which economies play a vital role (26-35-UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.114). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

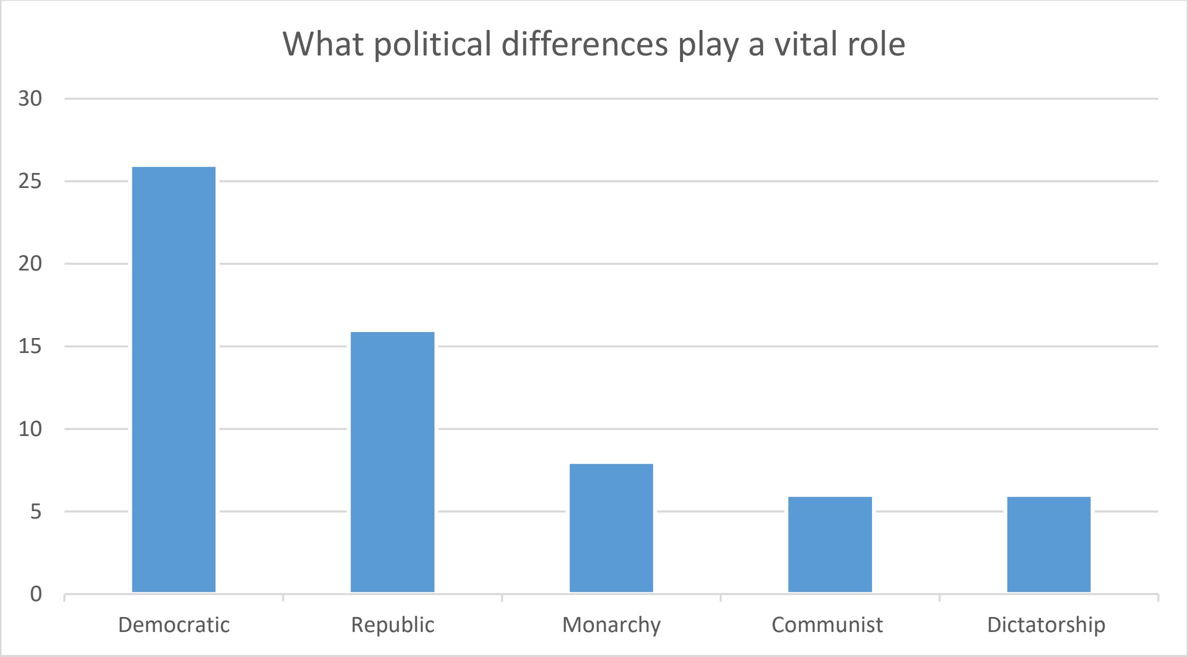


Figure E.115: What political differences play a vital role (26-35-UK)

The majority have chosen democratic political system (See figure E.115), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

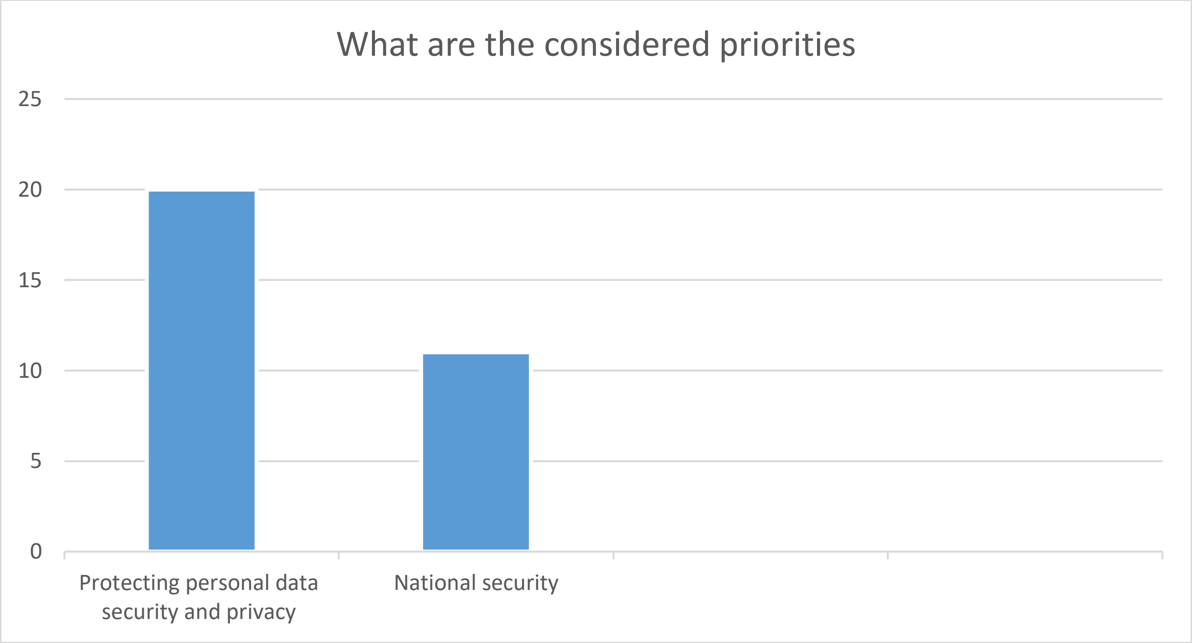


Figure E.116: What are the considered priorities (26-35-UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security (See figure E.116), which is a significant factor. However, in an incident of a personal data breach, there will potentially be a knock-on effect on national security, and it will also be felt right across the groups as well as the community alike.

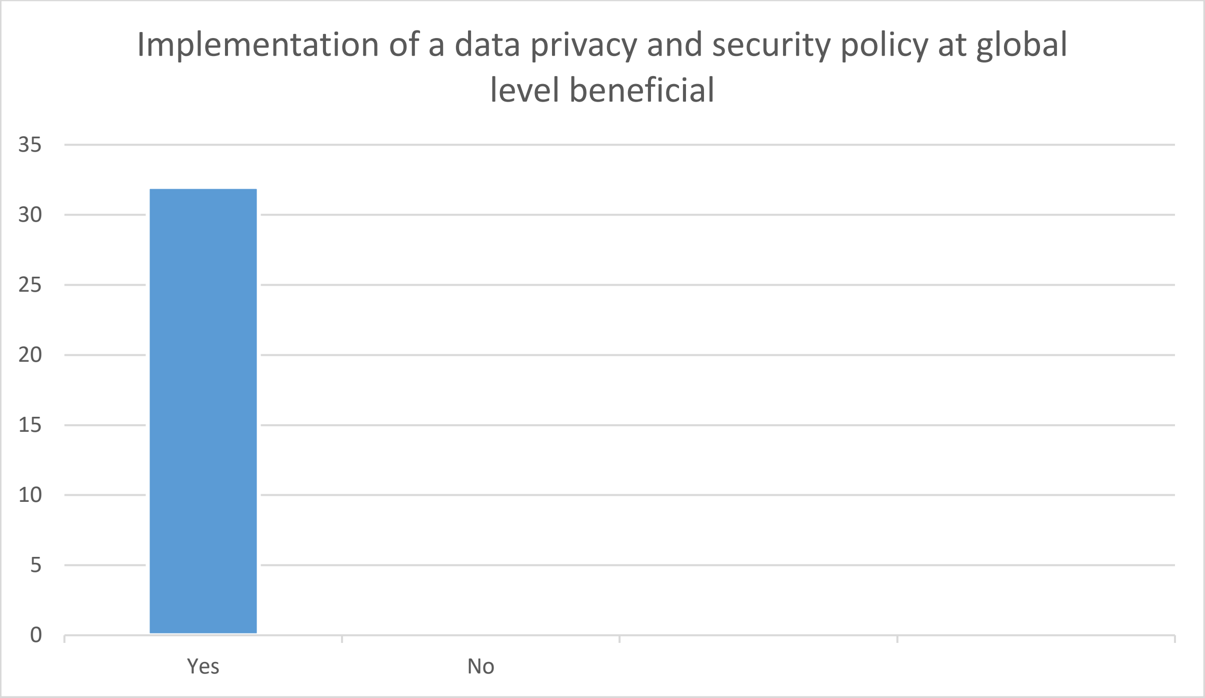


Figure E.117: Implementation of a data privacy and security policy at global level beneficial (26-35-UK)

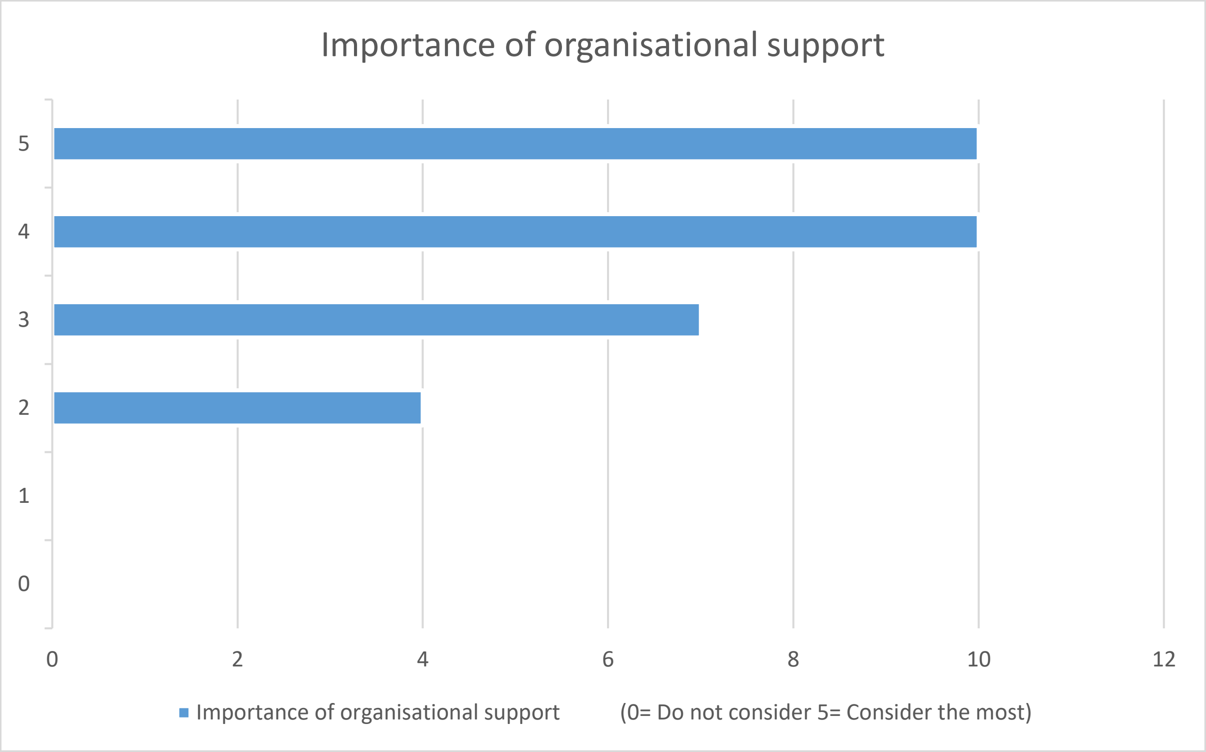


Figure E.118: Importance of organisational support (26-35-UK)

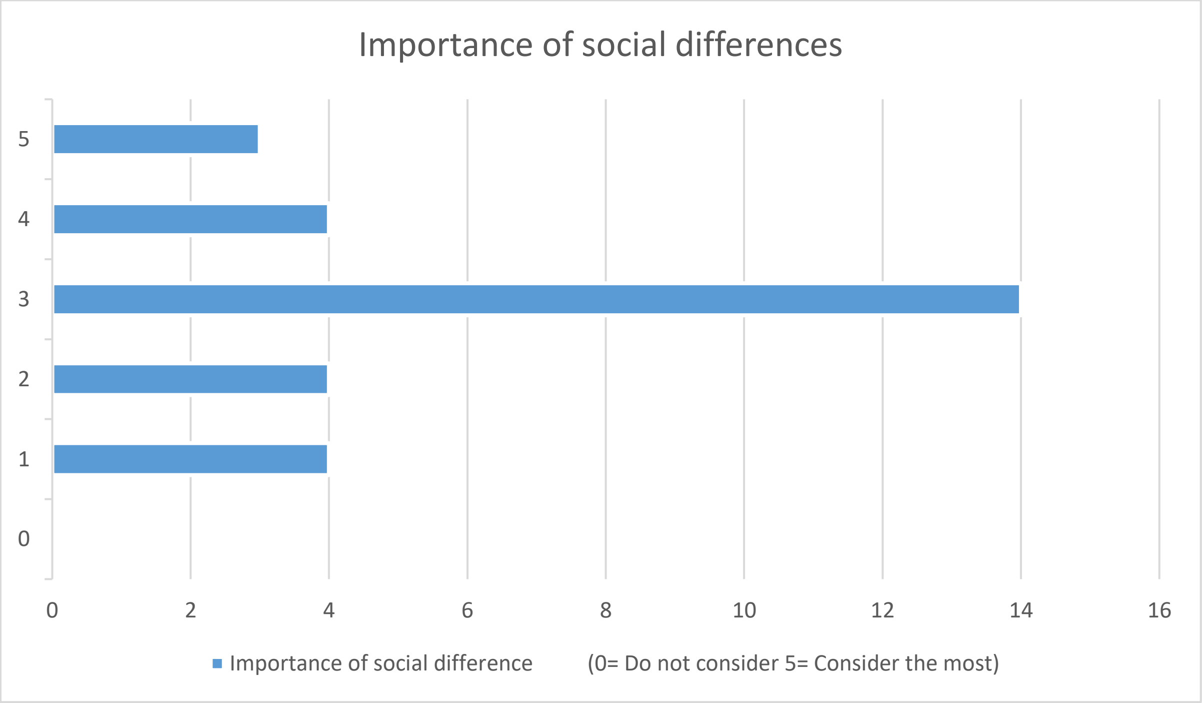


Figure E.119: Importance of social differences (26-35-UK)

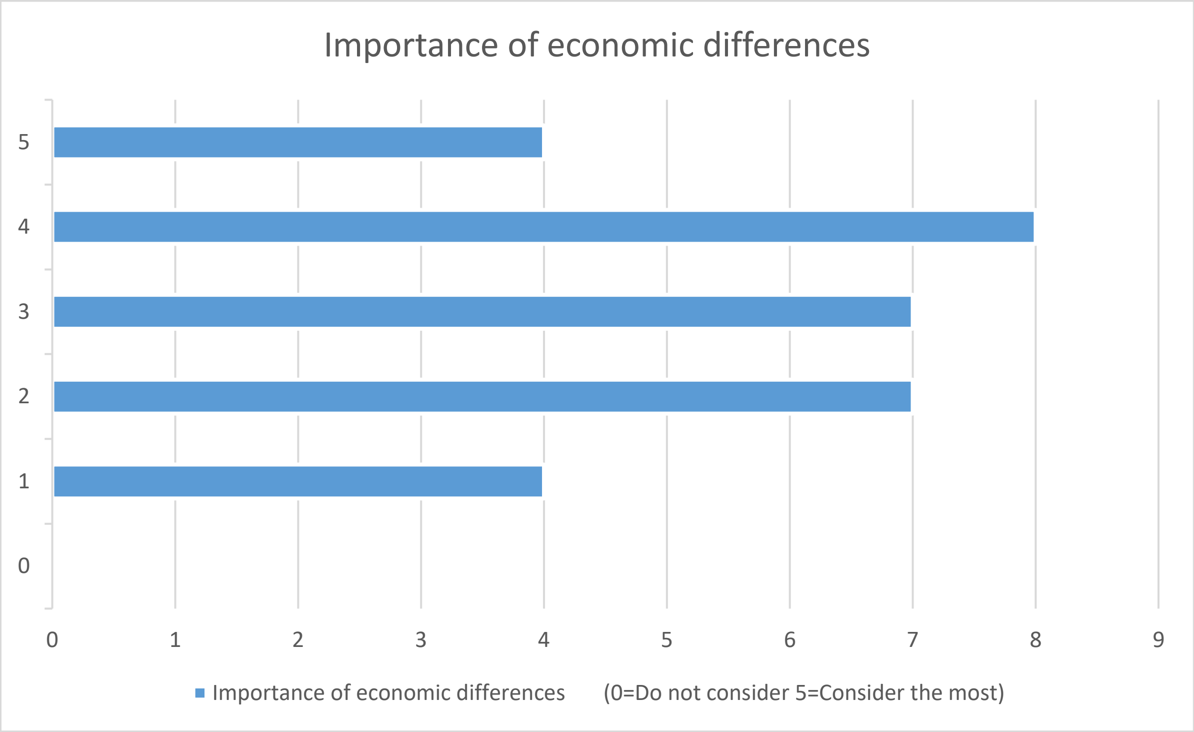


Figure E.120: Importance of economic differences (26-35-UK)

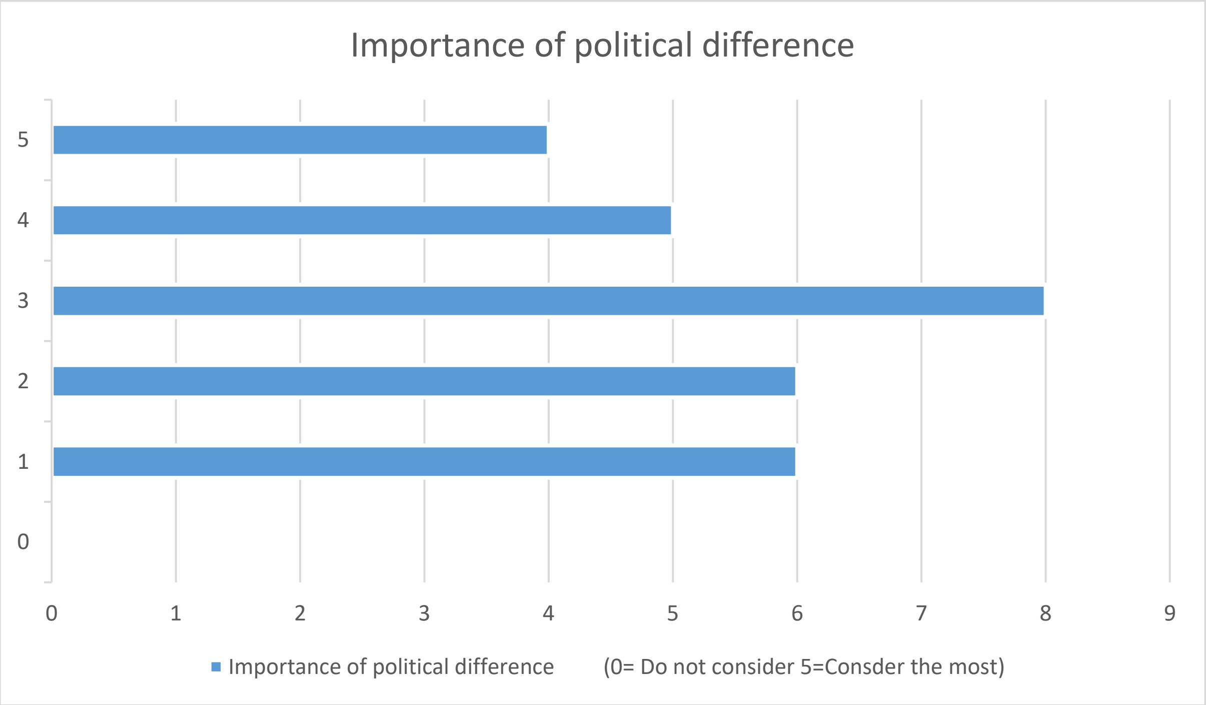


Figure E.121: Importance of political difference (26-35-UK)

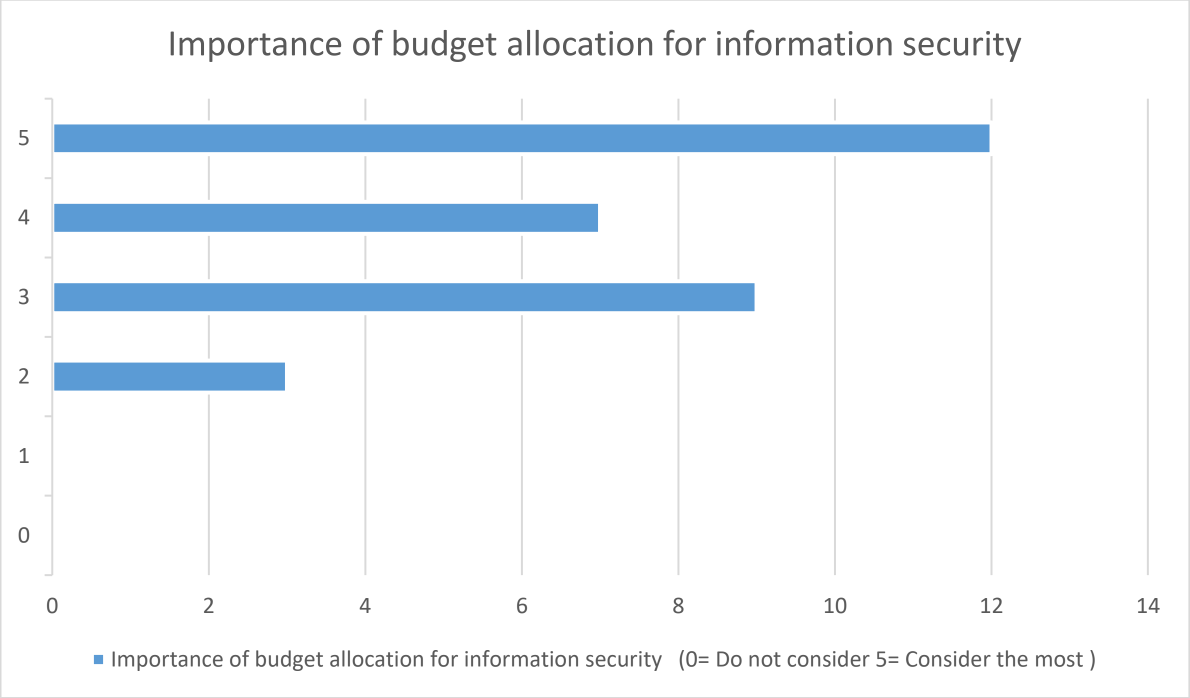


Figure E.122: Importance of budget allocation for information security (26-35-UK)

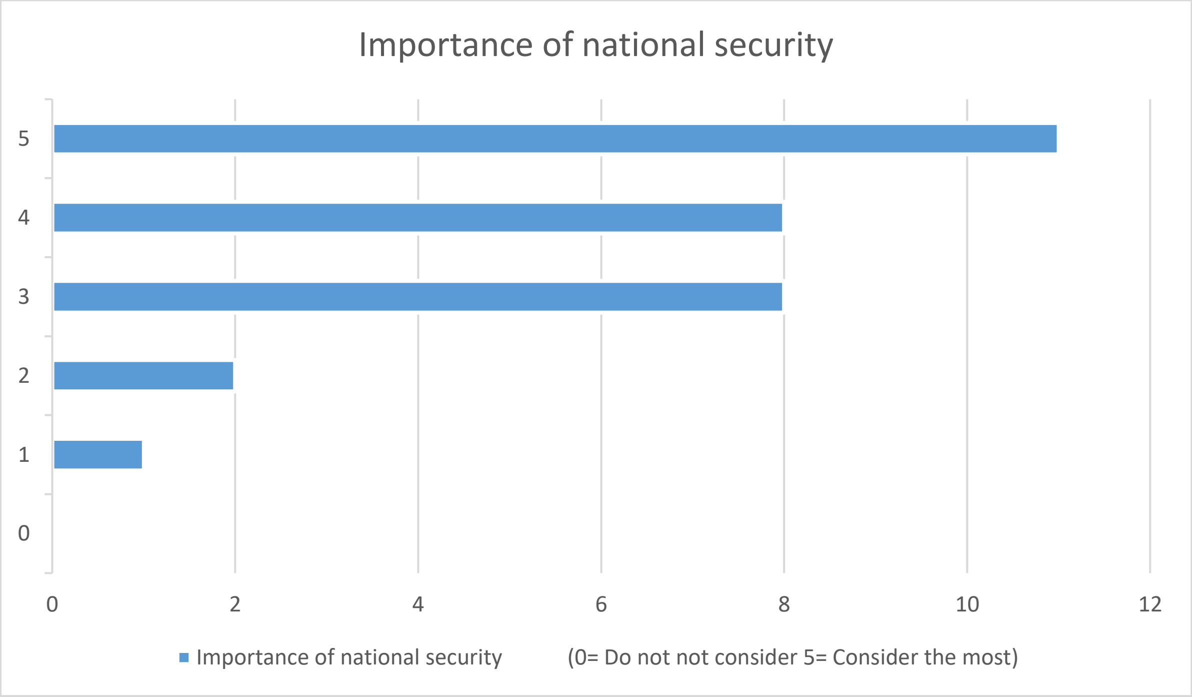


Figure E.123: Importance of national security (26-35-UK)

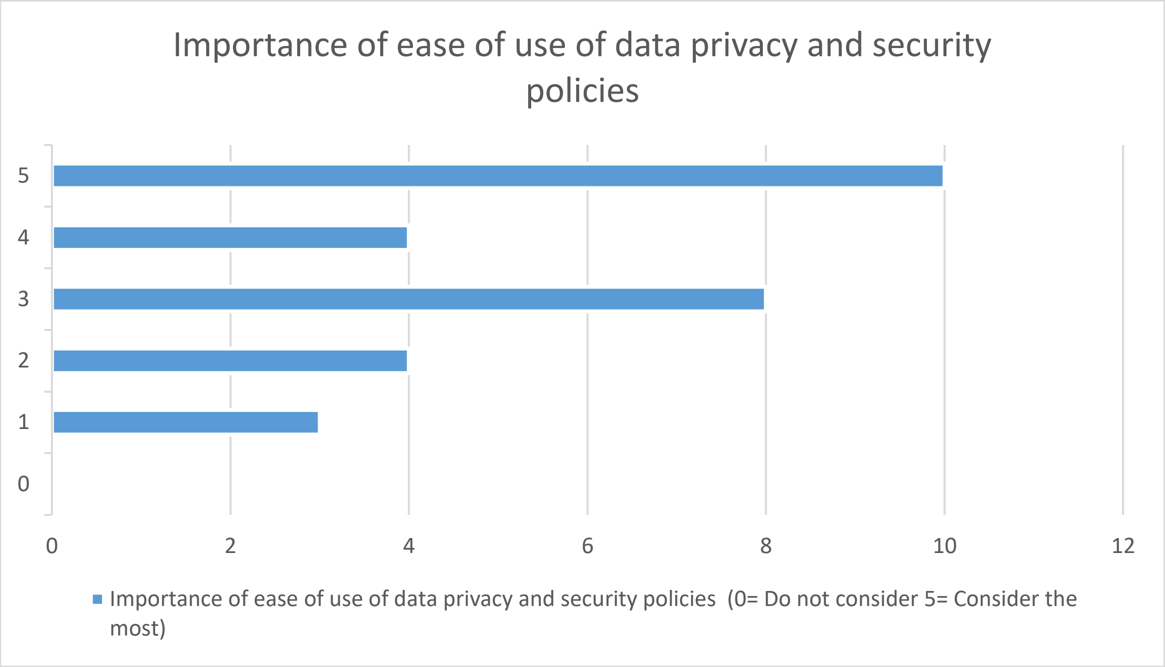


Figure E.124: Importance of ease of use of data privacy and security policies (26-35-UK)

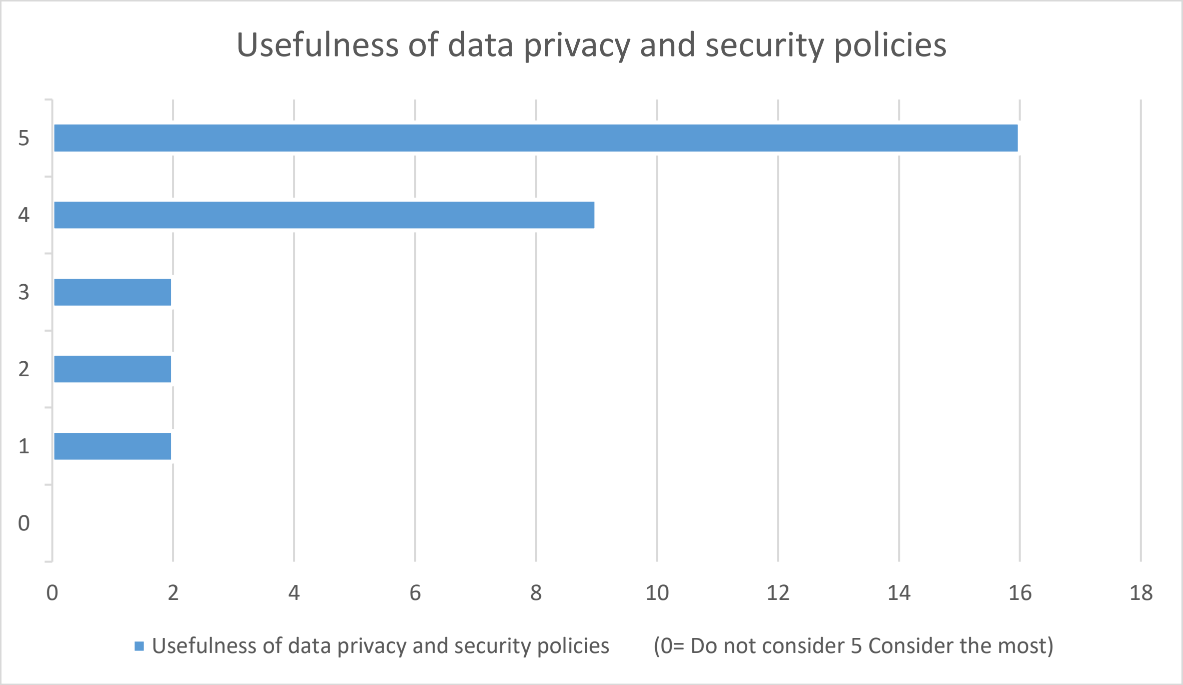


Figure E.125: Usefulness of data privacy and security policies (26-35-UK)

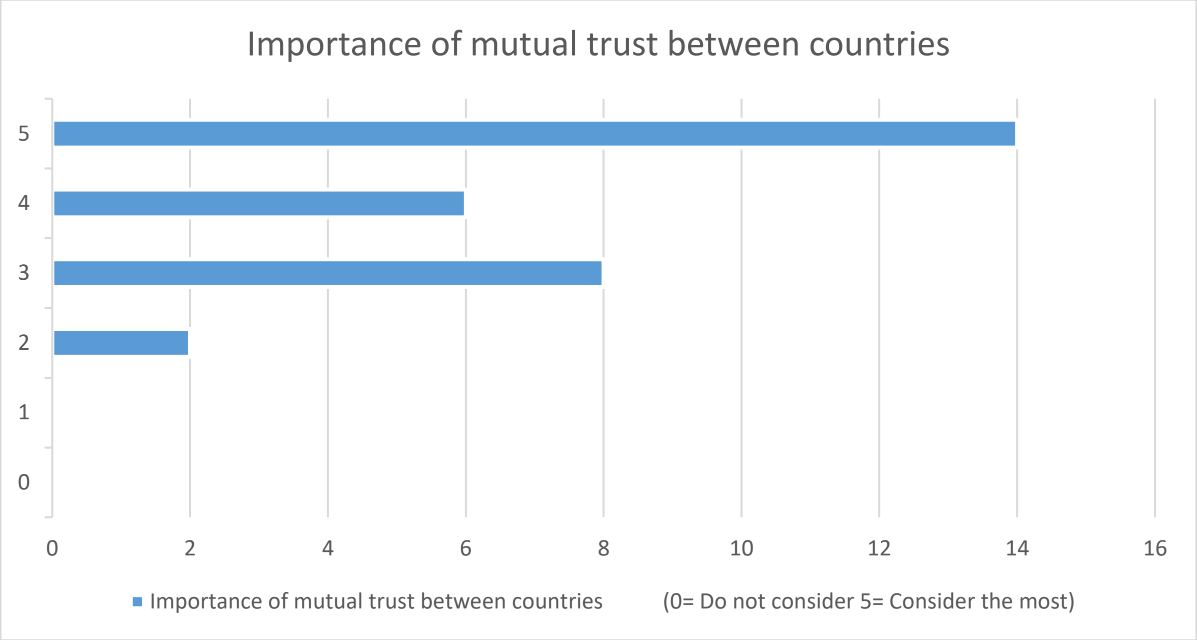


Figure E.126: Importance of mutual trust between countries (26-35-UK)

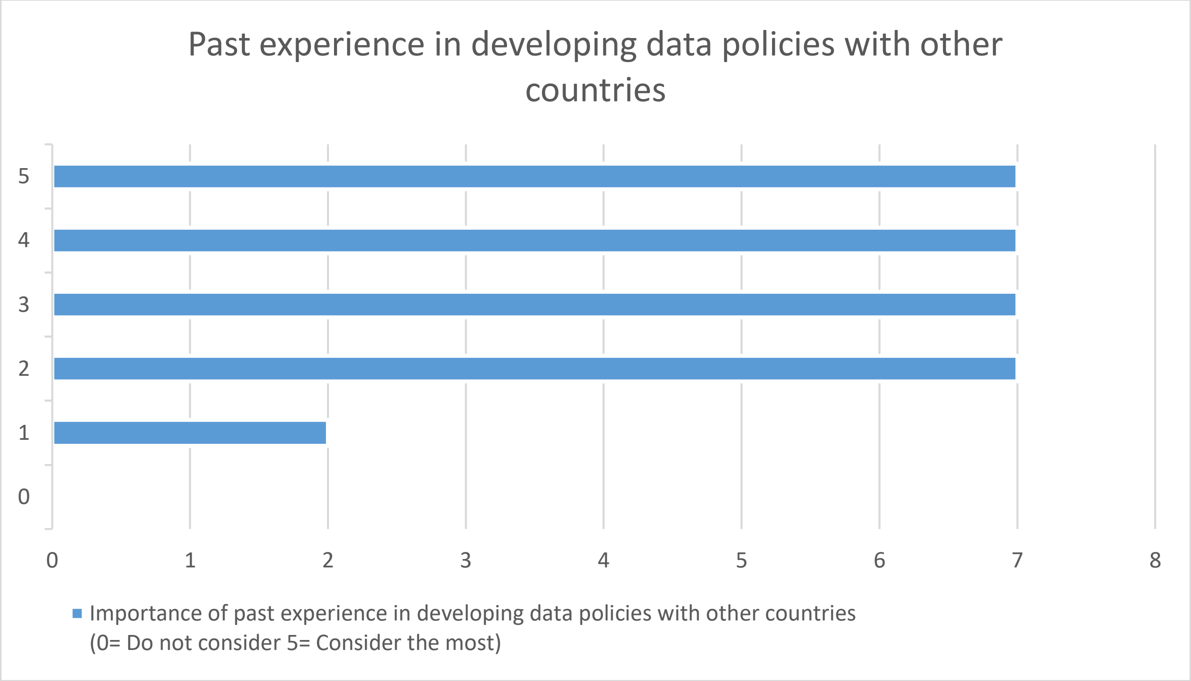


Figure E.127: Importance of past experience in developing data policies with other counties (26-35-UK)

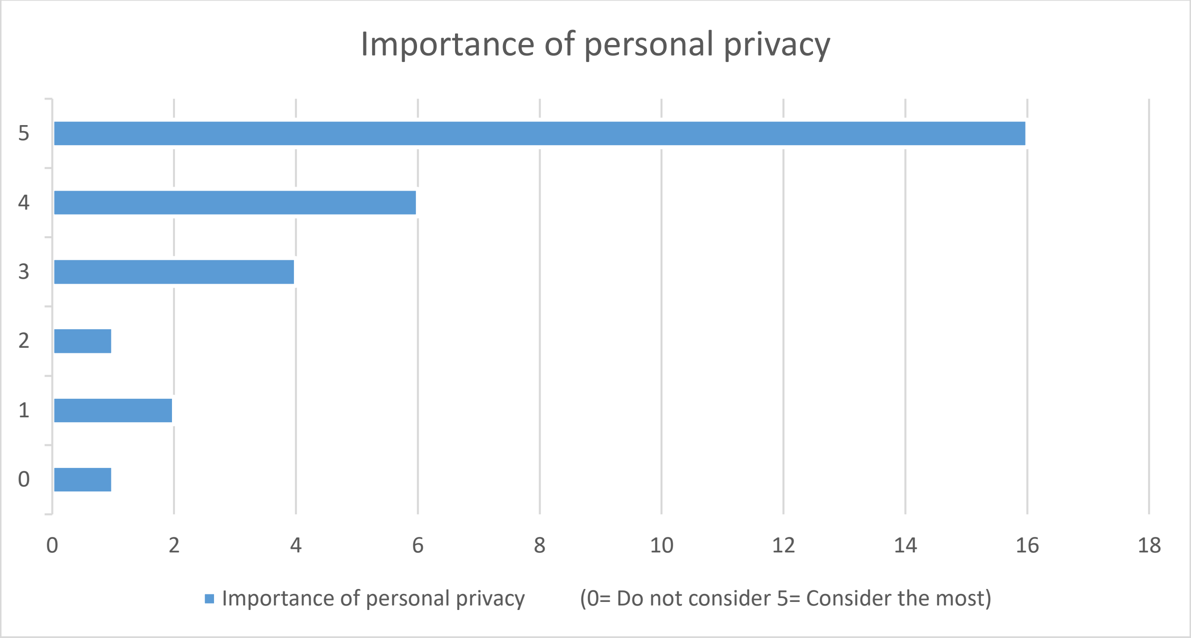


Figure E.128: Importance of personal privacy (26-35-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 70 percent of the respondents have endorsed (See figure E.117). The other social differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure E.106-116) (See figure E.118-128)

United Kingdom – 36- 45

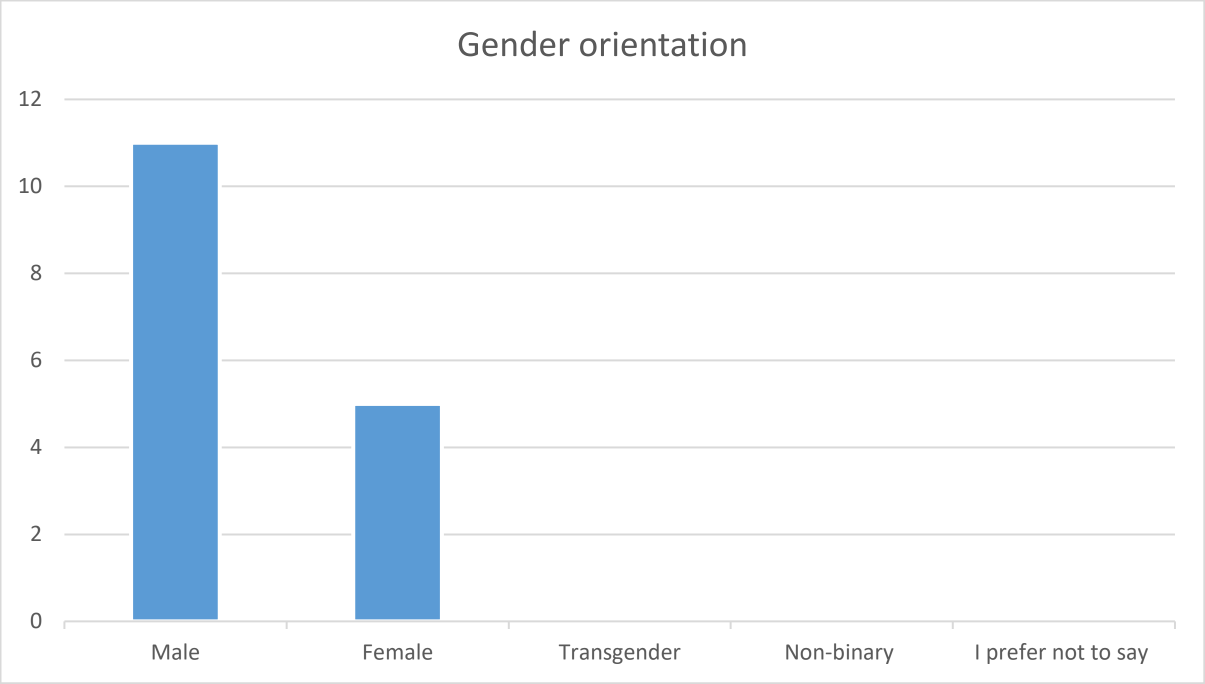


Figure E.129: Gender orientation (36-45-UK)

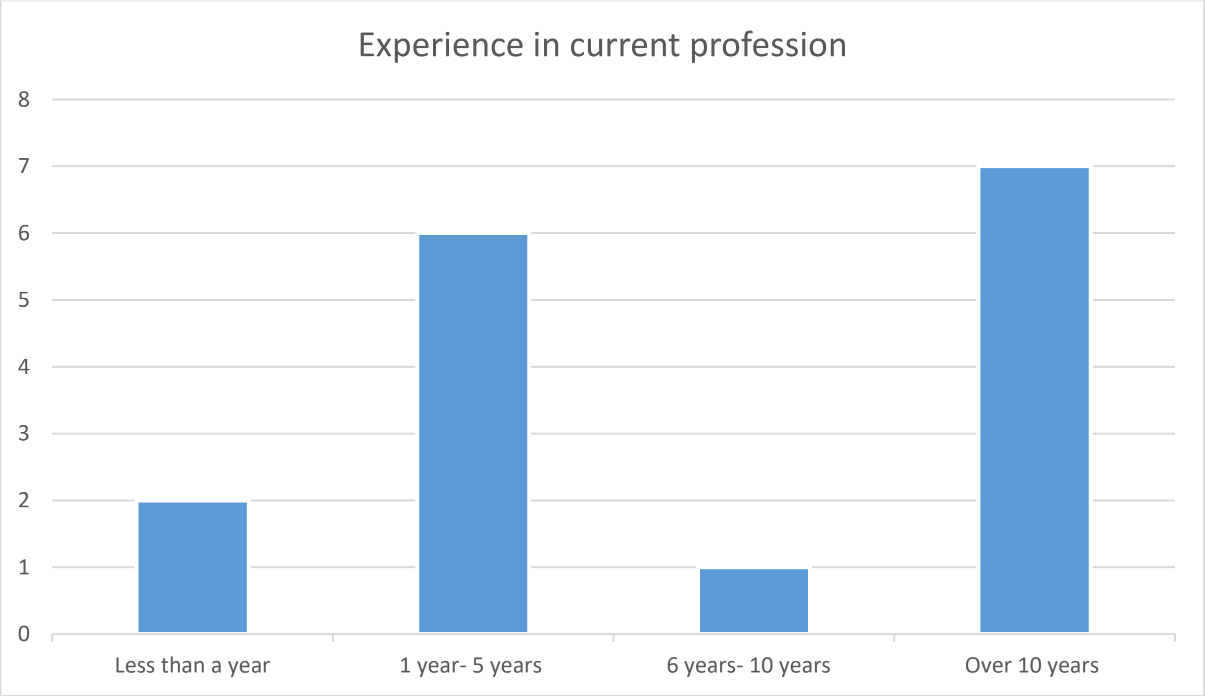


Figure E.130: Experience in current profession (36-45-UK)

This analysis is based on the responses received from United Kingdom participants aged 36-45 years. There were 16 participants and 11 out of them were males and 5 females (See figure E.129). They are from different industries and they have been in the industry for less than a year to over 10 years (See figure E.130).

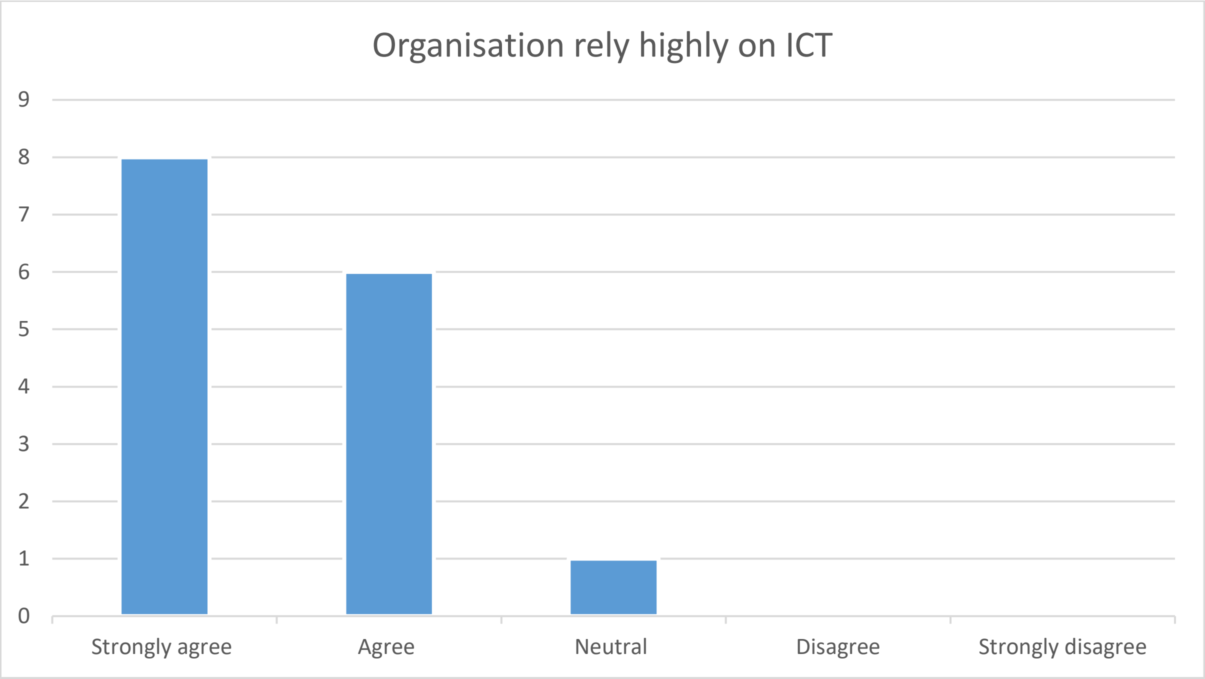


Figure E.131: Organisation rely highly on ICT (36-45-UK)

Out of the 16 respondents, 14 have worked in a technology reliance working environment and 1 unaware of reliance on technology because of the nature of the work assigned to them (See figure E.131). The majority of the employees within the 36-45 age range have a high reliance on ICT.

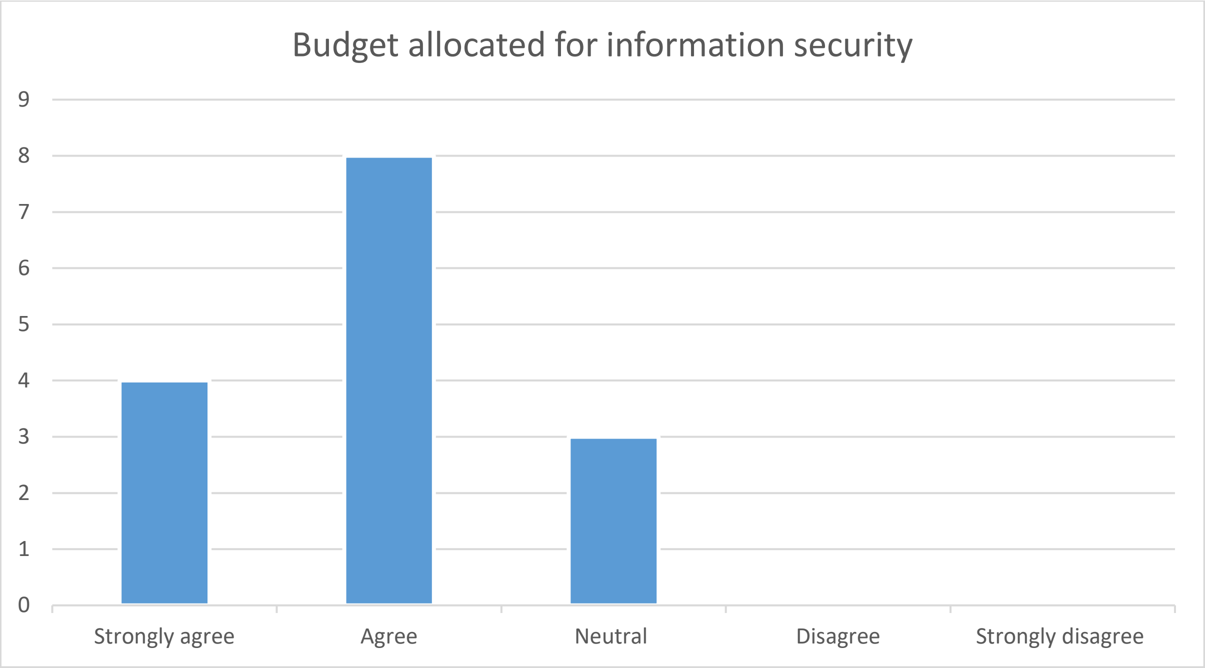


Figure E.132: Budget allocated for information security (36-45-UK)

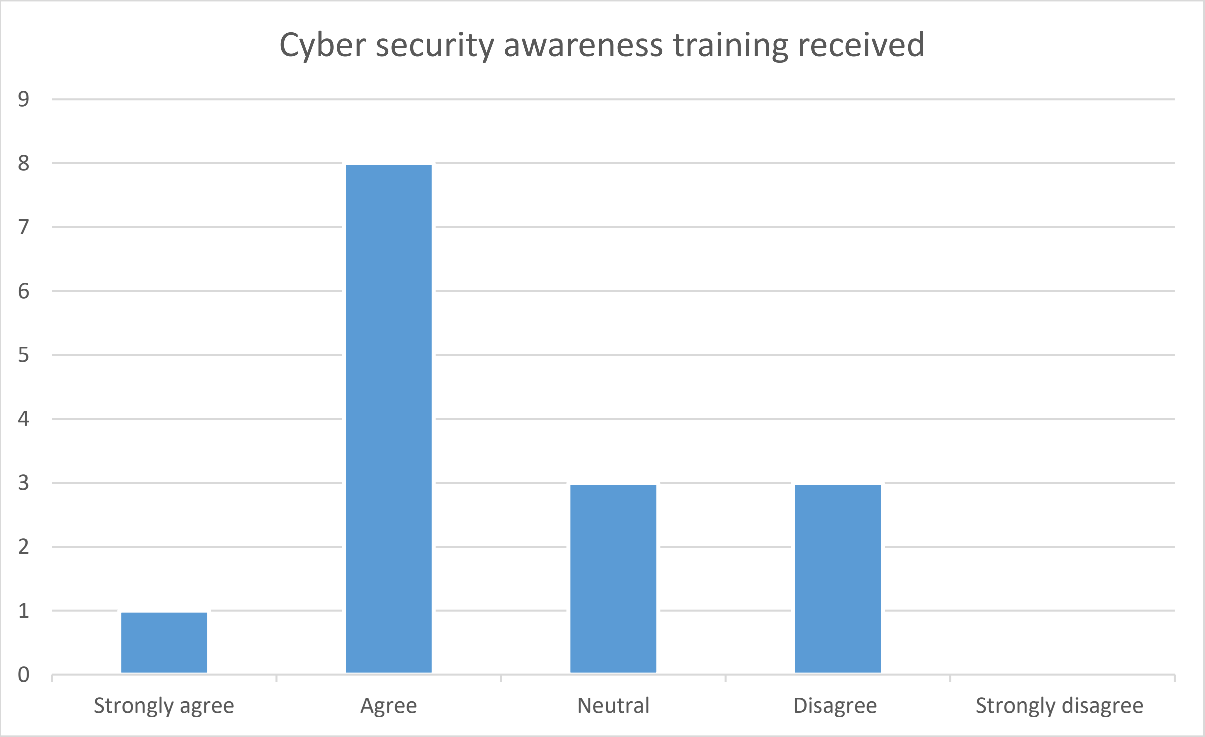


Figure E.133: Cyber security awareness training received (36-45-UK)

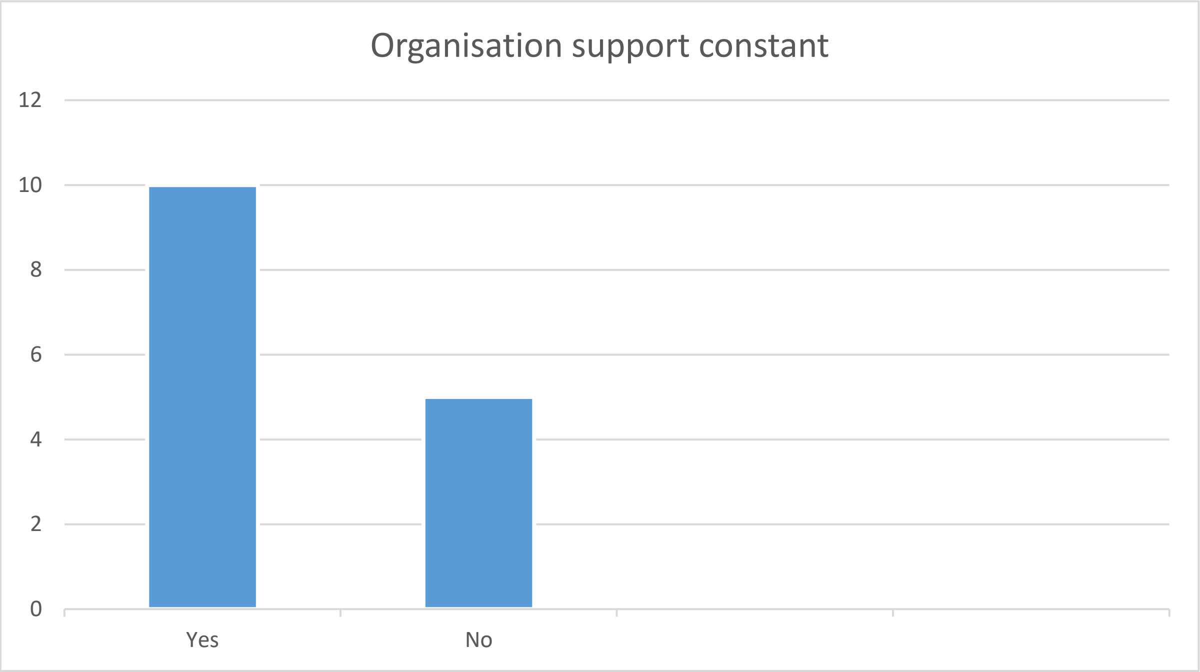


Figure E.134: Organisation support constant (36-45-UK)

12 out of the 16 indicated that their organisations had an allocated budget for information security and 3 had not expressed an opinion either way (See figure E.132). According to some of the participants, regular security awareness training received was adequate despite the satisfactory level of resources allocated for information security. 9 participants received regular cybersecurity awareness training; 3 neither agreed nor disagreed; 3 more participants not received (See figure E.133). In addition, 10 participants received support from the organisation to protect personal information, and 5 did not (See figure E.134). This clearly indicates that the organisations help their employees in every possible way to protect their customer information and minimise any potential breaches.

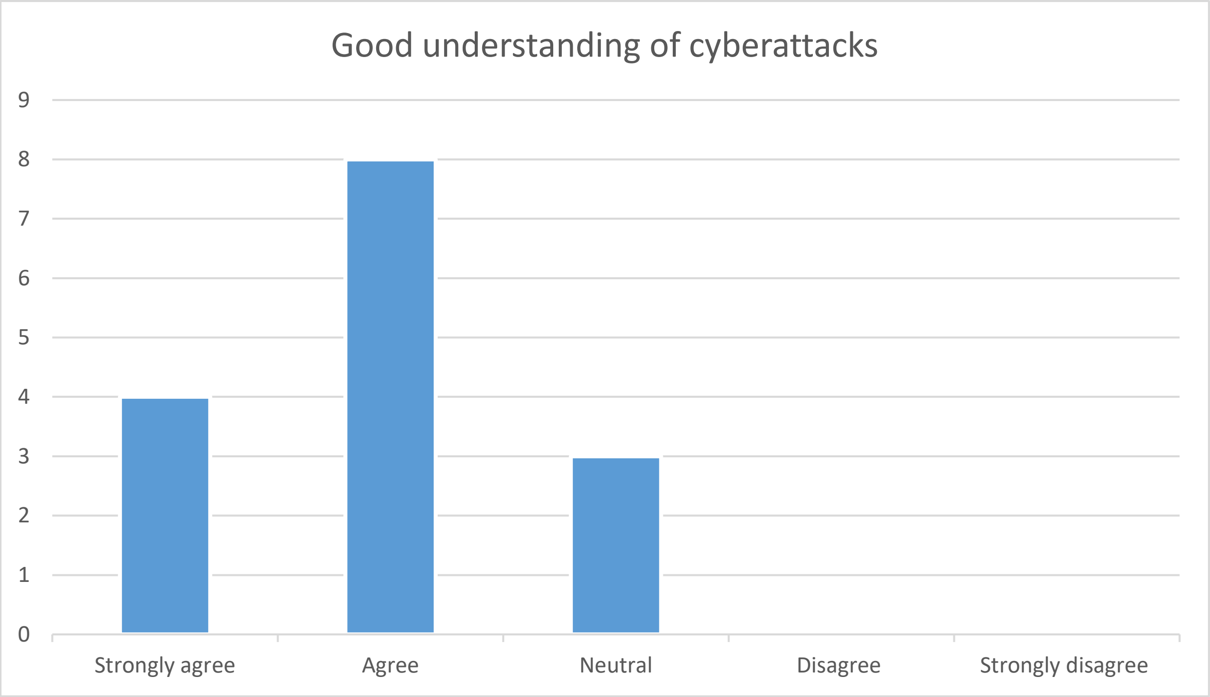


Figure E.135: Good understanding of cyberattacks (36-45-UK)

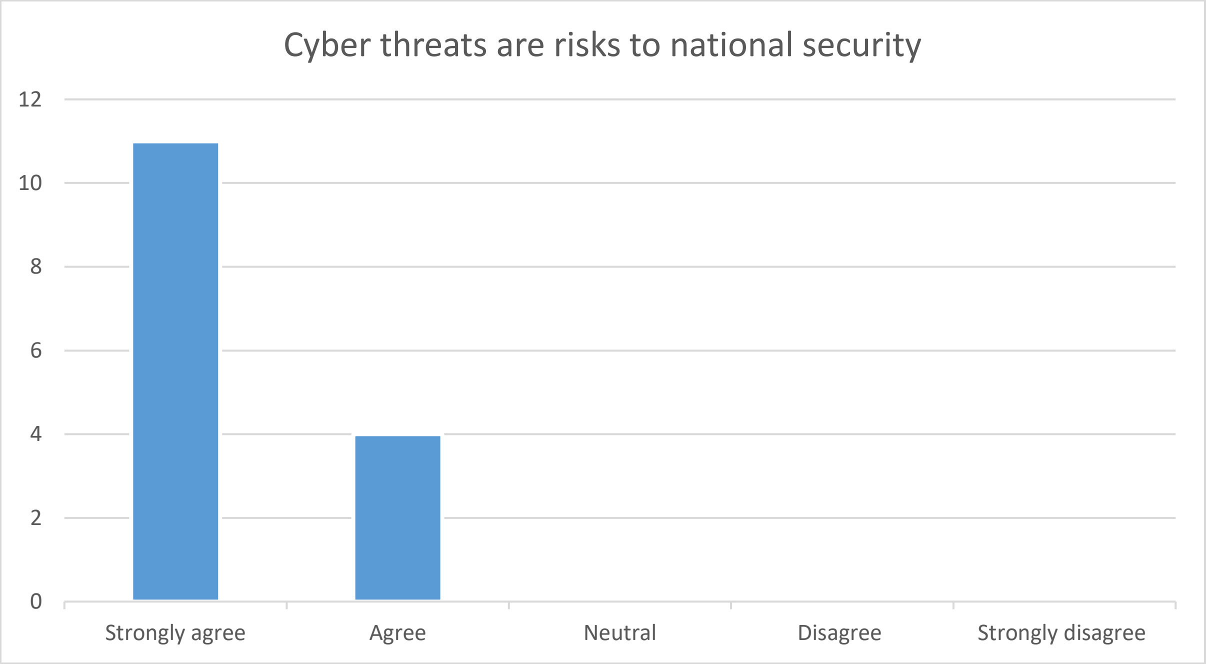


Figure E.136: Cyber threats are risks to national security (36-45-UK)

Despite the security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 12 participants do have, 3 have not expressed opinion either way (See figure E.135). Furthermore, 94 percent of the participants realise the potential threats to national security from cyber-attacks (See figure E.136). In general, understanding of cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism

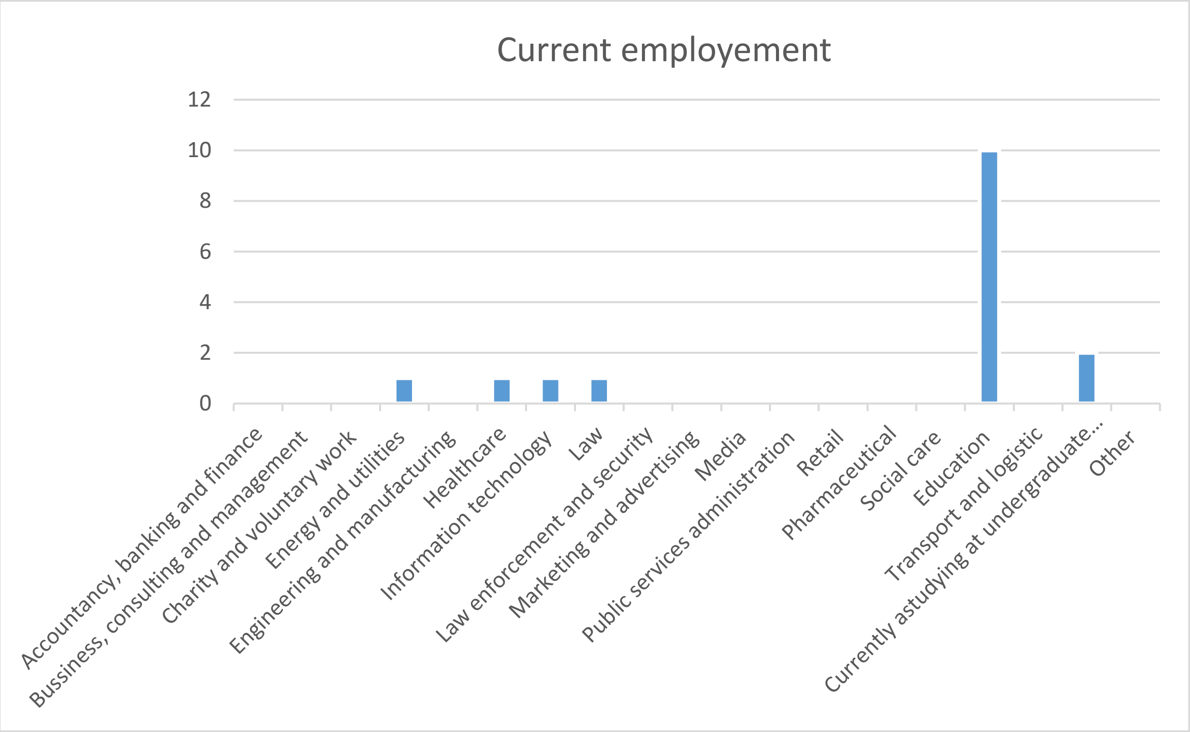


Figure 4.137: Current employment (36-45-UK)

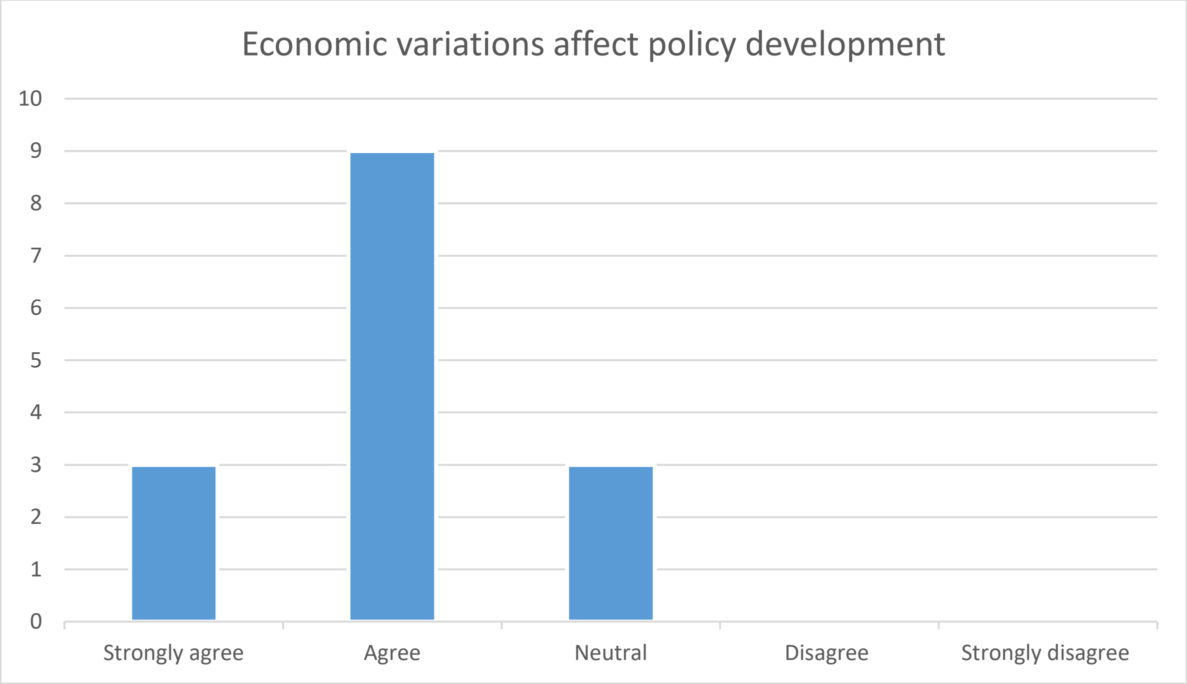


Figure E.138: Economic variations affect policy development (36-45-UK)

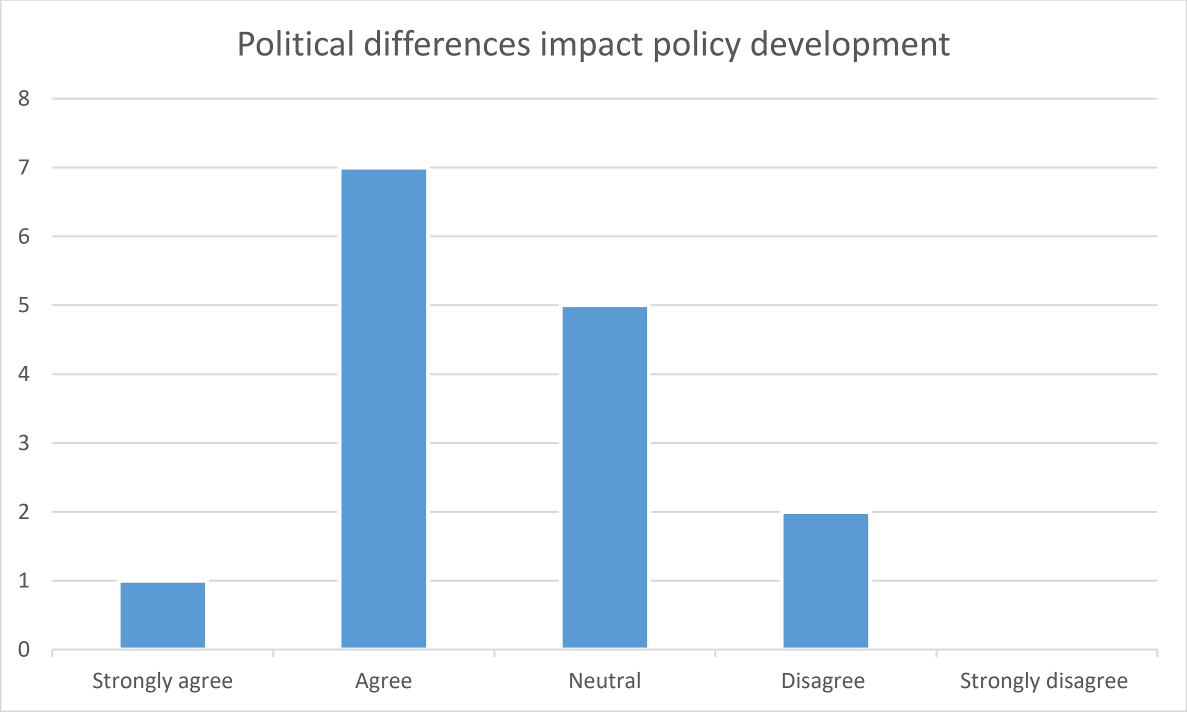


Figure E.139: Political differences impact policy development (36-45-UK)

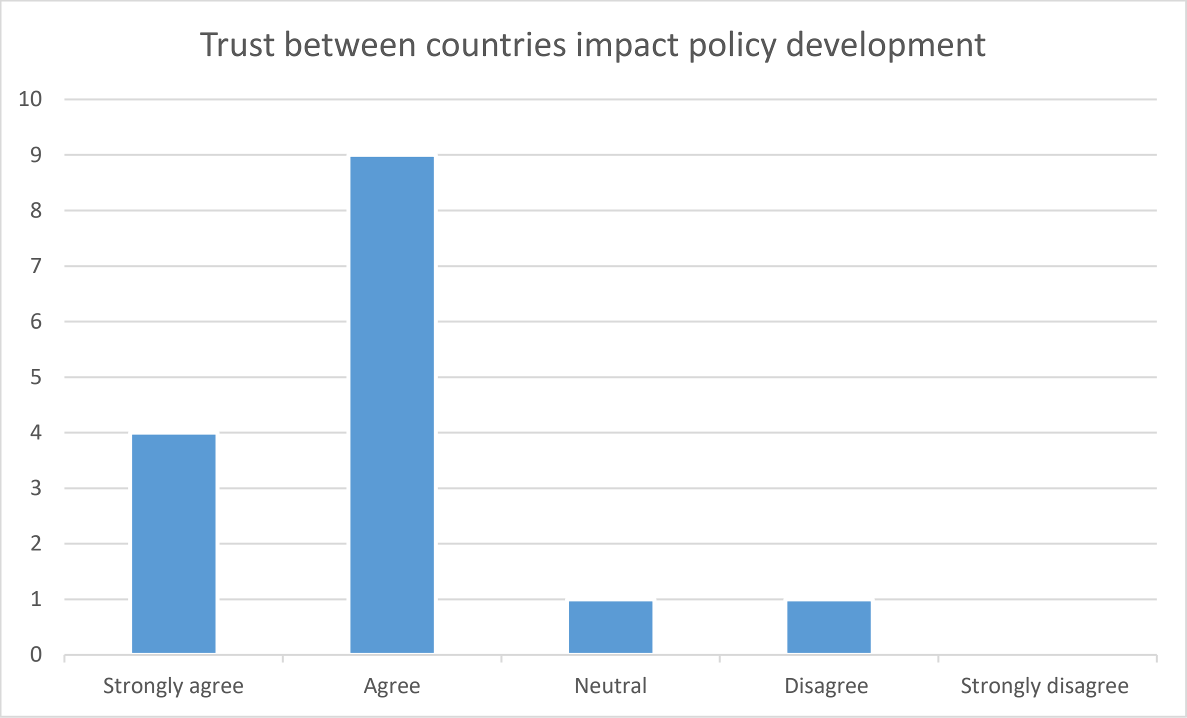


Figure E.140: Trust between countries impact policy development (36-45-UK)

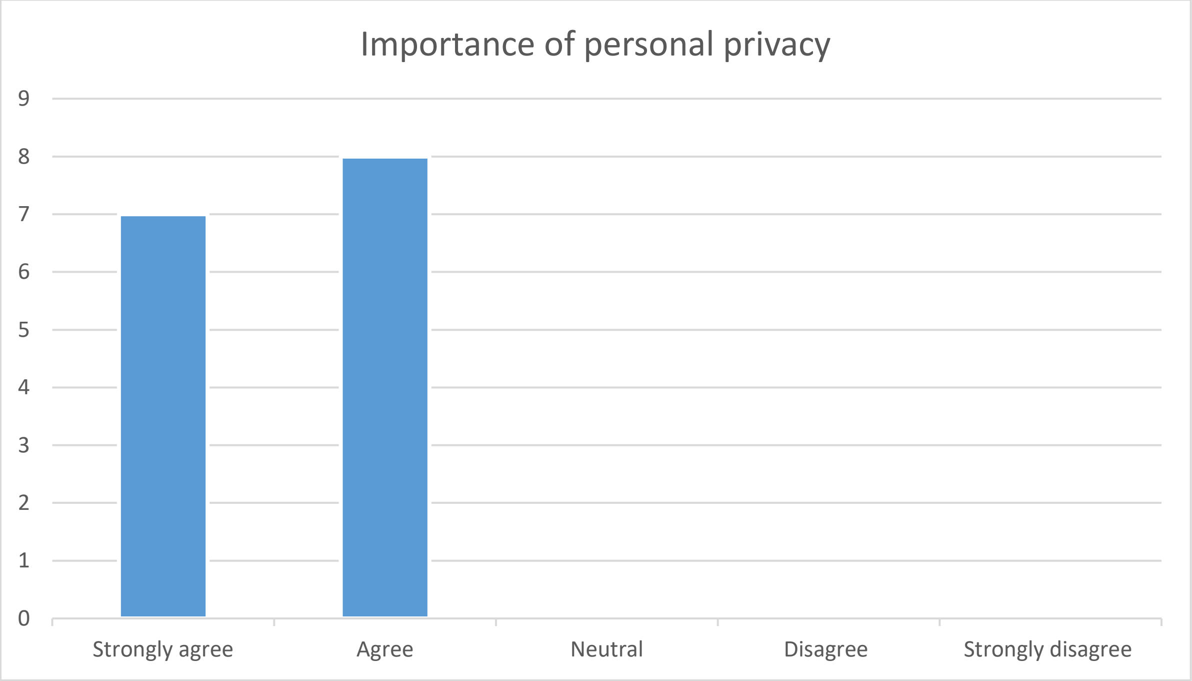


Figure E.141: Importance of personal privacy (36-45-UK)

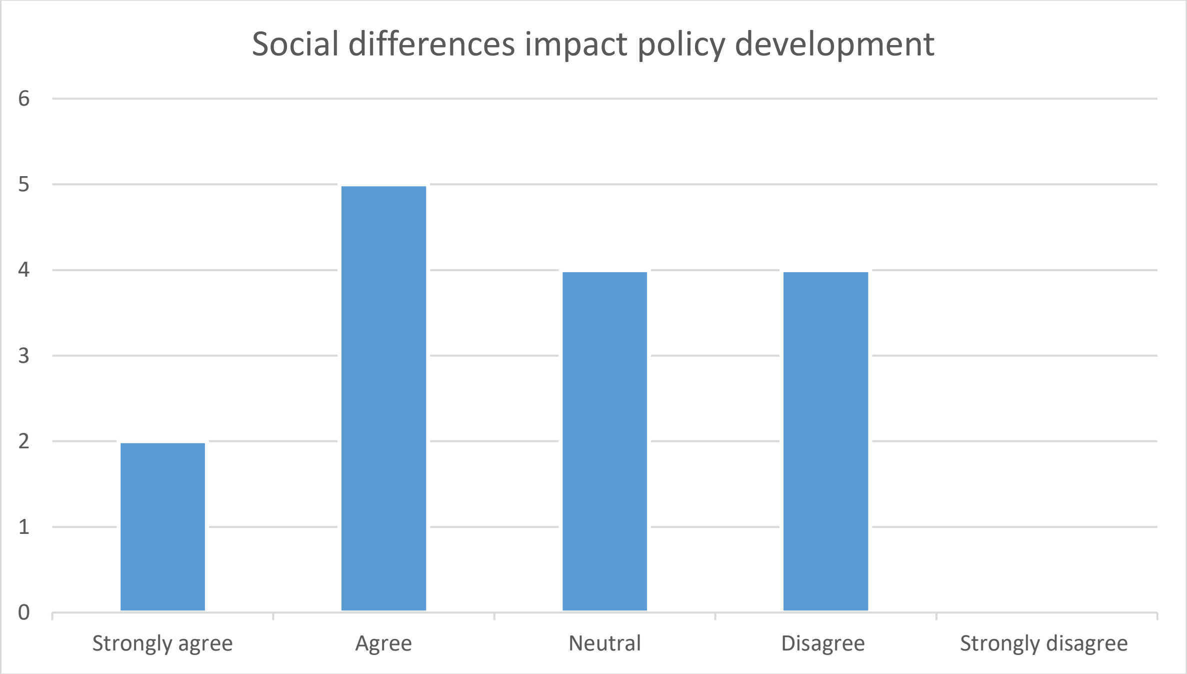


Figure E.142: Social differences impact policy development (36-45-UK)

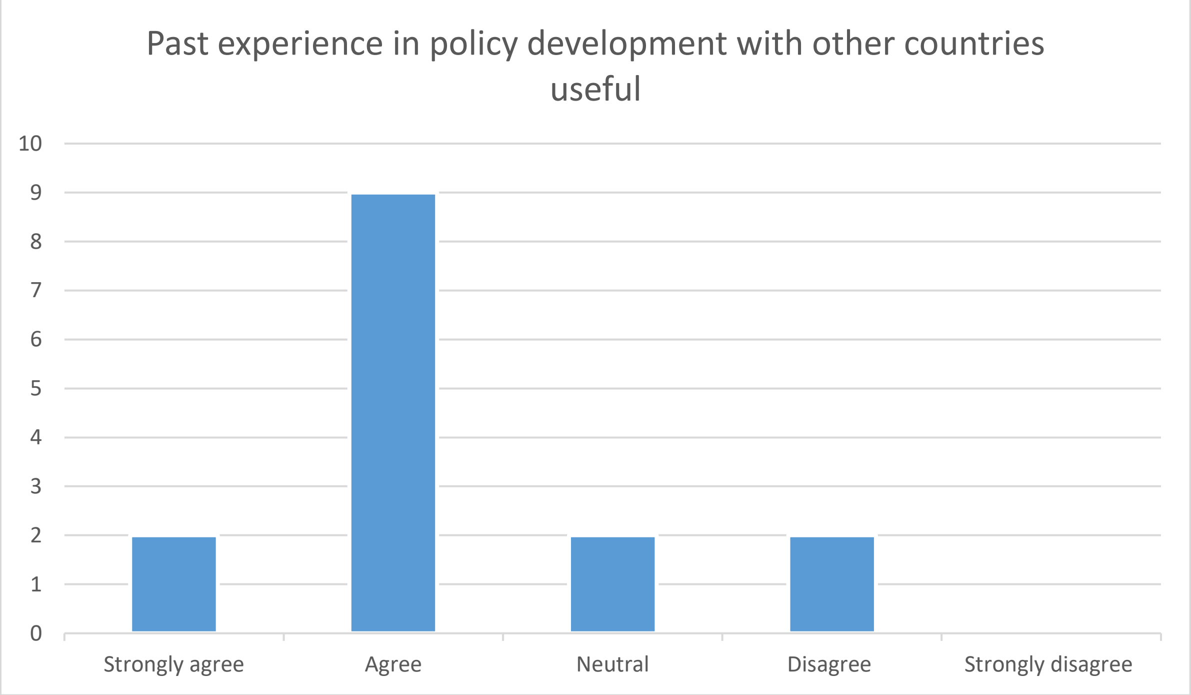


Figure E.143: Past experience in policy development with other countries useful (36-45-UK)

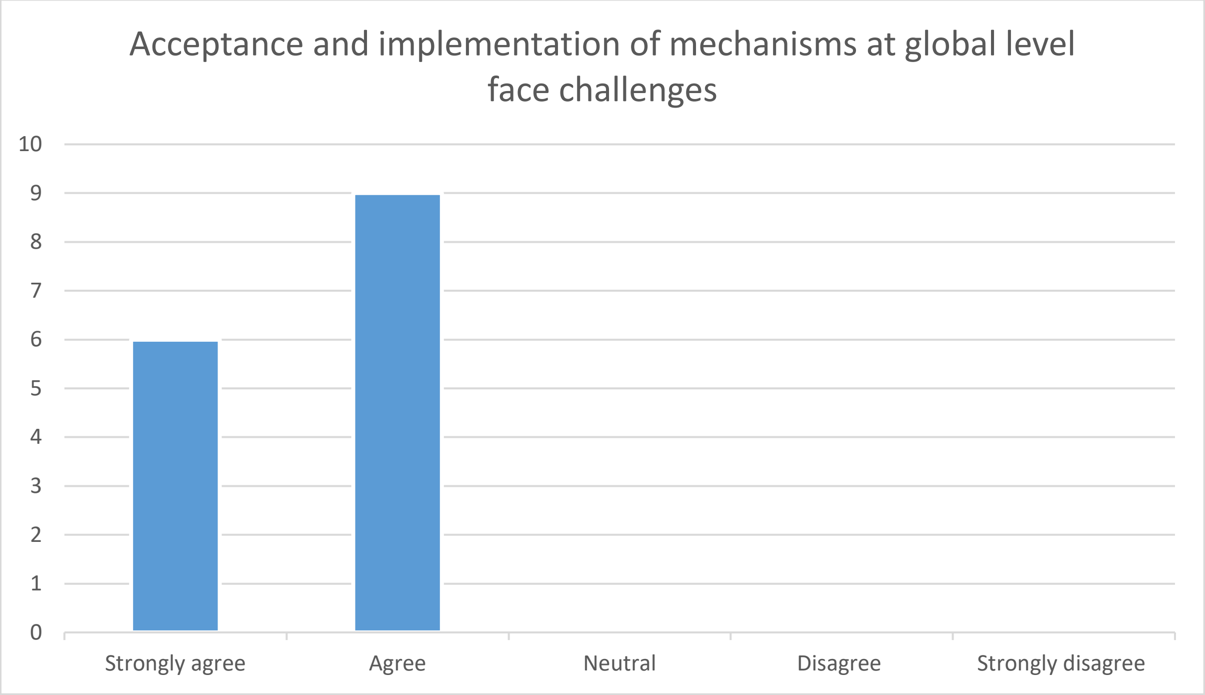


Figure E.144: Acceptance and implementation of mechanisms at global level face challenges (36-45-UK)

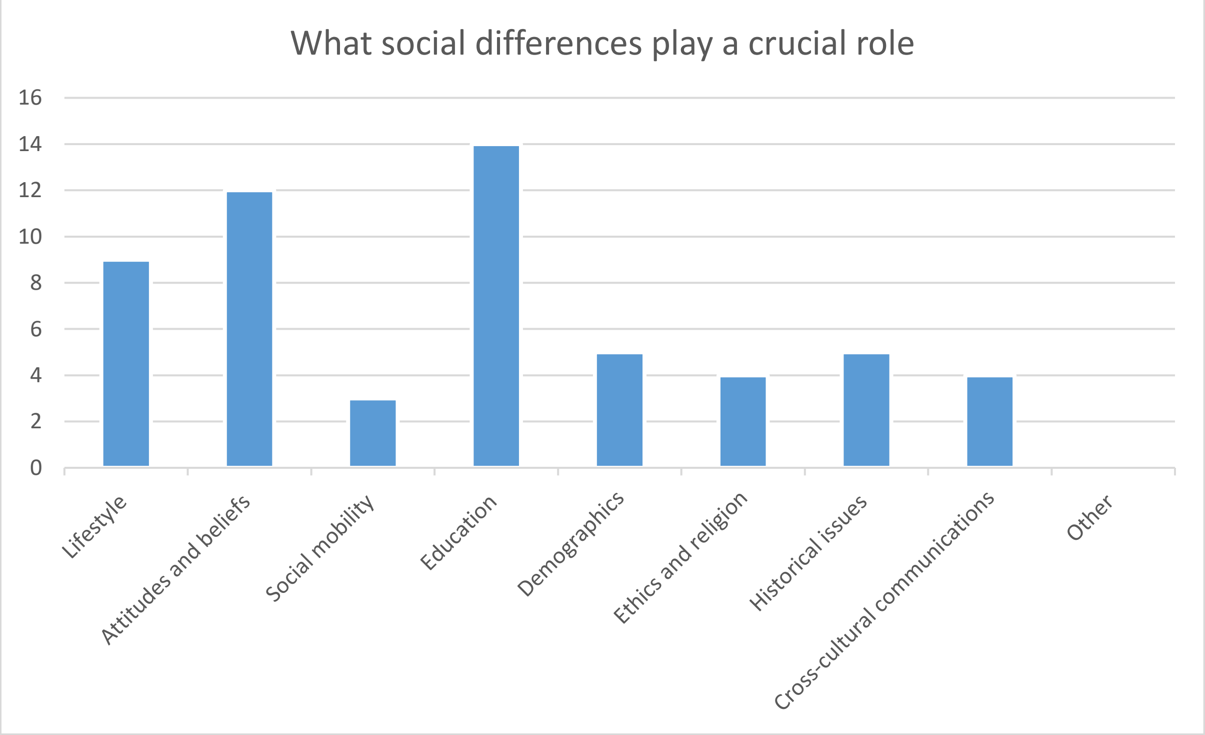


Figure E.145: What social differences play a crucial role (36-45-UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education, lifestyle and attitude and beliefs (See figure E.145). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. It becomes clear that educational training can be an effective way to make people understand the importance of privacy and the implications associated with privacy violations. People will have to make a crucial choice in their lifestyles when considering reliance on technology at the workplace. If there is a high reliance on technology in sharing or handling personal information, the demand for accepting and implementing policies associated with data privacy and security also should be high. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

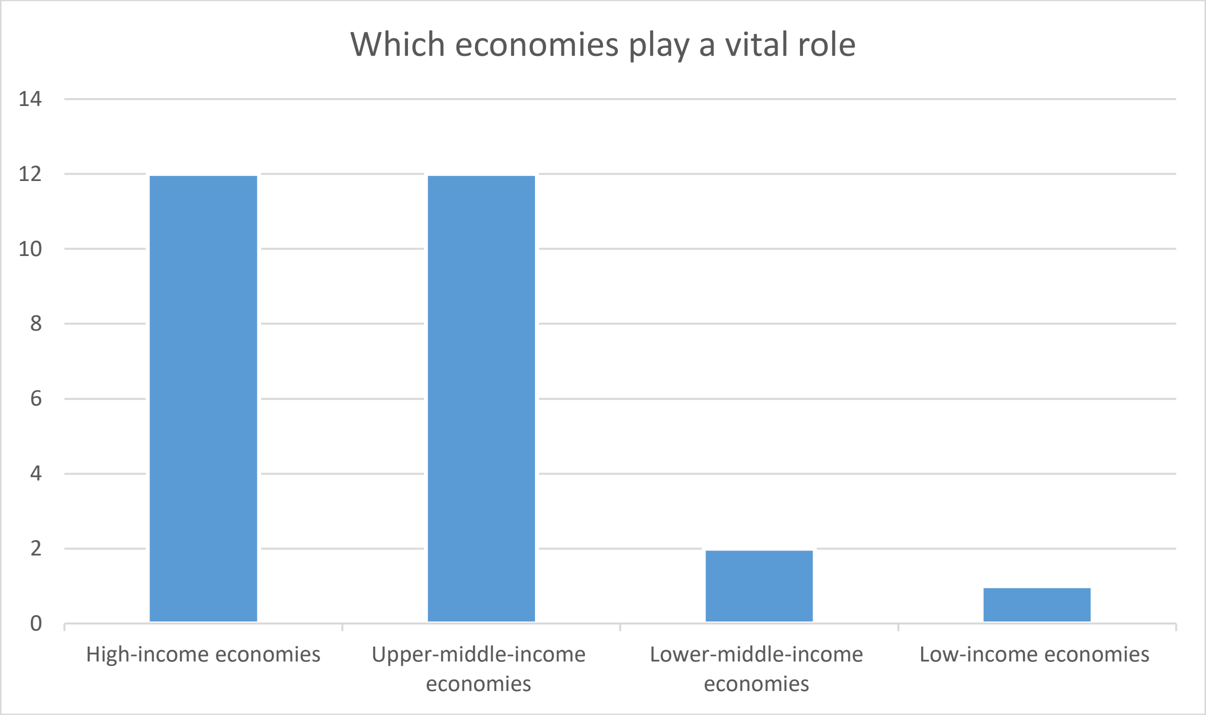


Figure E.146: Which economies play a vital role (36-45-UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.146). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

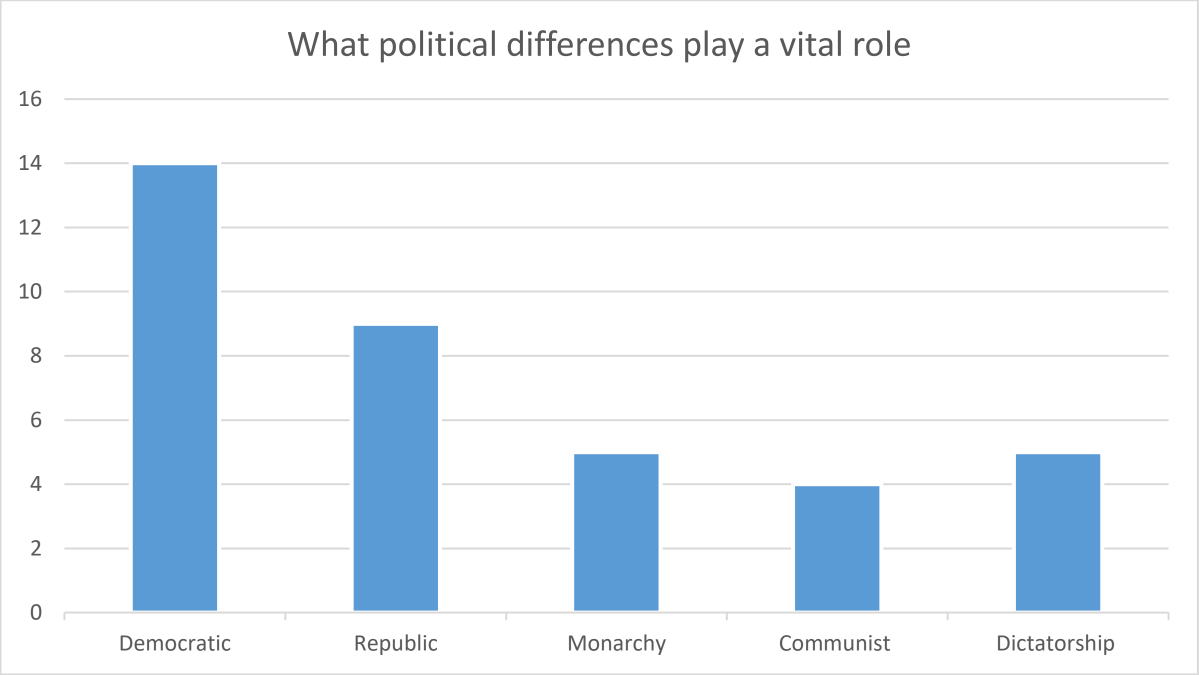


Figure E.147: What political differences play a vital role (36-45-UK)

The majority have chosen a democratic political system (See figure E.147), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

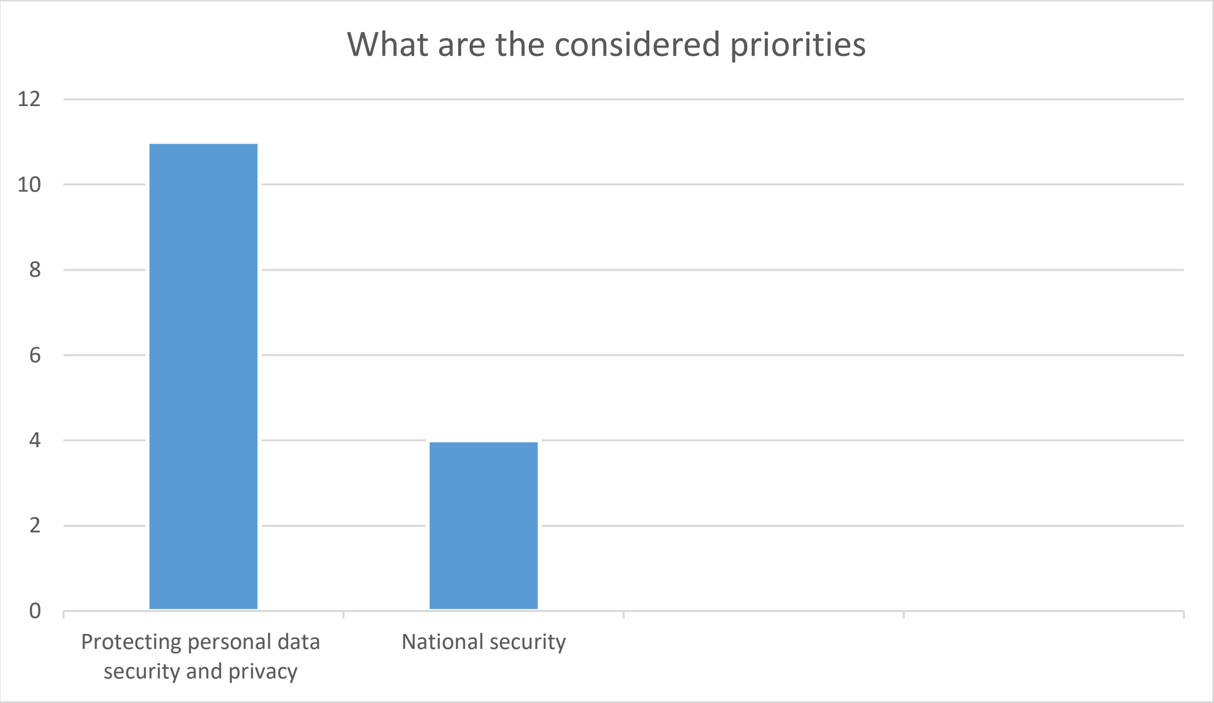


Figure E.148: What are the considered priorities (36-45-UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security (See figure E.148), which is a significant factor. However, in an incident of a personal data breach, there will potentially be a knock-on effect on personal data security and privacy, and national security, and it will also be felt right across the groups as well as the community alike.

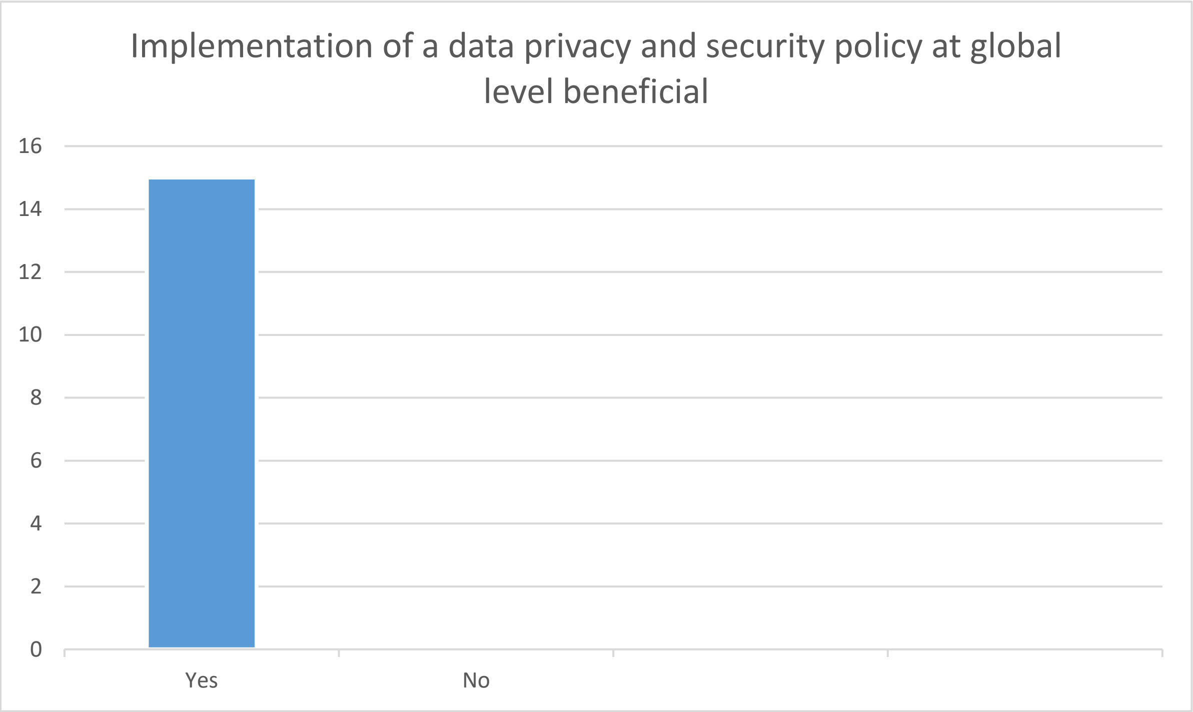


Figure E.149: Implementation of a data privacy and security policy at global level beneficial (36-45-UK)

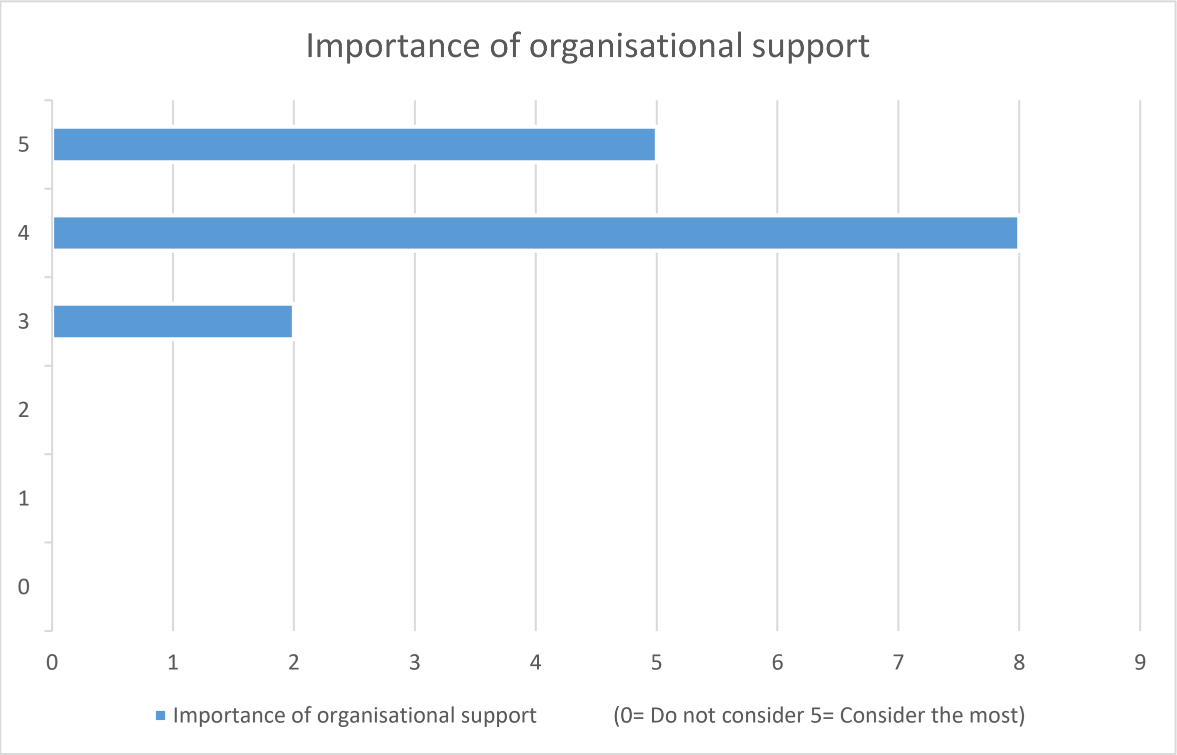


Figure E.150: Importance of organisational support (36-45-UK)

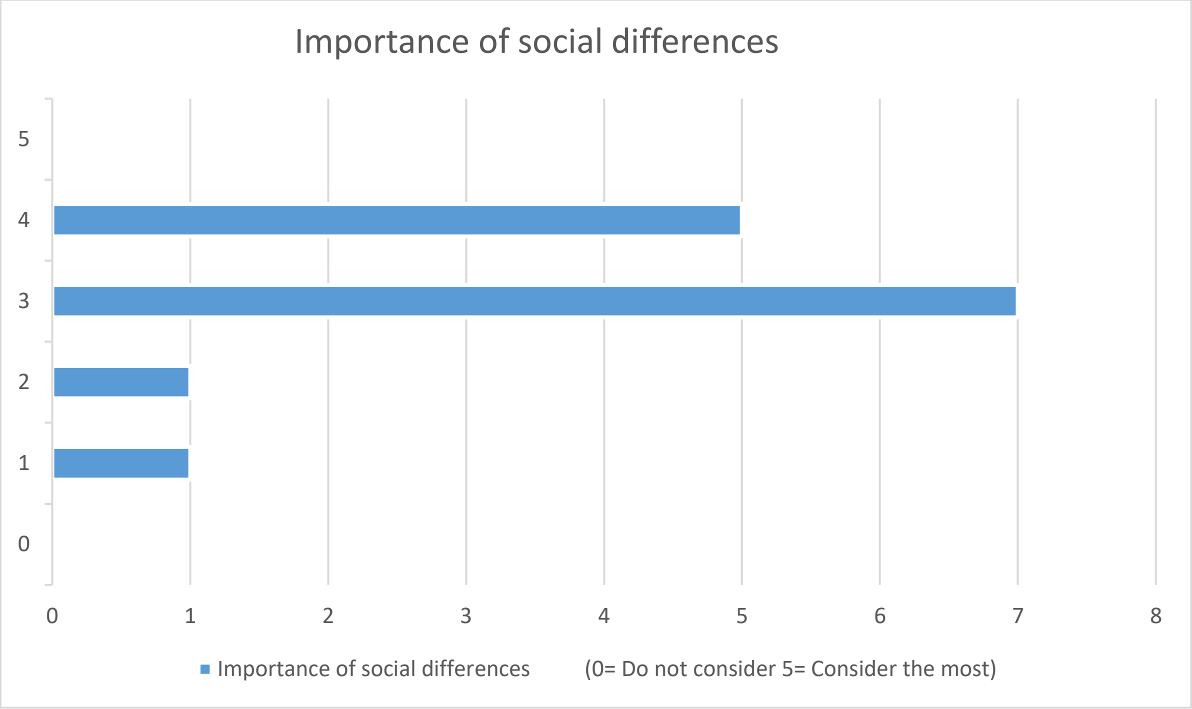


Figure E.151: Importance of social differences (36-45-UK)

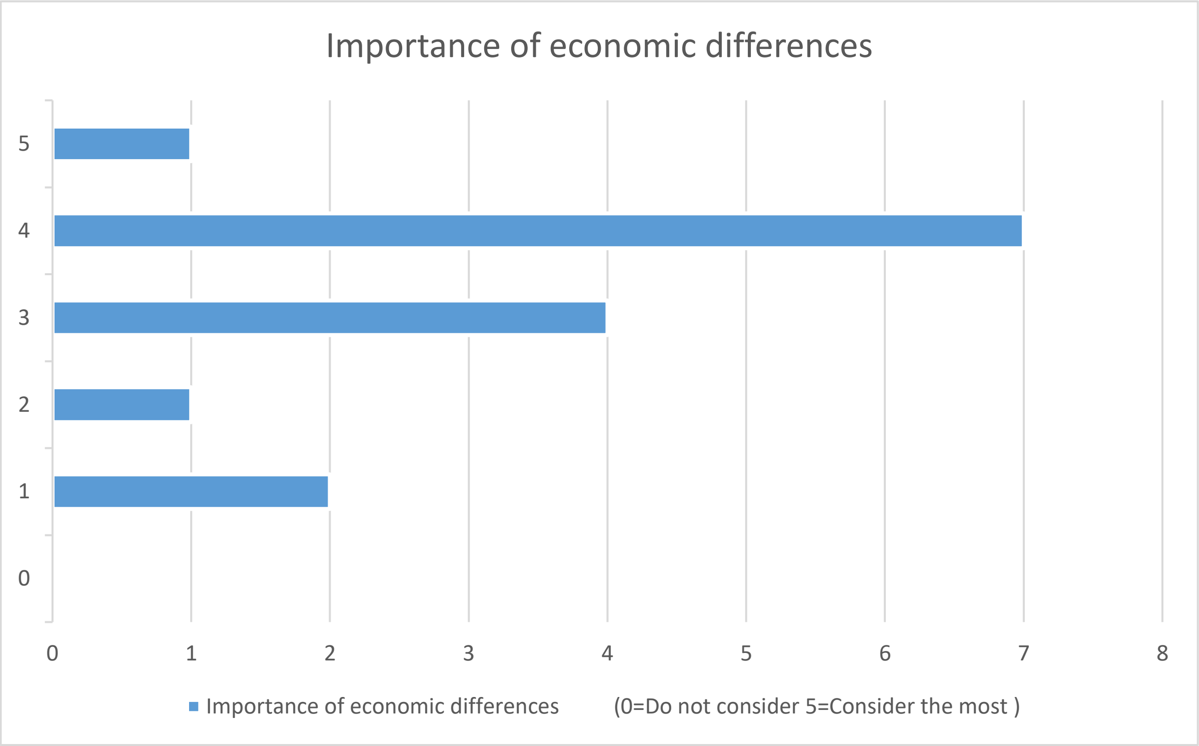


Figure E.152: Importance of economic differences (36-45-UK)

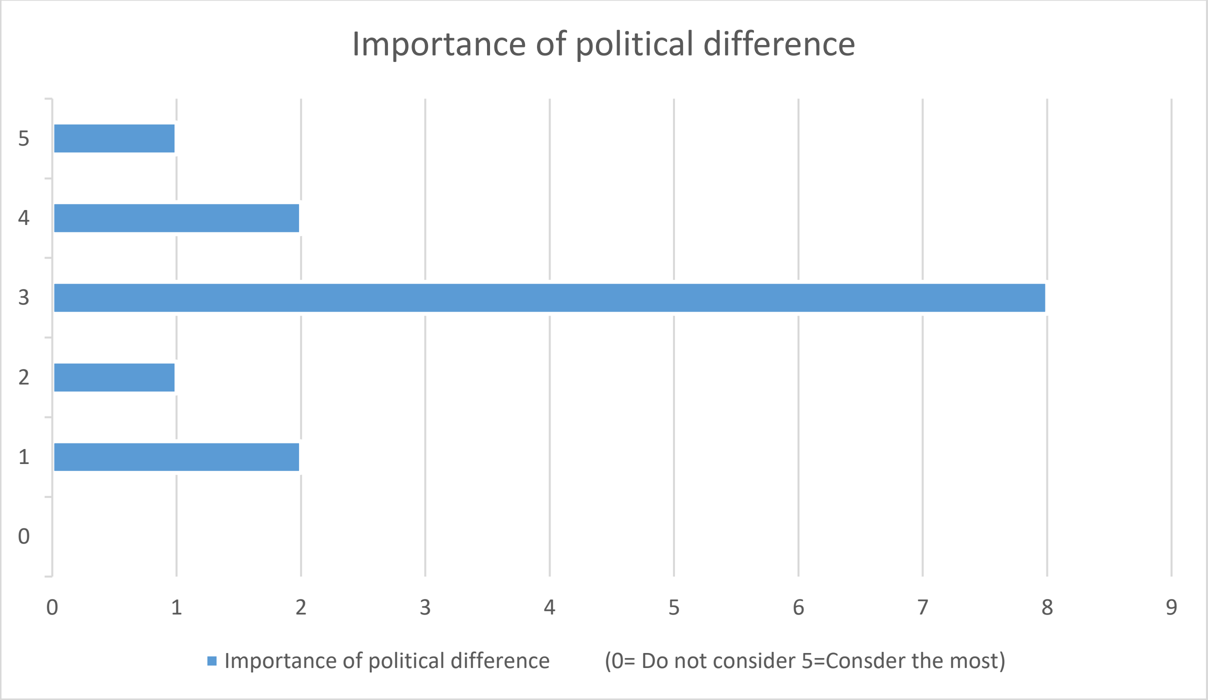


Figure E.153: Importance of political difference (36-45-UK)

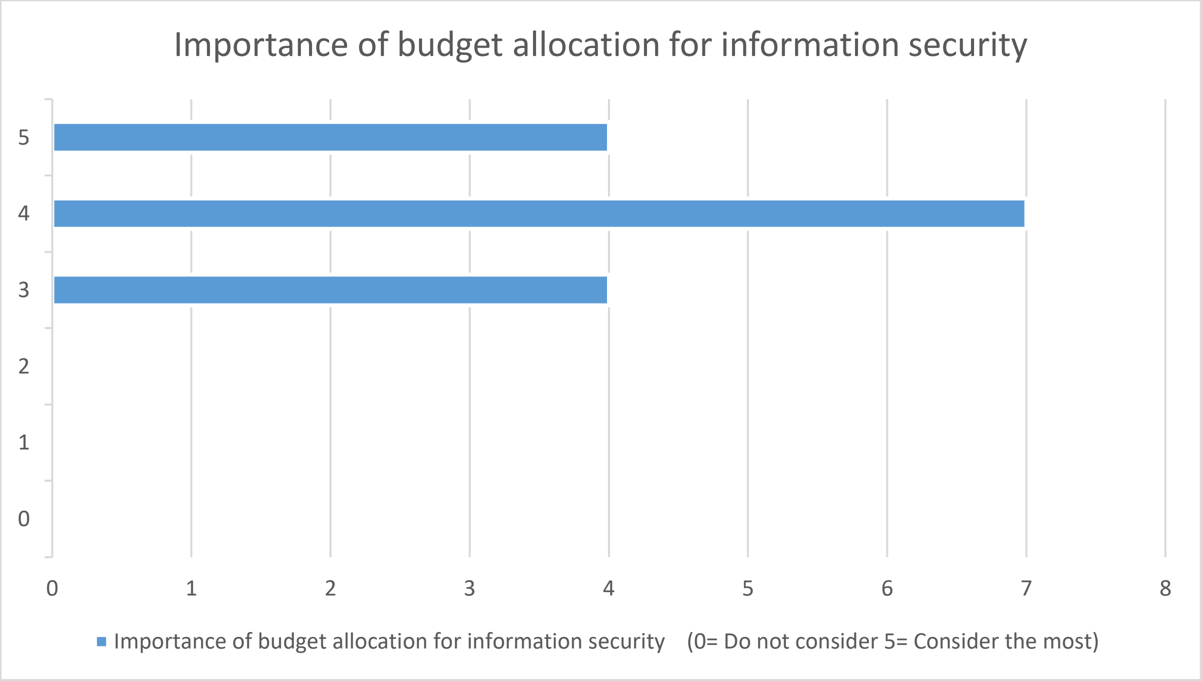


Figure E.154: Importance of budget allocation for information security (36-45-UK)

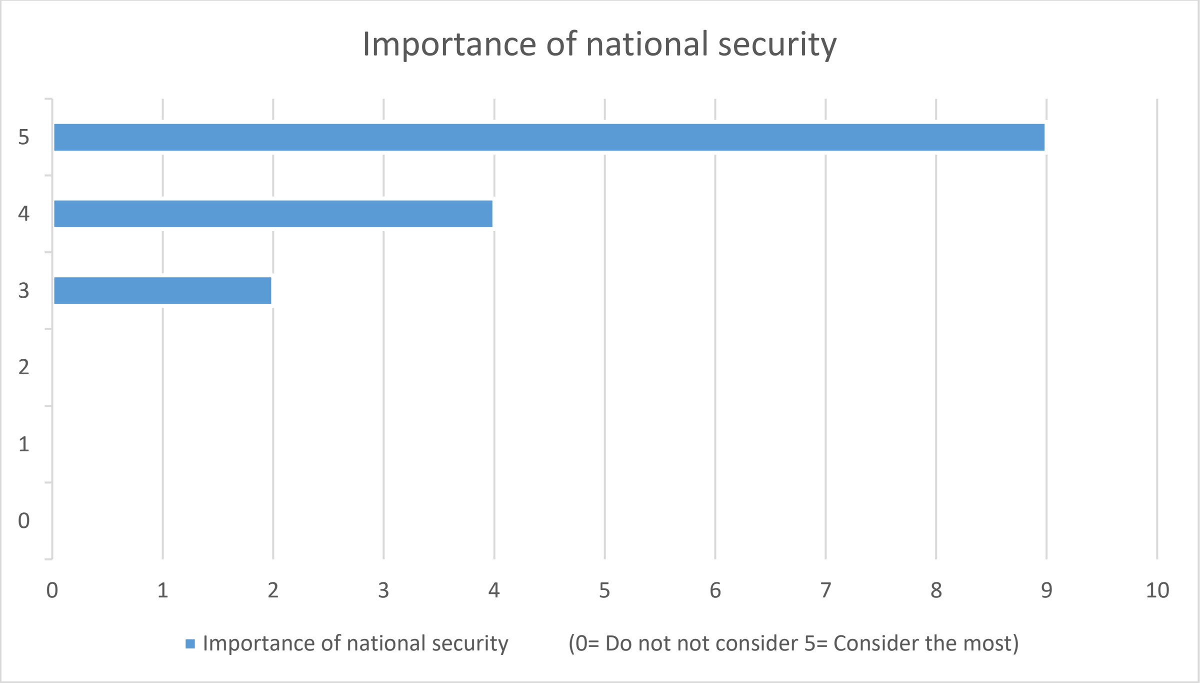


Figure E.155: Importance of national security (36-45-UK)

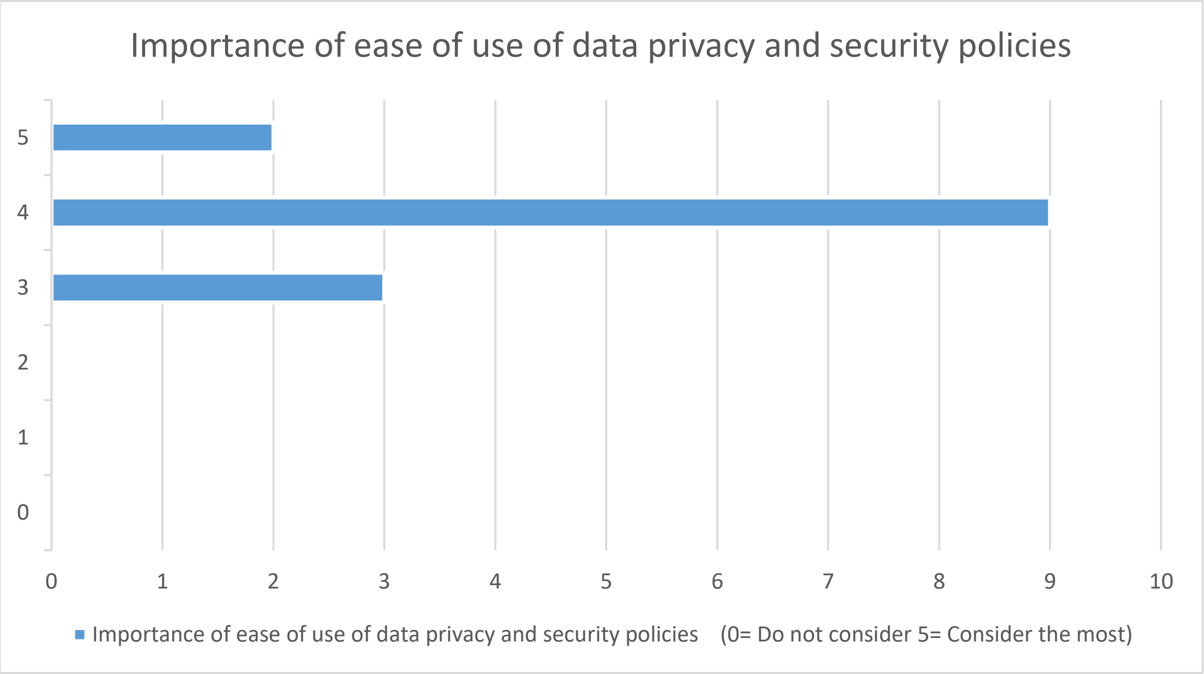


Figure E.156: Importance of ease of use of data privacy and security policies (36-45-UK)

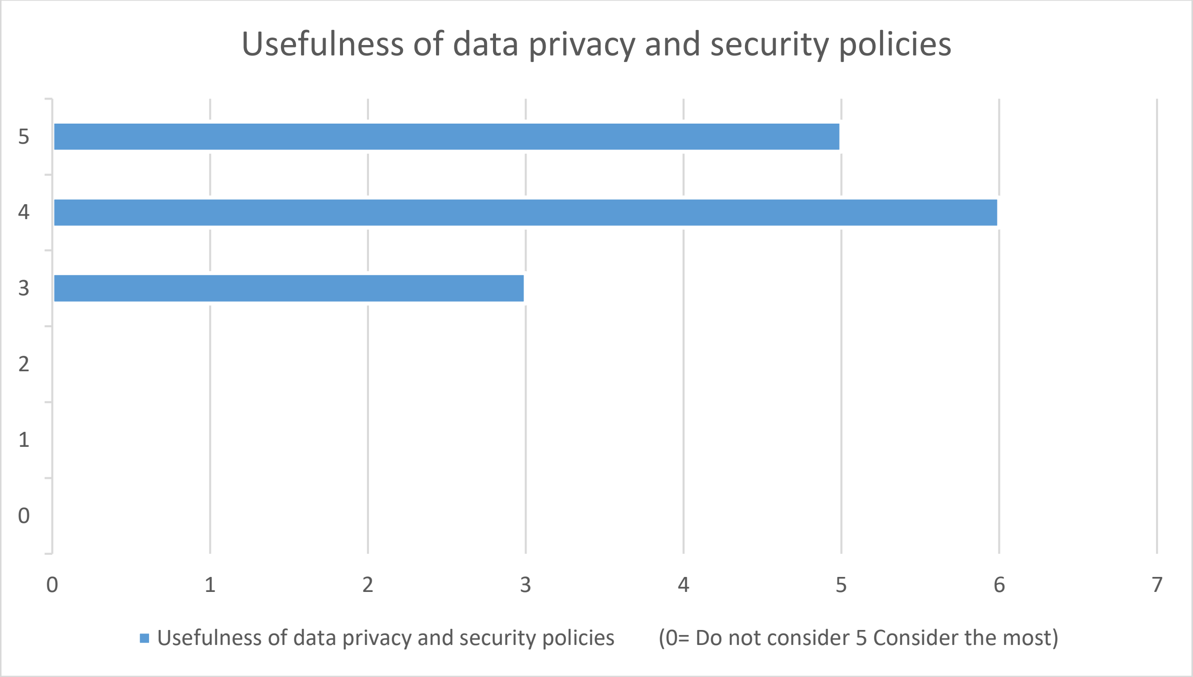


Figure E.157: Usefulness of data privacy and security policies (36-45-UK)

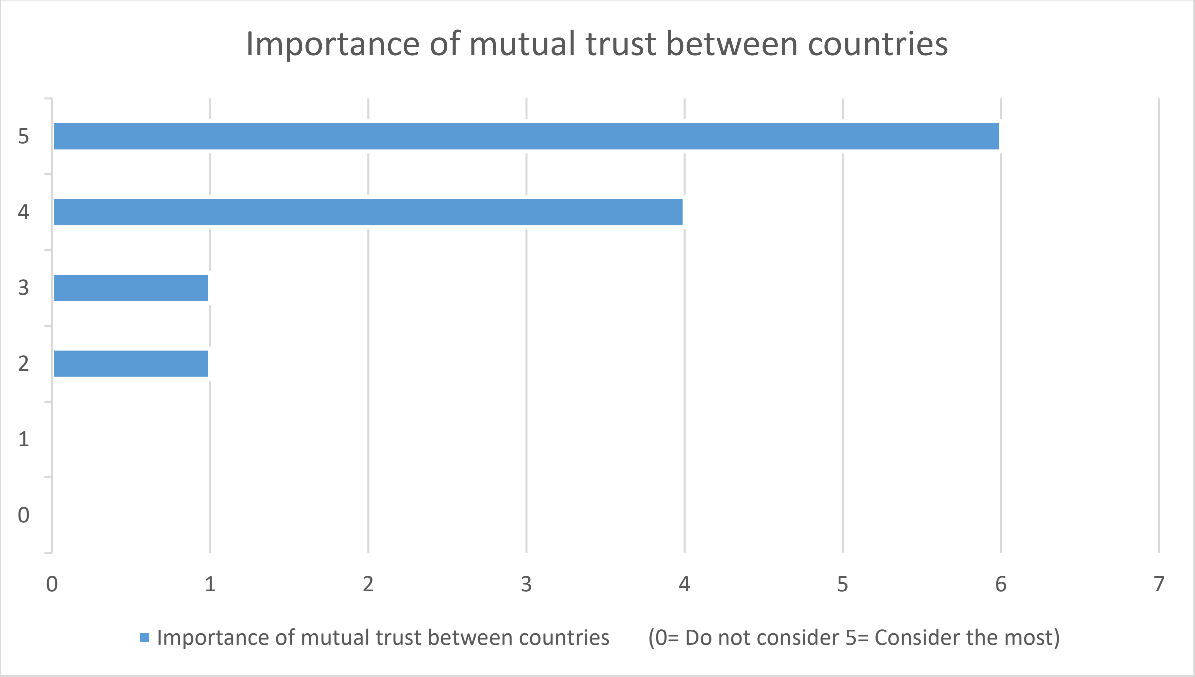


Figure E.158: Importance of mutual trust between countries (36-45-UK)

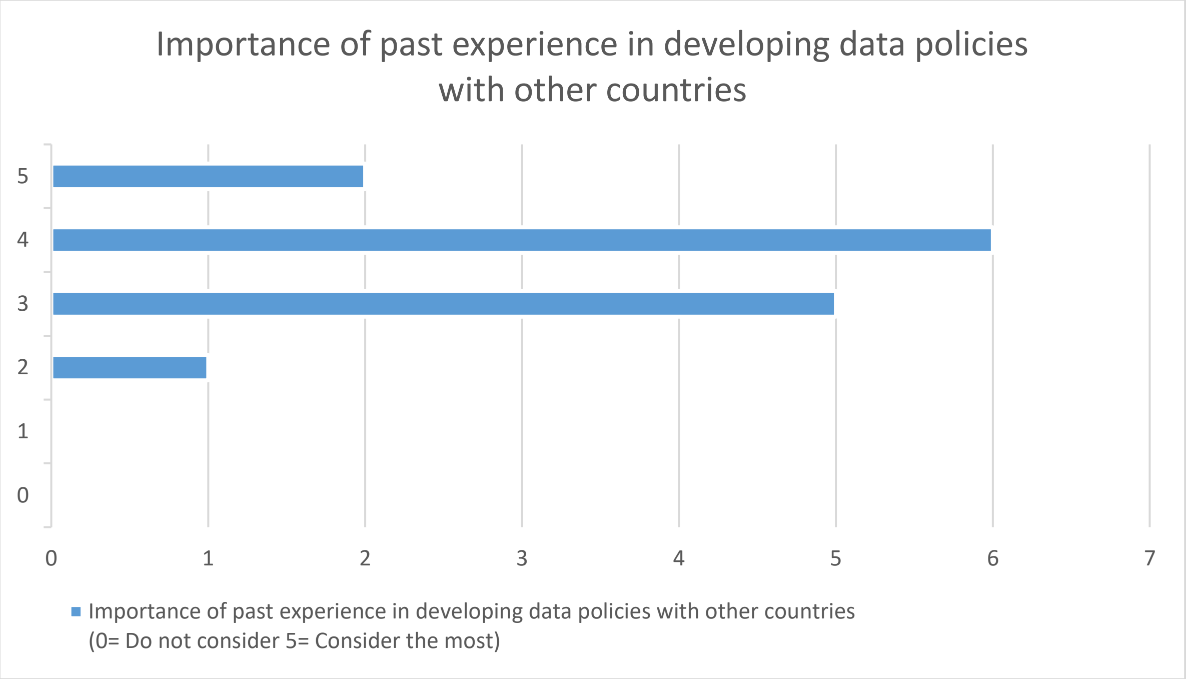


Figure E.159: Importance of past experience in developing data policies with other counties (36-45-UK)

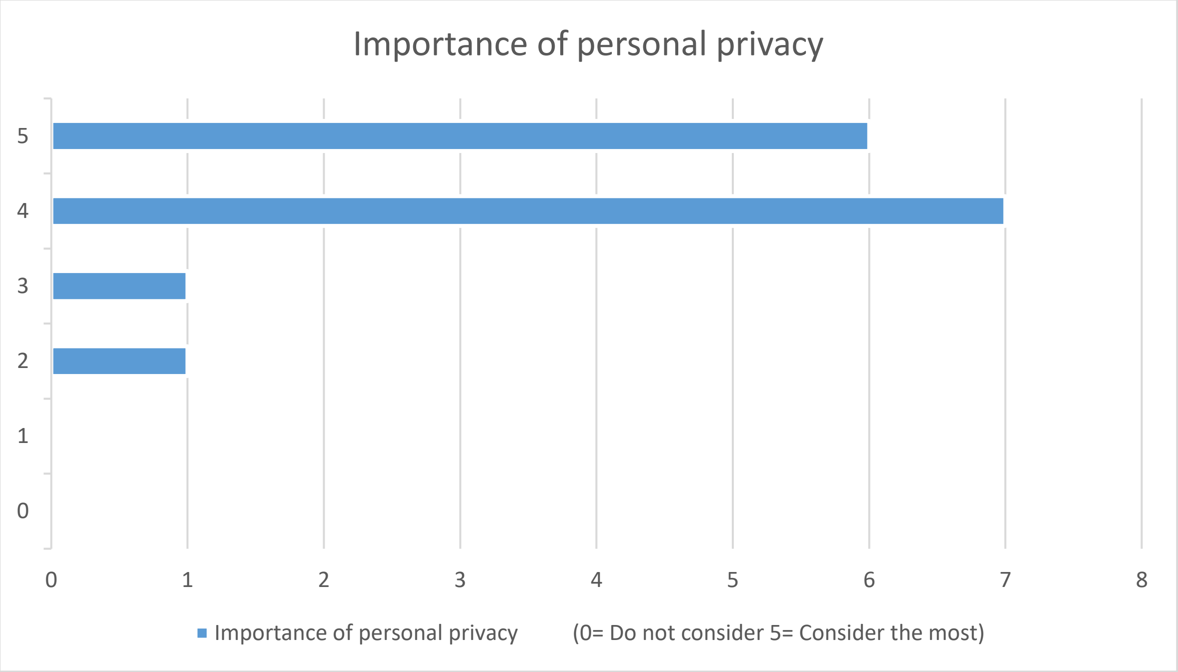


Figure E.160: Importance of personal privacy (36-45-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 94 percent of the respondents have endorsed (See figure E.149). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, political differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure E.138-148) (See figure E-150-160).

United Kingdom – 46-55

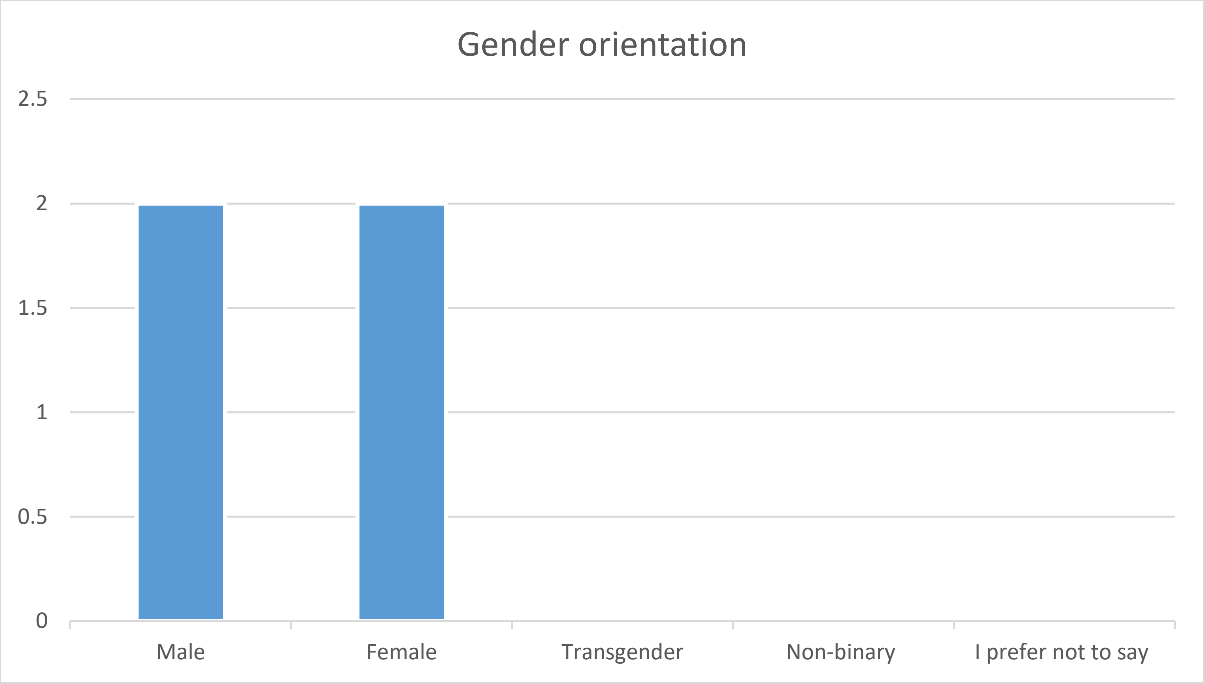


Figure E.161: Gender orientation (46-55-UK)

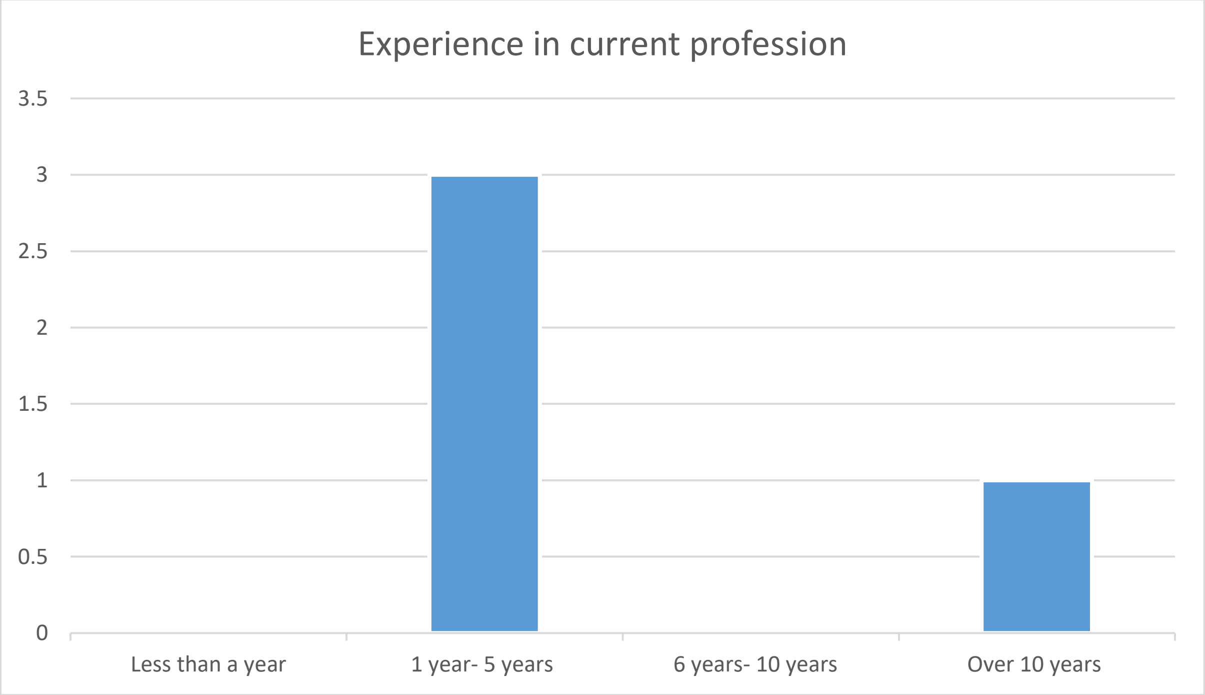


Figure E.162: Experience in current profession (46-55-UK)

This analysis is based on the responses received from United Kingdom participants aged between 46-55. There were 4 participants and 2 out of them were males and 2 females (See figure E.161). The participants employed in different industries between 1 and over 10 years (See figure E.162).

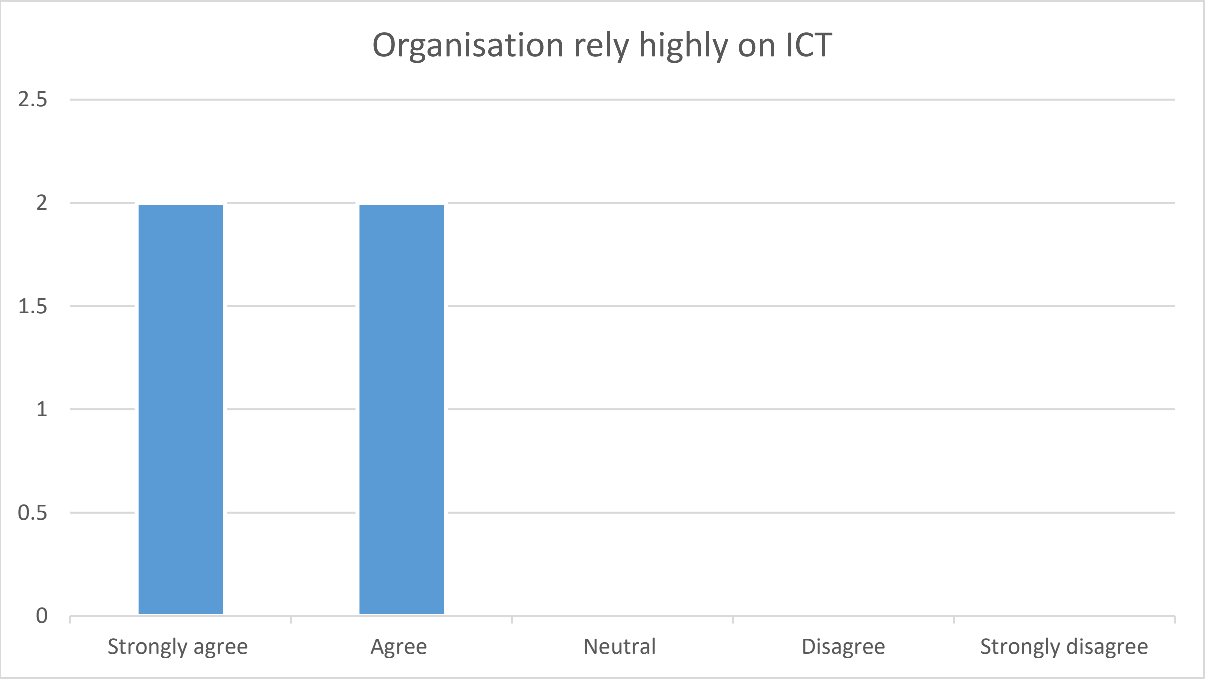


Figure E.163: Organisation rely highly on ICT (46-55-UK)

Out of the 4 respondents, all the participants have worked in a technology reliance working environment (See figure E.163).

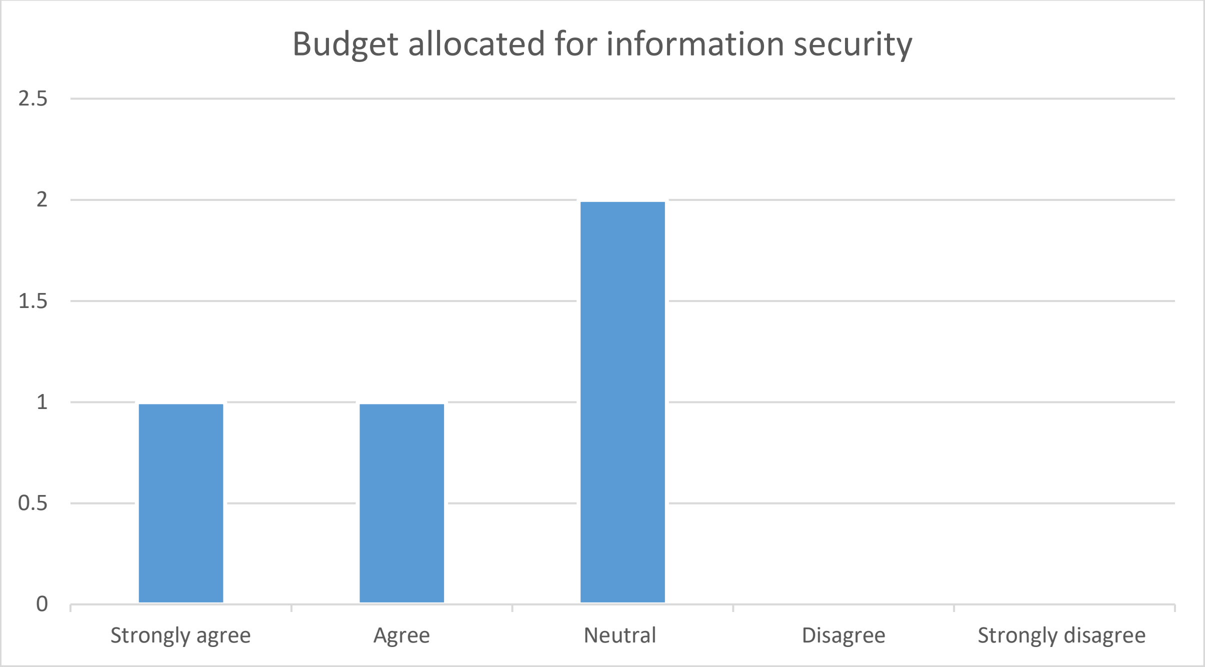


Figure E.164: Budget allocated for information security (46-55-UK)

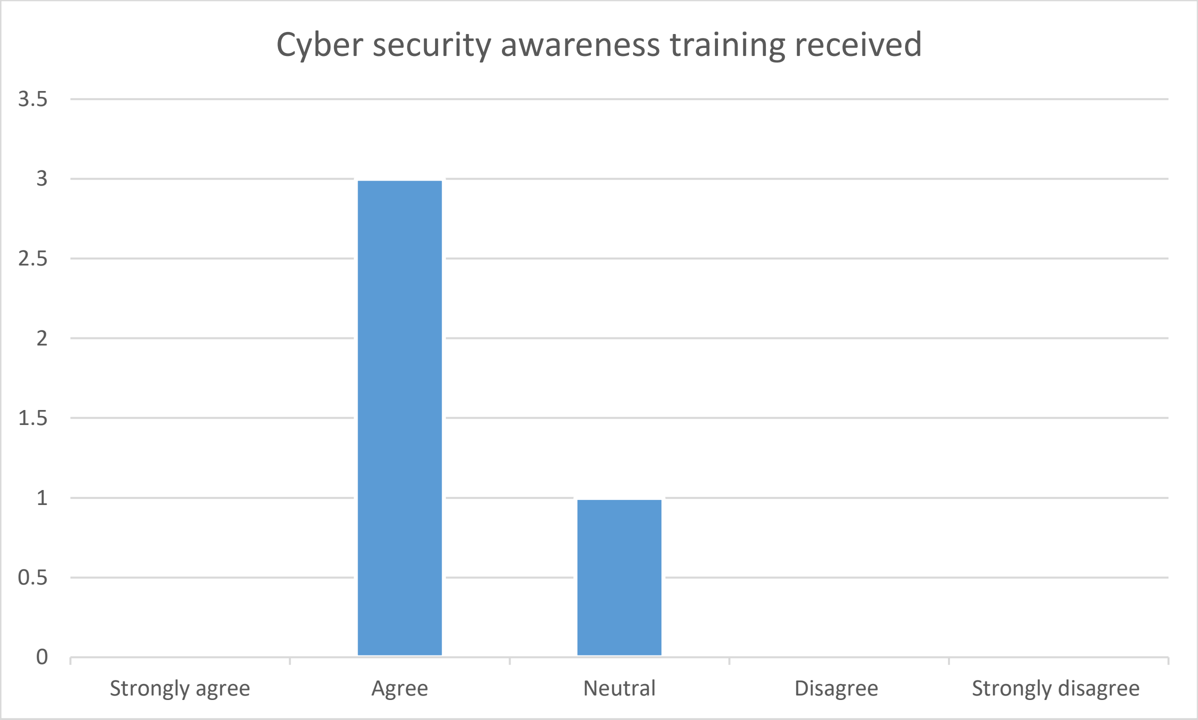


Figure E.165: Cyber security awareness training received (46-55-UK)

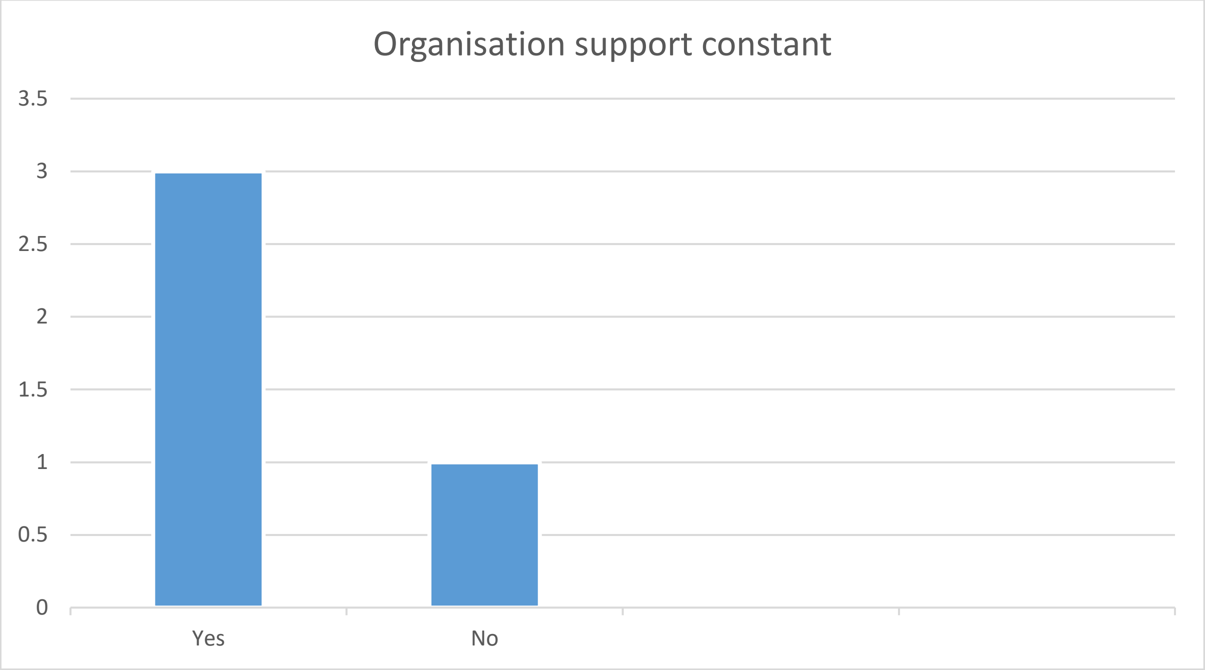


Figure E.166: Organisation support constant (46-55-UK)

Funding has been sketchy. 2 out of the 4 have indicated that their organisations had an allocated budget for information security, whilst 2 had not expressed an opinion either way (See figure E.164). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was adequate. 3 participants have received regular cybersecurity awareness training, whilst 1 neither agreed nor disagreed (See figure E.165). In addition, only 1 participant had not received support from the organisation to protect personal information, whilst 3 did (See figure E.166). Participants in 46-55 age range received necessary support from their organisations in terms of awareness training and support toward protecting personal information.

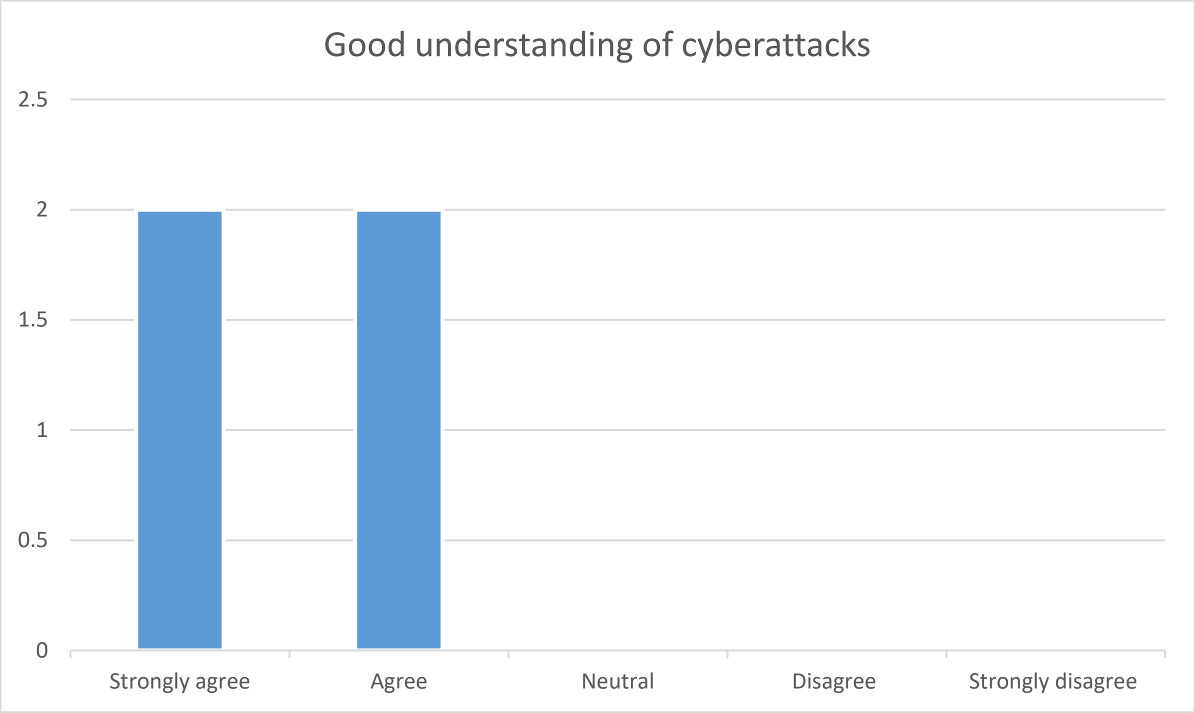


Figure E.167: Good understanding of cyberattacks (46-55-UK)

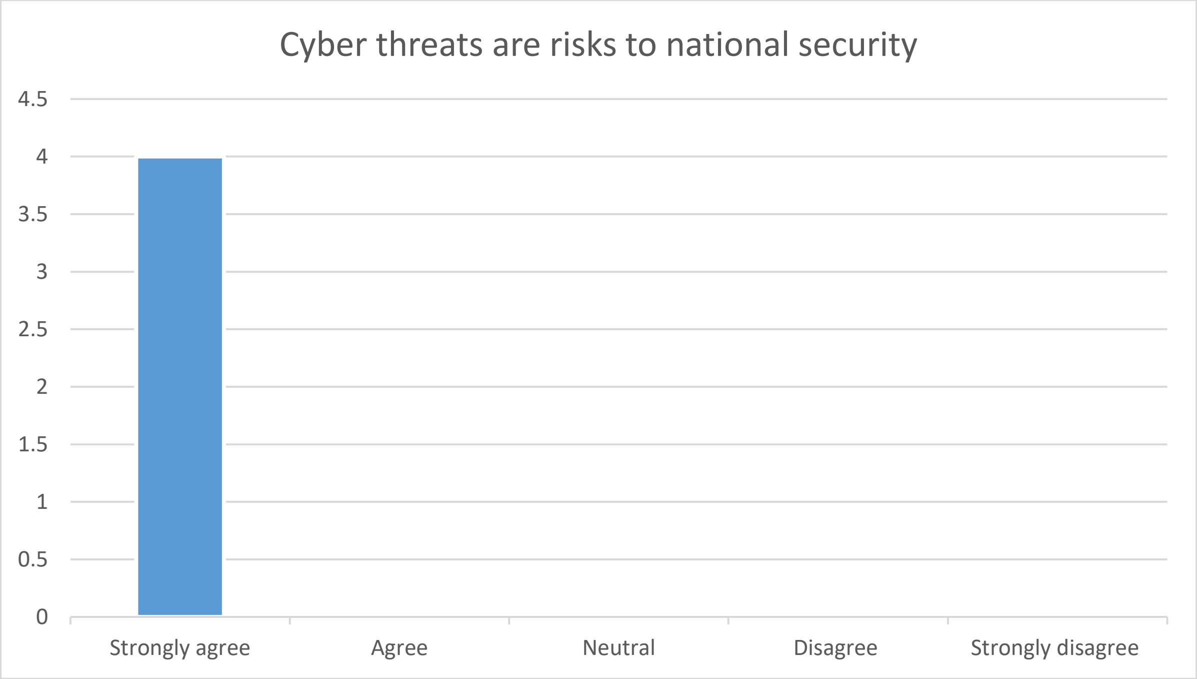


Figure E.168: Cyber threats are risks to national security (46-55-UK)

Despite the security awareness training, all the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation (See figure E.167). Furthermore, 100 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure E.168). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

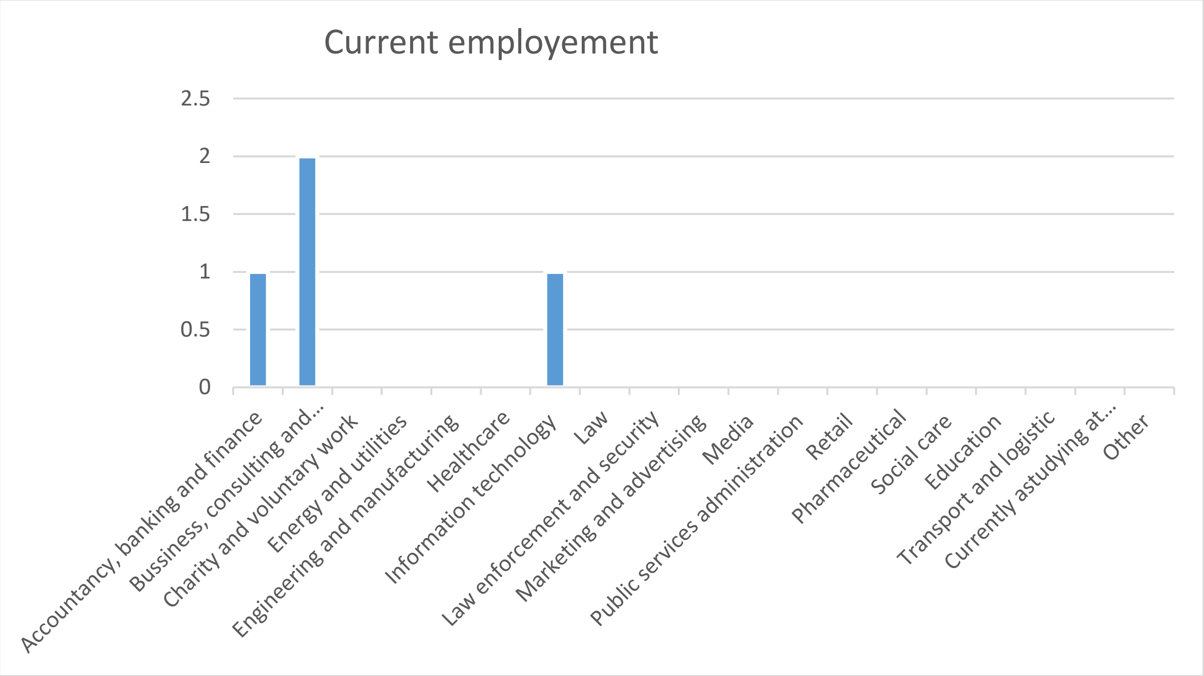


Figure E.169: Current employment (46-55-UK)

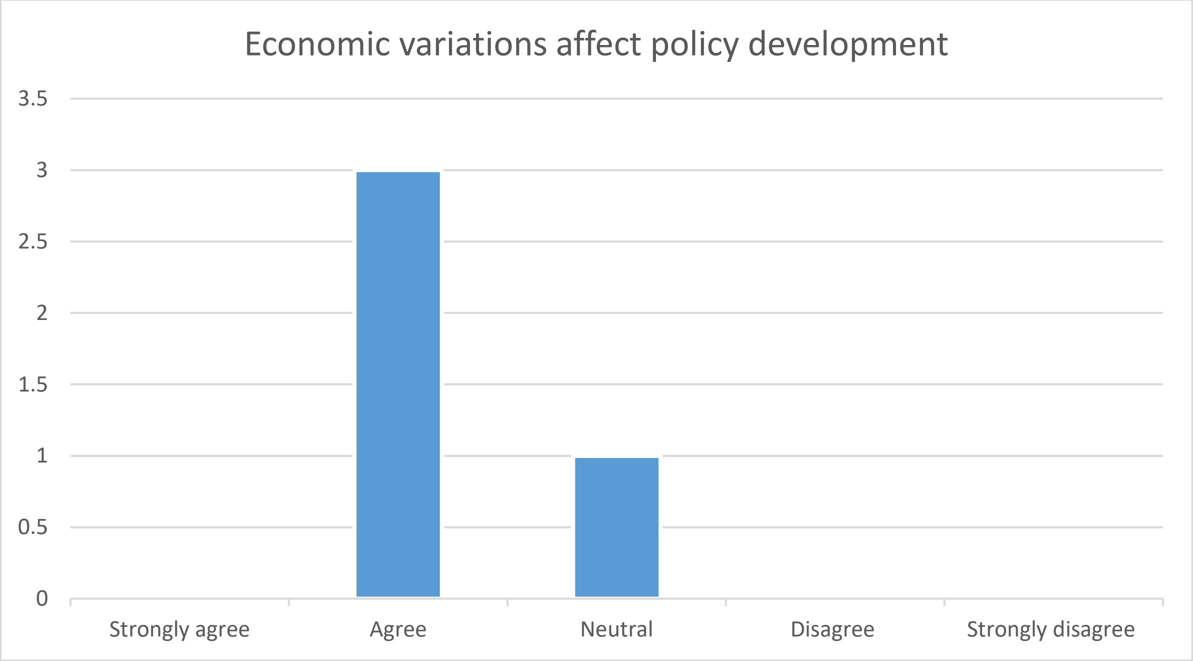


Figure E.170: Economic variations affect policy development (46-55-UK)

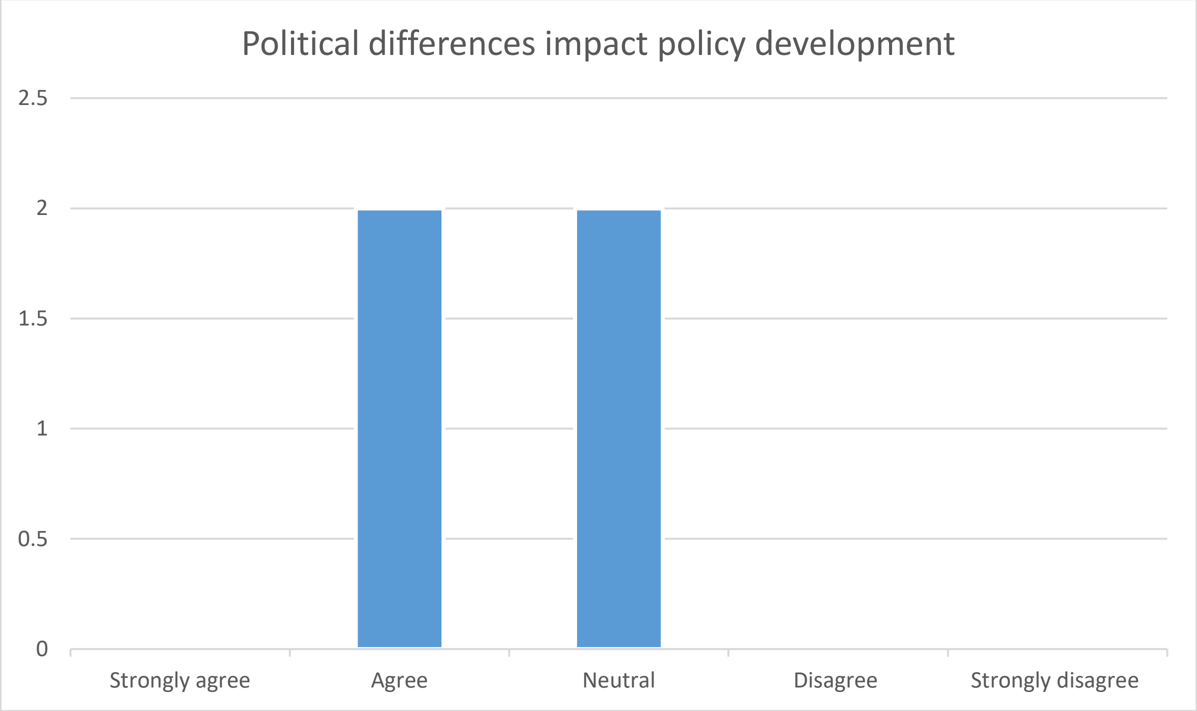


Figure E.171: Political differences impact policy development (46-55-UK)

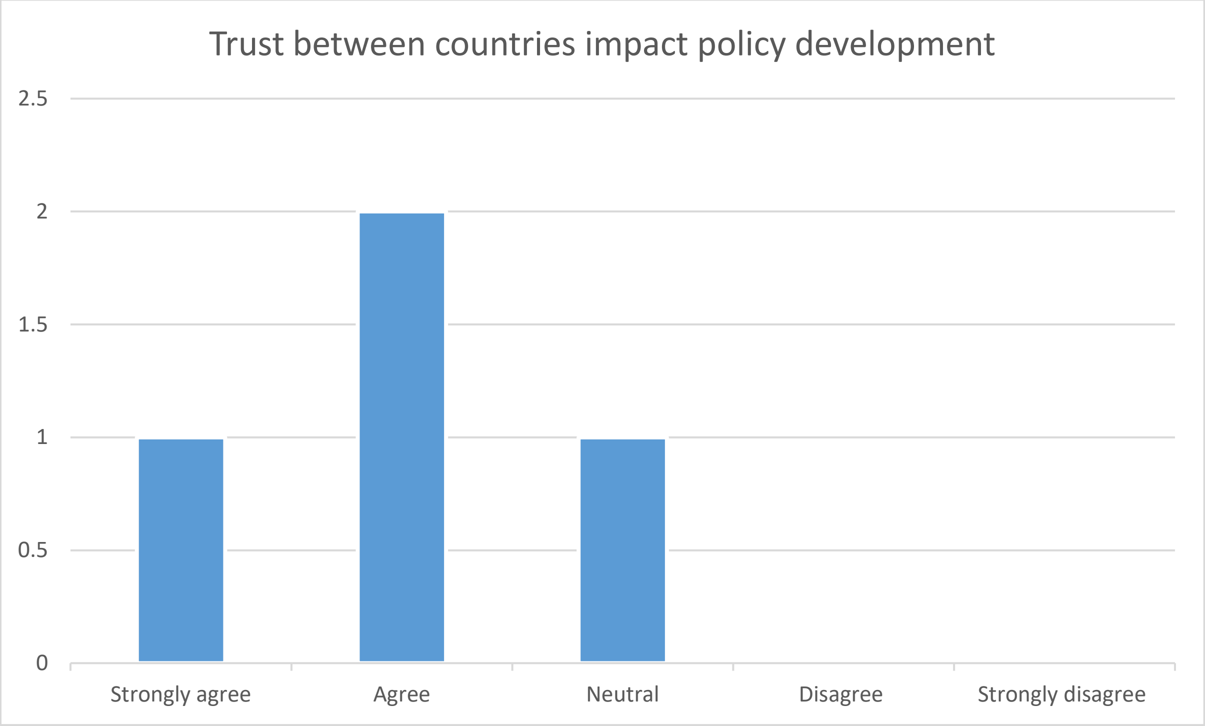


Figure E.172: Trust between countries impact policy development (46-55-UK)

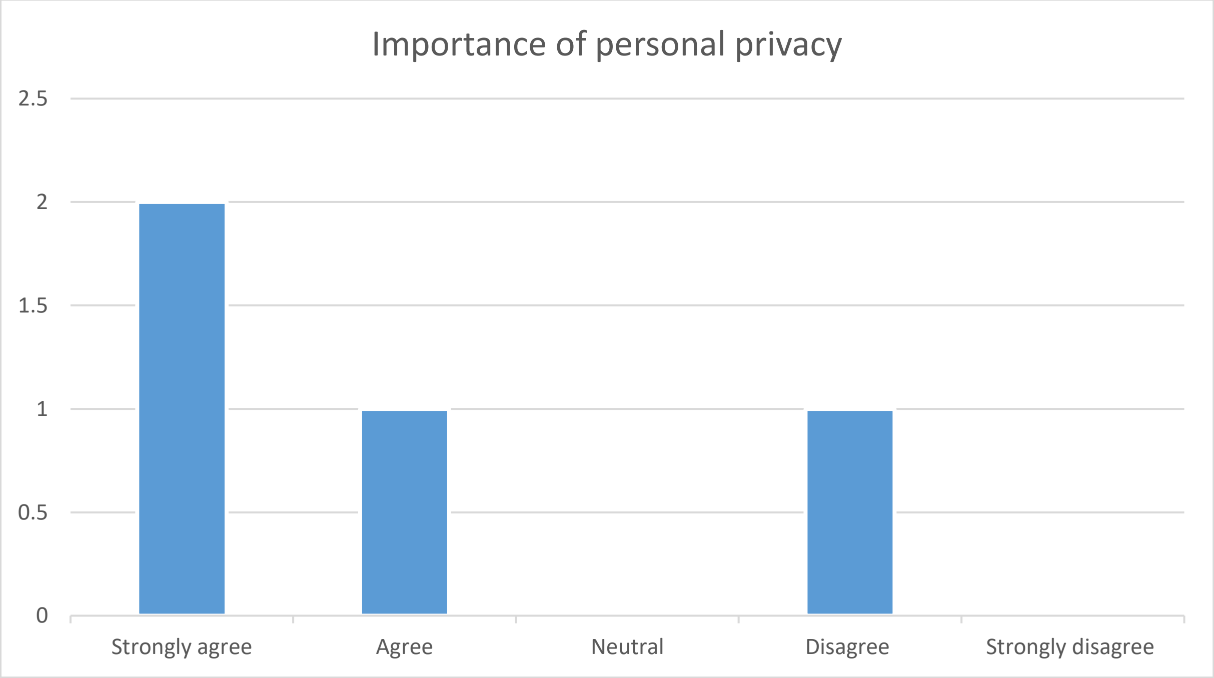


Figure E.173: Importance of personal privacy (46-55-UK)

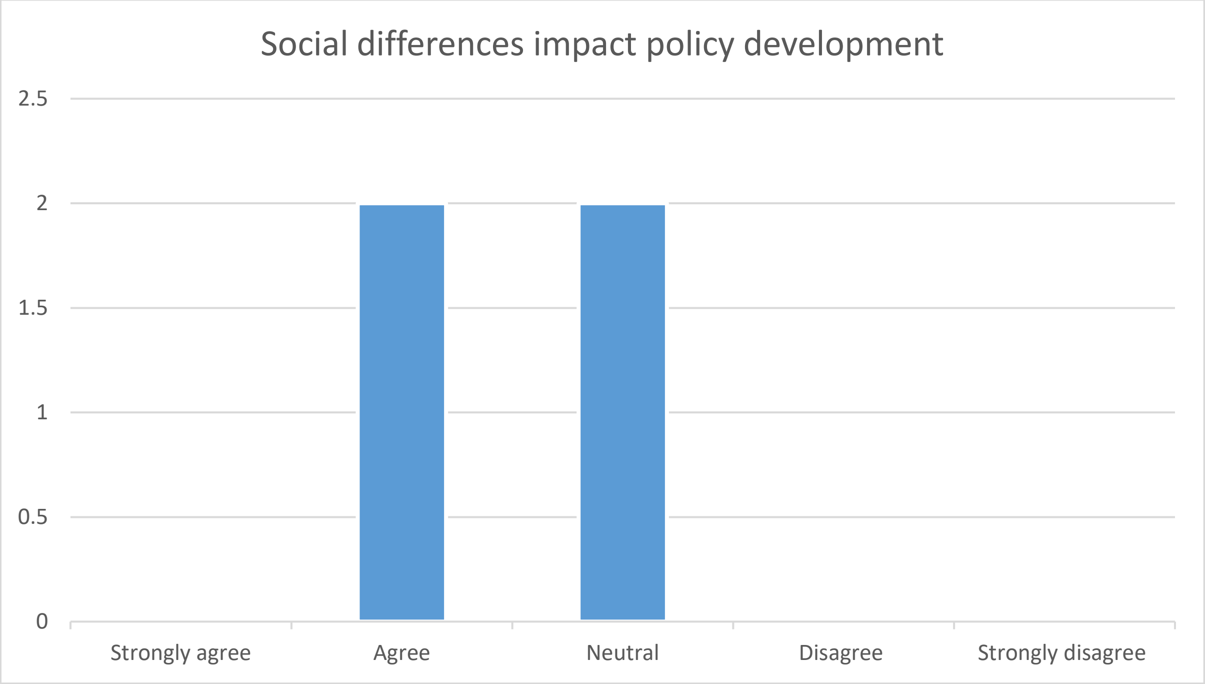


Figure E.174: Social differences impact policy development (46-55-UK)

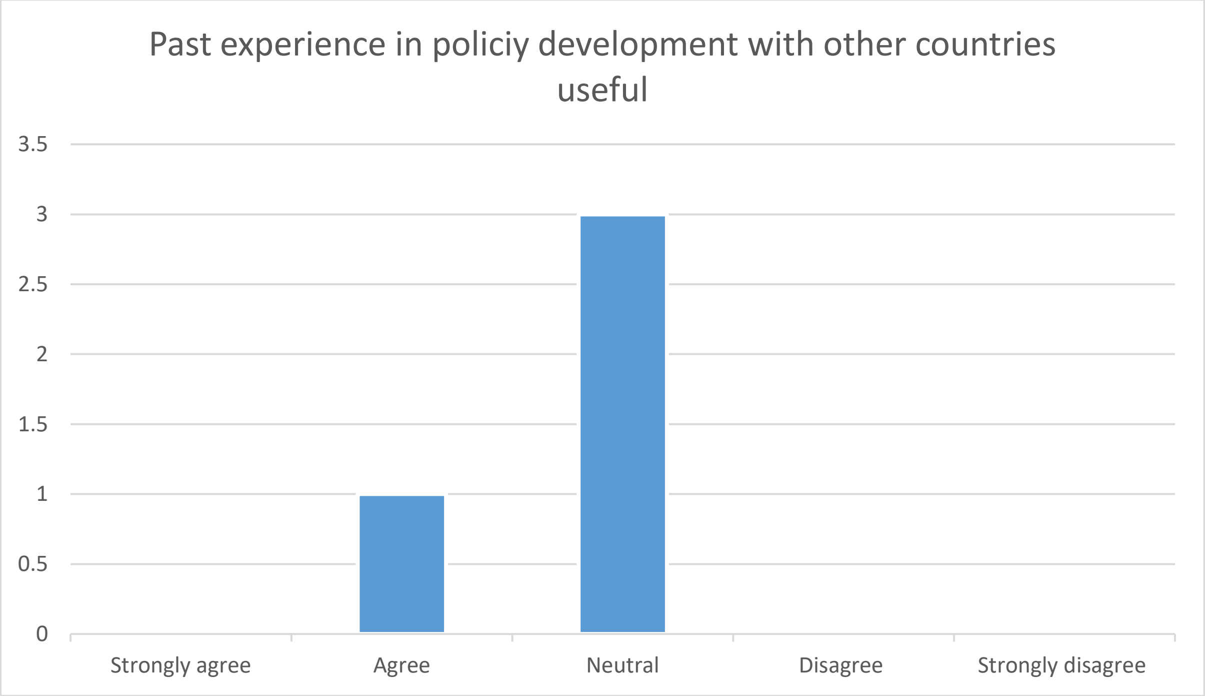


Figure E.175: Past experience in policy development with other countries useful (46-55-UK)

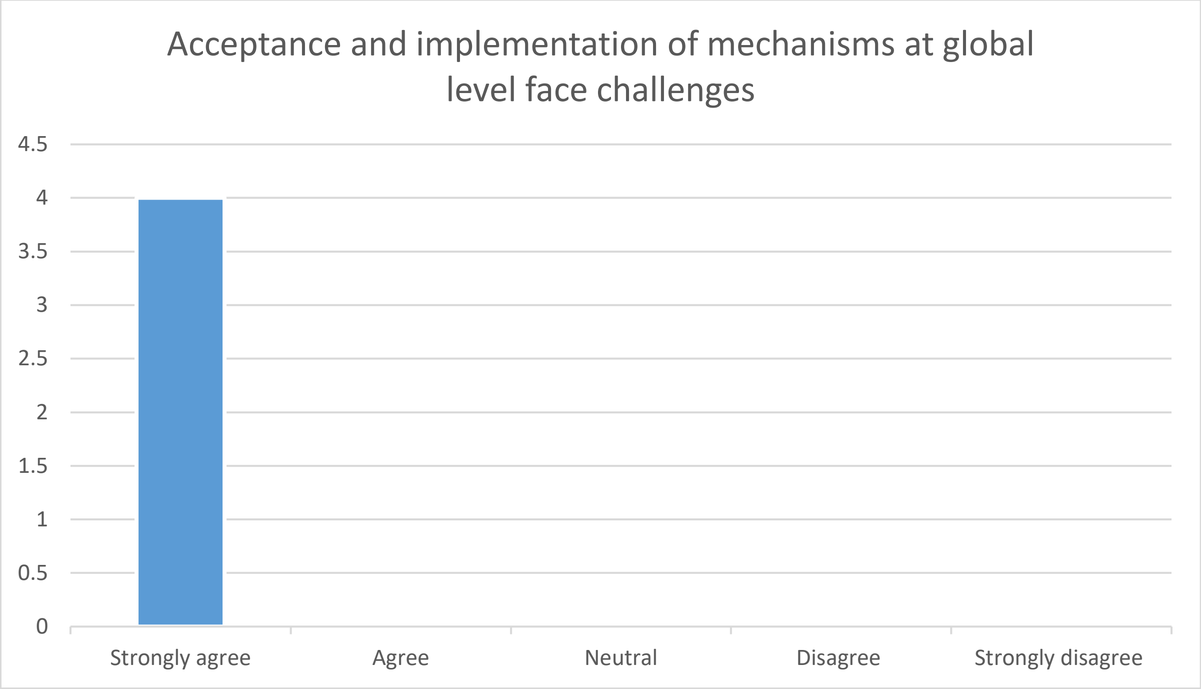


Figure E.176: Acceptance and implementation of mechanisms at global level face challenges (46-55-UK)

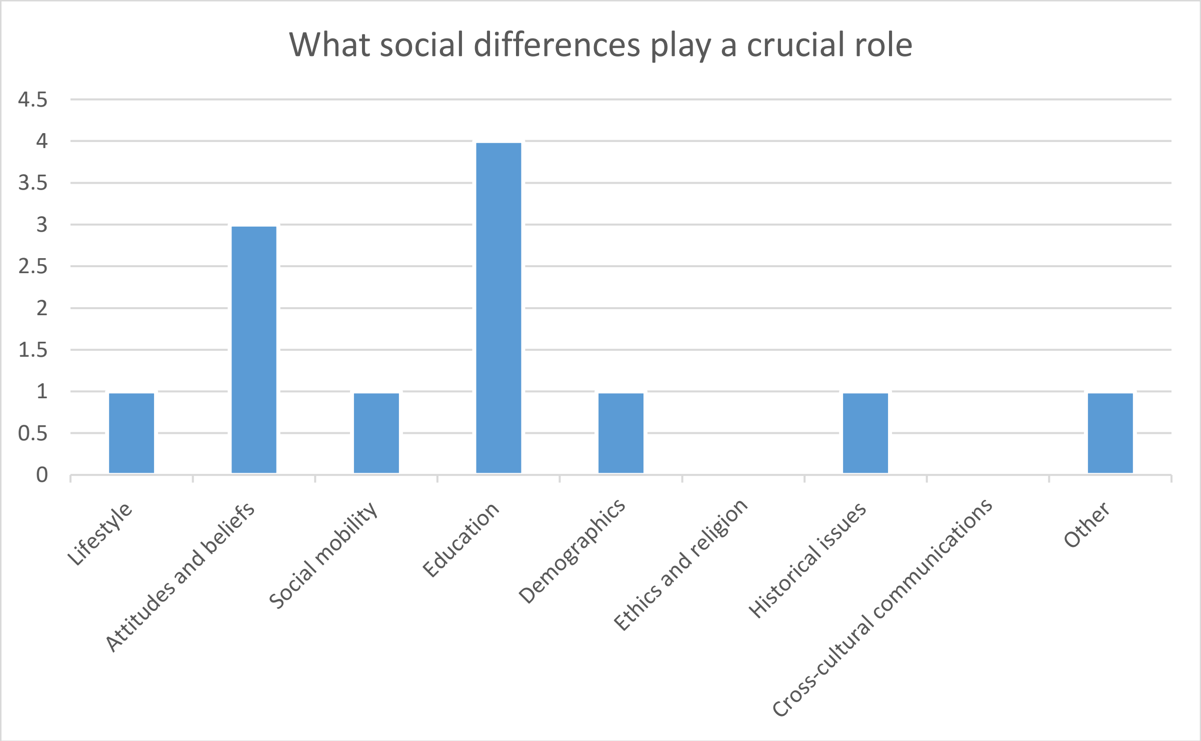


Figure E.177: What social differences play a crucial role (46-55-UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure E.177). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

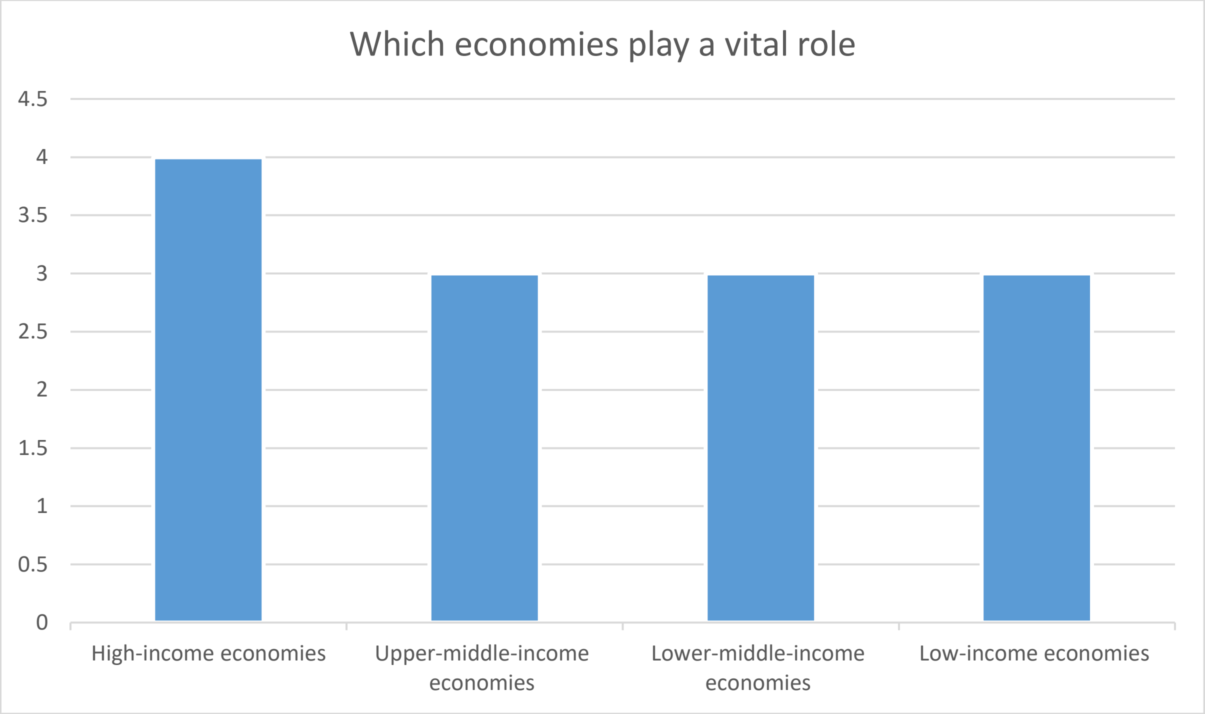


Figure E.178: Which economies play a vital role (46-55-UK)

According to the majority the high-income upper-middle-income, lower middle income and low-income countries play a vital role in accepting and implementing a data protection mechanism (See figure E.178). They are the only respondents to have chosen lower middle income and low-income countries. The reason may be regardless of the economic status, the hackers take advantages of vulnerabilities. The key stages in policymaking are to identify policymaker aims, policies to achieve those aims, select a policy measure, identify the necessary resources, implement, and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking. Any country without sufficient financial resources should work together with other countries to find solutions. The countries with stable economies have a responsibility to provide support to lower-income countries in terms of grants towards enhancing cyber defence mechanisms.

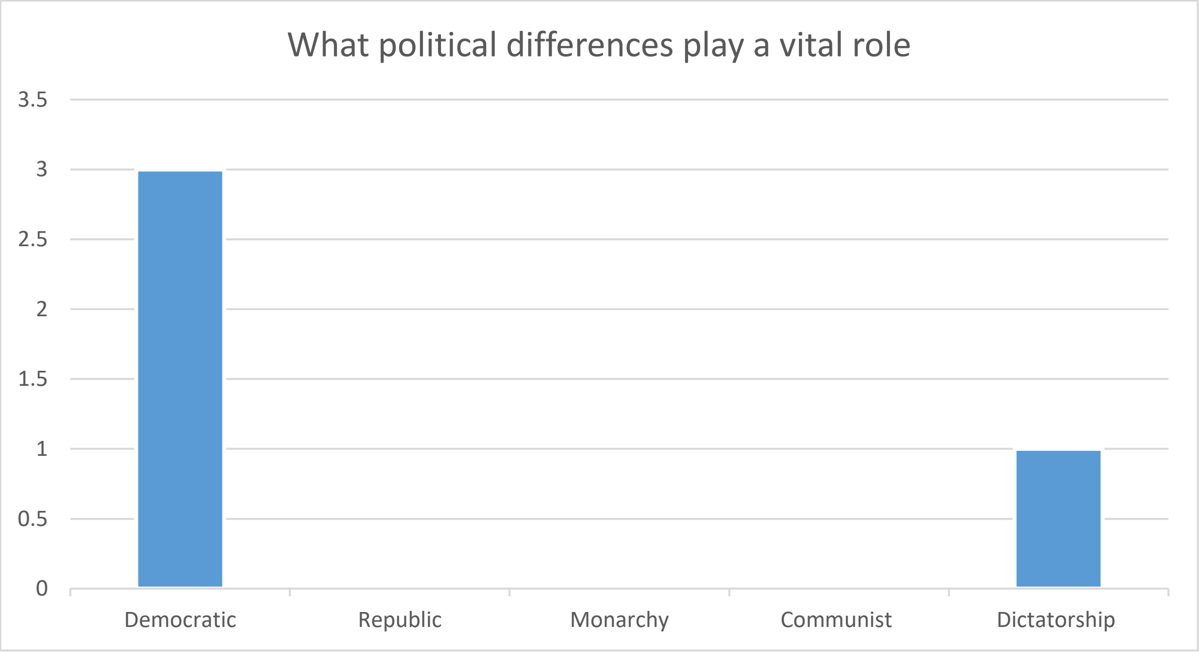


Figure E.179: What political differences play a vital role (46-55-UK)

The majority have chosen a democratic political system (See figure E.179), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

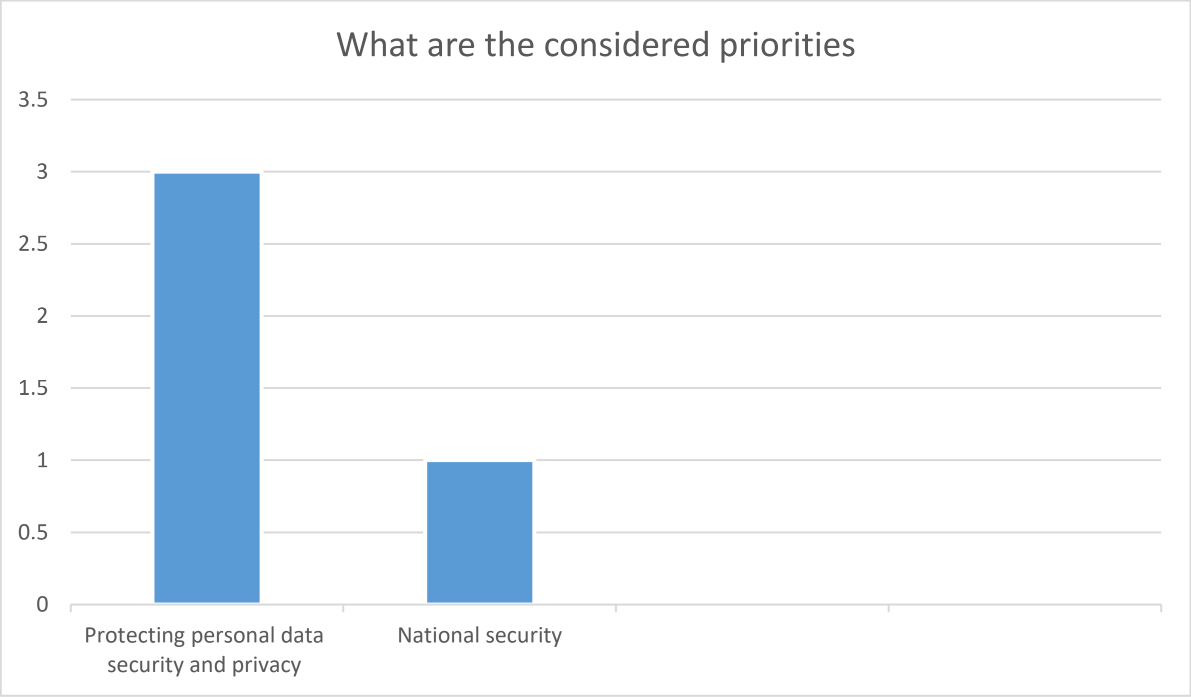


Figure E.180: What are the considered priorities (46-55-UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security (See figure E.180), which is a significant factor. However, in an incident of a personal data breach, there will potentially be a knock-on effect on both personal data security and privacy, and national security, and it will also be felt right across the groups as well as the community alike.

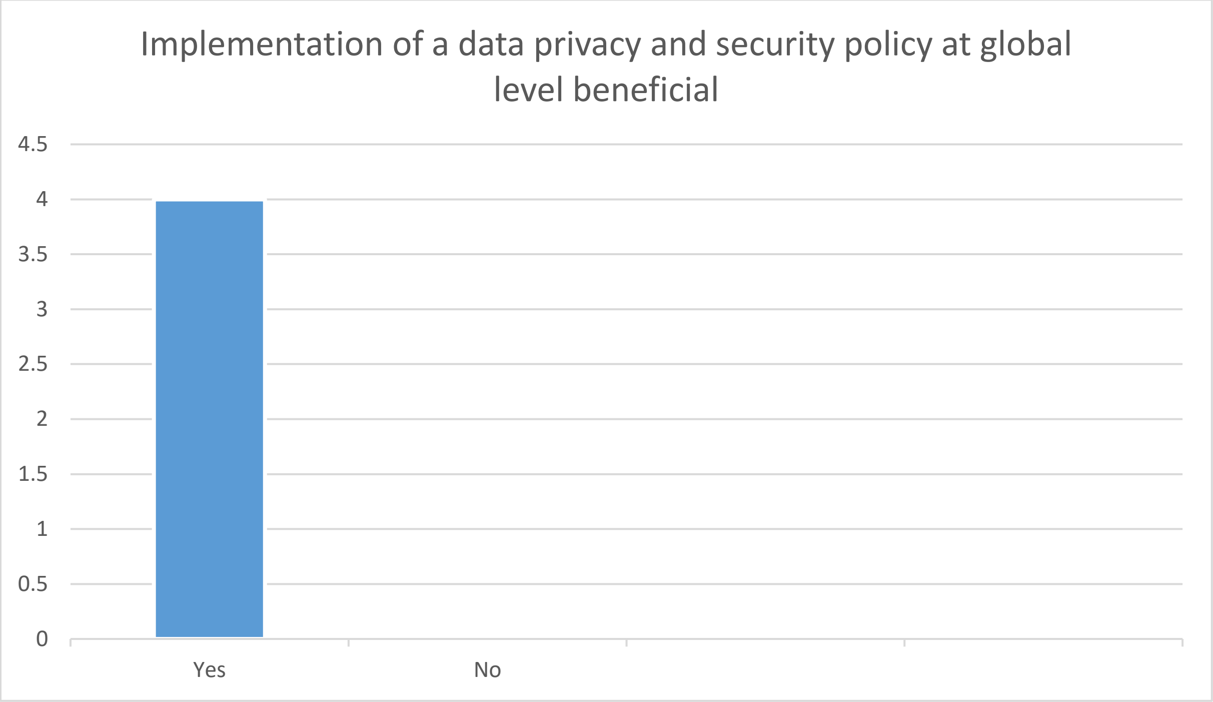


Figure 4.181: Implementation of a data privacy and security policy at global level beneficial (46-55-UK)

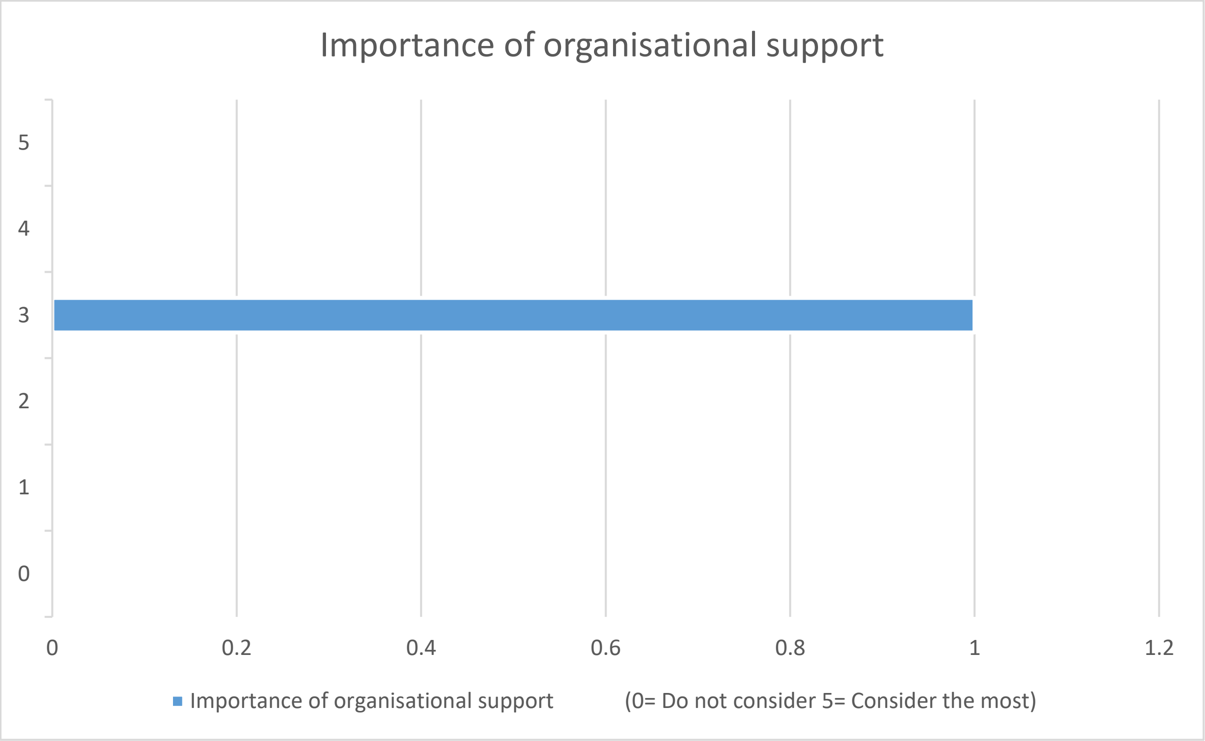


Figure E.182: Importance of organisational support (46-55-UK)

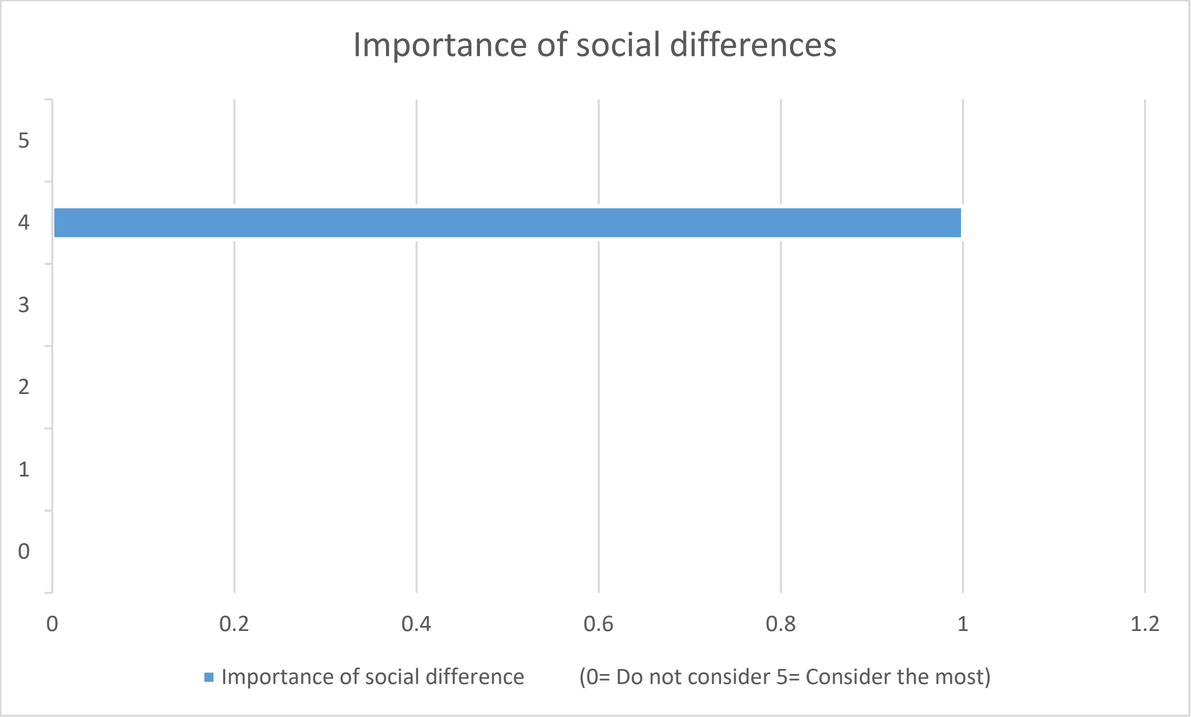


Figure E.183: Importance of social differences (46-55-UK)

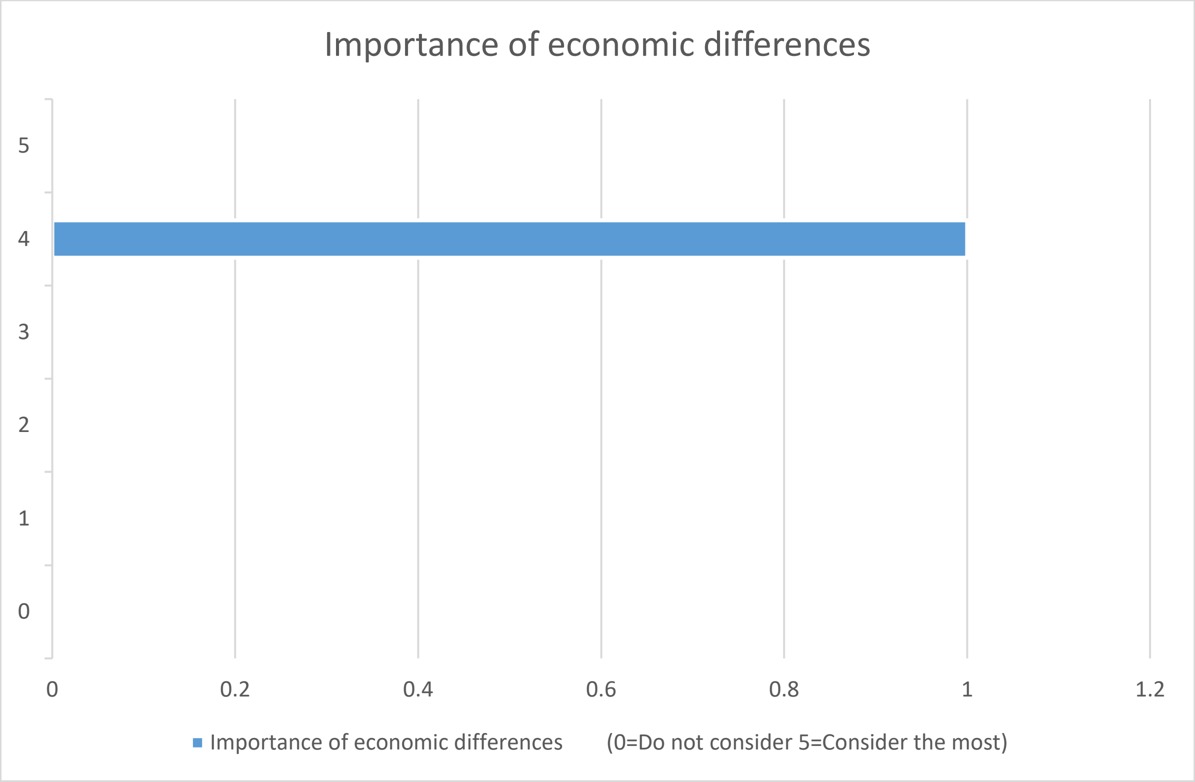


Figure E.184: Importance of economic differences (46-55-UK)

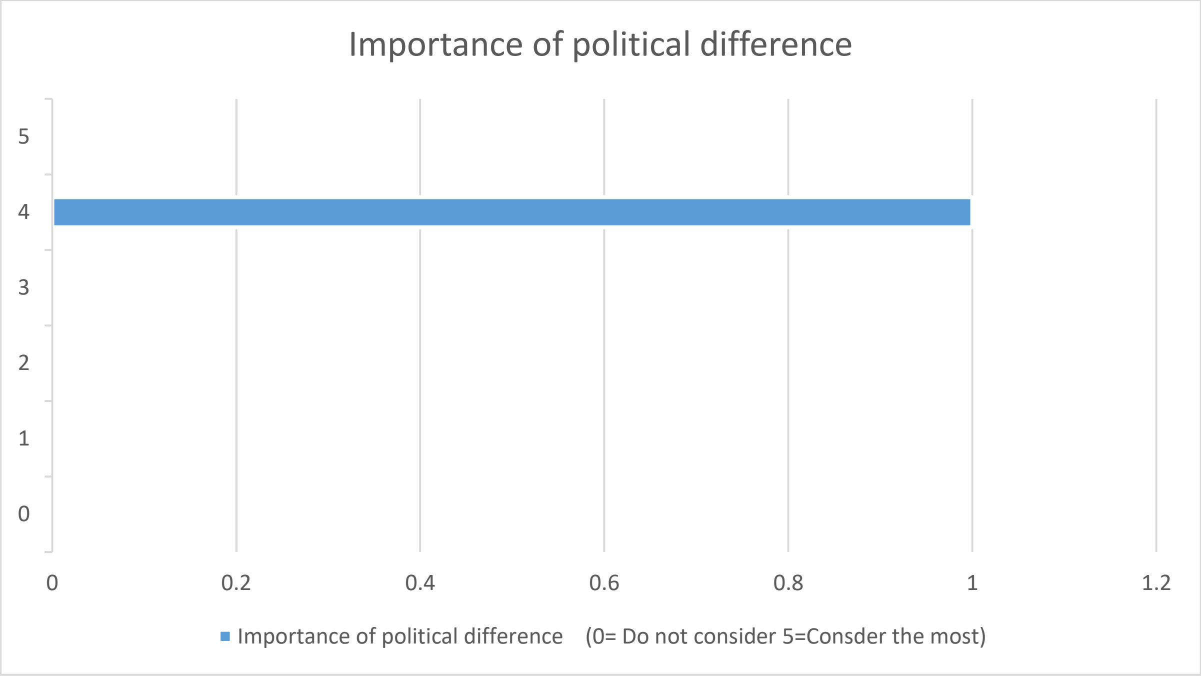


Figure E.185: Importance of political difference (46-55-UK)

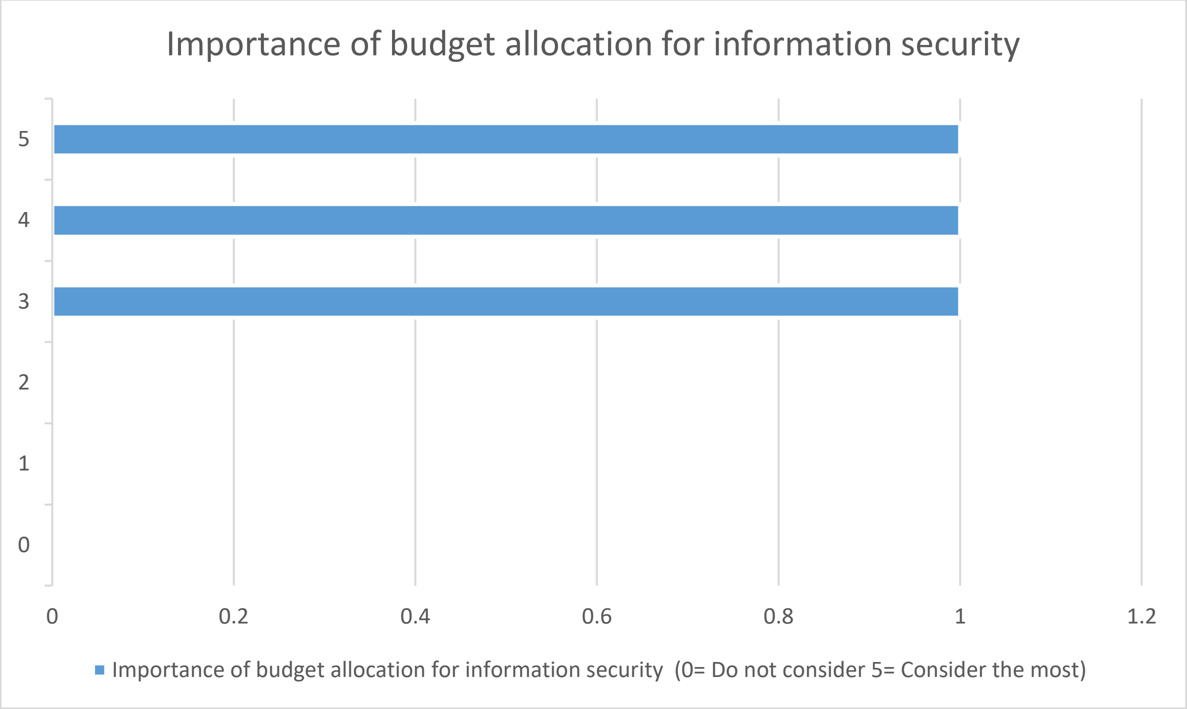


Figure E.186: Importance of budget allocation for information security (46-55-UK)

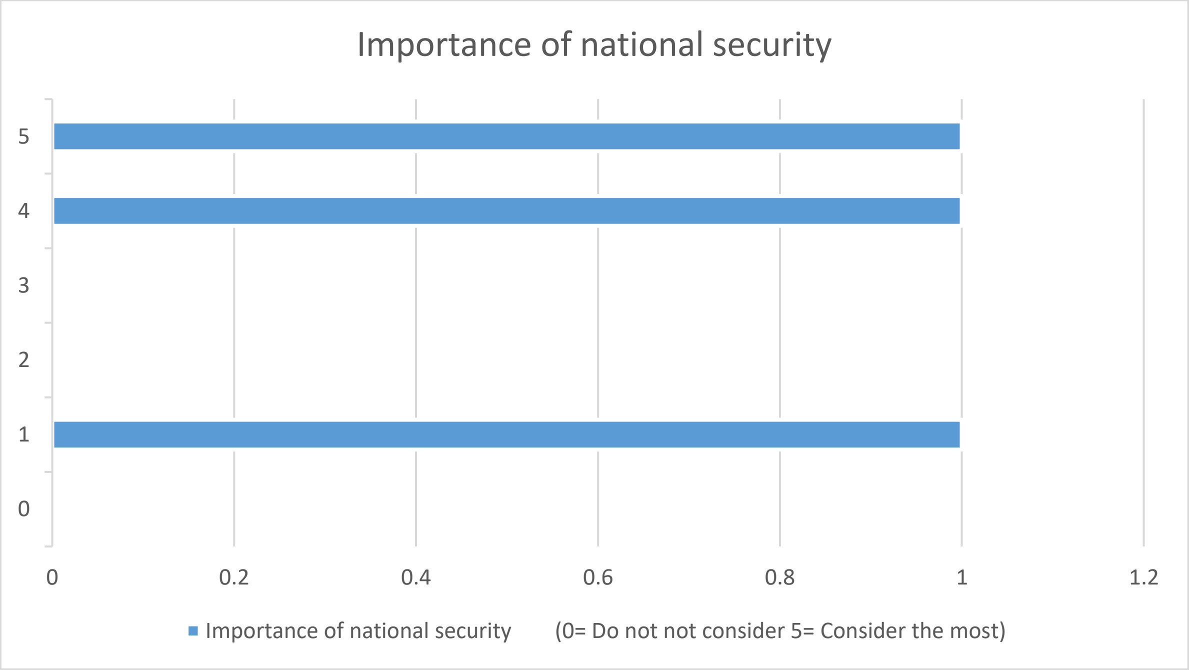


Figure E.187: Importance of national security (46-55-UK)

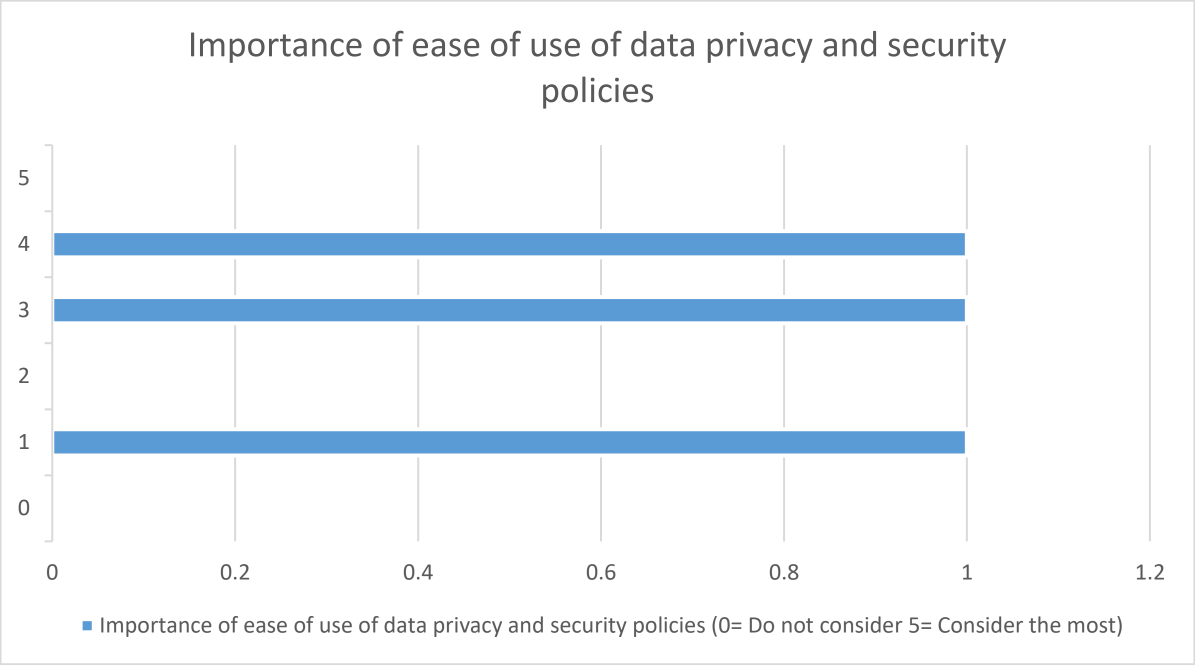


Figure E.188: Importance of ease of use of data privacy and security policies (46-55-UK)

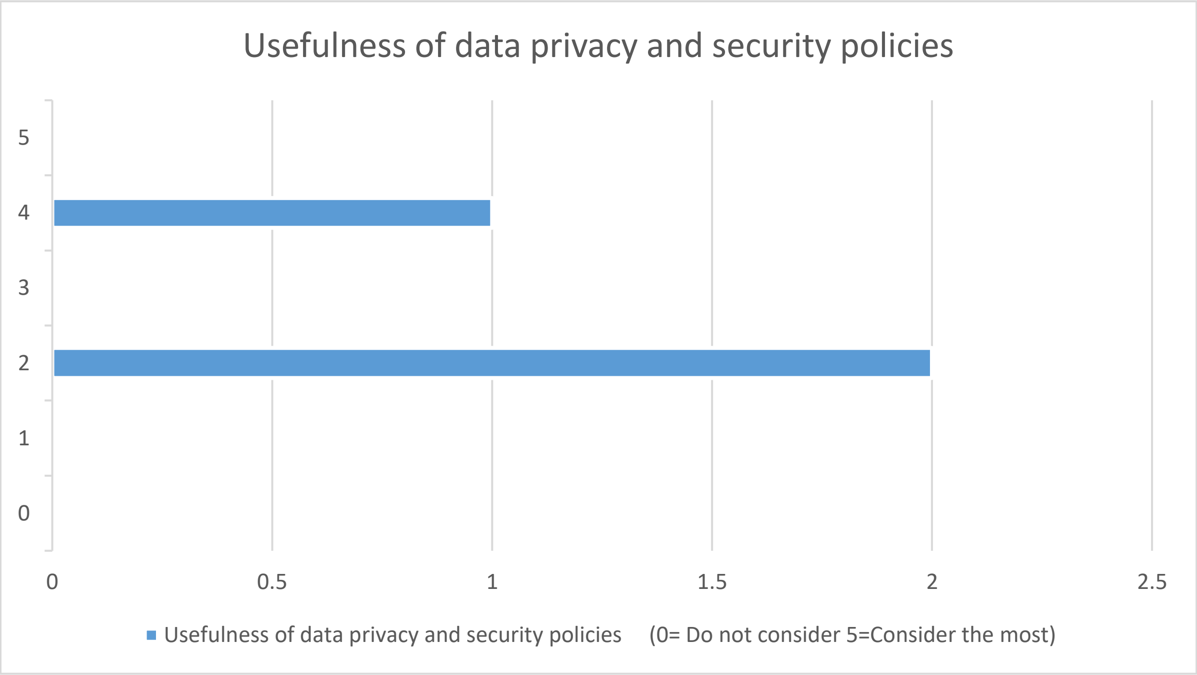


Figure E.189: Usefulness of data privacy and security policies (46-55-UK)

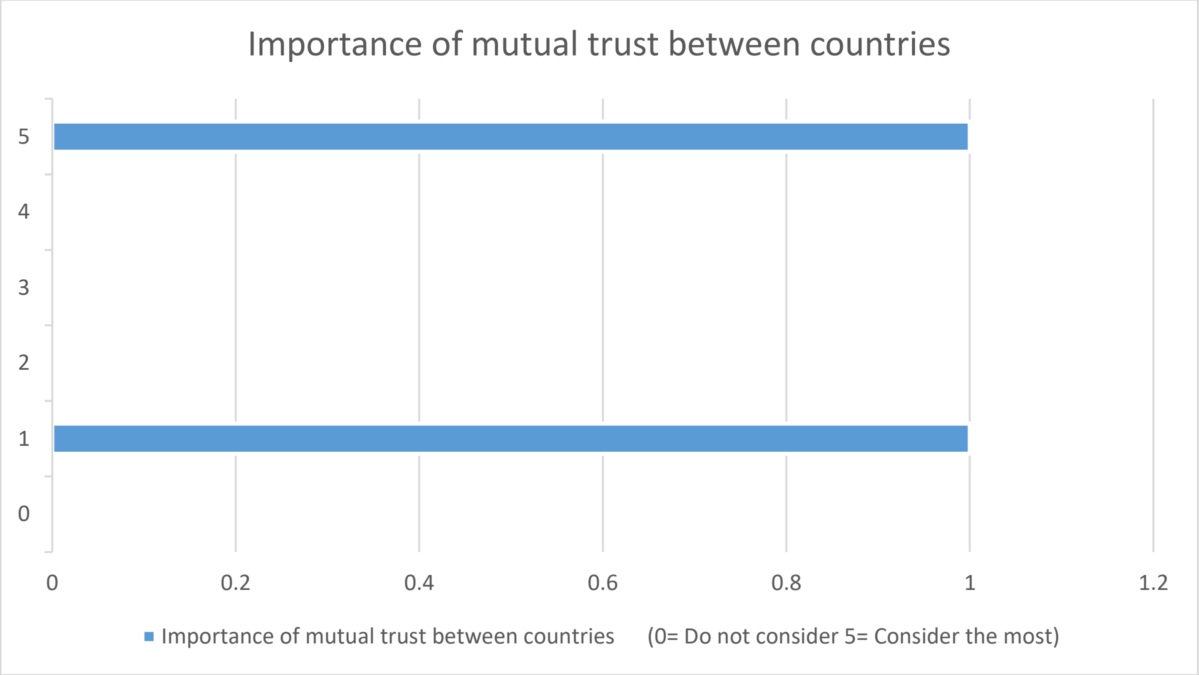


Figure E.190 Importance of mutual trust between countries (46-55-UK)

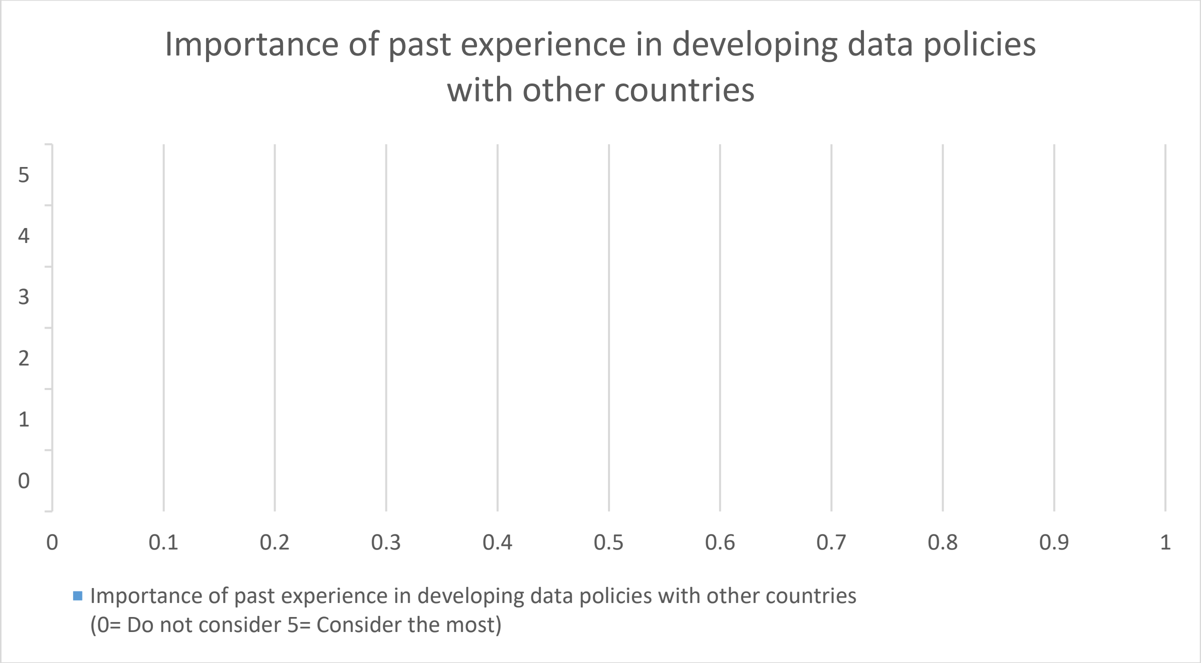


Figure E.191: Importance of past experience in developing data policies with other counties (46-55-UK)

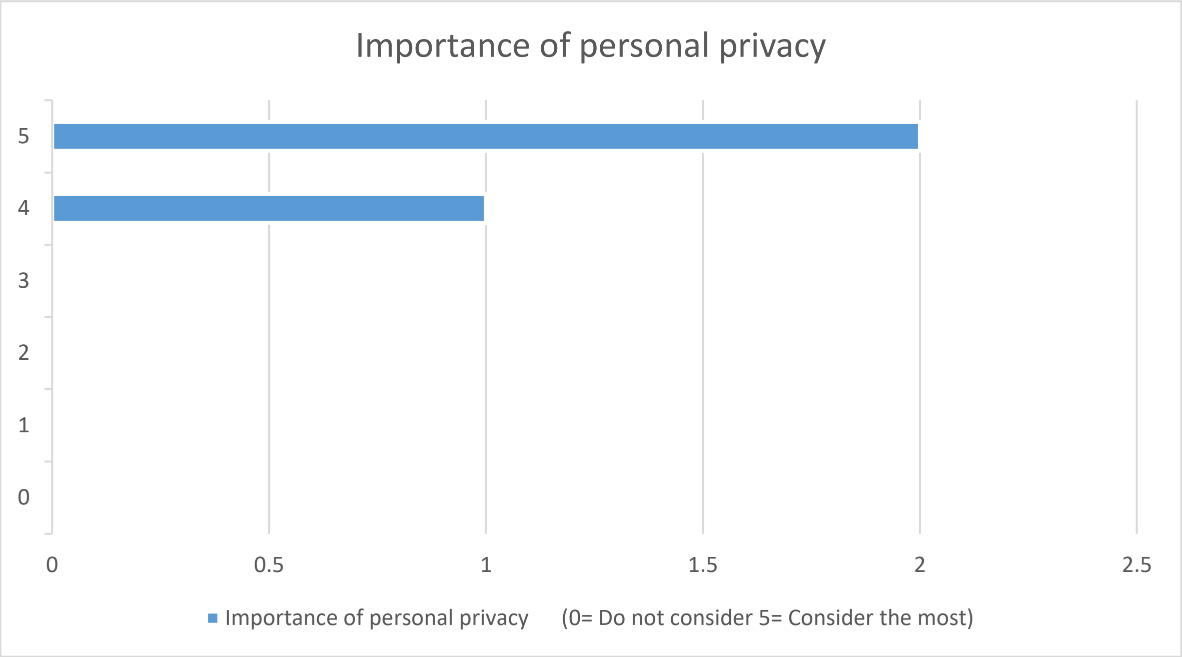


Figure E.192: Importance of personal privacy (46-55-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 100 percent of the respondents have endorsed (See figure E.181). The other notable factors that have come out of the survey are budget allocation, personal privacy, national security, ease of use of data privacy and security policies (See figure E.170-180) (See figure E.182-192). Notably, everyone has ignored the previous experience with other countries in developing policies (See figure E.191).

United Kingdom – 56-65

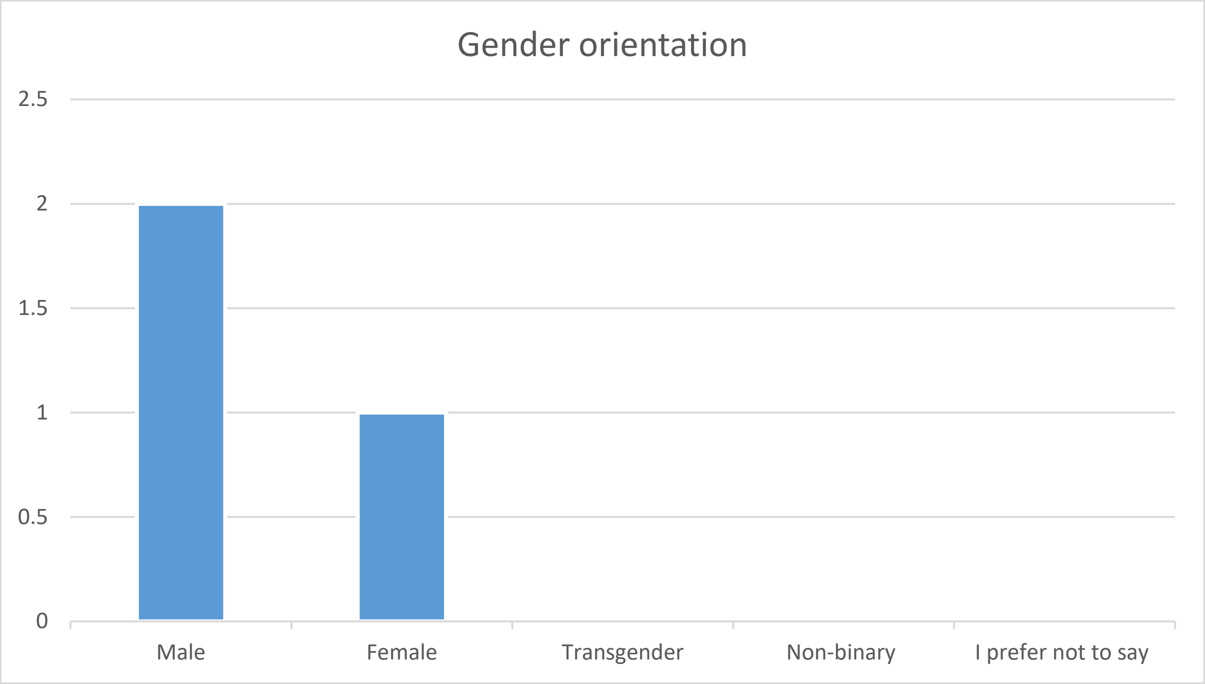


Figure E.193: Gender orientation (56-65-UK)

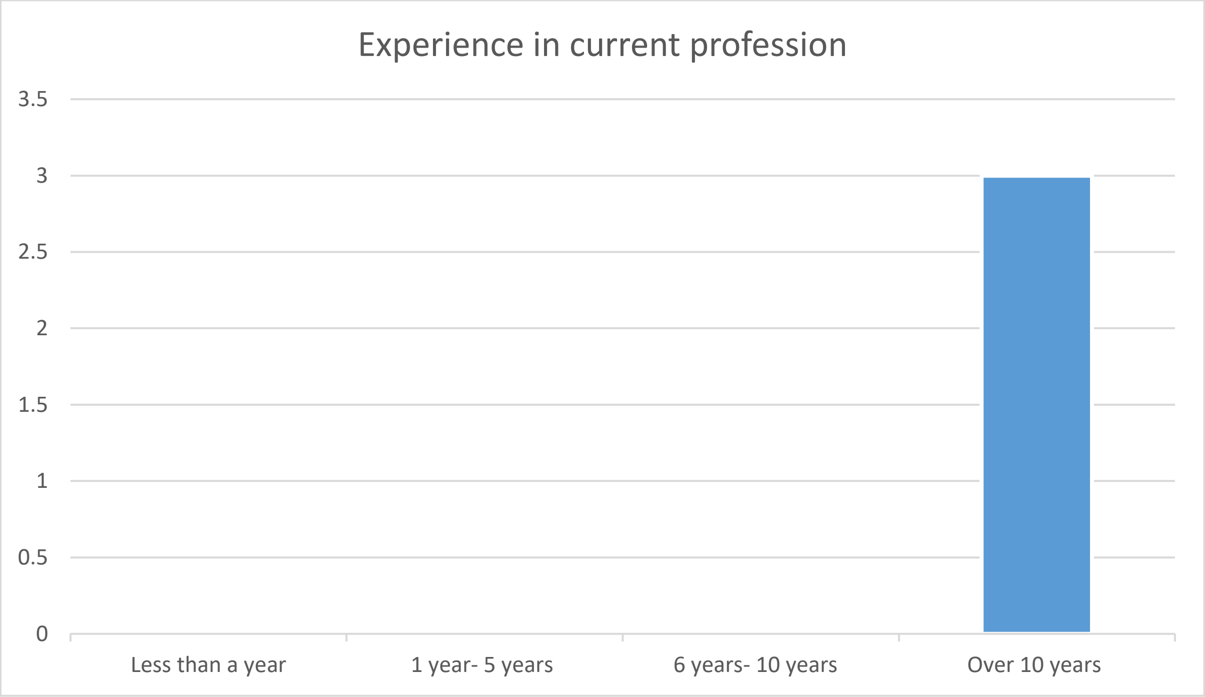


Figure E.194: Experience in current profession (56-65-UK)

This analysis is based on the responses received from United Kingdom participants aged between 56-65. There were 3 participants and 2 out of them were males and 1 female (See figure E.193). The participants employed in different industries for over 10 years (See figure E.194).

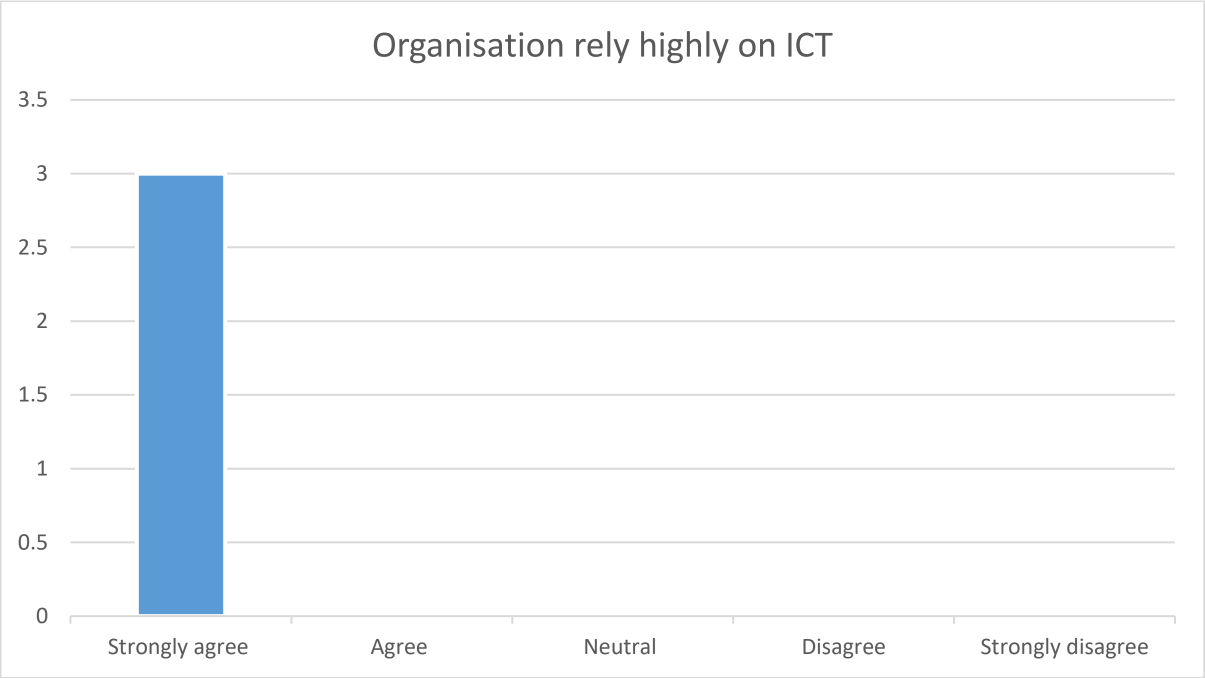


Figure E.195: Organisation rely highly on ICT (56-65-UK)

Out of the 3 respondents, all the participants have worked in a technology reliance working environment (See figure E.195).

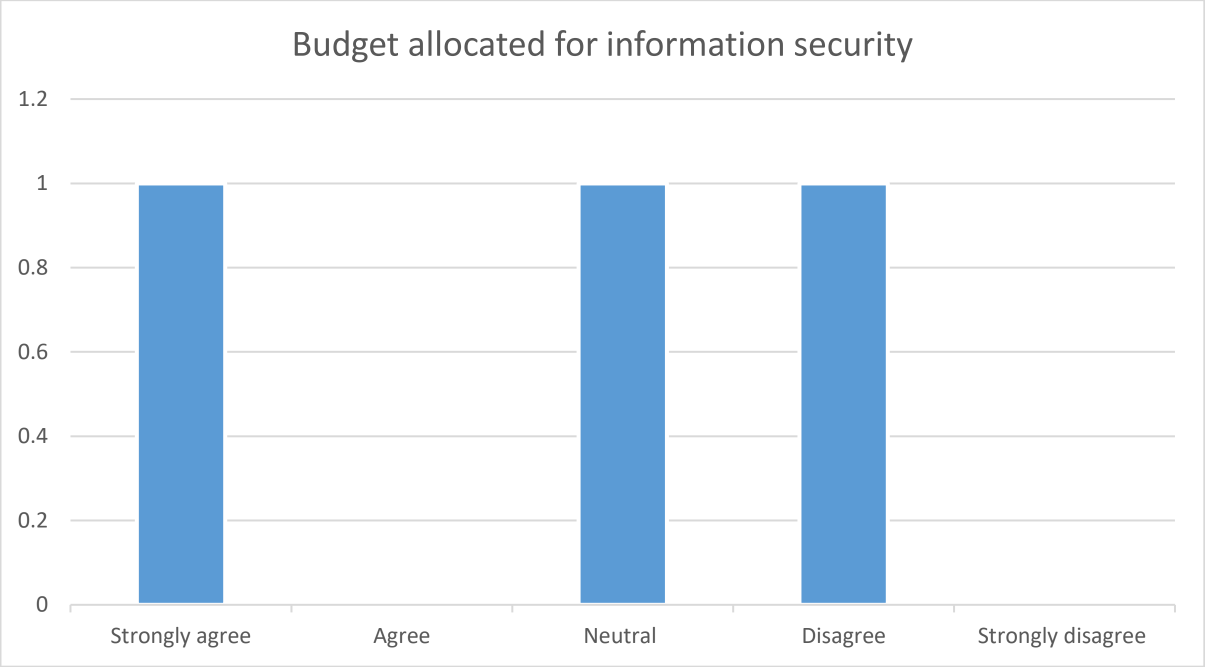


Figure E.196: Budget allocated for information security (56-65-UK)

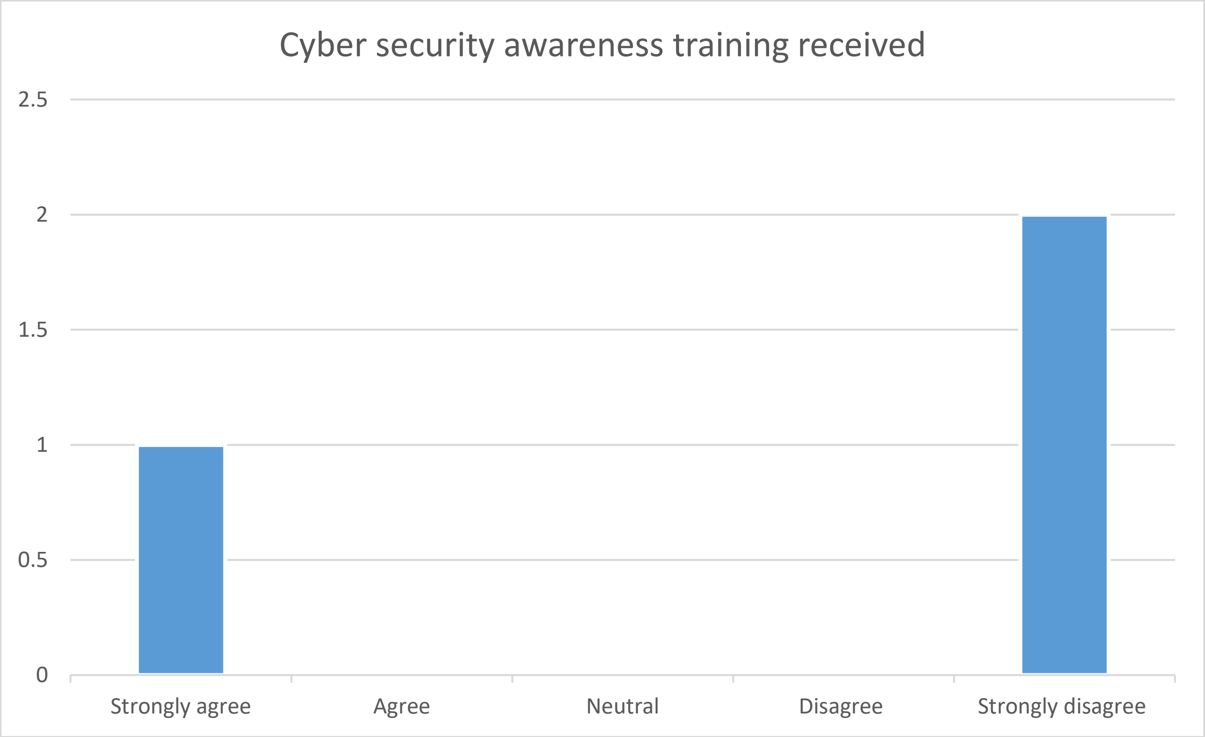


Figure E.197: Cyber security awareness training received (56-65-UK)

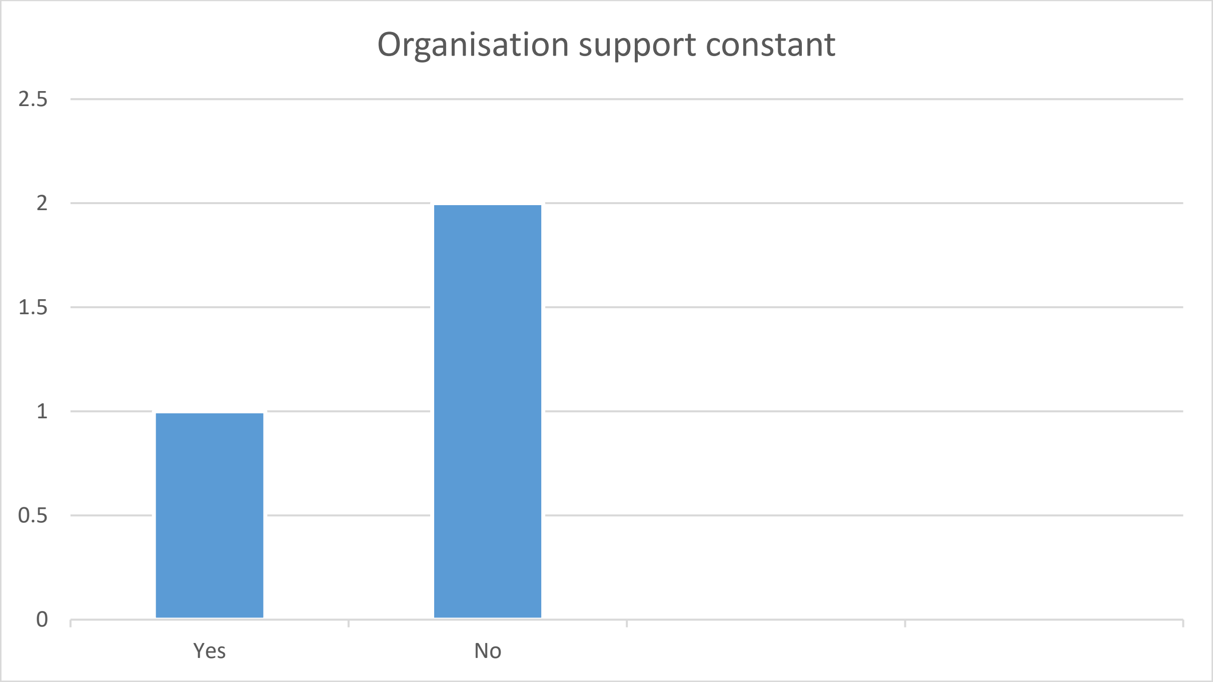


Figure E.198: Organisation support constant (56-65-UK)

The allocated budget is insufficient according to the participants. Only 1 out of the 3 indicated that their organisations allocated funding for information security, 1 expressed no opinion either way, and 1 disagreed (See figure E.196). In comparison, this age groups received less funding for information security. The responses show the inadequacy of regular security awareness training received. Only 1 participant received regular cybersecurity awareness training, and 2 participants did not (See figure E.197). In addition, only 1 participant received support from the organisation to protect personal information, 2 did not (See figure E.198). The reason for non- provision of regular training and support to protect personal information could be that the organisation/s had no budget allocation ring fenced for information security. Given the age of the participants in this group, it is possible that having considered the low level or to a lesser extent the risks from cyber threats, the organisations did not see the need for a separate budget for training purposes which might have had an impact on the employees.

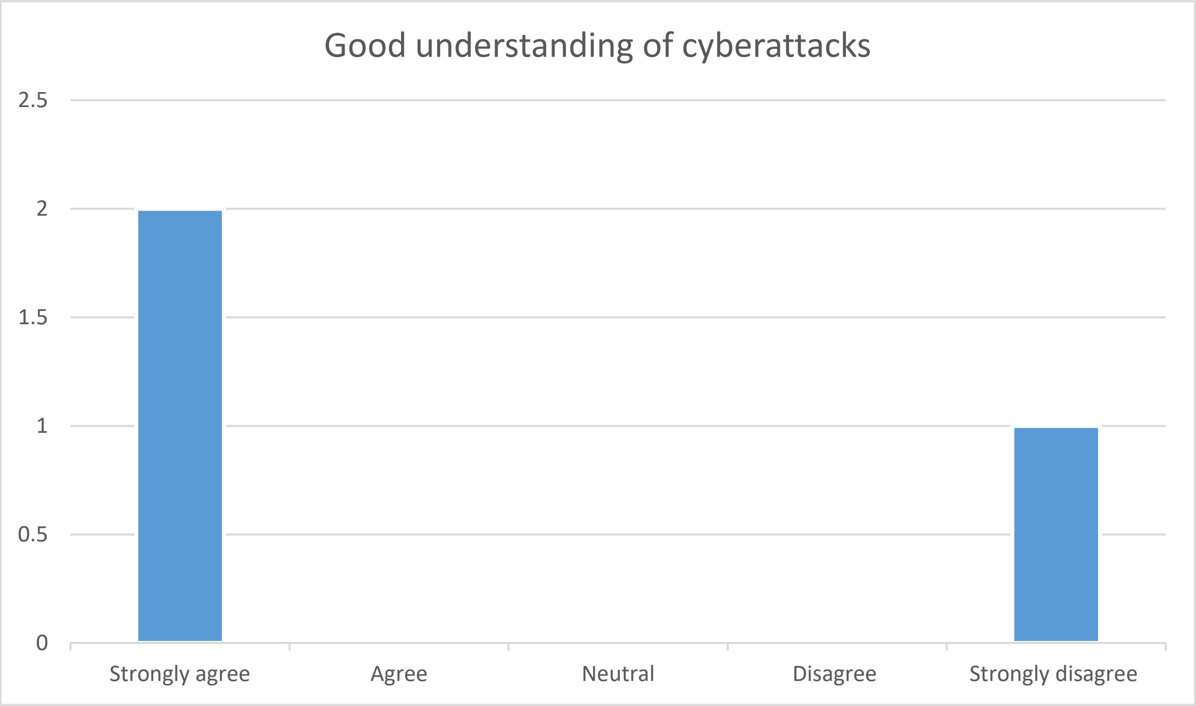


Figure E.199: Good understanding of cyberattacks (56-65-UK)

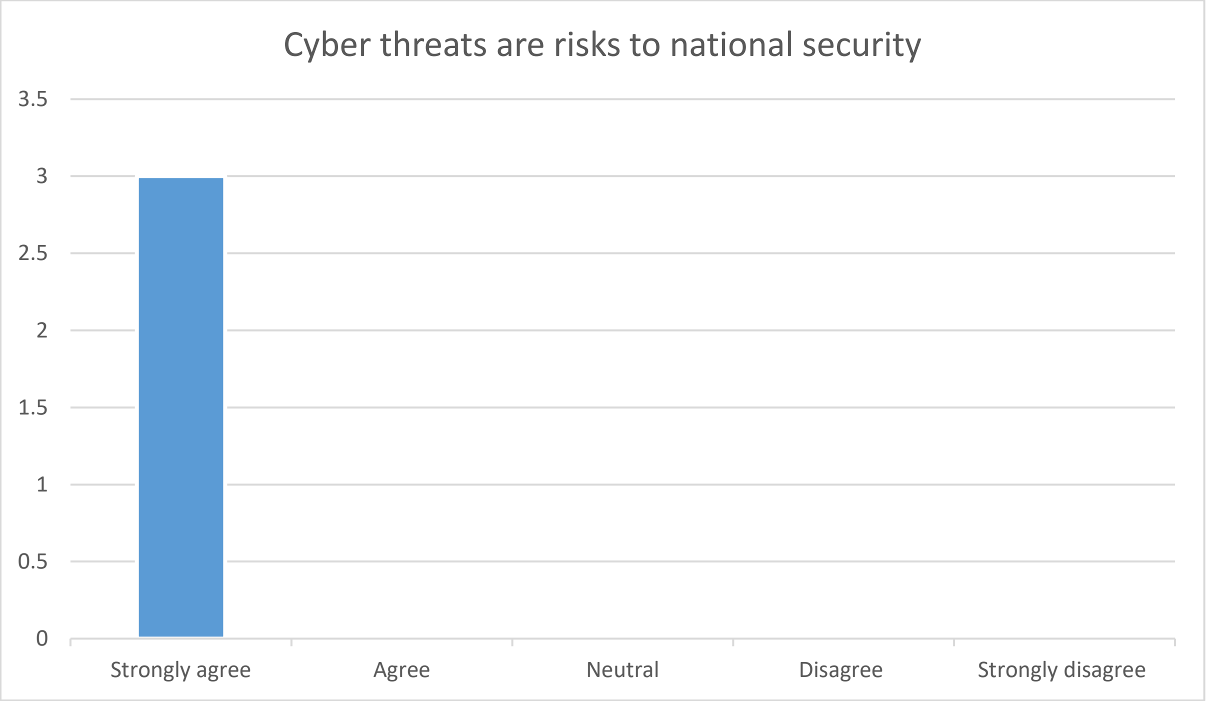


Figure E.200: Cyber threats are risks to national security (56-65-UK)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 2 participants do have, only 1 participant had no understanding (See figure E.199). Furthermore, 100 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure E.200). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

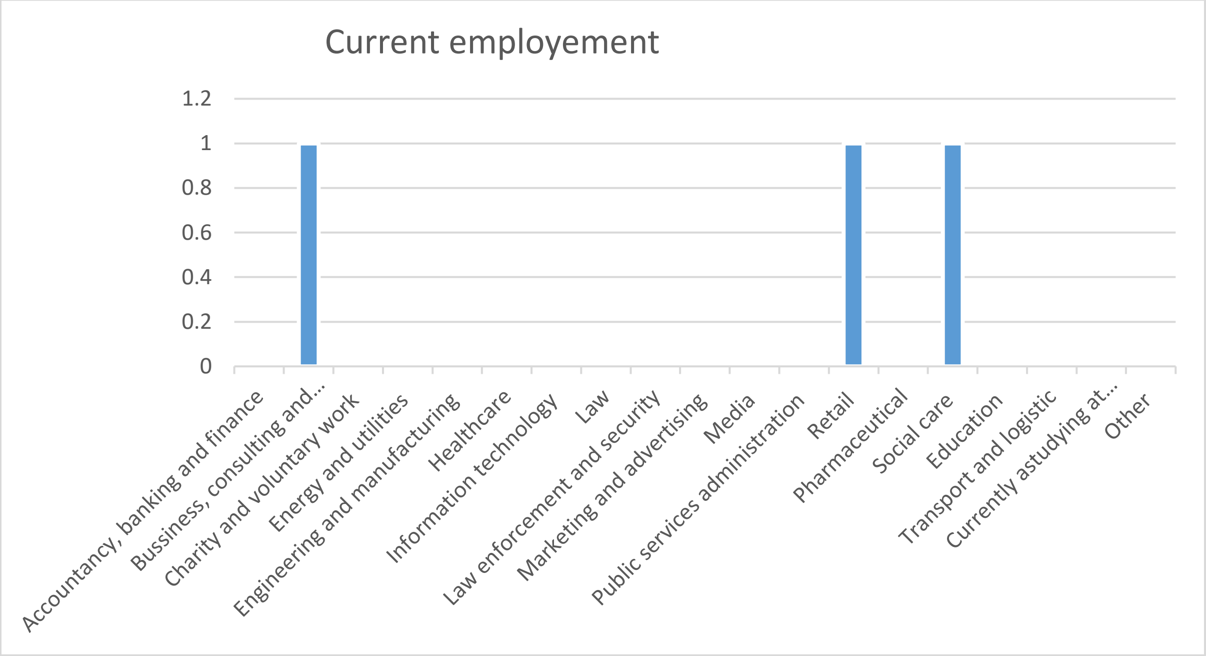


Figure E.201: Current employment (56-65-UK)

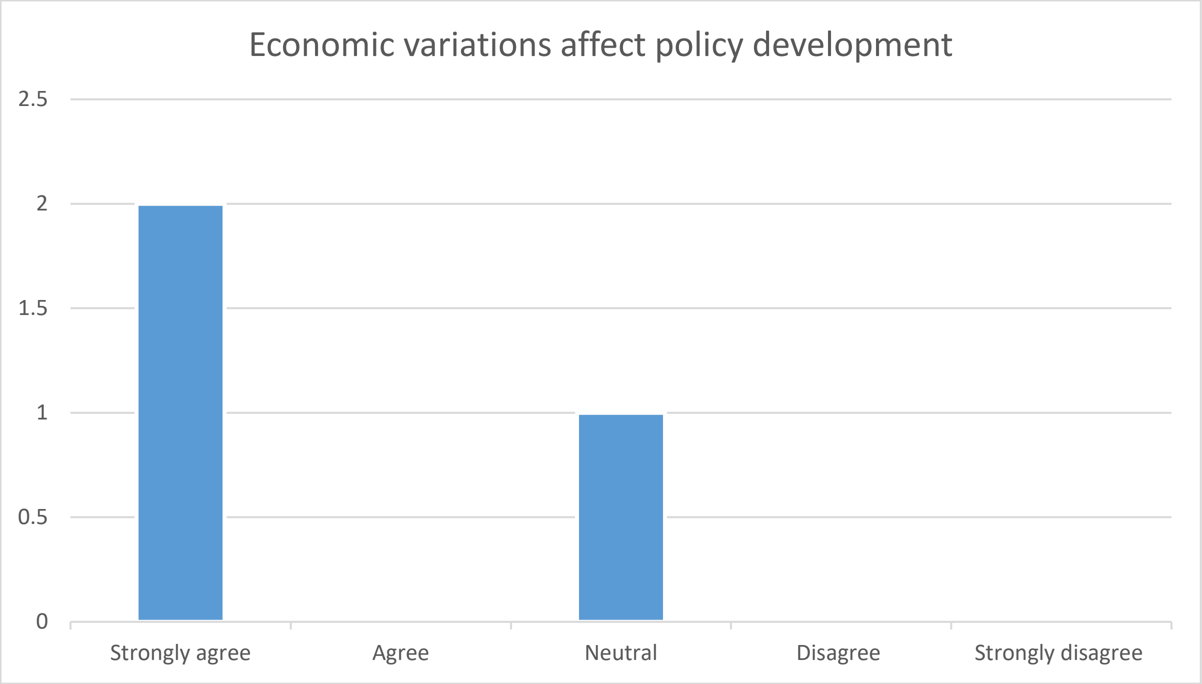


Figure E.202: Economic variations affect policy development (56-65-UK)

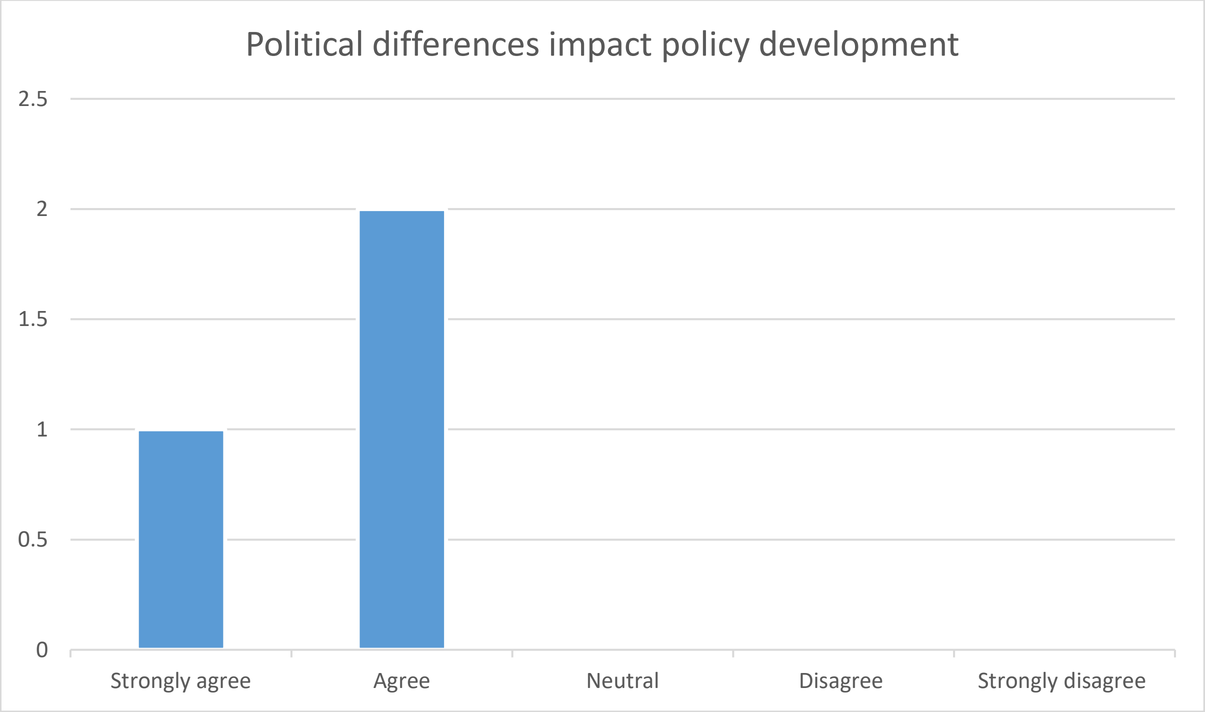


Figure E.203: Political differences impact policy development (56-65-UK)

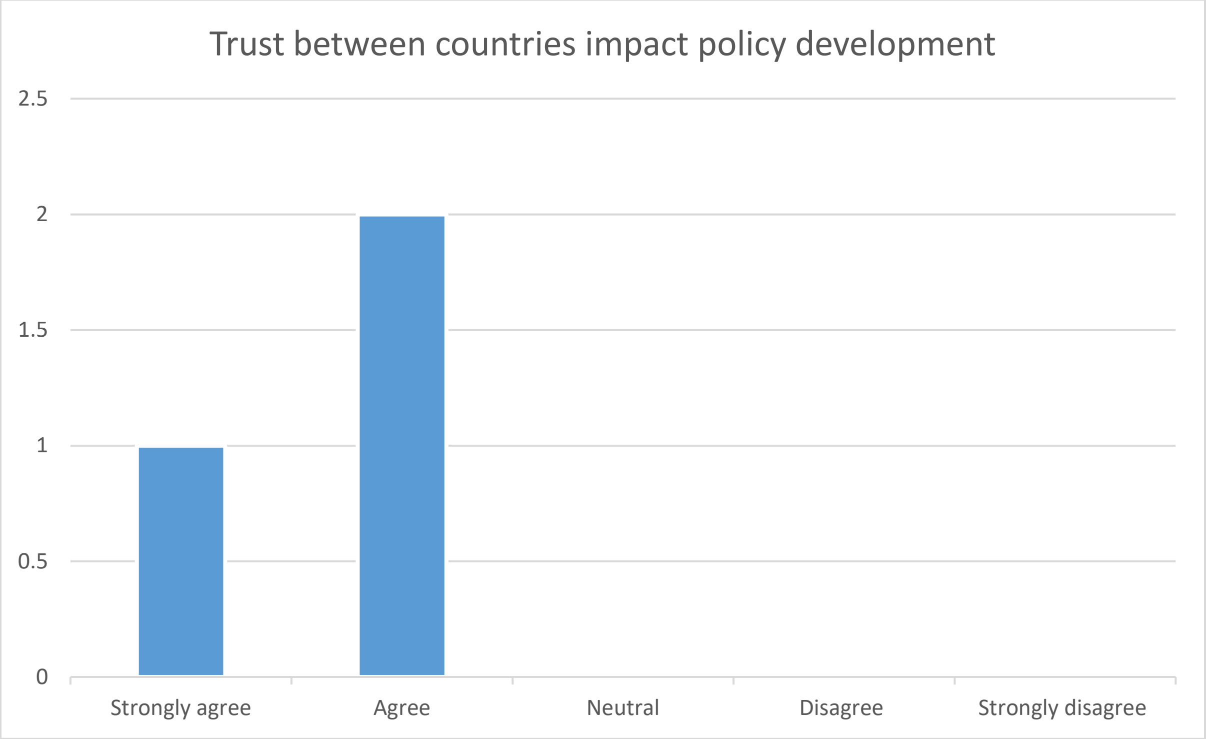


Figure E.204: Trust between countries impact policy development (56-65-UK)

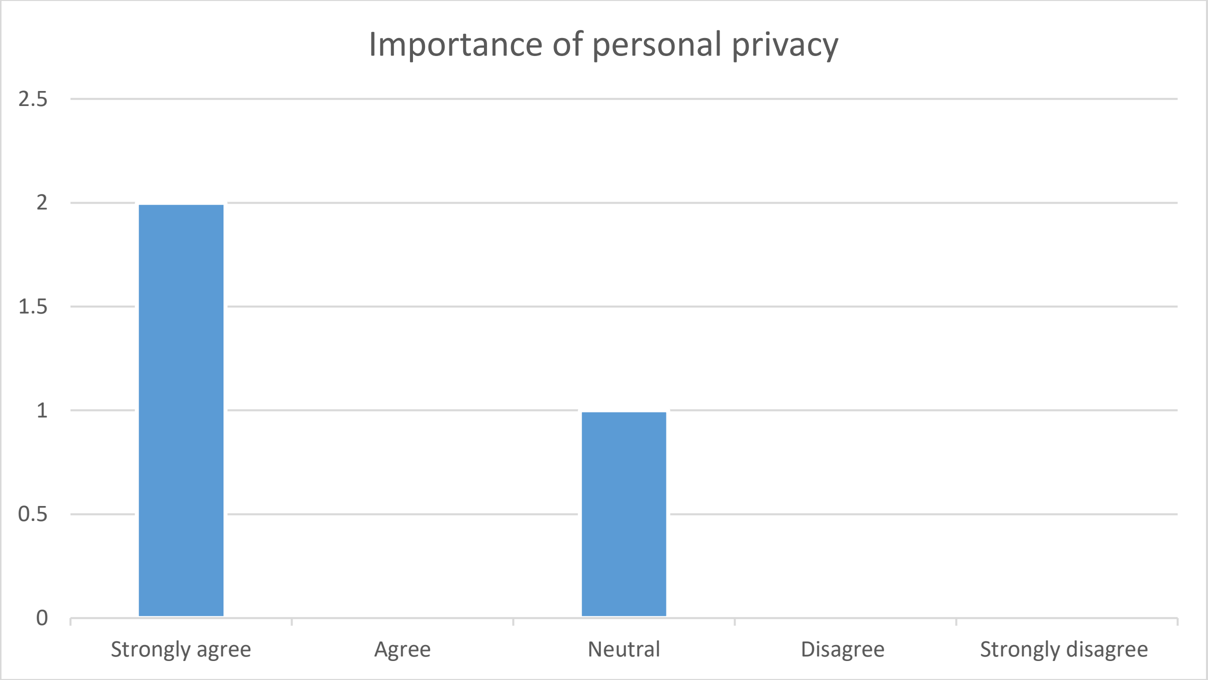


Figure E.205: Importance of personal privacy (56-65-UK)

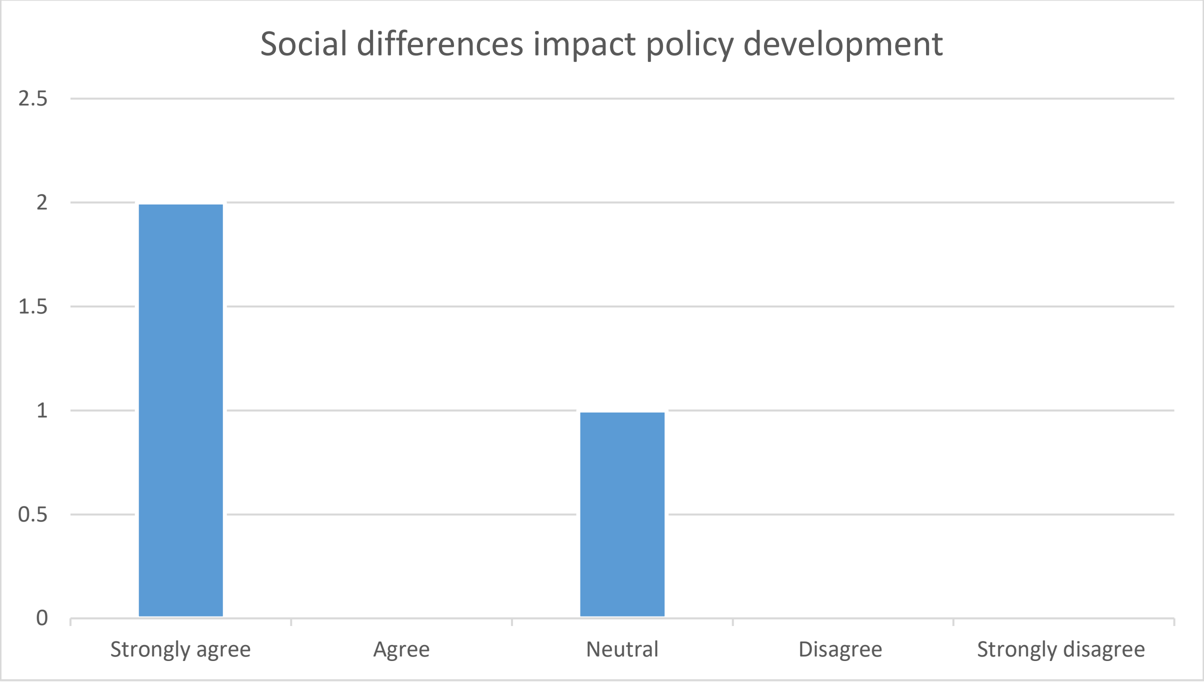


Figure E.206: Social differences impact policy development (56-65-UK)

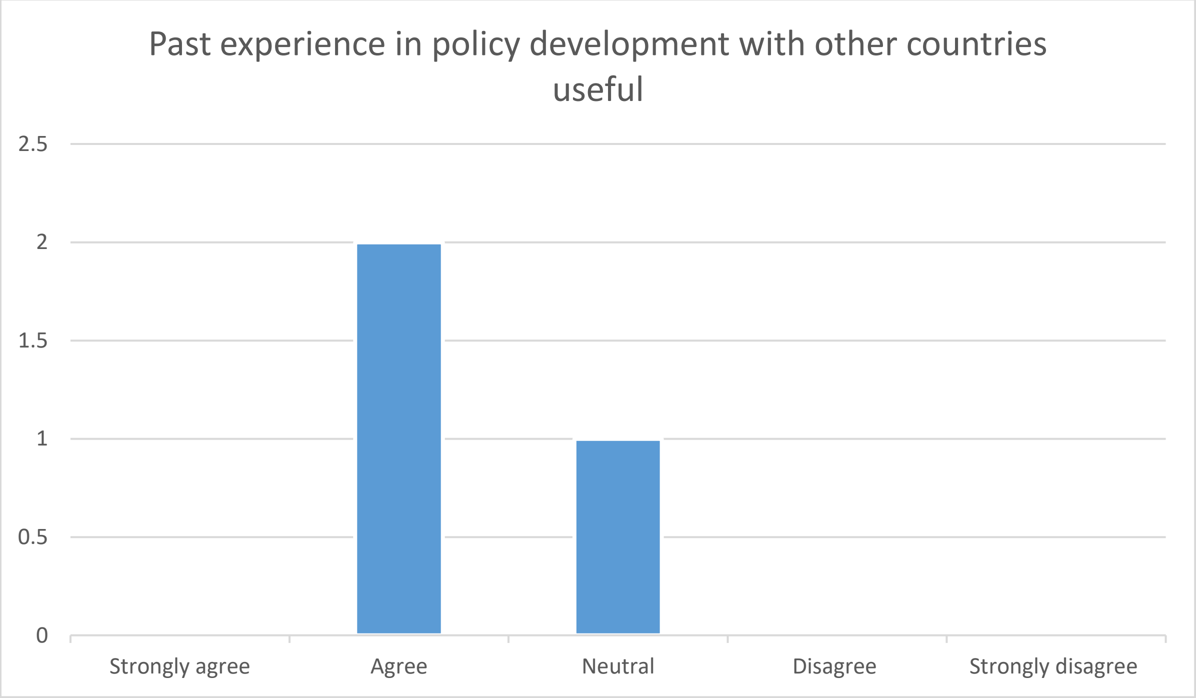


Figure E.207: Past experience in policy development with other countries useful (56-65-UK)

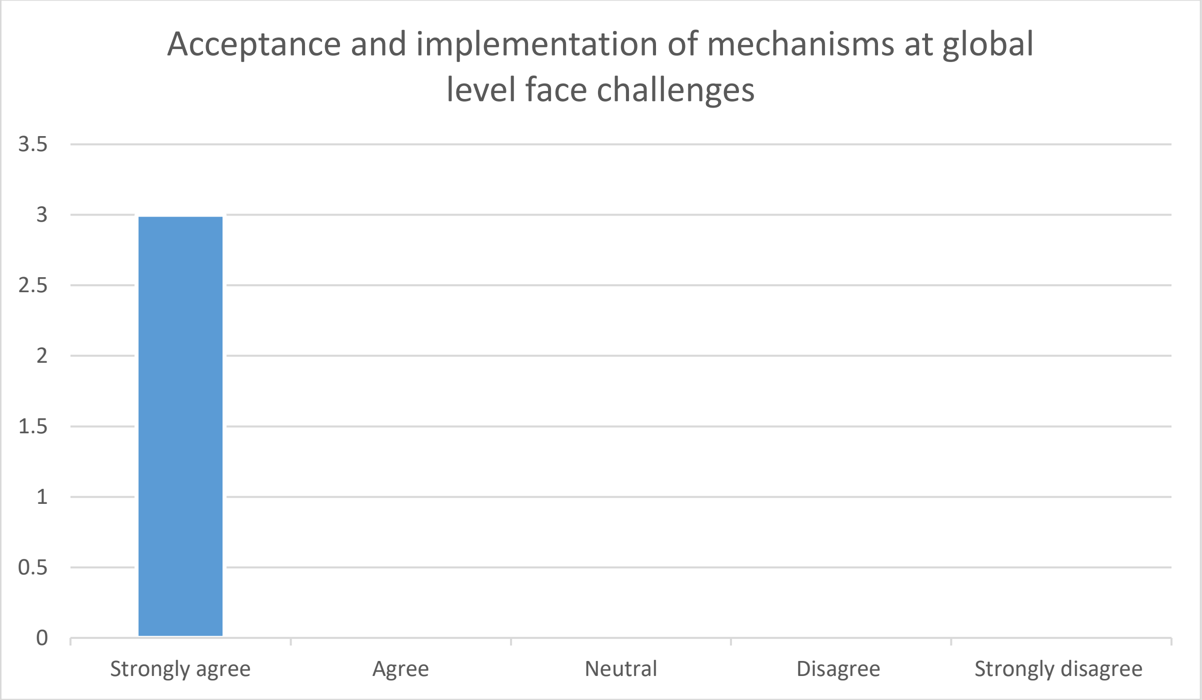


Figure E.208: Acceptance and implementation of mechanisms at global level face challenges (56-65-UK)

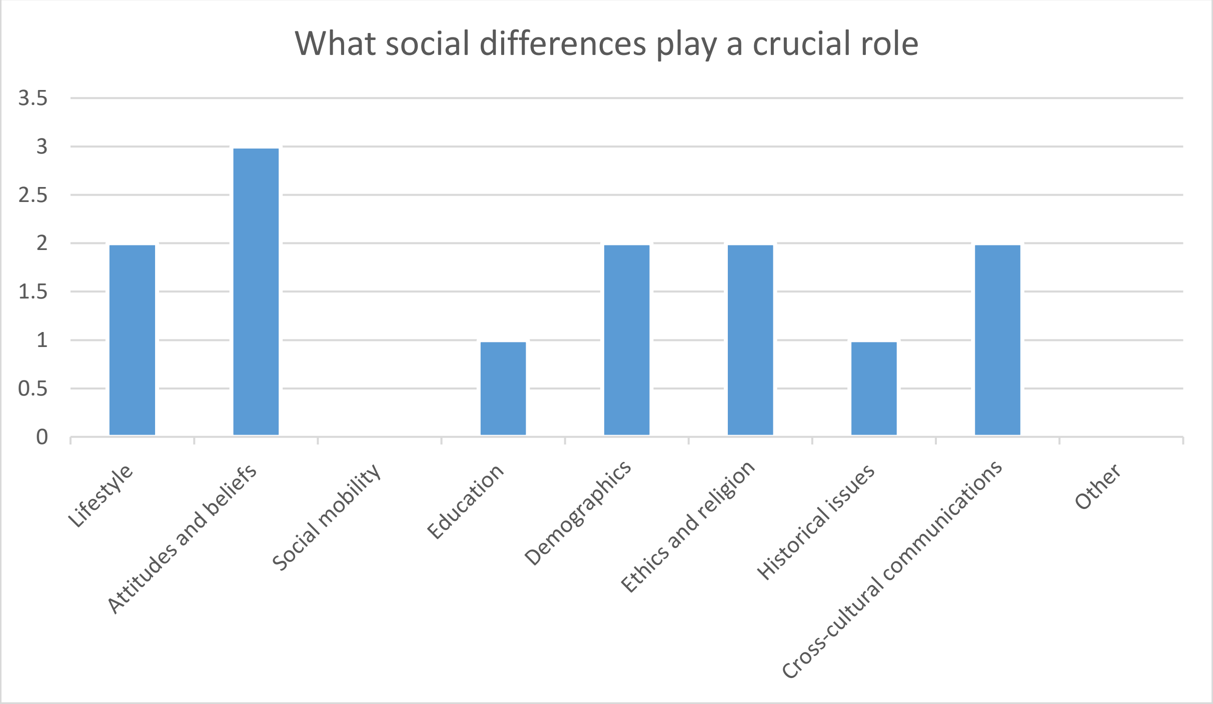


Figure E.209: What social differences play a crucial role (56-65-UK)

The participants in this group, in contrast to the other aged groups, the majority recognise the importance of social factors such as lifestyle, demography, ethnic and religious cross-cultural communication, and attitude and beliefs, without recognising the importance of education (See figure E.209).

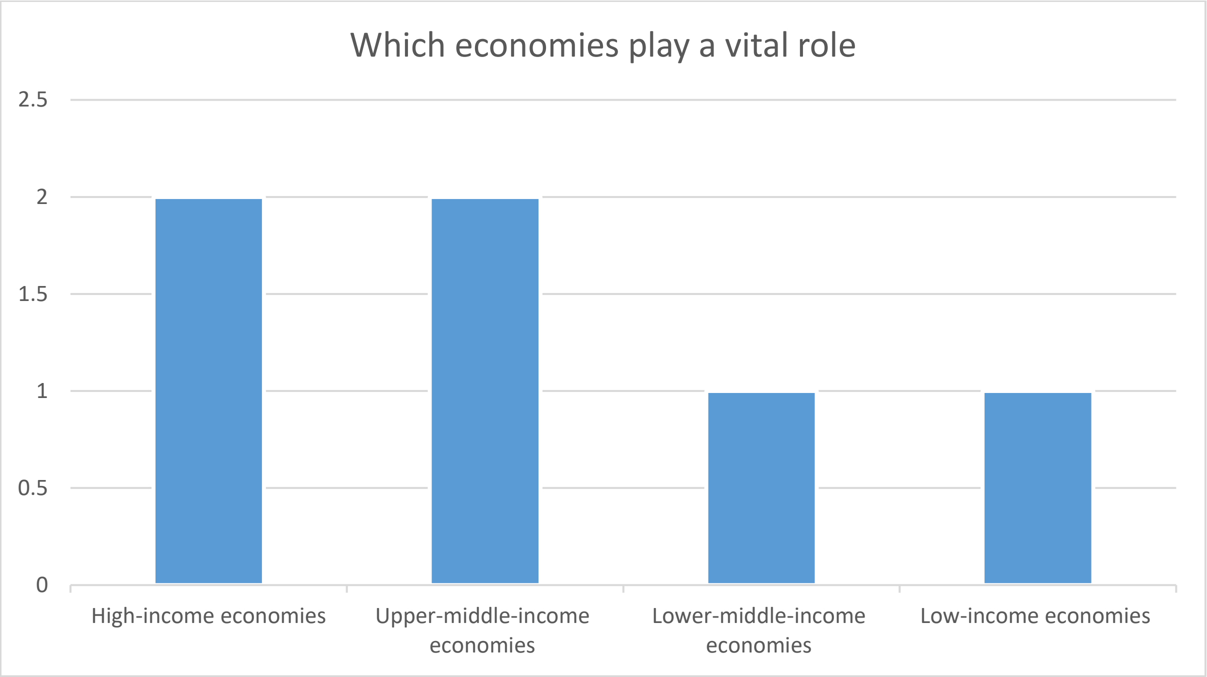


Figure E.210: Which economies play a vital role (56-65-UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role. There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

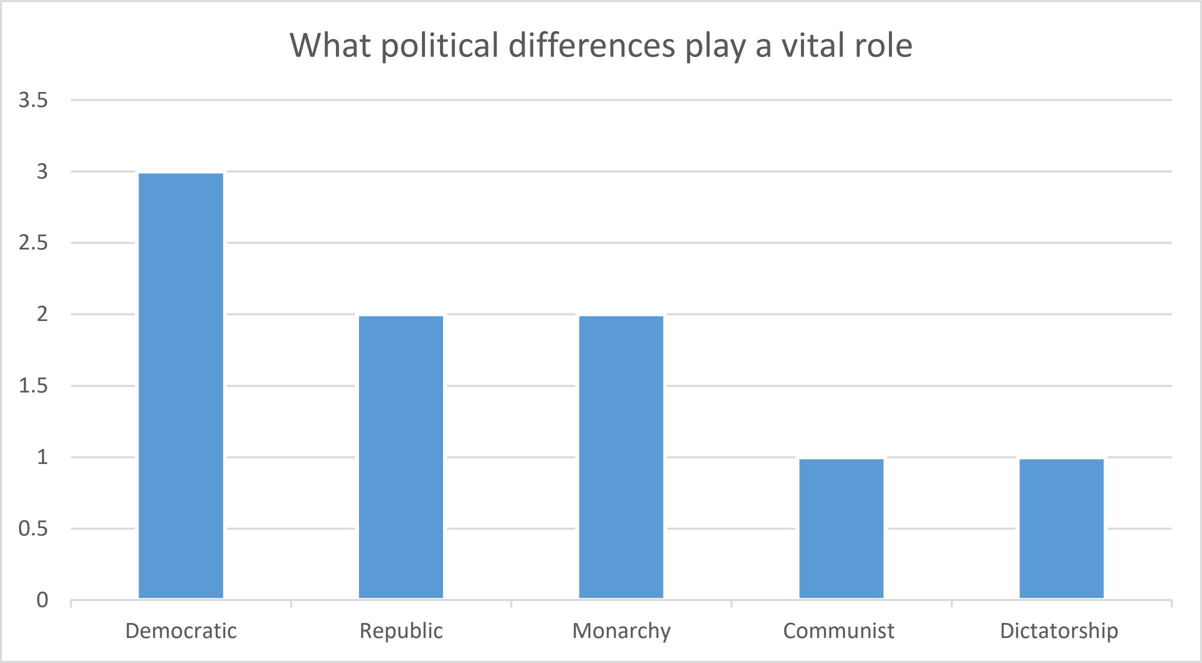


Figure E.211: What political differences play a vital role (56-65-UK)

In contrast, those in this age group choose democratic, republic and monarchist system (See figure E.211). In a democratic system, the public influence contributes to the policy development process and ensures consensus based collective responsibility for their actions. This provides an effective way to develop trust between the public and the organisations and strengthen coherence and transparency in the policy development process. In a Republican system, the people and their elected representatives hold power, and in accordance with the constitution the public has the right to seek assurances from those collect, share, and store personal information to protect personal information without compromising personal privacy for any reason. In a Monarchist system, an individual, through his or her heredity status assumes absolute power and functions as the head of state, and freedom of expression is prohibited or limited. Having compared the governance characteristics of the three systems and given the bureaucratic procedures involved in the other two options, the respondents might have opted for the Monarchist system to speed up the process of developing a data protection mechanism.

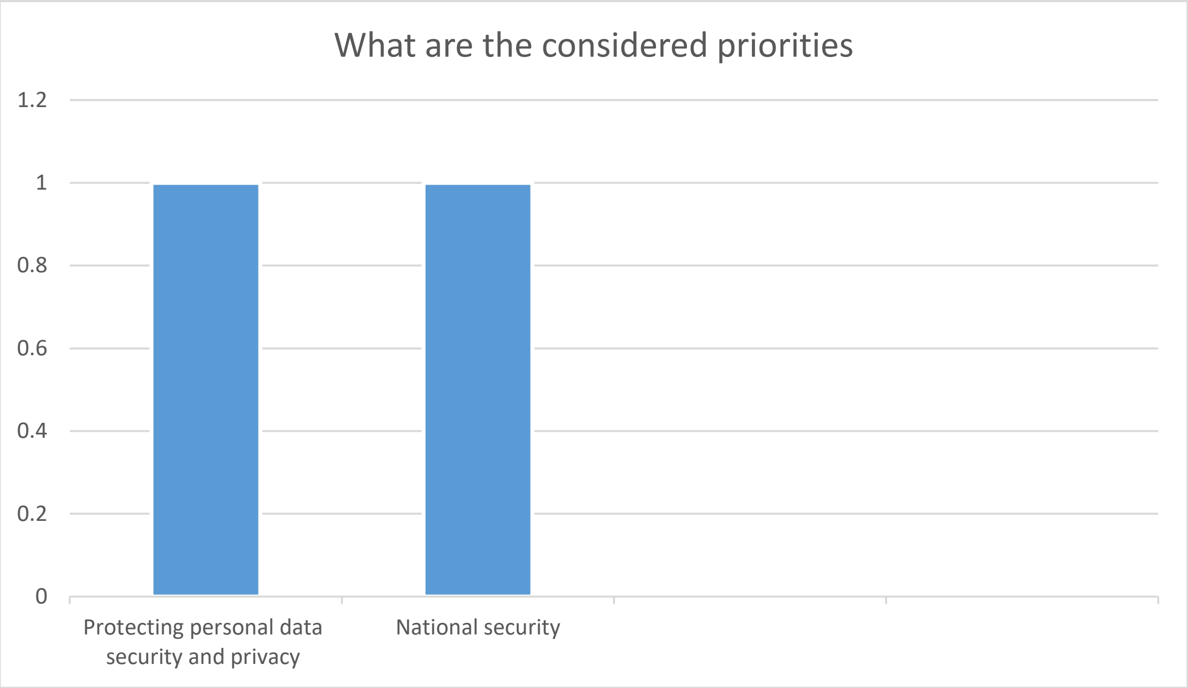


Figure E.212: What are the considered priorities (56-65-UK)

The majority not considered either the importance of protection of personal data security and privacy or protection of national security, in accepting and implementing a global data privacy and security policies (See figure E.212).

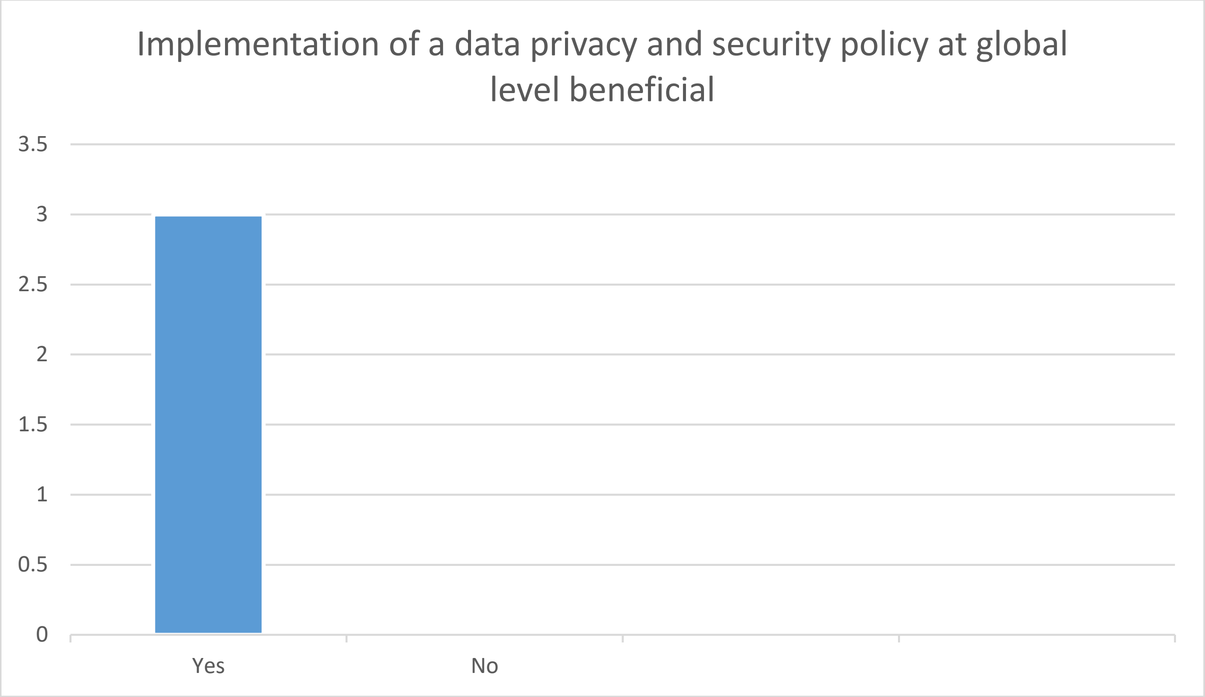


Figure E.213: Implementation of a data privacy and security policy at global level beneficial (56-65-UK)

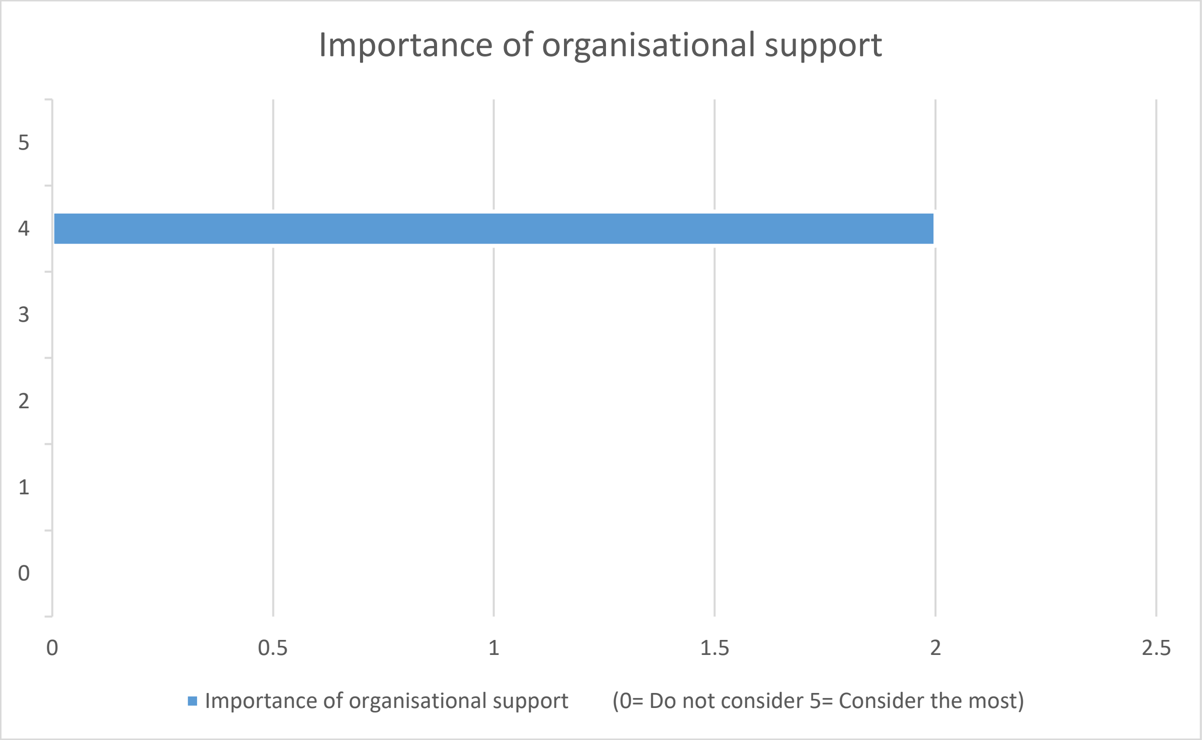


Figure E.214: Importance of organisational support (56-65-UK)

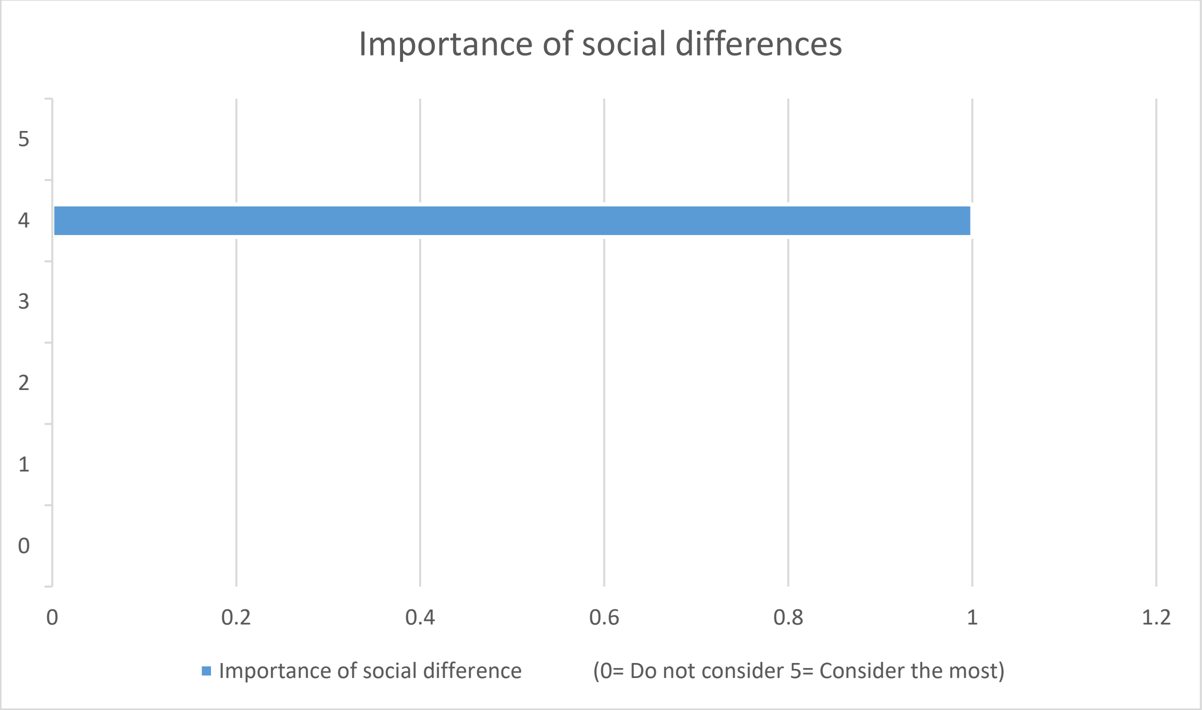


Figure E.215: Importance of social differences (56-65-UK)

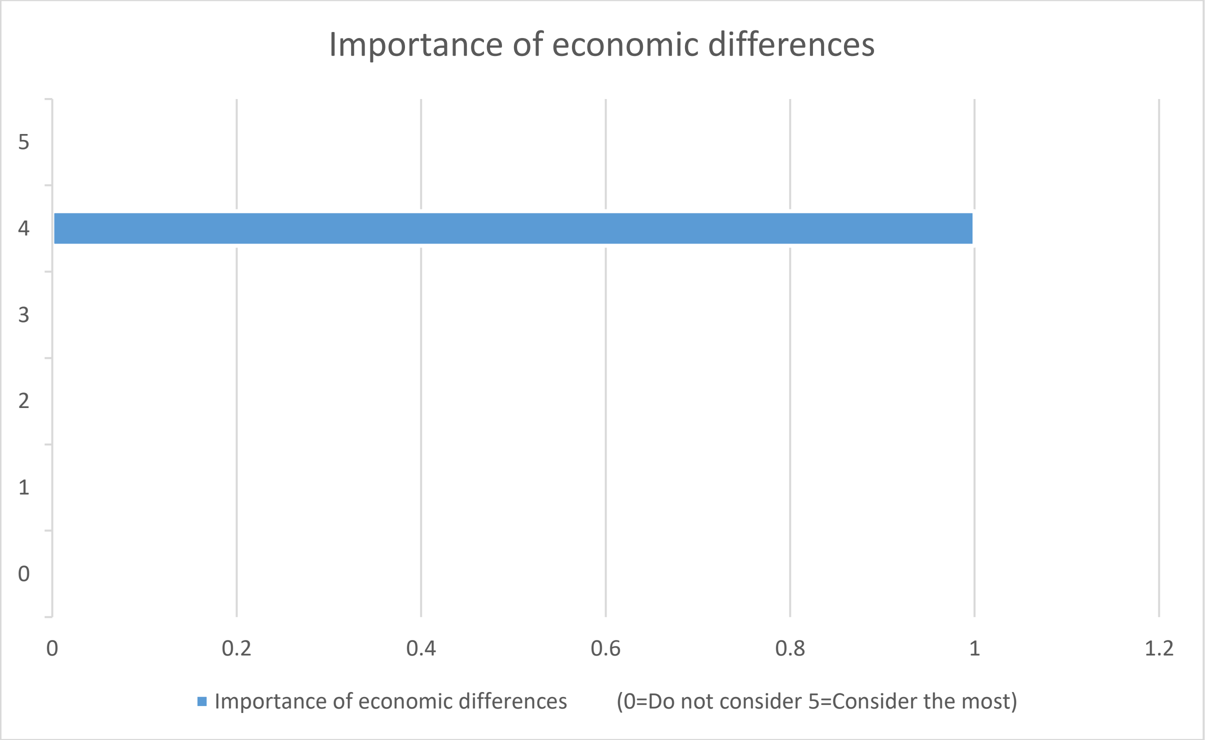


Figure E.216: Importance of economic differences (56-65-UK)

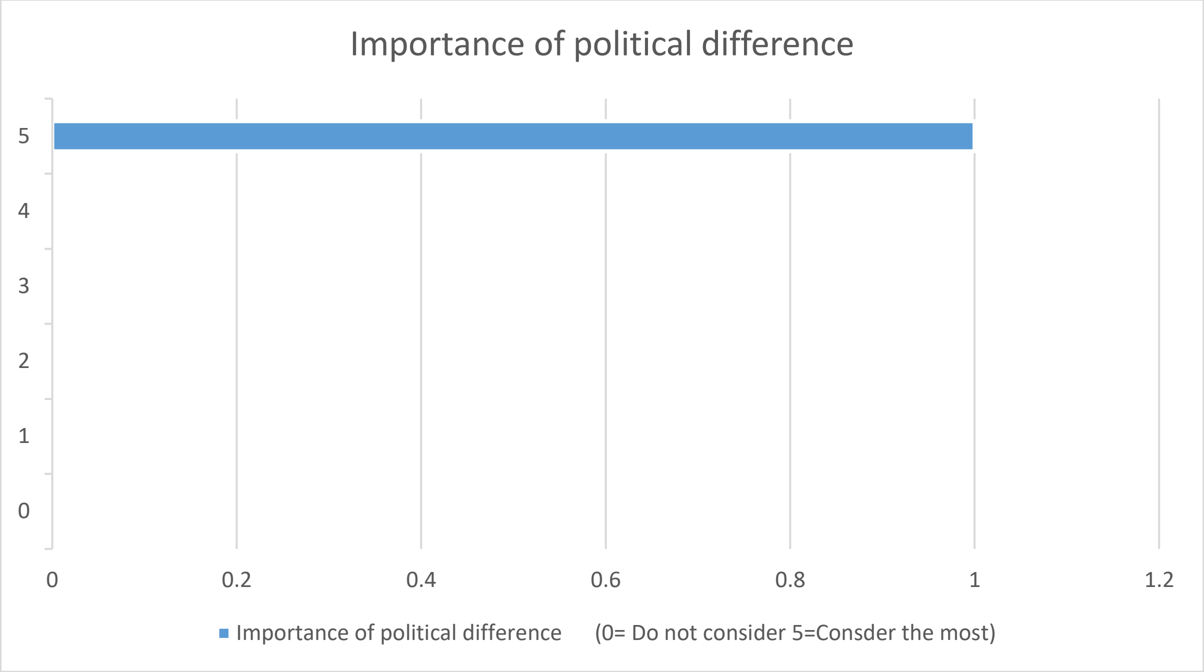


Figure E.217: Importance of political difference (56-65-UK)

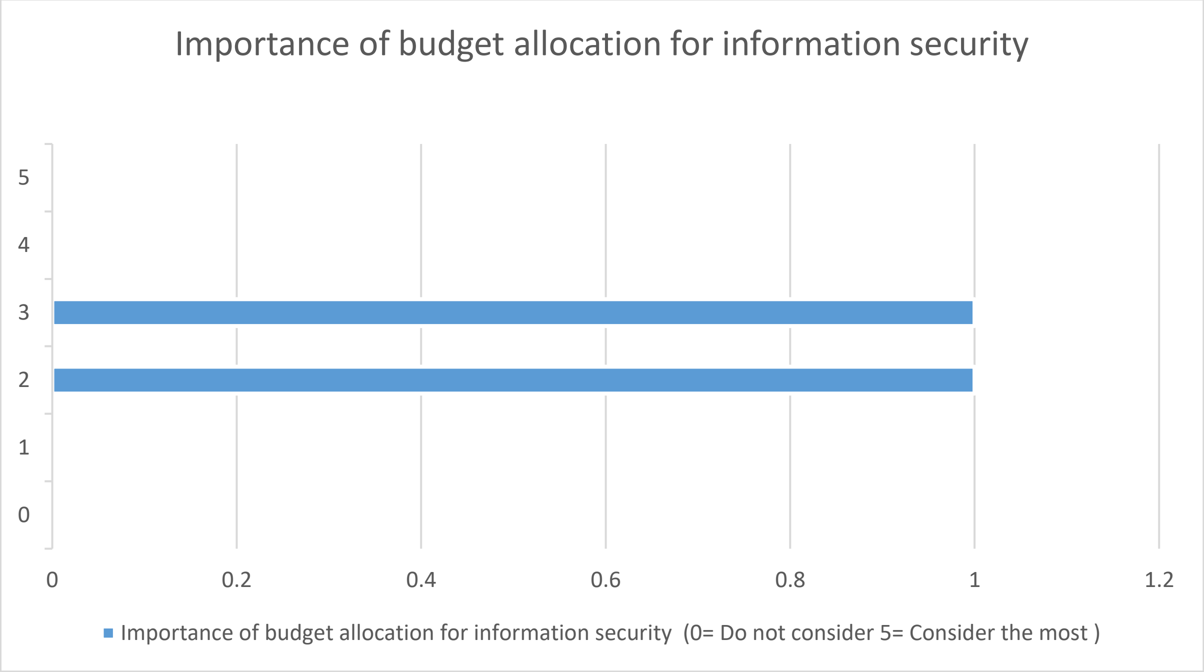


Figure E.218: Importance of budget allocation for information security (56-65-UK)

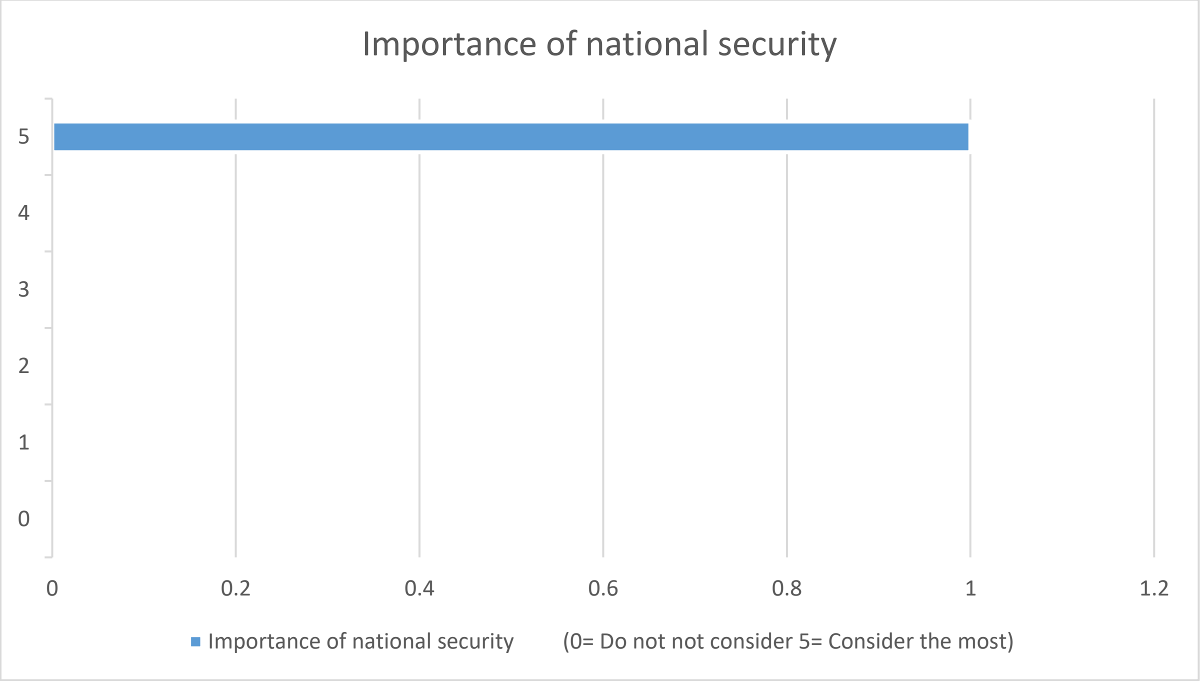


Figure E.219: Importance of national security (56-65-UK)

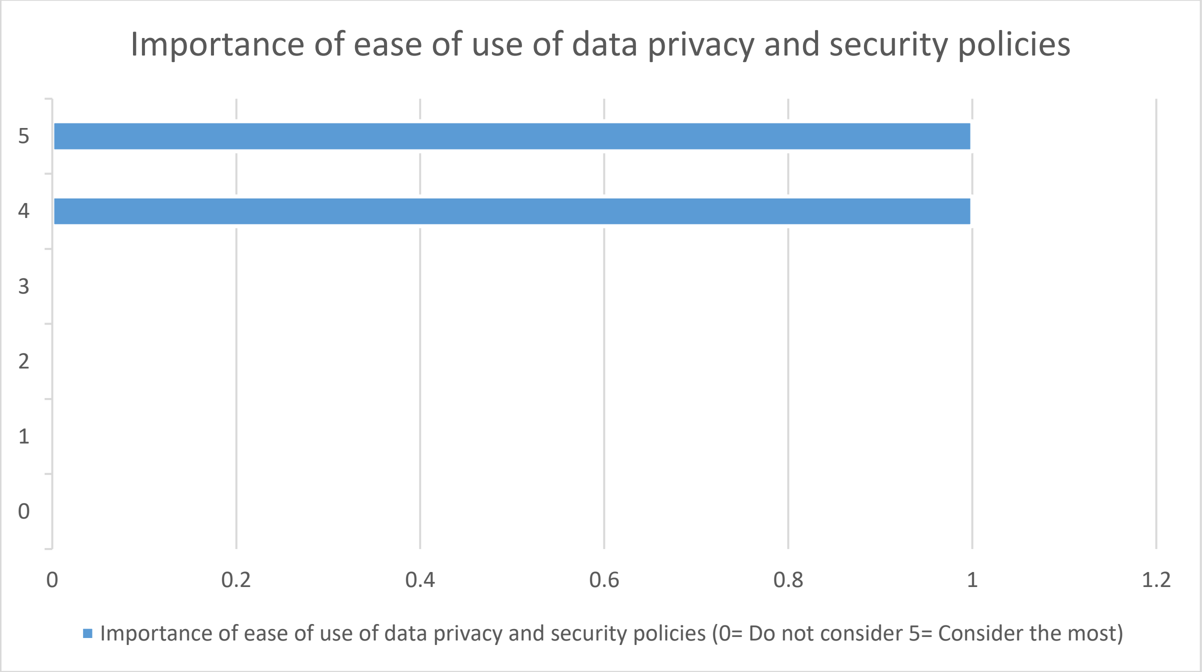


Figure E.220: Importance of ease of use of data privacy and security policies (56-65-UK)

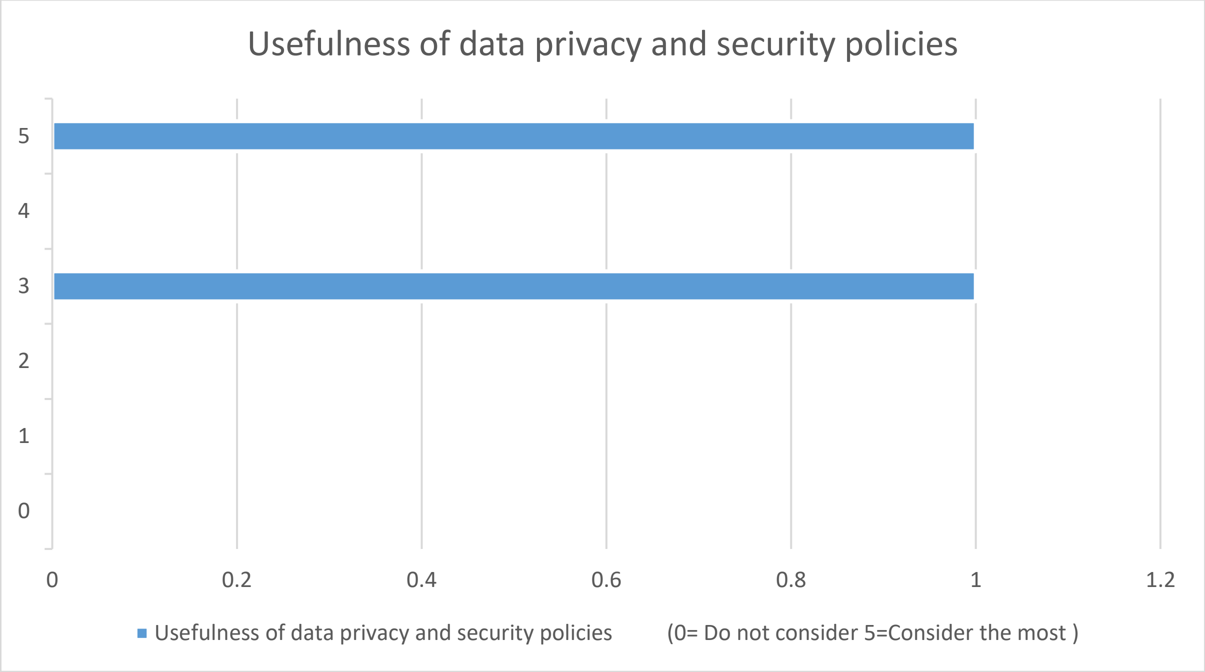


Figure E.221: Usefulness of data privacy and security policies (56-65-UK)

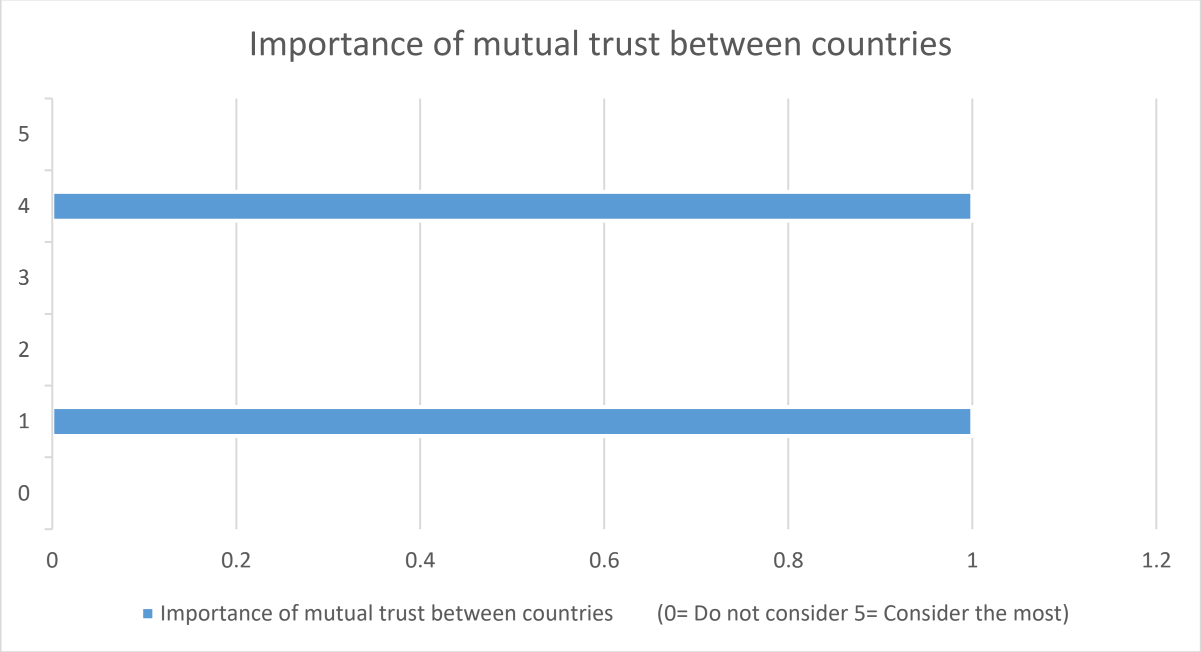


Figure E.222: Importance of mutual trust between countries (56-65-UK)

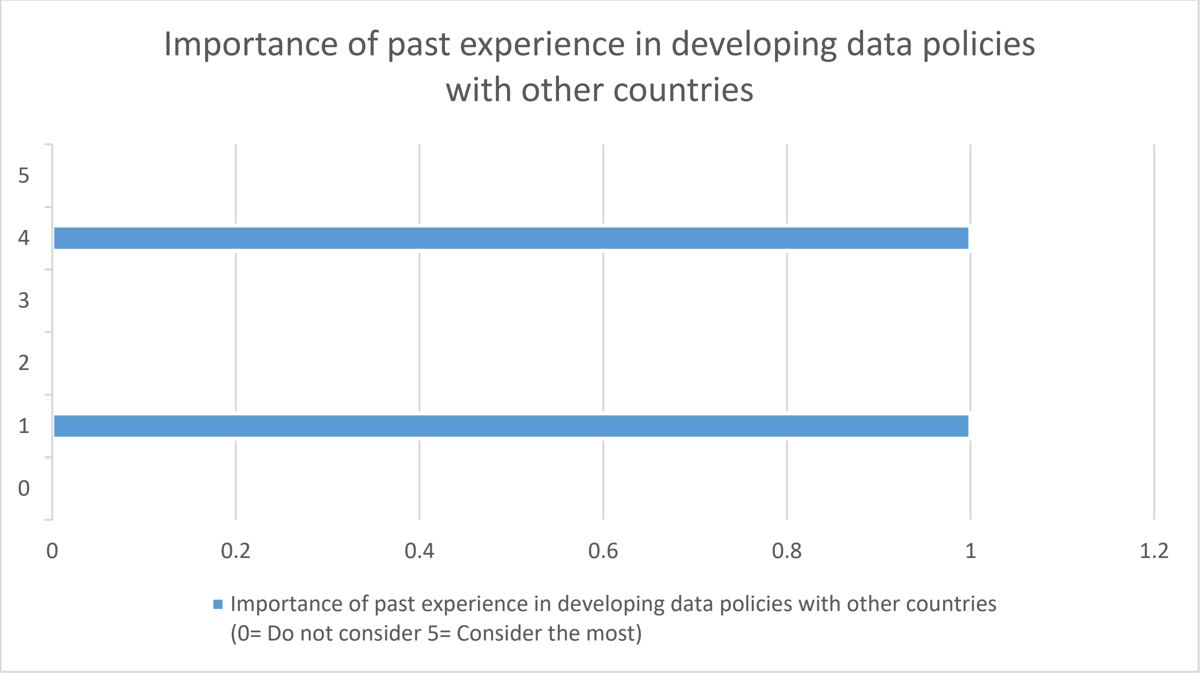


Figure E.223: Importance of past experience in developing data policies with other counties (56-65-UK)

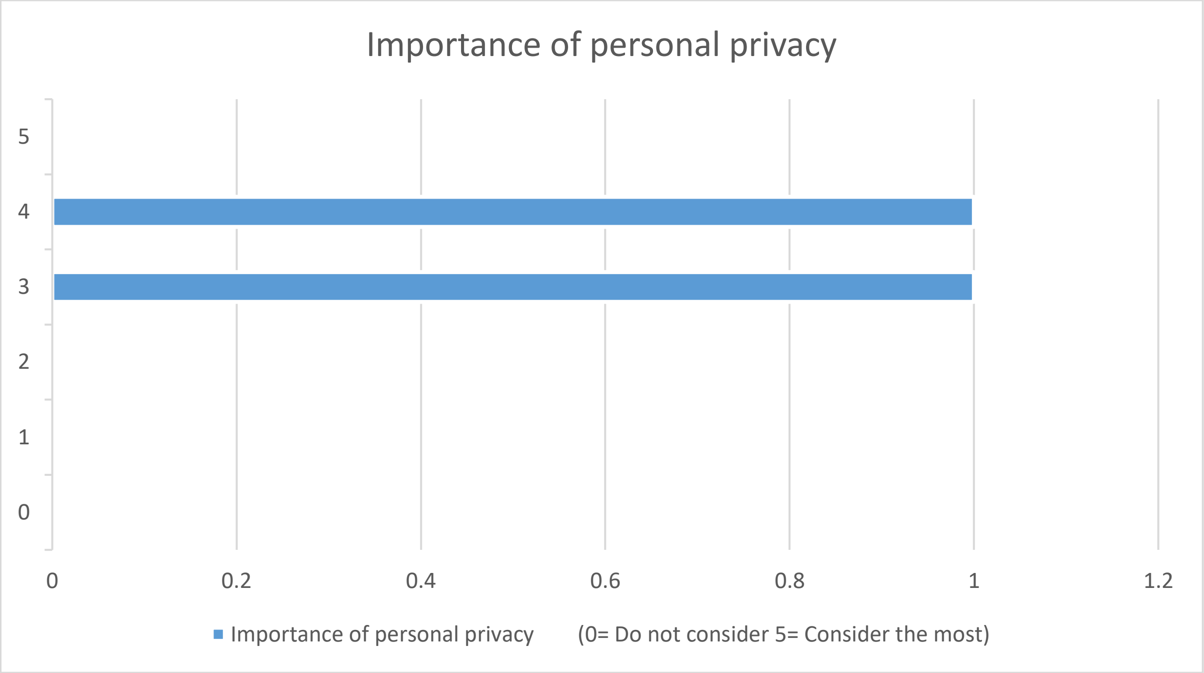


Figure E.224: Importance of personal privacy (56-65-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 100 percent of the respondents have endorsed (See figure E.213). The other notable factors that have come out of the survey are organisational support, personal privacy, ease of use of data privacy and security policies and usefulness of data privacy and security policies (See figure E.202-212) (See figure E.214-224).

United Kingdom 65+

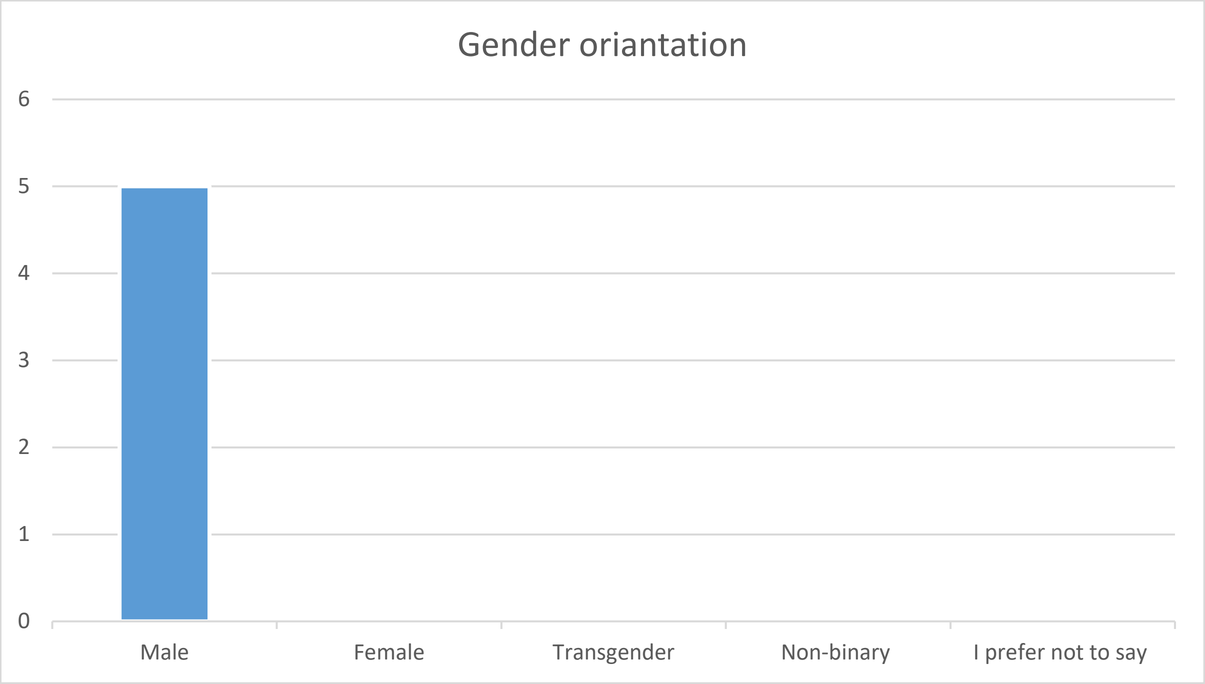


Figure E.225 Gender orientation (65+ UK)

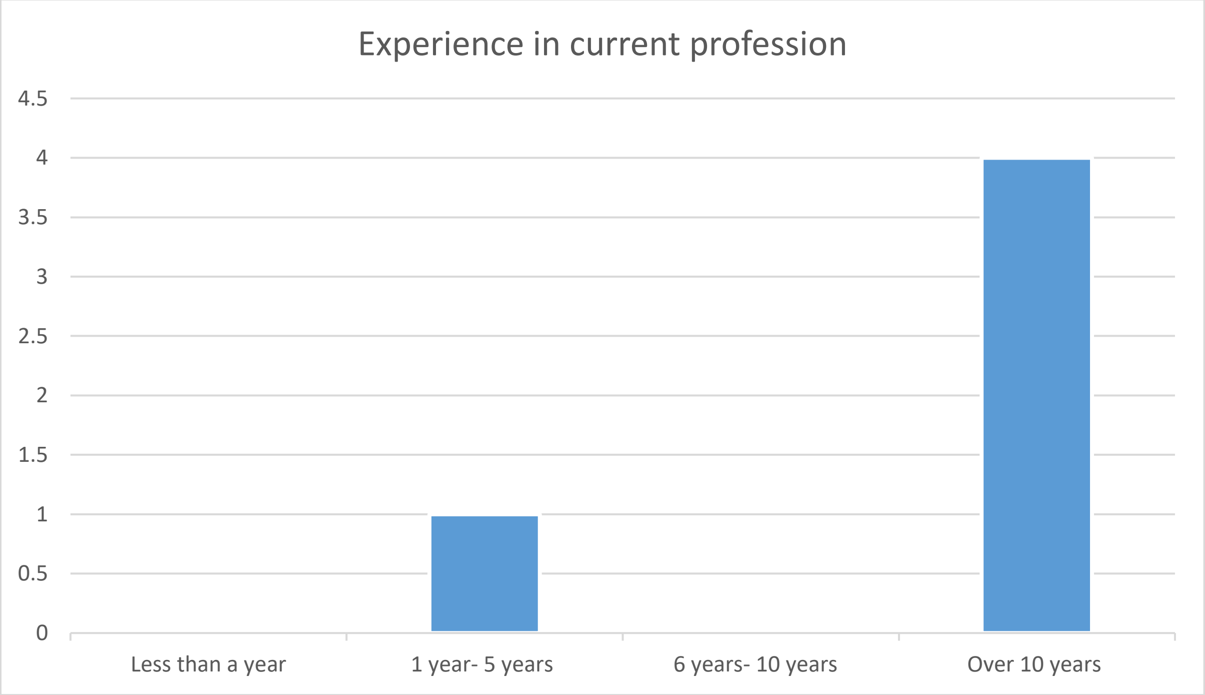


Figure E.226: Experience in current profession (65+ UK)

This analysis is based on the responses received from United Kingdom participants aged over 65. There were 5 participants and all of them were males (See figure E.225). The participants employed in industry between 1 and over 10 years. (See figure E.226)

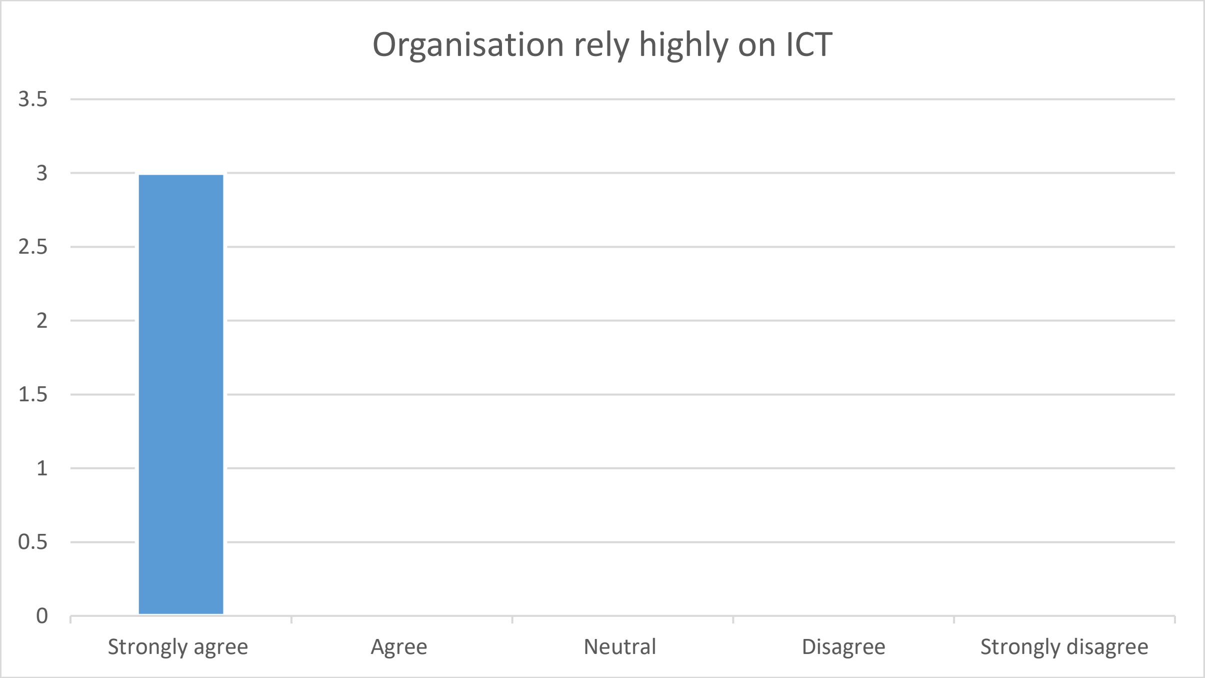


Figure E.227: Organisation rely highly on ICT (65+ UK)

Out of the 5 respondents, 3 have worked in a technology reliance working environment (See figure E.227).

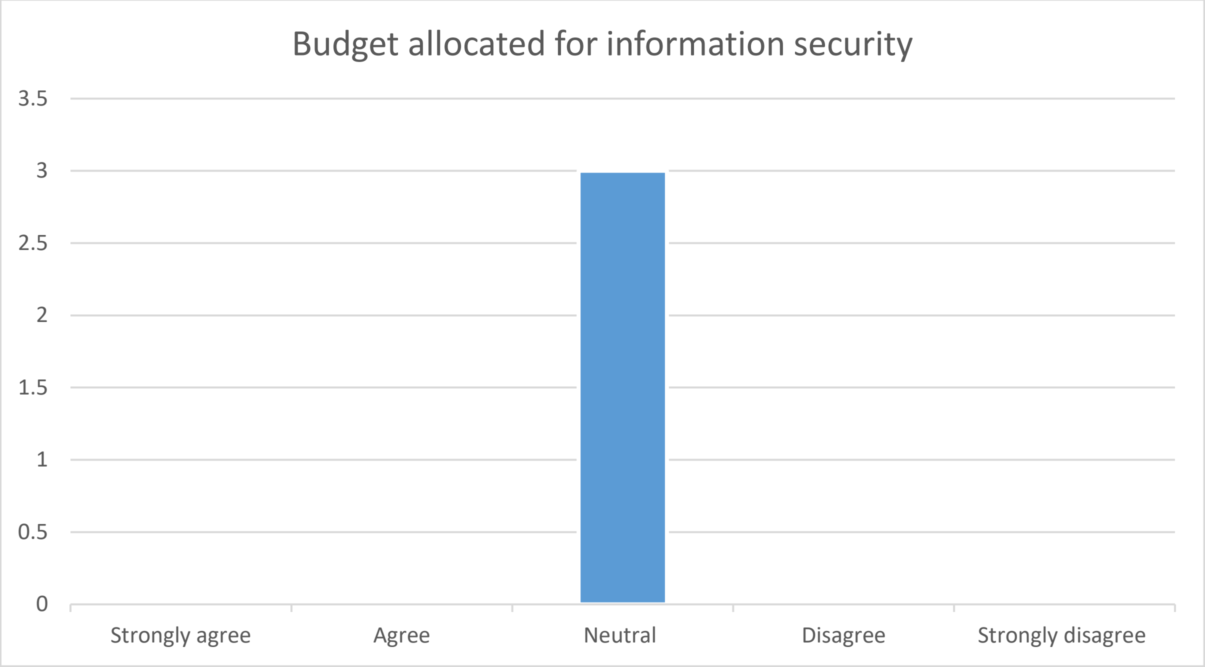


Figure E.228: Budget allocated for information security (65+ UK)

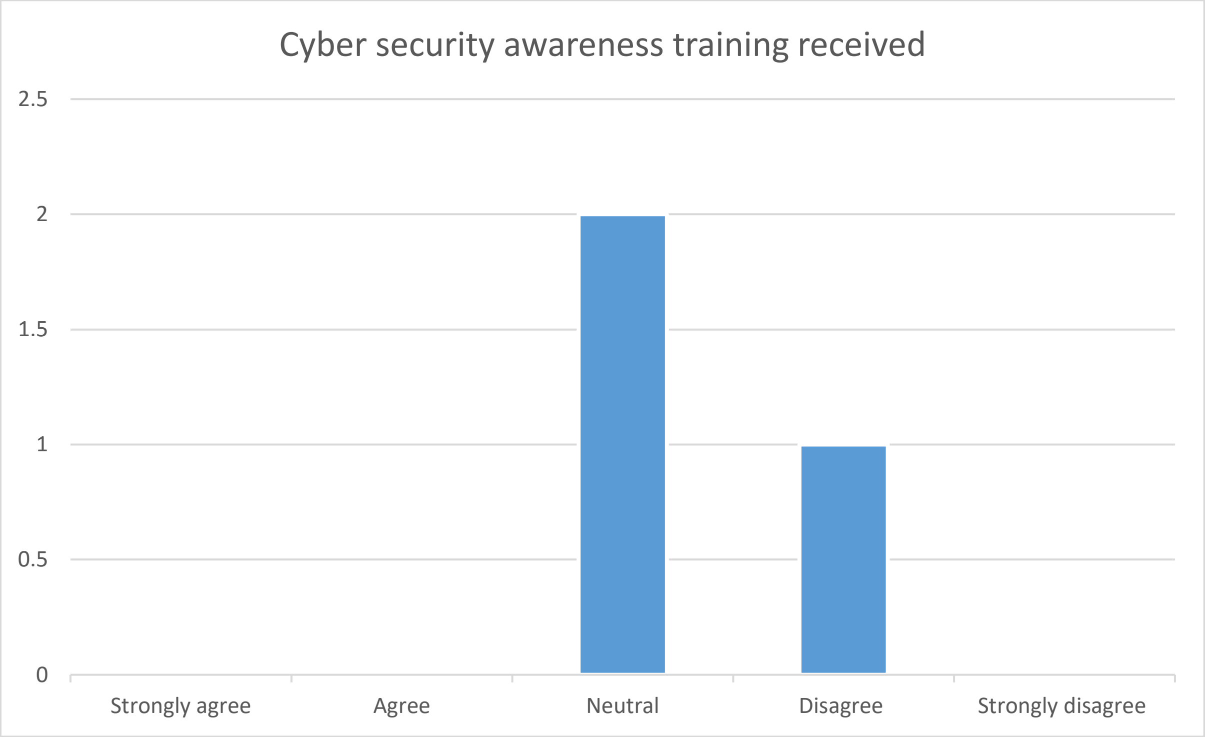


Figure E229: Cyber security awareness training received (65+ UK)

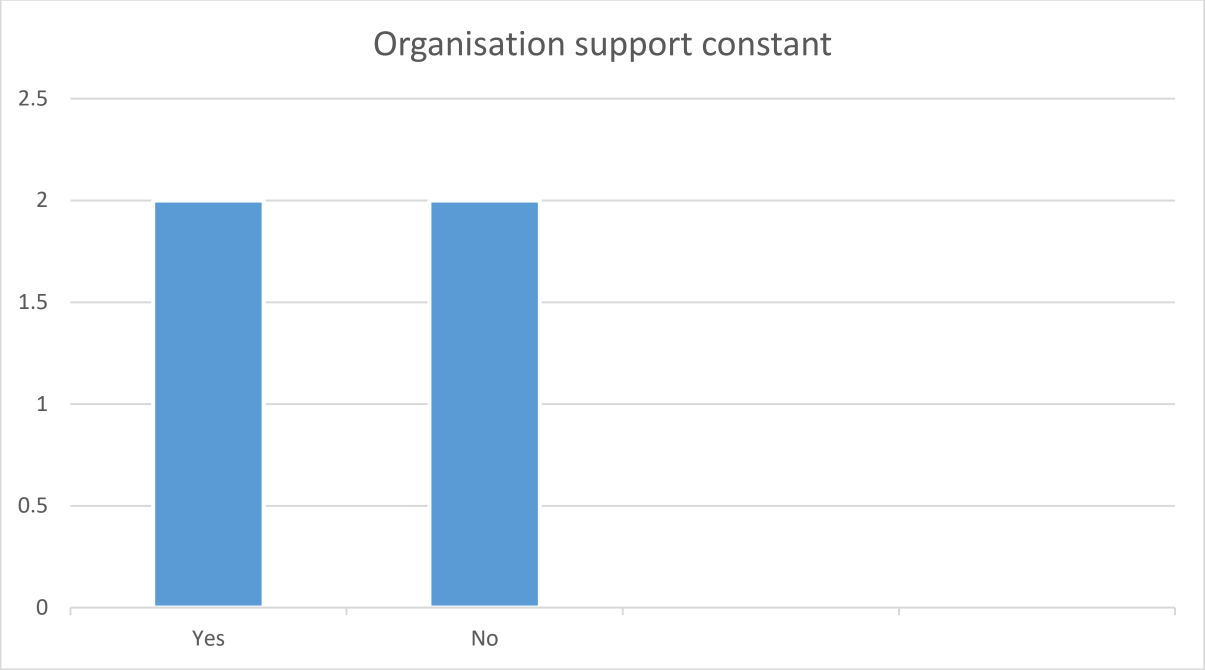


Figure E.230: Organisation support constant (65+ UK)

Comparing with the responses received from other participants in other age groups, interestingly 60 percent of the participants does not express an opinion on whether their organisation have an allocated budget for information security or not (See figure E.228). The level of regular security awareness training received is also inadequate, 1 had none, 2 neither agreed nor disagreed (See figure E.229). Also, 2 participants not received support from the organisation to protect personal information, but 2 did (See figure E.230). These participants have been in employment in the industry for more than 10 years and, given their age and the period in active employment, cyber threat factor would not have been a concerning issue. Therefore, it is reasonable to assume that, in the light of no budget allocation, seemingly no training offered to the staff and the organisation provided less support to protect personal information.

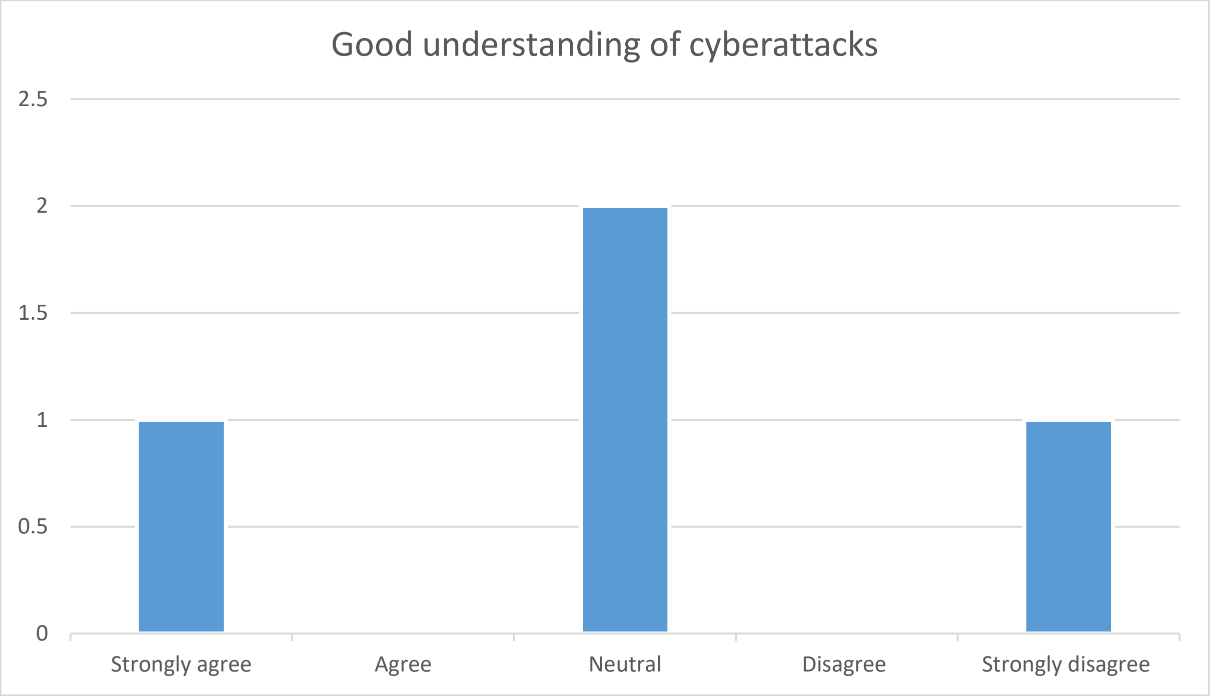


Figure E231: Good understanding of cyberattacks (65+UK)

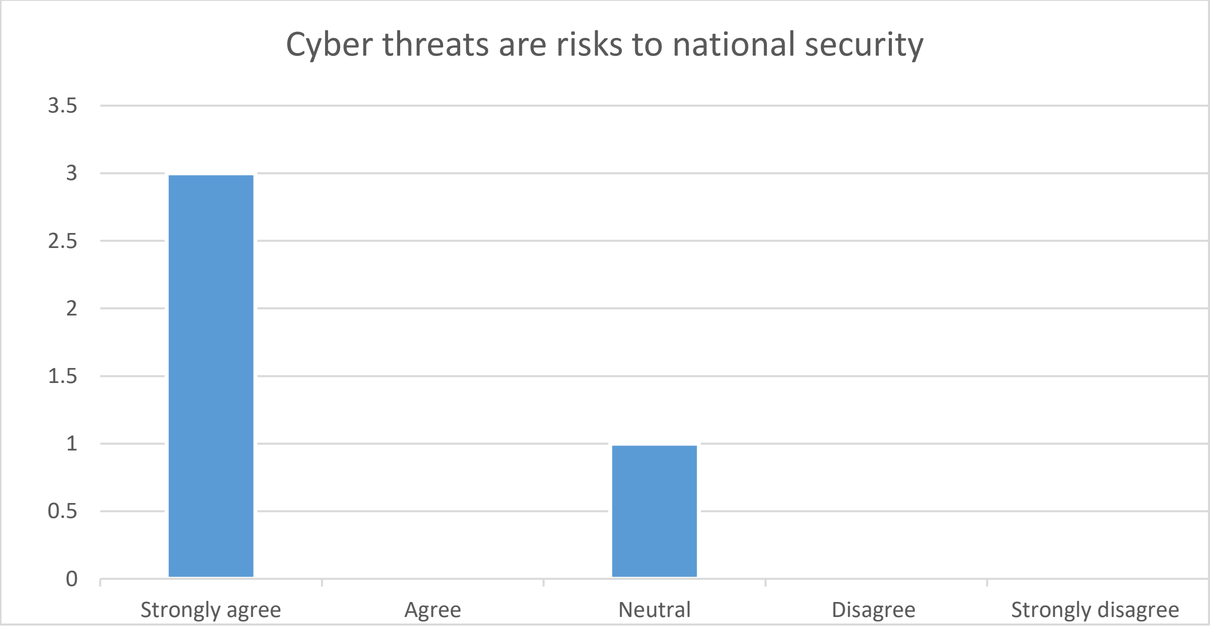


Figure E.232: Cyber threats are risks to national security (65+ UK)

The lack of security awareness training also has affected the participant's level of understanding of the impact of cyber-attacks on the public and the organisation to the extent that only 1 participant has a good level of understanding, 1 participant has no understanding, and 2 have no opinion either way (See figure E.231). However, 60 percent of the participants realise the potential threats to national security from cyber-attacks (See figure E.232). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

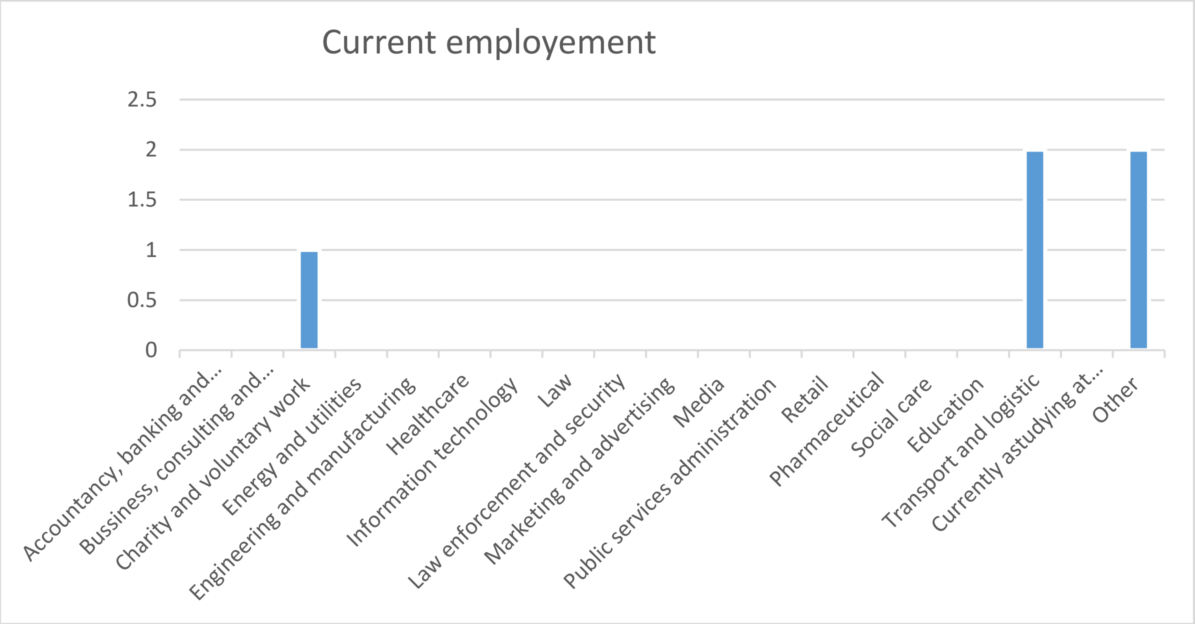


Figure E.233: Current employment (65+ UK)

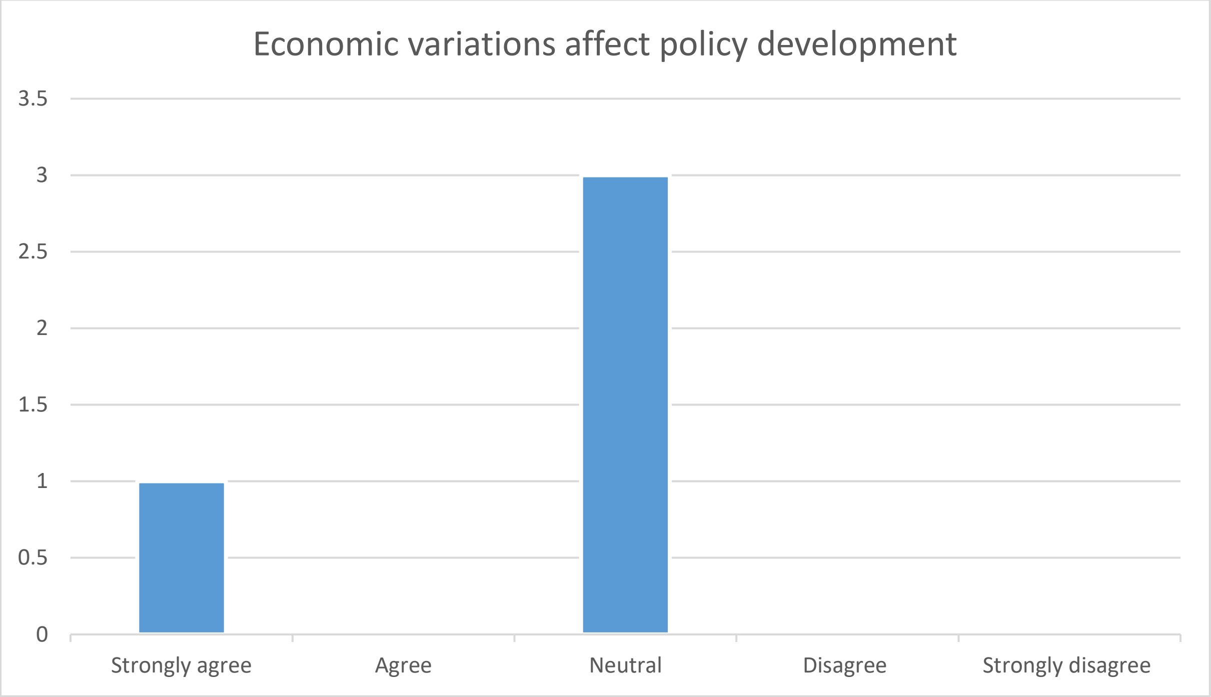


Figure E.234: Economic variations affect policy development (65+ UK)

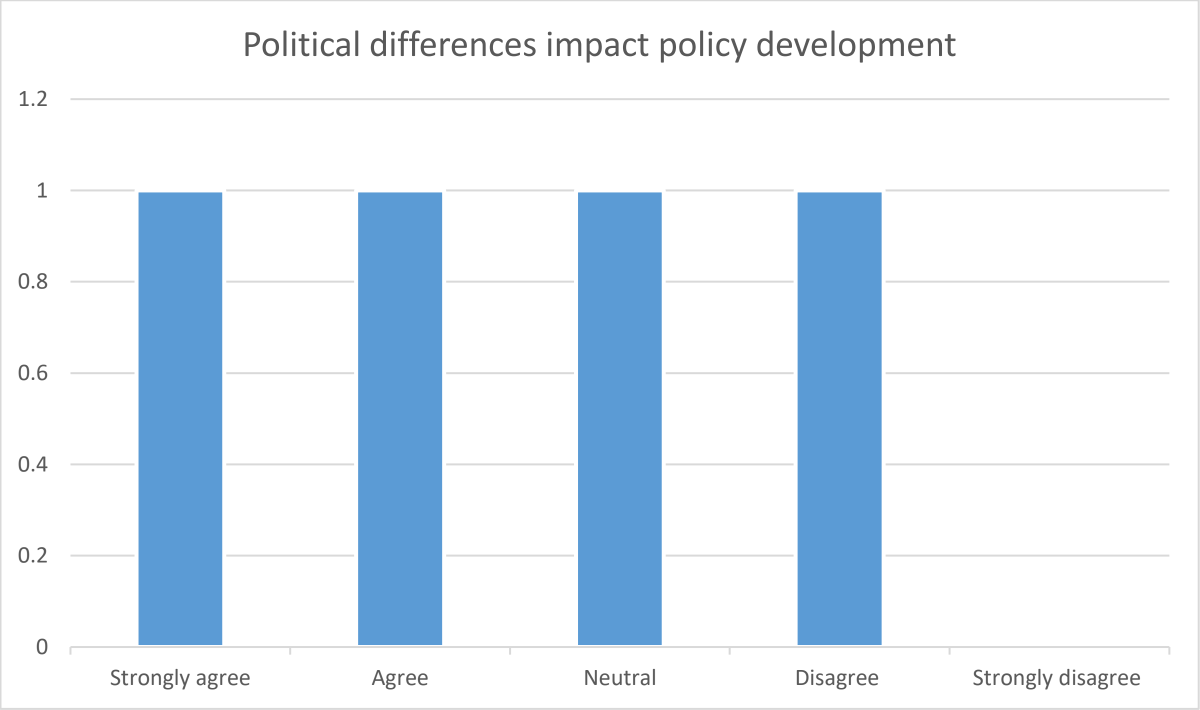


Figure E.235: Political differences impact policy development (65+ UK)

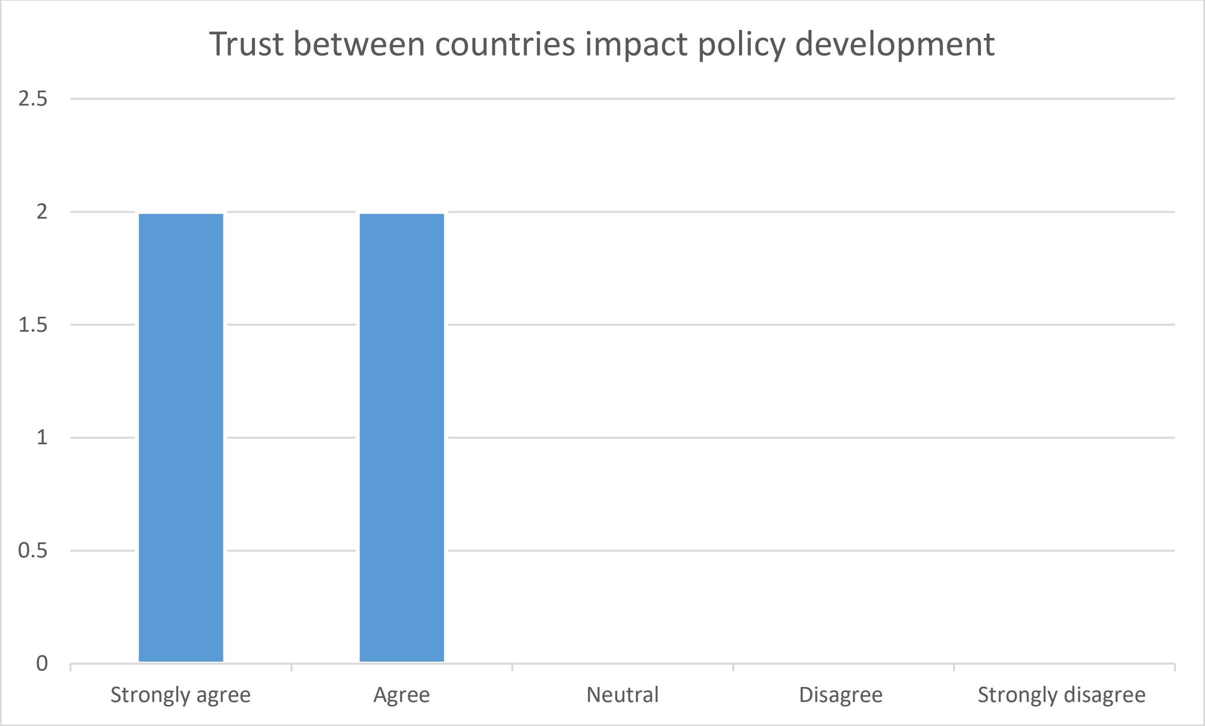


Figure E.236: Trust between countries impact policy development (65+ UK)

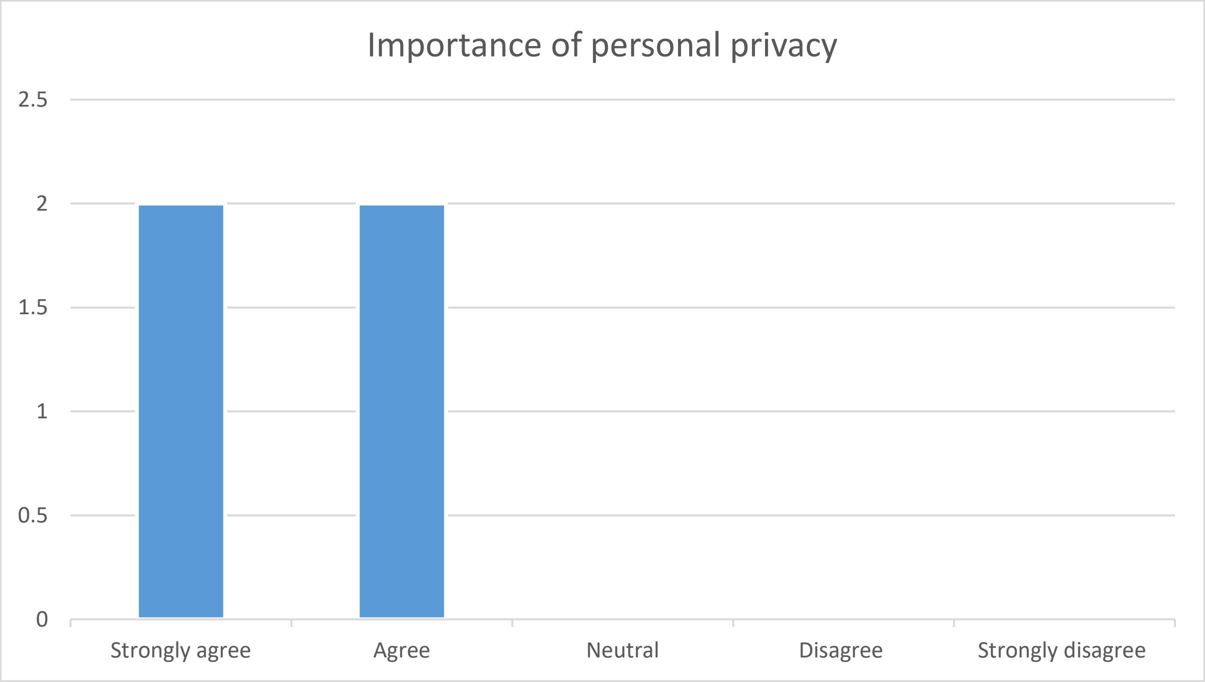


Figure E.237: Importance of personal privacy (65+ UK)

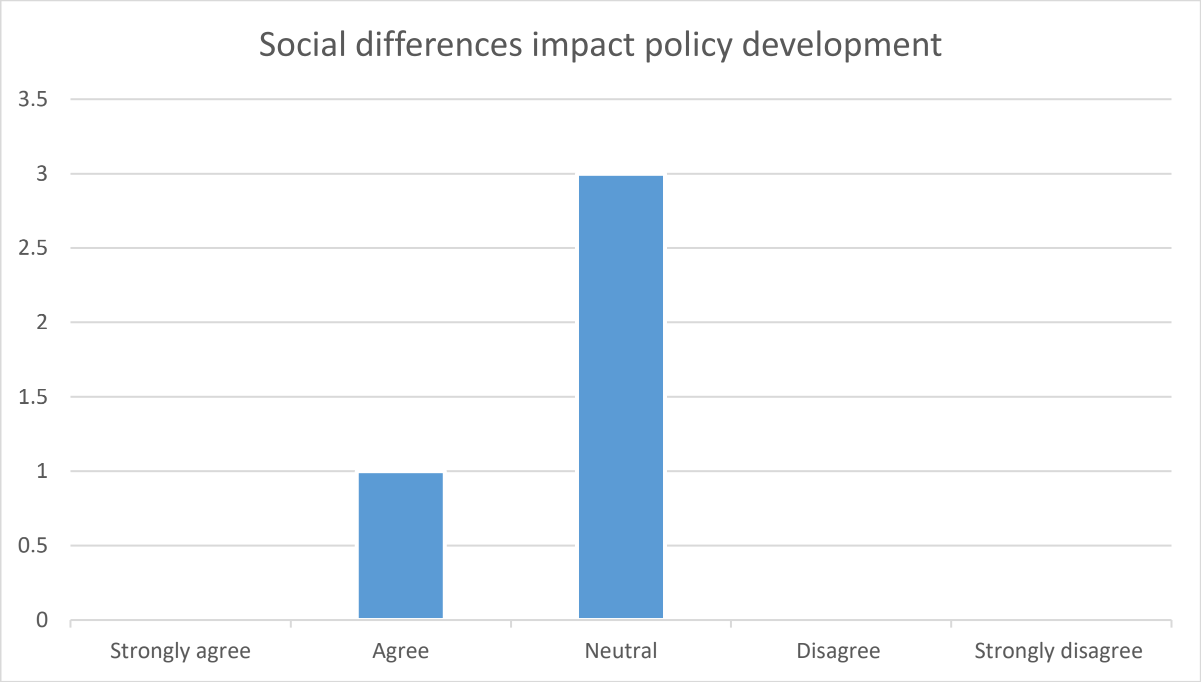


Figure E.238: Social differences impact policy development (65+ UK)

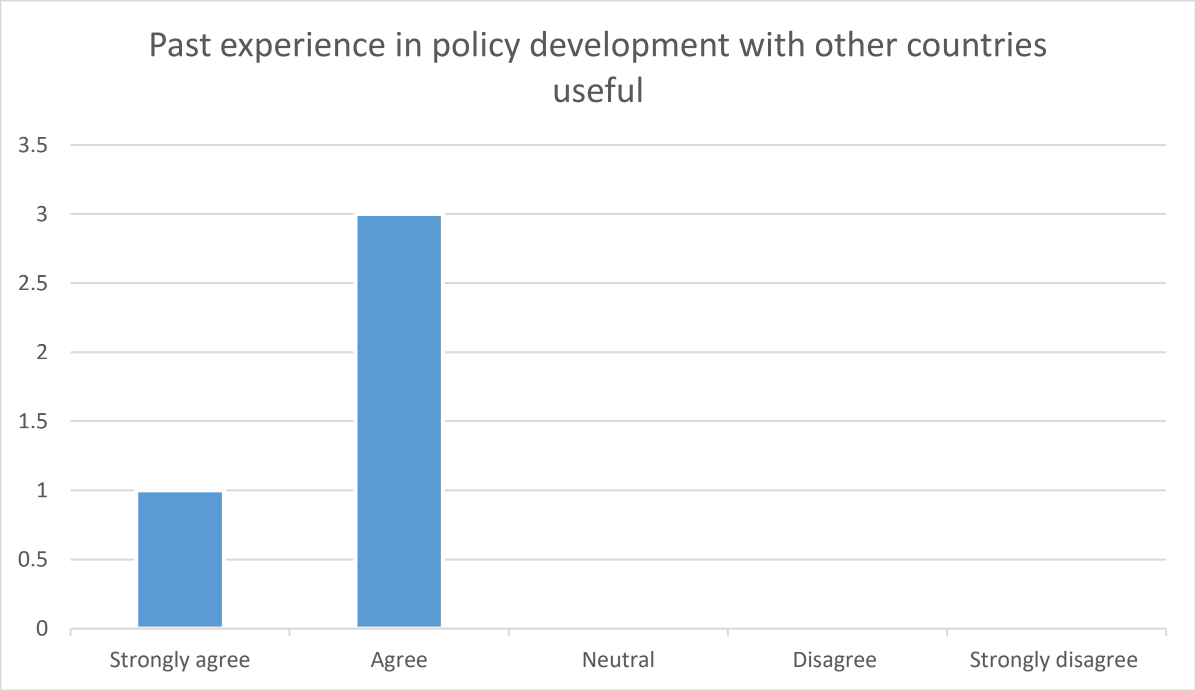


Figure E.239: Past experience in policy development with other countries useful (65+ UK)

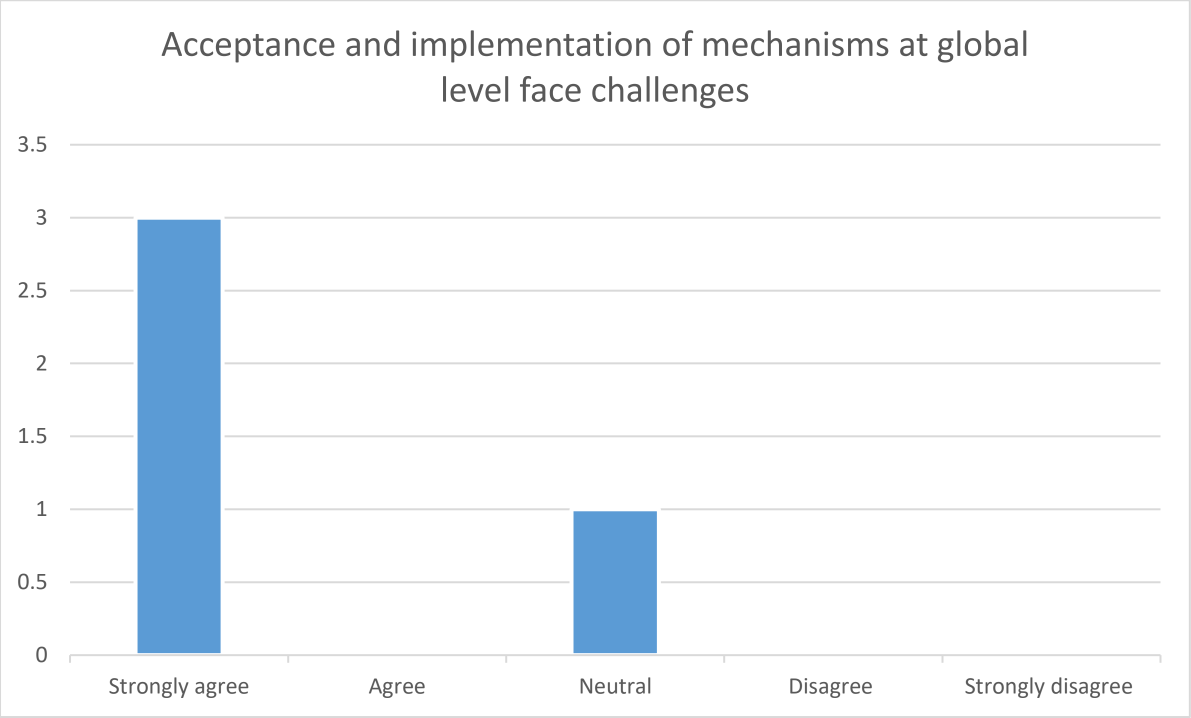


Figure E.240: Acceptance and implementation of mechanisms at global level face challenges (65+ UK)

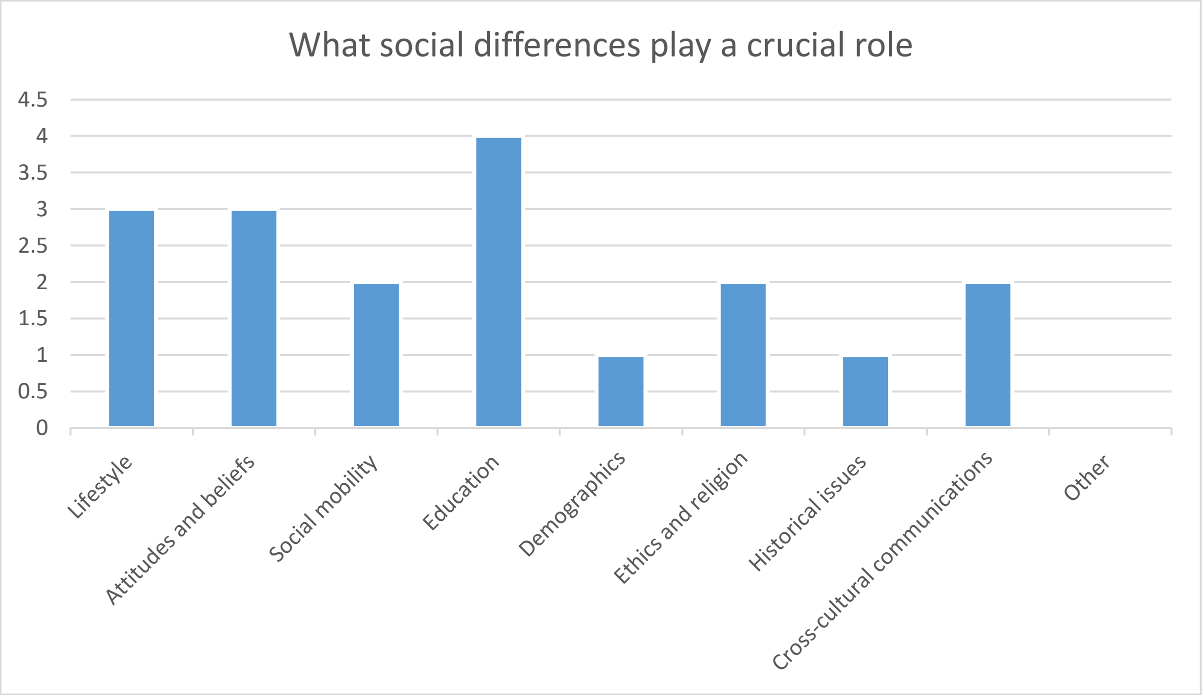


Figure E.241: What social differences play a crucial role (65+ UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education, lifestyle and attitude and beliefs (See figure E.241). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. It becomes clear that educational training can be an effective way to make people understand the importance of privacy and the implications associated with privacy violations. People will have to make a crucial choice in their lifestyles when considering reliance on technology at the workplace. If there is a high reliance on technology in sharing or handling personal information, the demand for accepting and implementing policies associated with data privacy and security also should be high. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

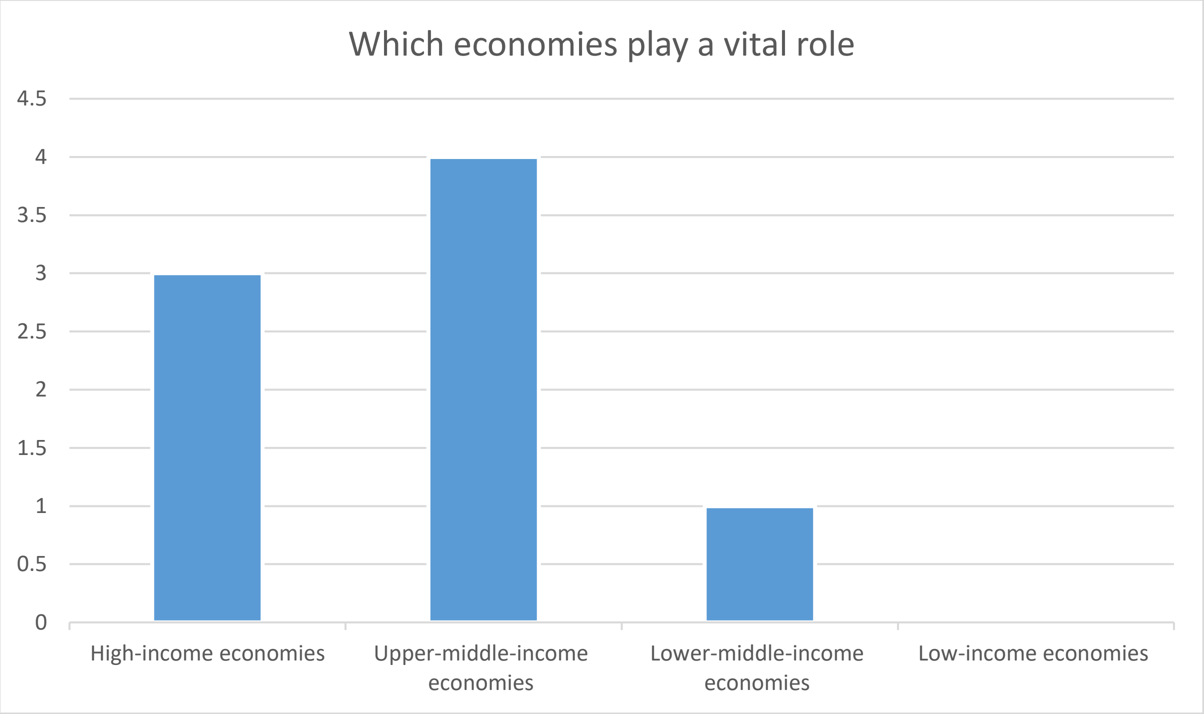


Figure E.242: Which economies play a vital role (65+ UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.242). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

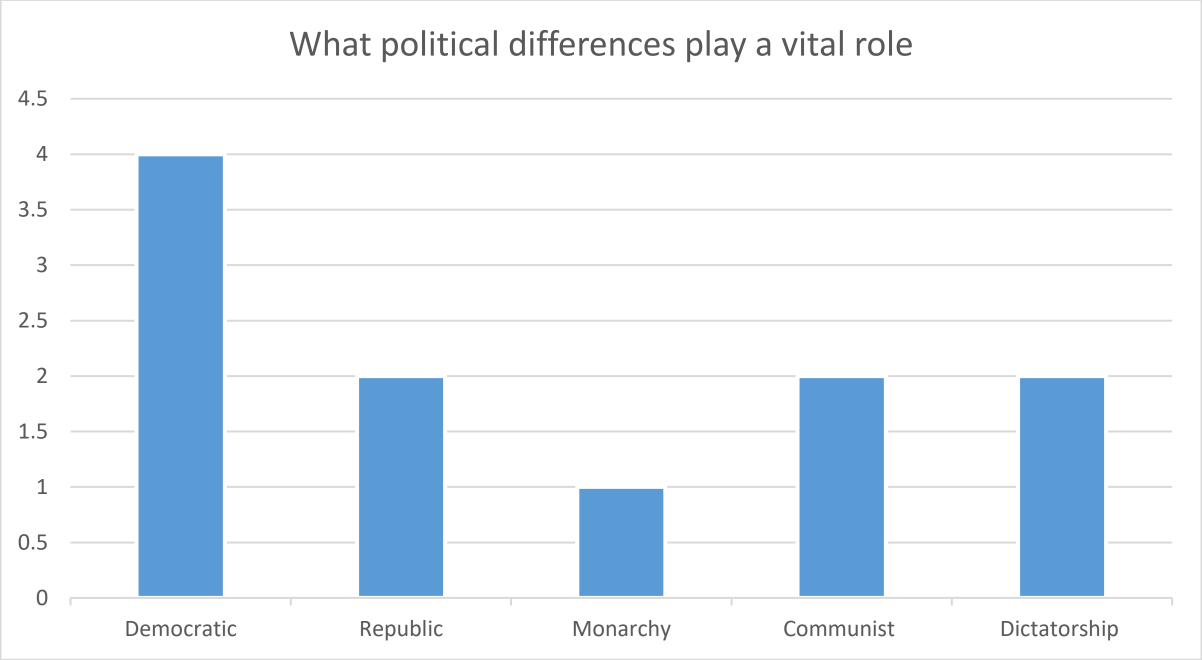


Figure E.243: What political differences play a vital role (65+ UK)

The majority have chosen a democratic political system (See figure E.243), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

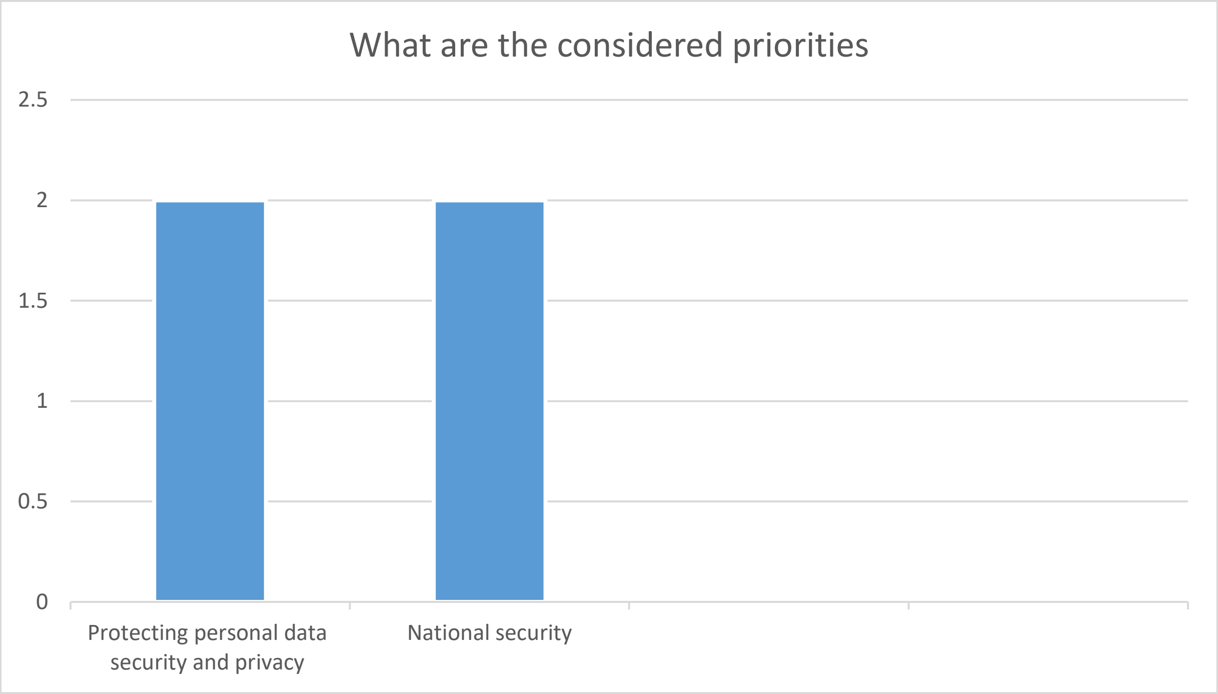


Figure E.244: What are the considered priorities (65+ UK)

The majority not considered either the importance of protection of personal data security and privacy or protection of national security, in accepting and implementing a global data privacy and security policies (See figure E.244). However, in an incident of a personal data breach, there will potentially be a knock-on effect on both personal data security and privacy, and national security, and it will also be felt right across the groups as well as the community alike.

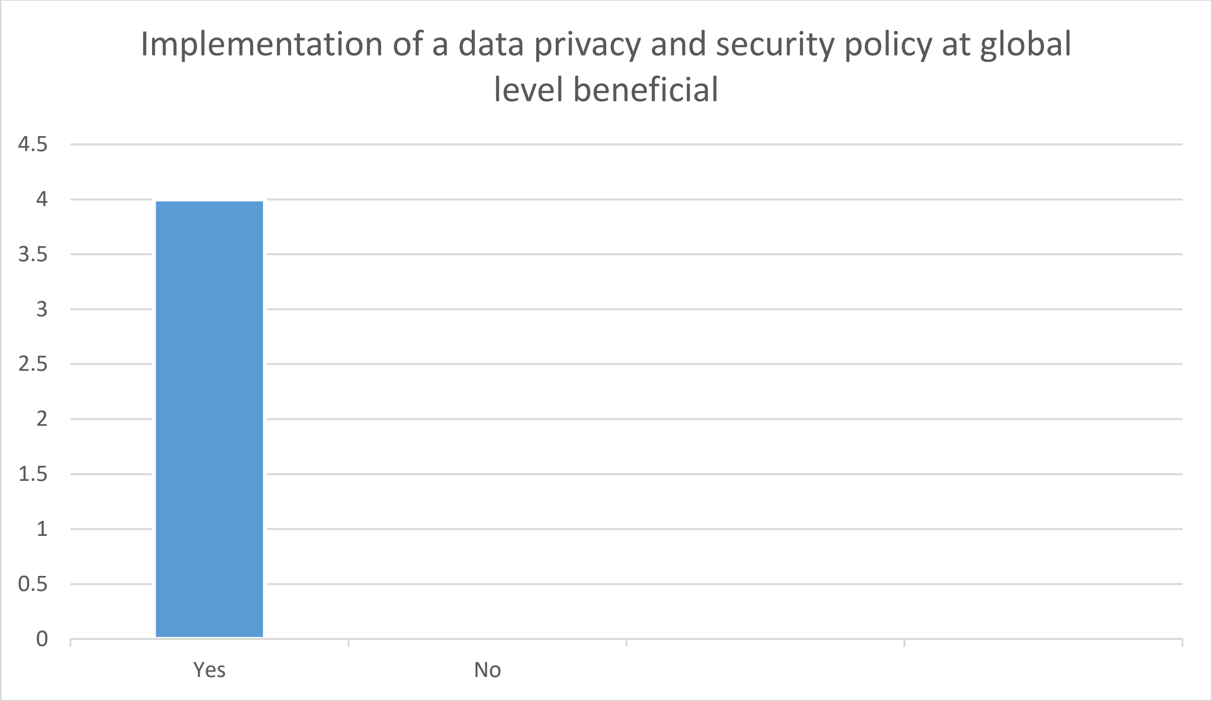


Figure E.245: Implementation of a data privacy and security policy at global level beneficial (65+ UK)

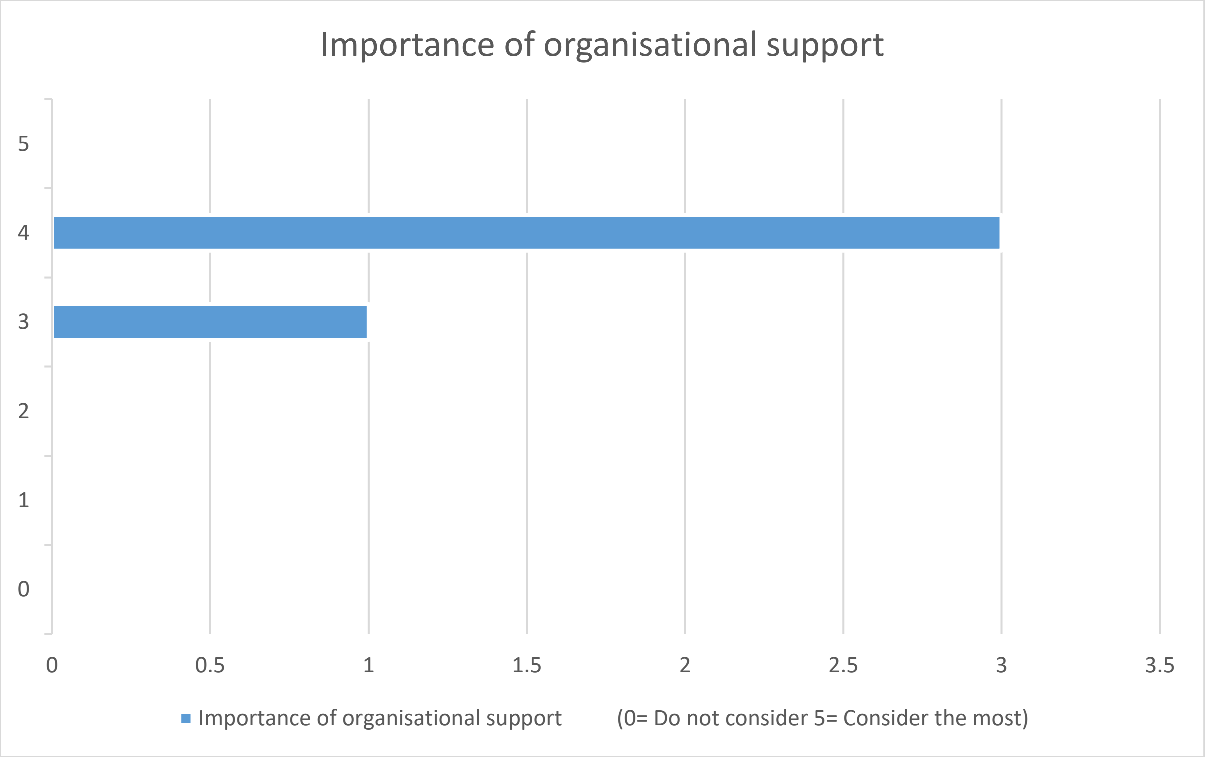


Figure E.246: Importance of organisational support (65+ UK)

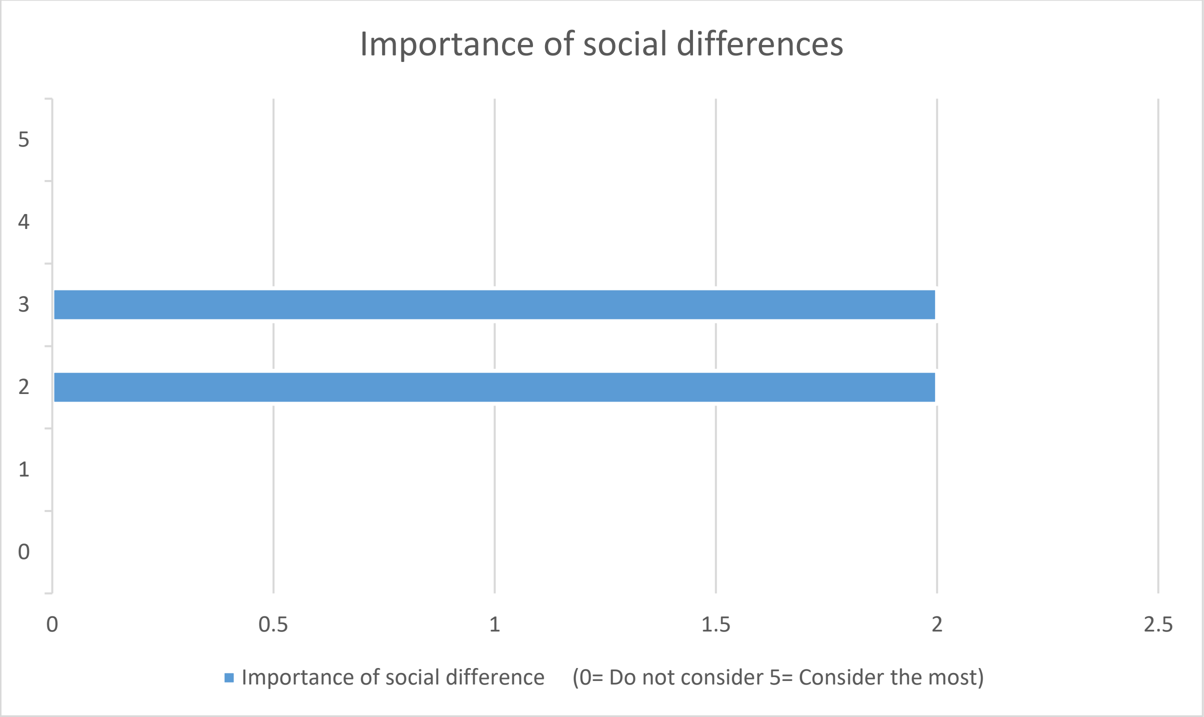


Figure E.247: Importance of social differences (65+ UK)

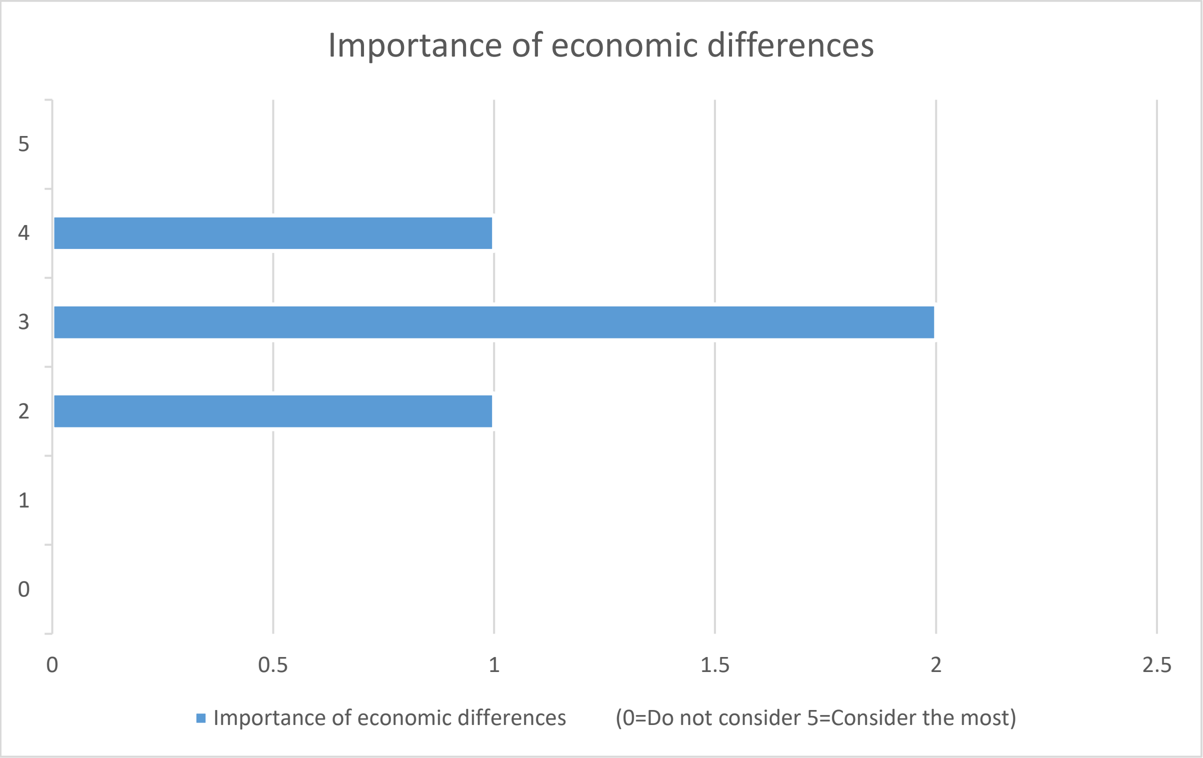


Figure E.248: Importance of economic differences (65+ UK)

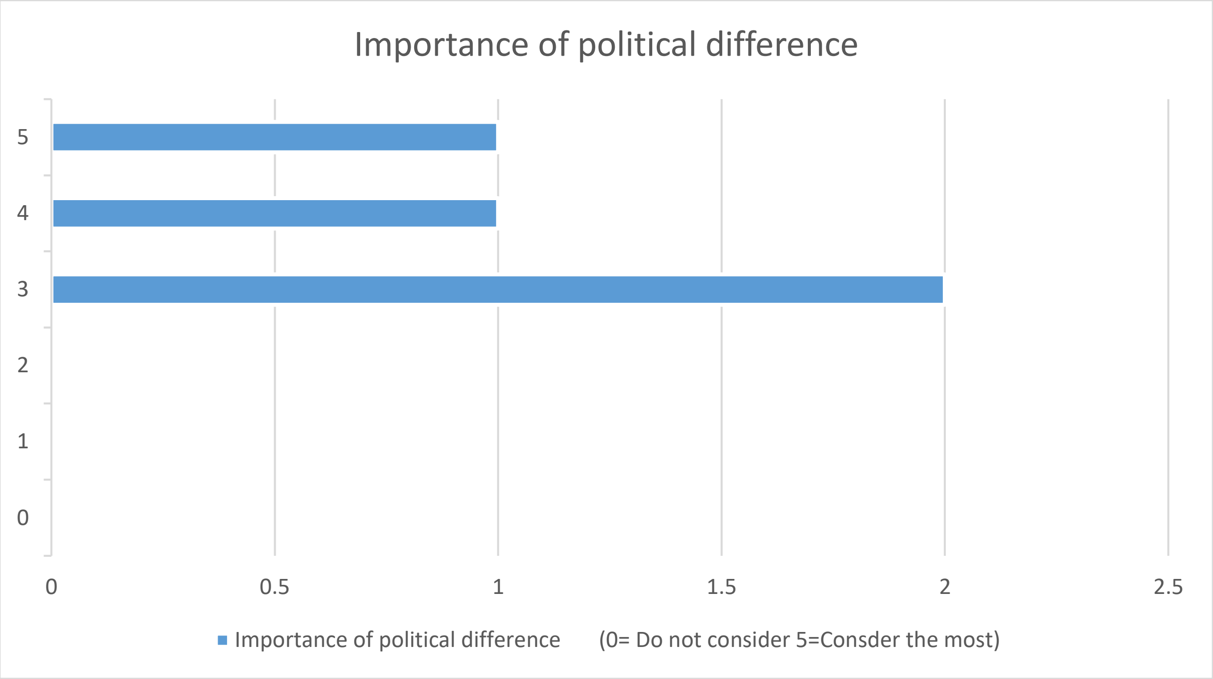


Figure E.249: Importance of political difference (65+ UK)

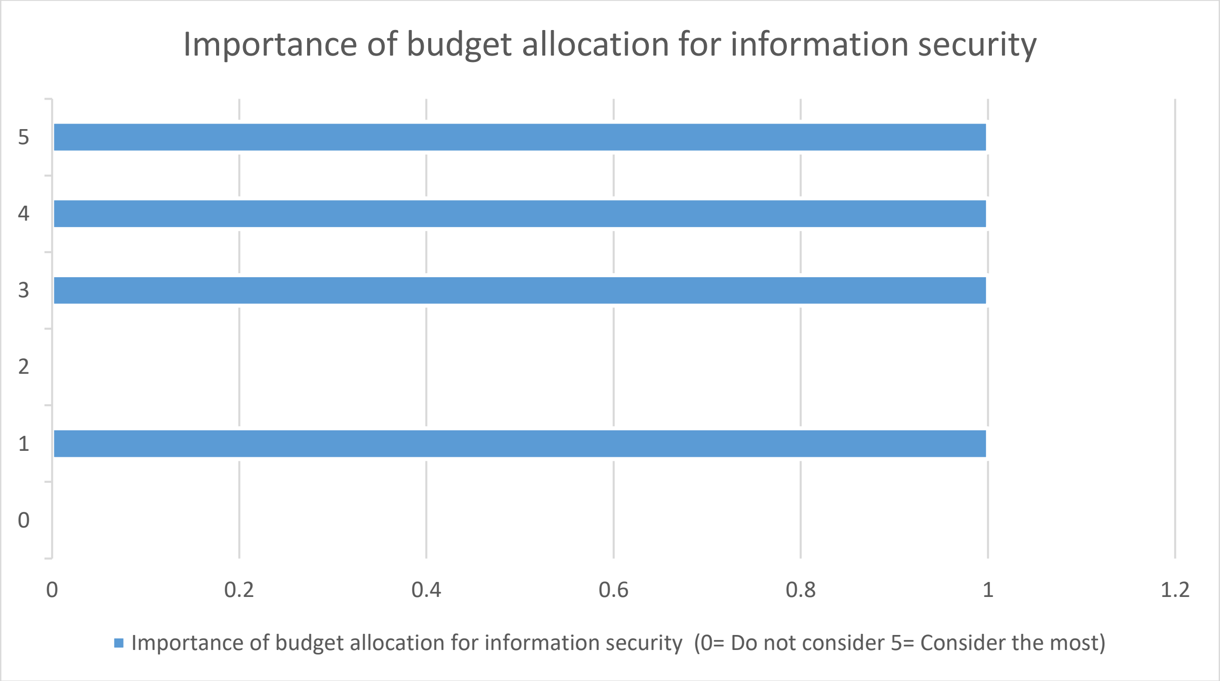


Figure E.250: Importance of budget allocation for information security (65+ UK)

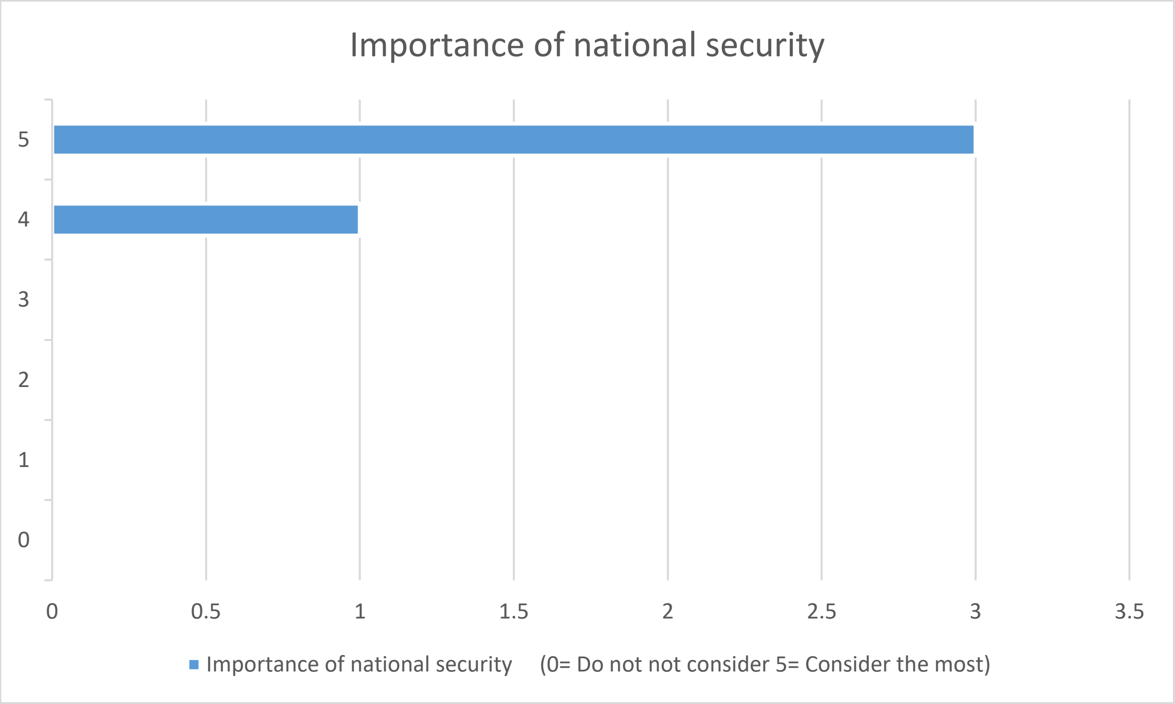


Figure E.251: Importance of national security (65+ UK)

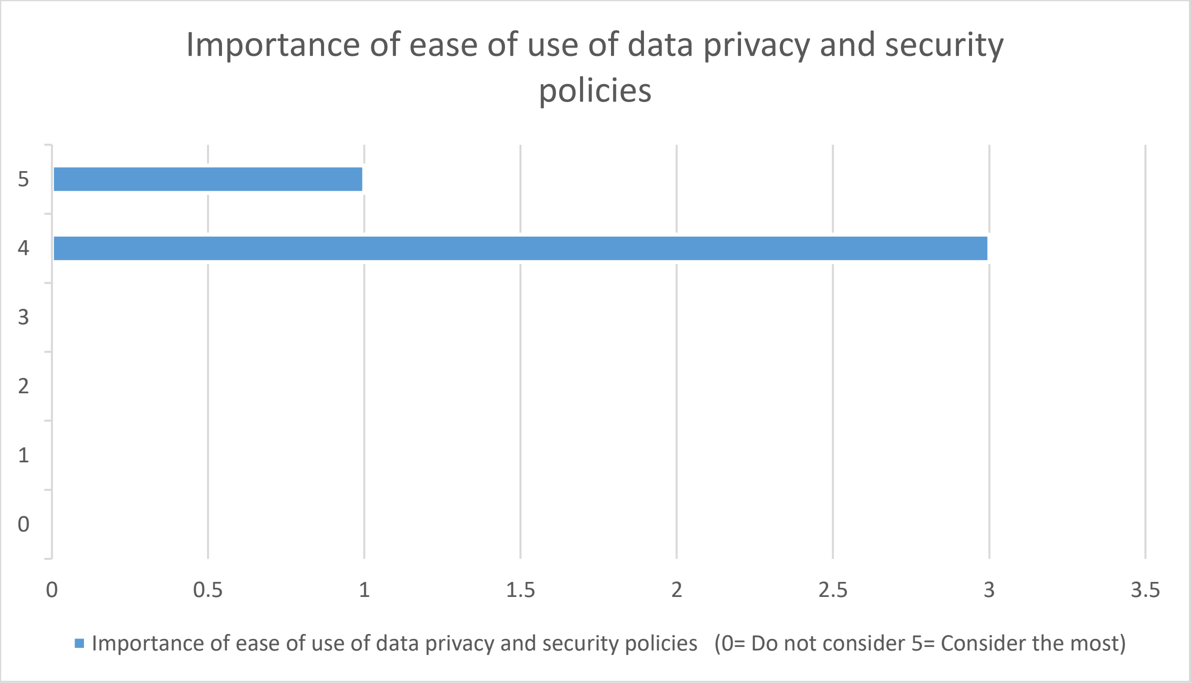


Figure E.252: Importance of ease of use of data privacy and security policies (65+ UK)

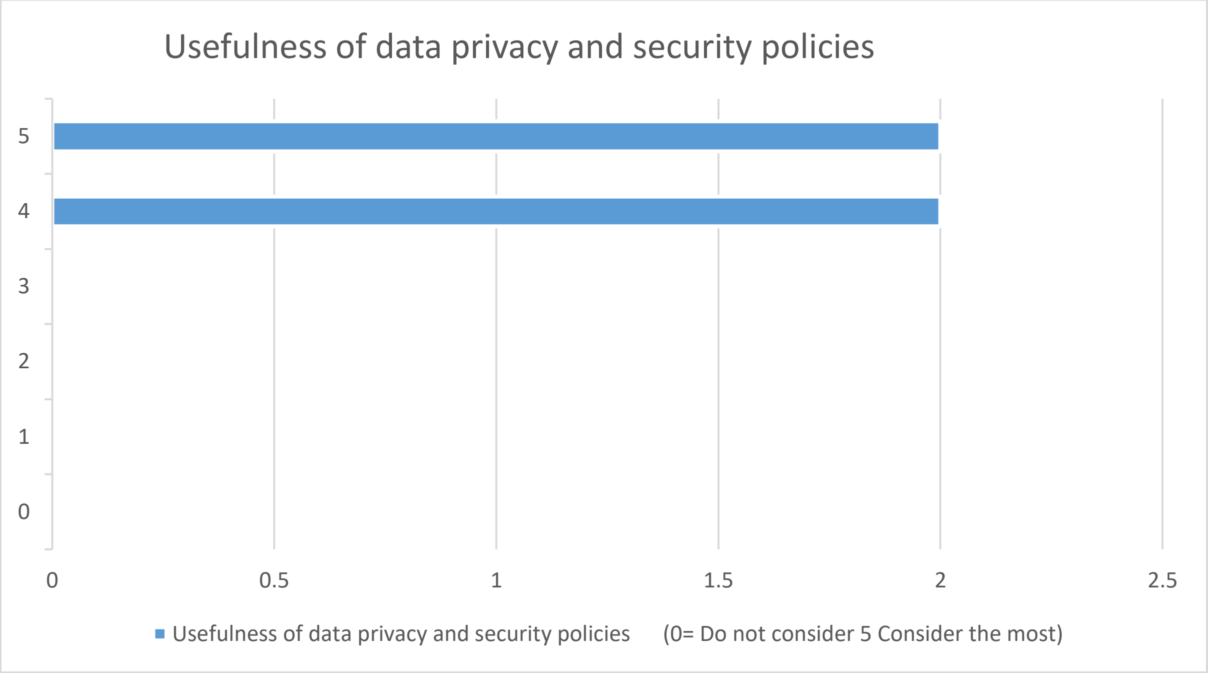


Figure E.253: Usefulness of data privacy and security policies (65+ UK)

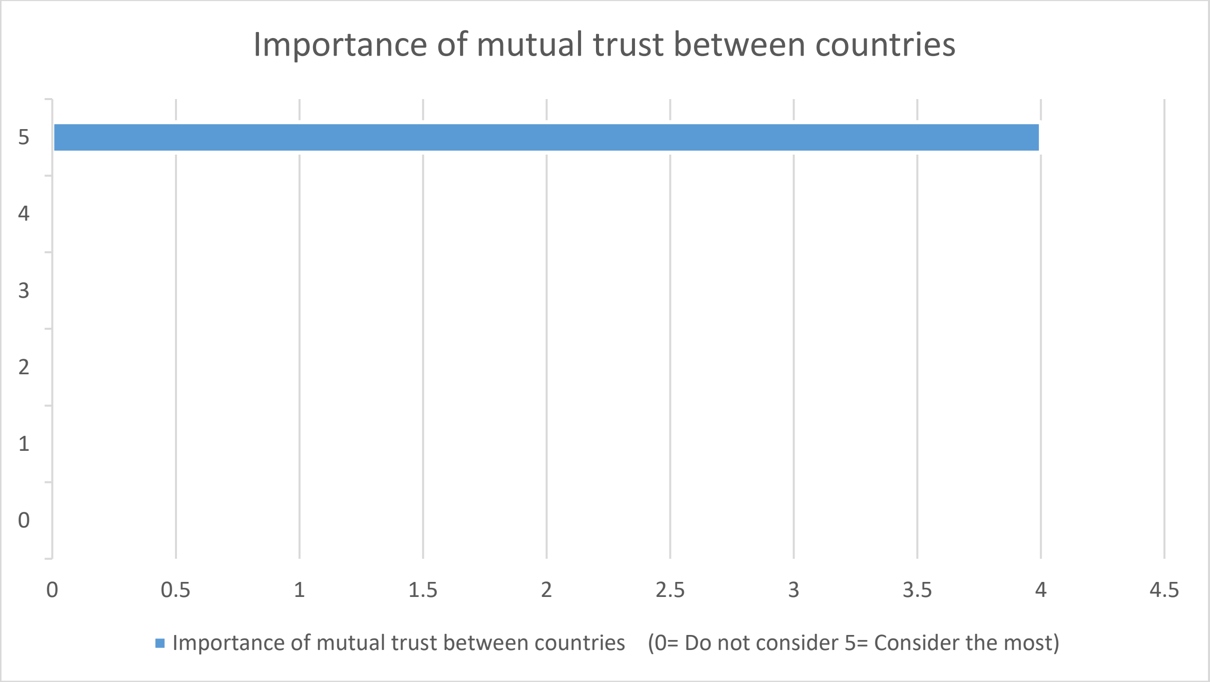


Figure E.254 Importance of mutual trust between countries (65+ UK)

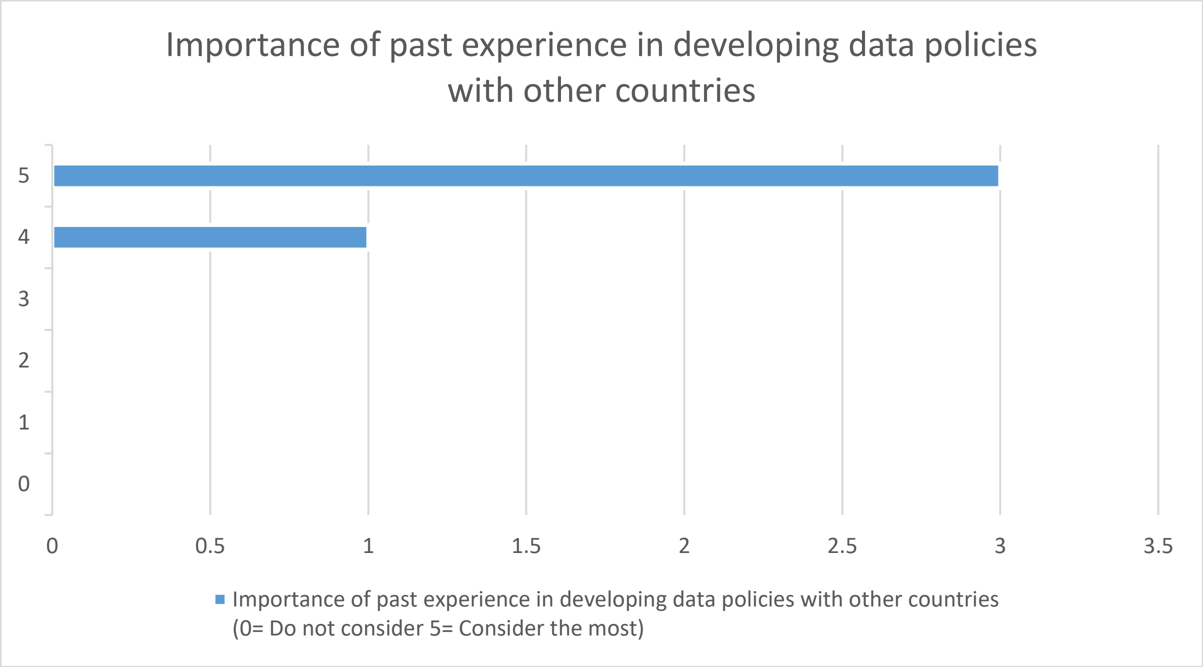


Figure E.255: Importance of past experience in developing data policies with other counties (65+ UK)

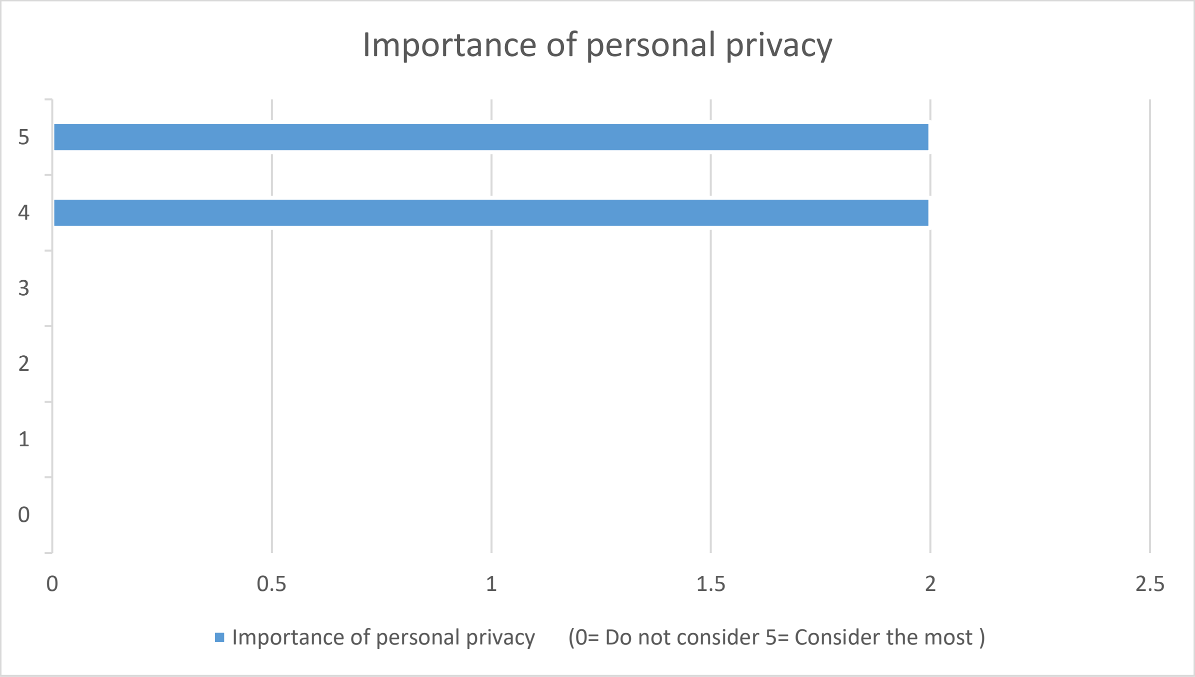


Figure E.256: Importance of personal privacy (65+ UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 80 percent of the respondents have endorsed (See figure E.245). The other notable factors that have come out of the survey are organisational support, budget allocation, political differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure E.234-244) (See figure E.246-256).

United Kingdom – Less than a year

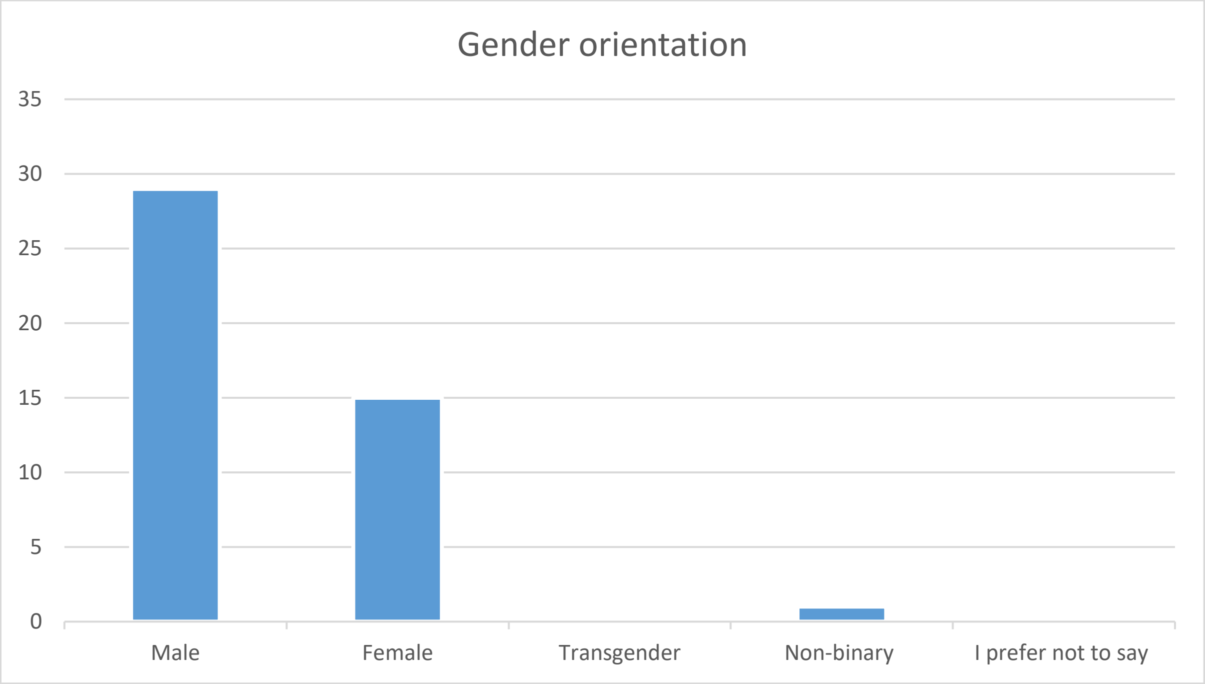


Figure E.257: Gender orientation (Less than a year-UK)

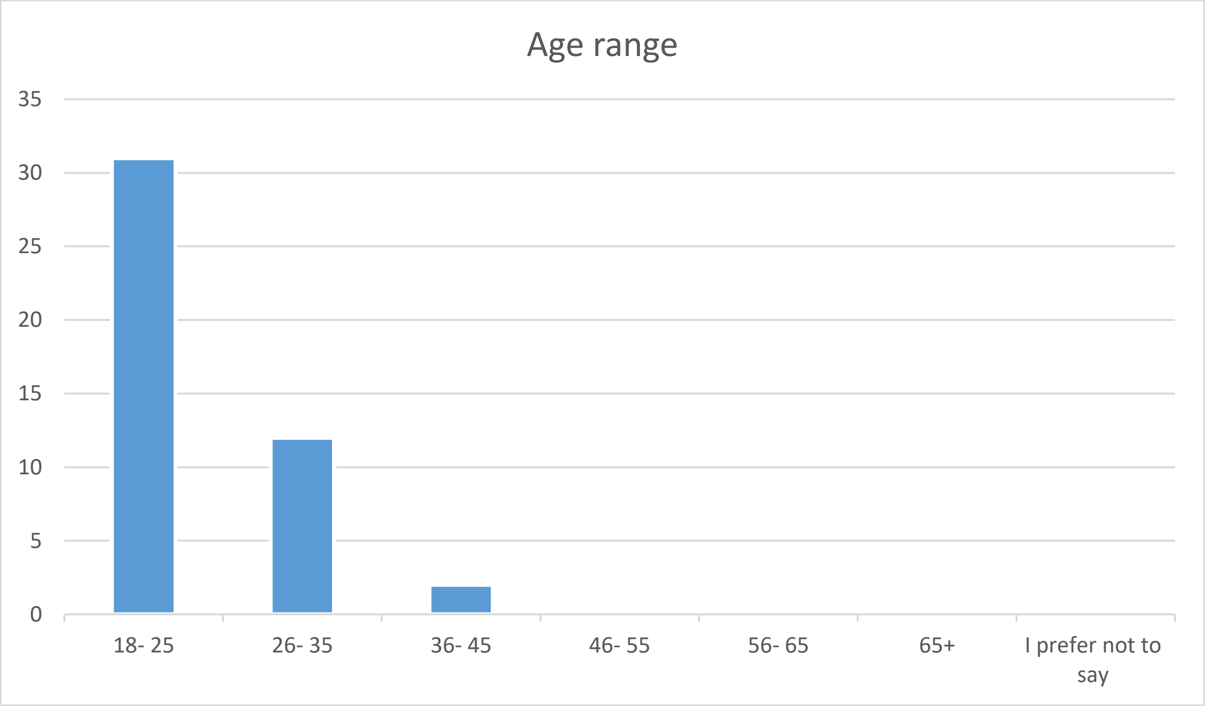


Figure E.258: Age range (Less than a year-UK)

This analysis is based on the responses received from United Kingdom participants with less than a year of employment in the industry. There were 45 participants and 29 out of them were males, 15 females and 1 non-binary (See figure E.257). They were within the 18-45 age range out of which 31 in the 18-25, 12 in the 26-35, and 2 in the 36-45 range (See figure E.258). Also, the figures show that the age range of the majority of the employees with less than a year of service is between 18-25.

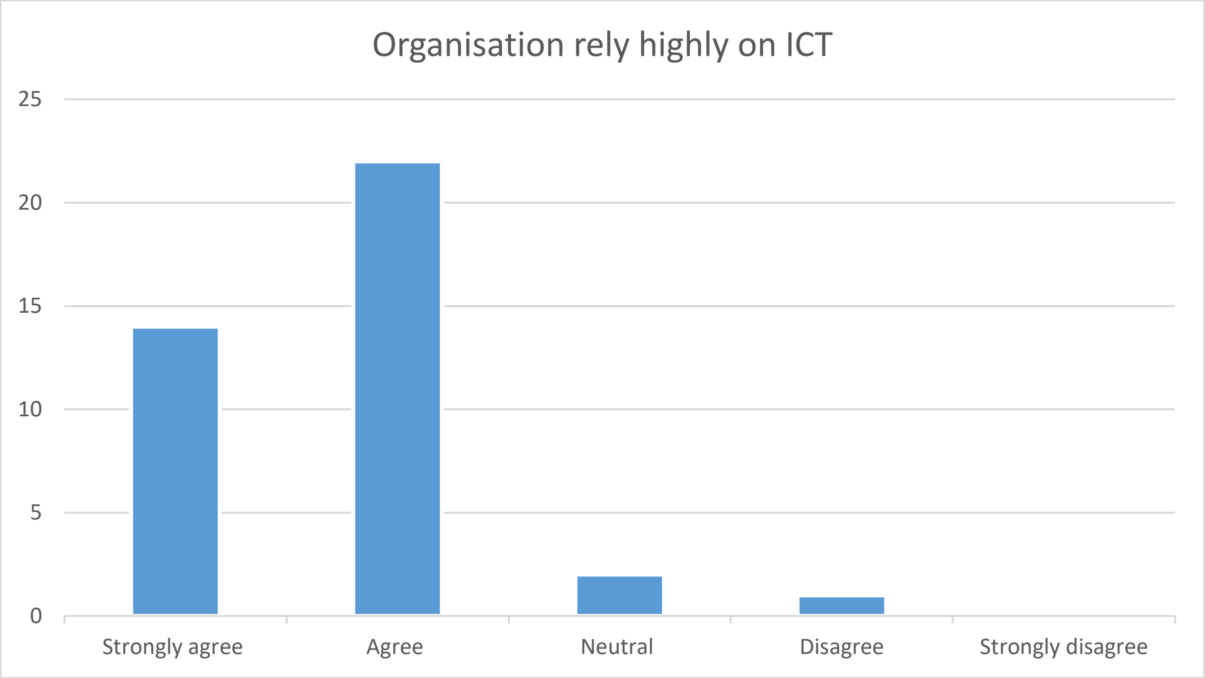


Figure E.259: Organisation rely highly on ICT (Less than a year-UK)

Out of the 45 respondents, 36 have worked in a technology reliance working environment, 2 unaware of reliance on technology because of the nature of the work assigned to them, 1 has marked ‘disagree’ on ICT (See figure E.259). This indicates a majority of those who have been working in an organisation for less than a year have had a high reliance on ICT.

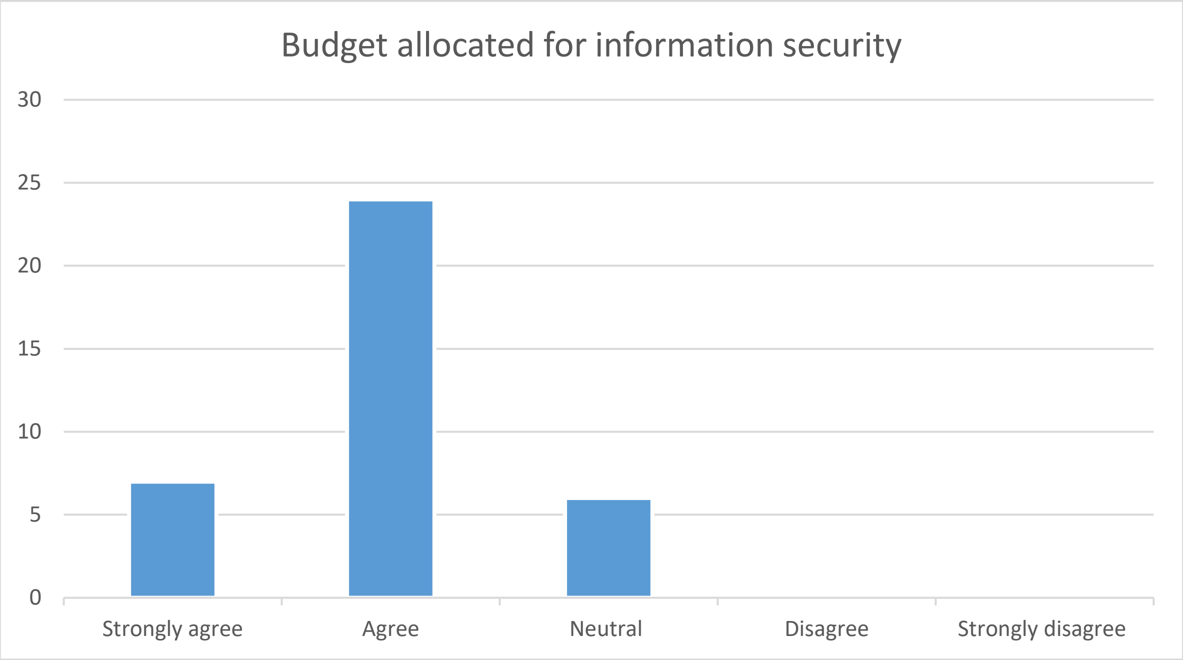


Figure E.260: Budget allocated for information security (Less than a year-UK)

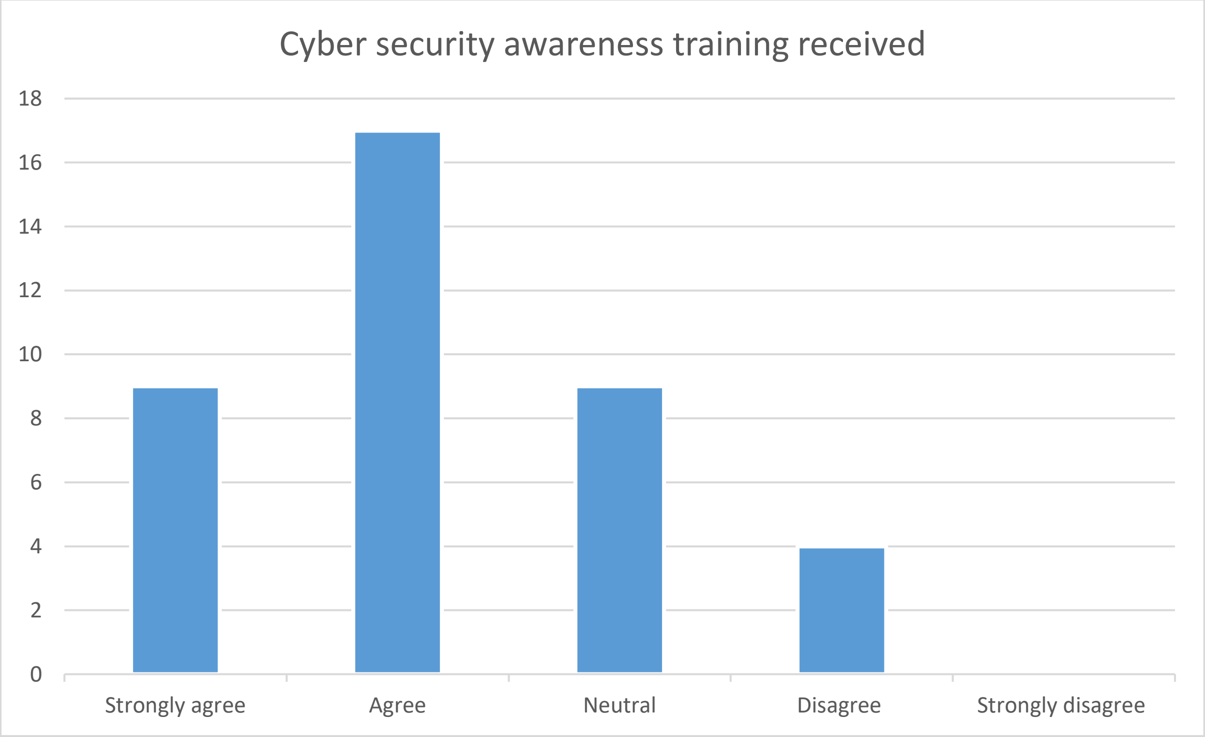


Figure E.261: Cyber security awareness training received (Less than a year-UK)

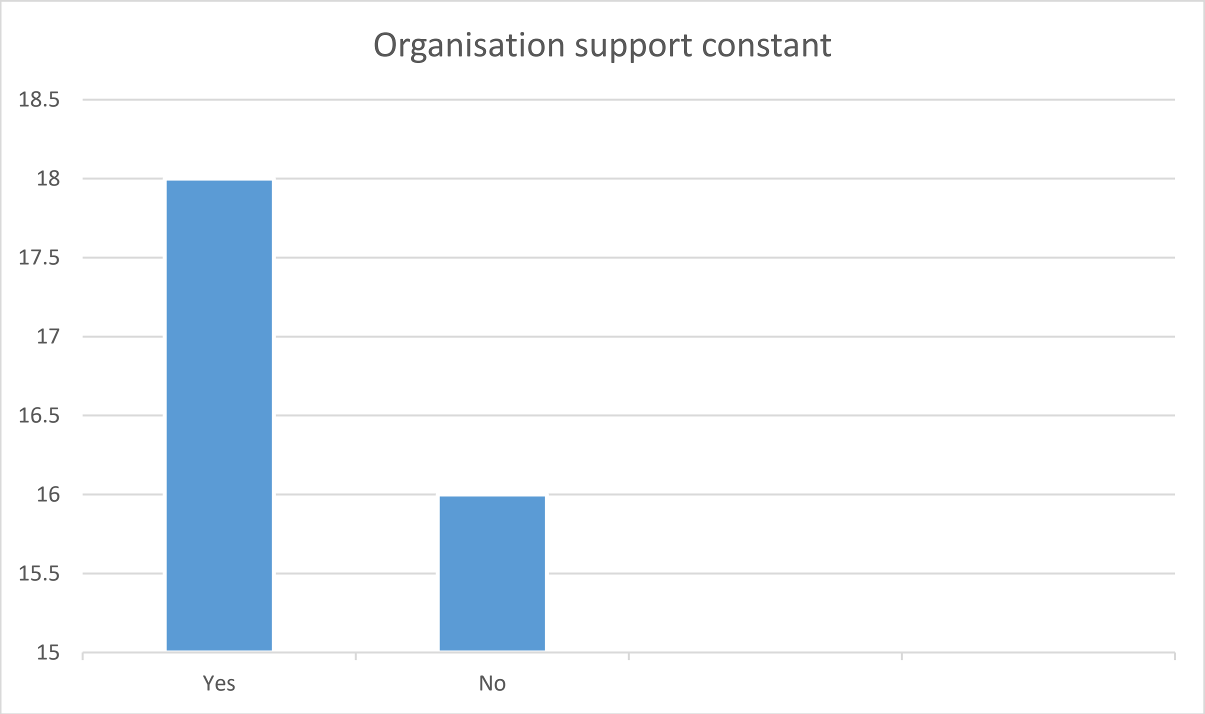


Figure E.262: Organisation support constant (Less than a year-UK)

Funding has been sketchy. 31 out of the 45 have indicated that their organisations had an allocated budget for information security, whilst 6 had not expressed an opinion either way (See figure E.260). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was adequate. 26 participants have received regular cybersecurity awareness training, whilst 9 neither agreed nor disagreed, and 4 participants had not regularly received security awareness training (See figure E.261). In addition, 16 participants had not received support from the organisation to protect personal information, whilst 18 did (See figure E.262). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

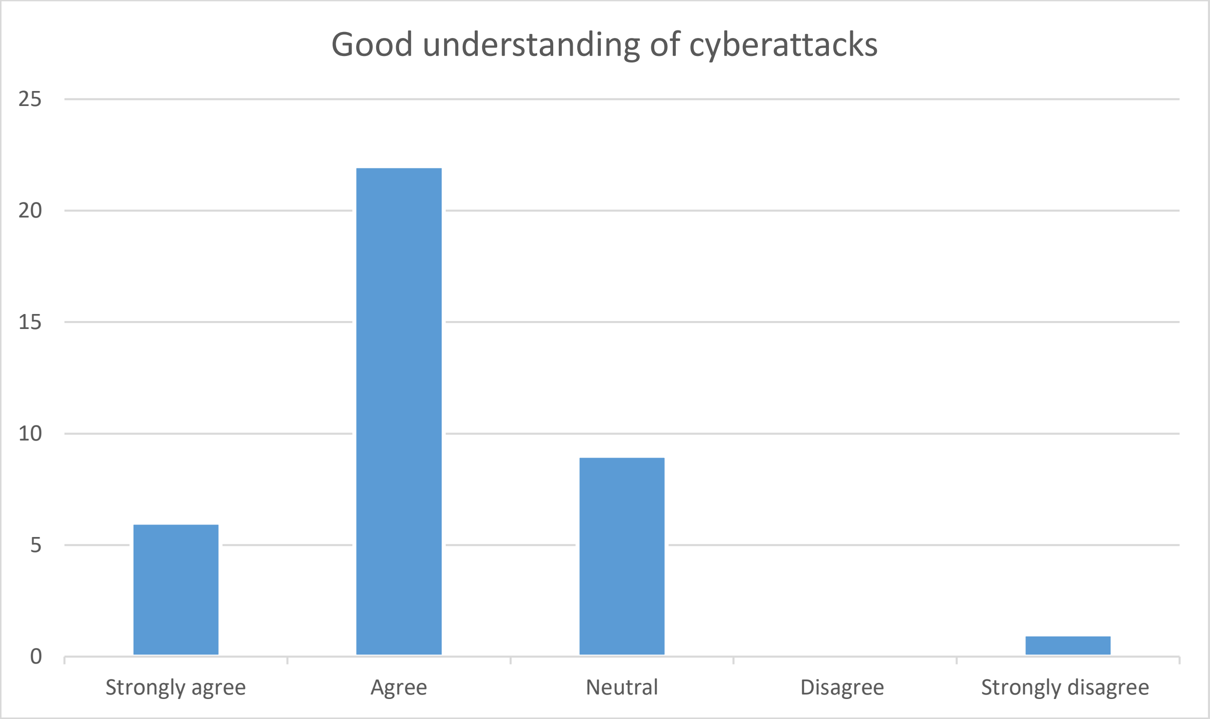


Figure E.263: Good understanding of cyberattacks (Less than a year-UK)

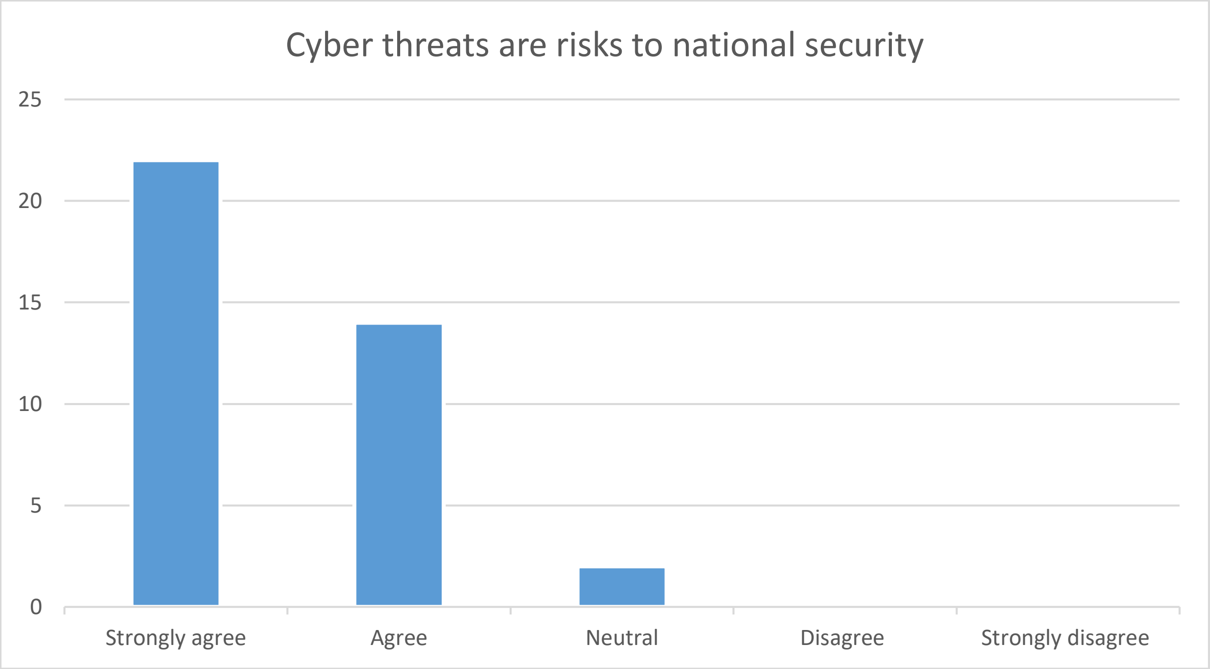


Figure E.264: Cyber threats are risks to national security (Less than a year-UK)

Despite the security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 28 participants do have, 9 have not expressed opinion either way, and only 1 participant had no understanding (See figure E.263). Furthermore, 80 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure E.264). In general, understanding of cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

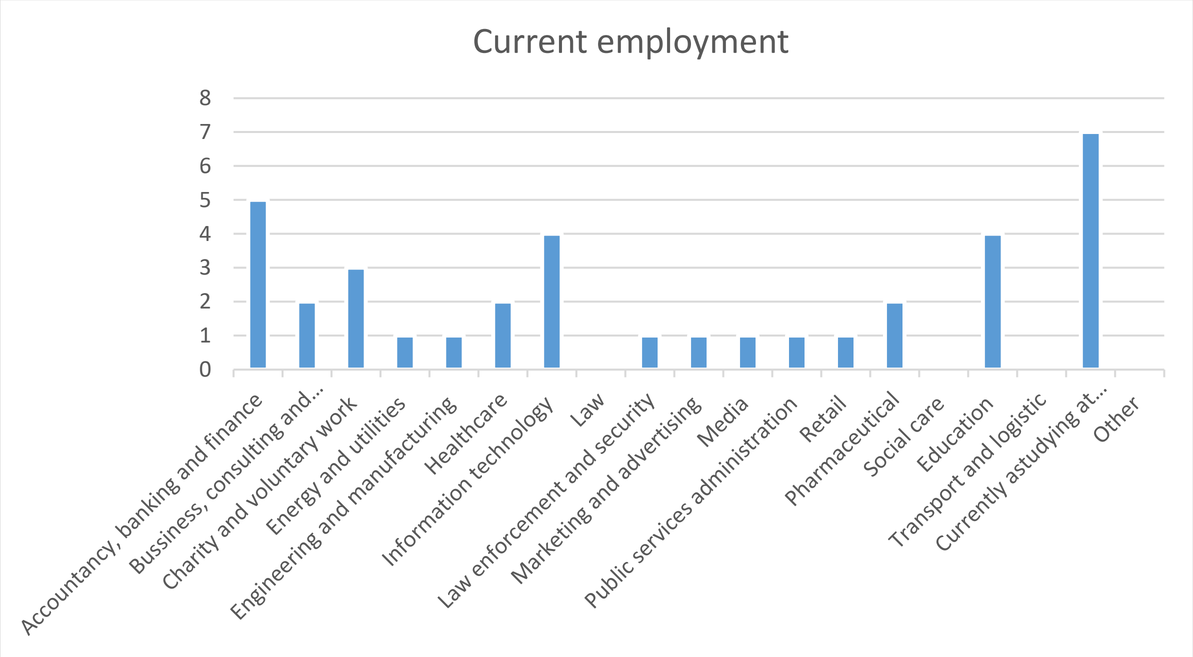


Figure E.265: Current employment (Less than a year-UK)

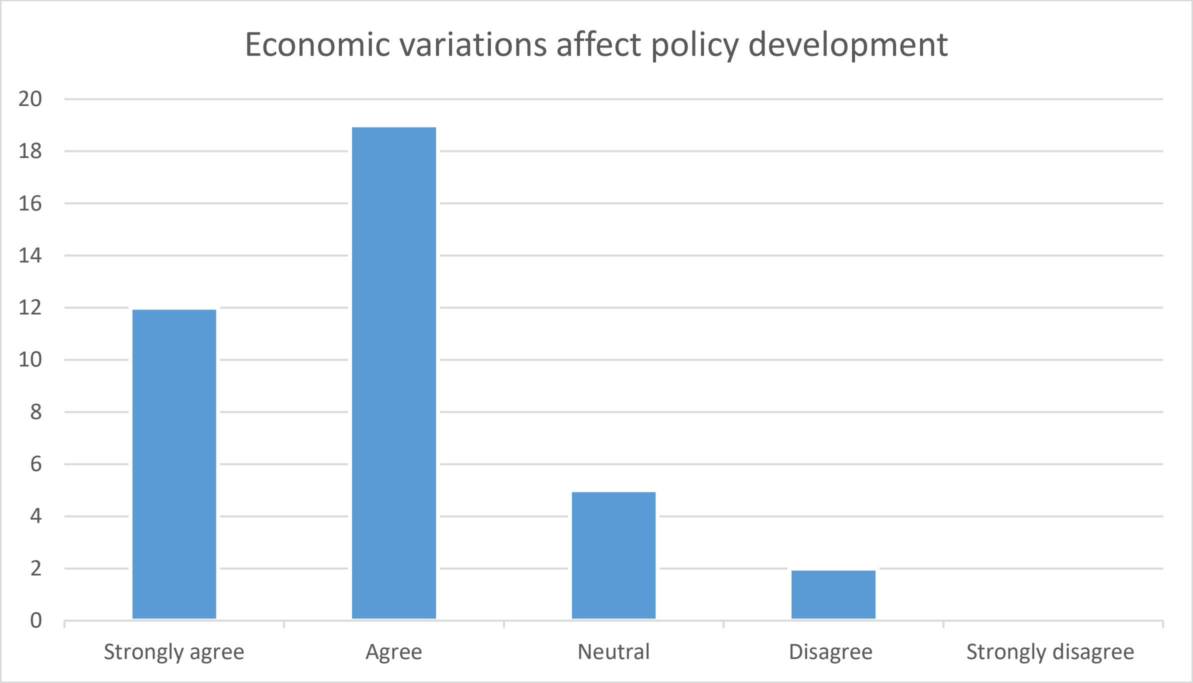


Figure E.266: Economic variations affect policy development (Less than a year-UK)

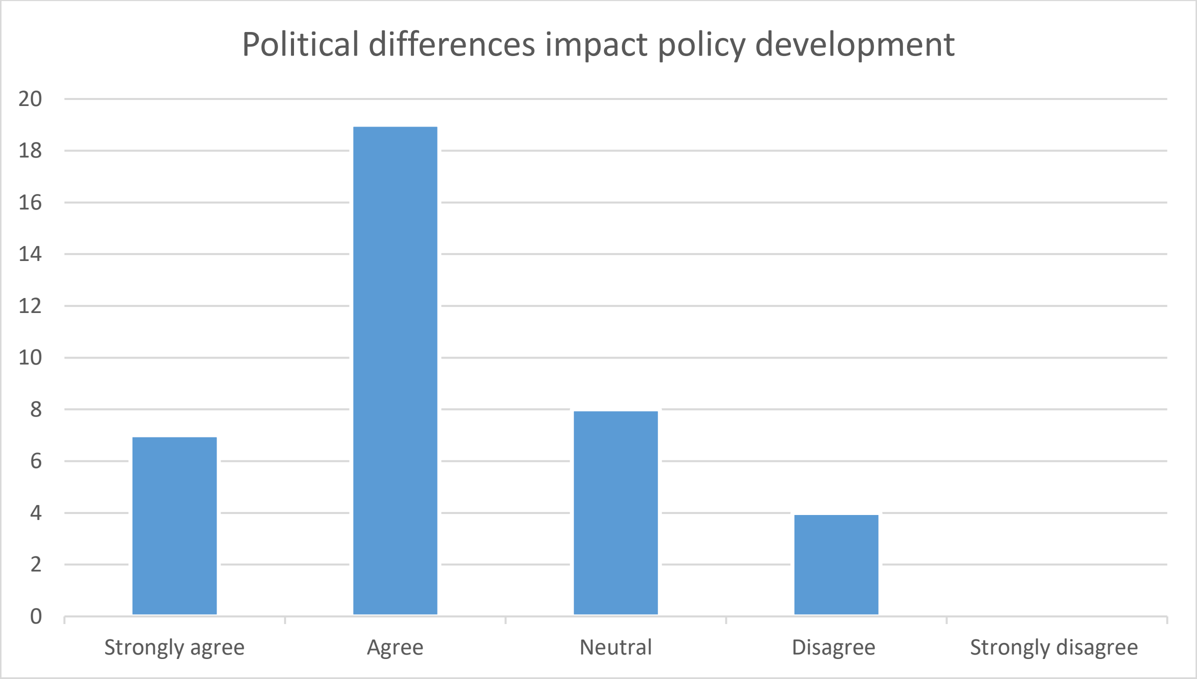


Figure E.267: Political differences impact policy development (Less than a year-UK)

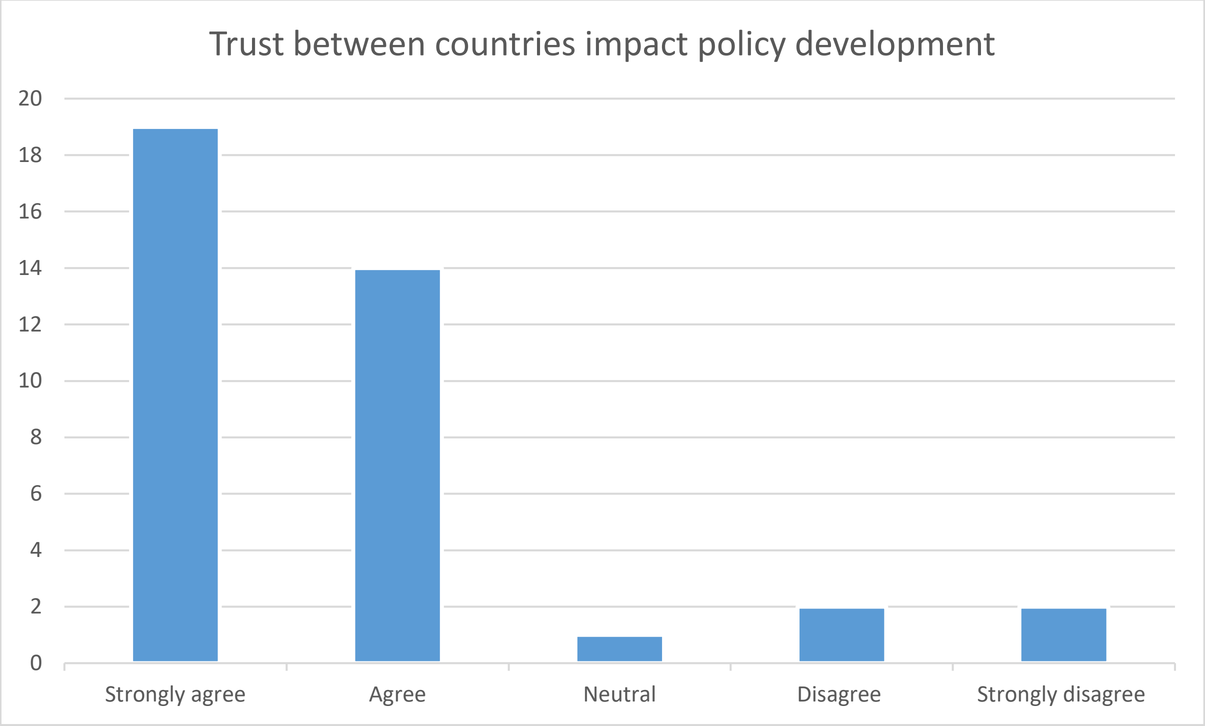


Figure E.268: Trust between countries impact policy development (Less than a year-UK)

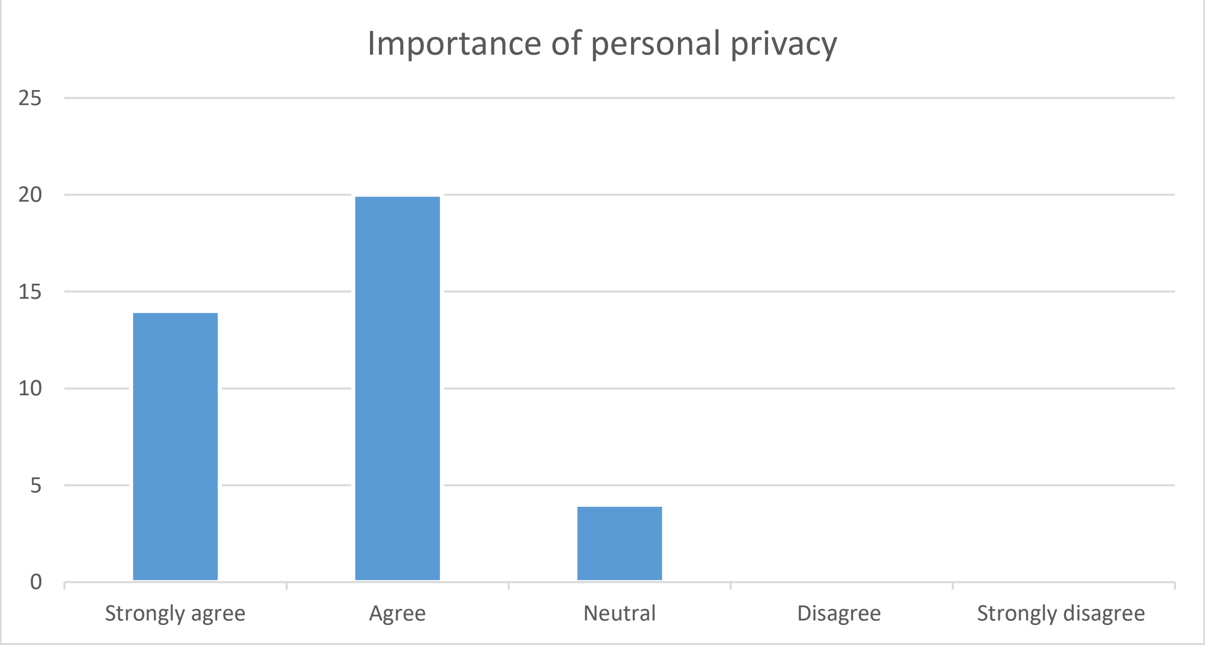


Figure E.269: Importance of personal privacy (Less than a year-UK)

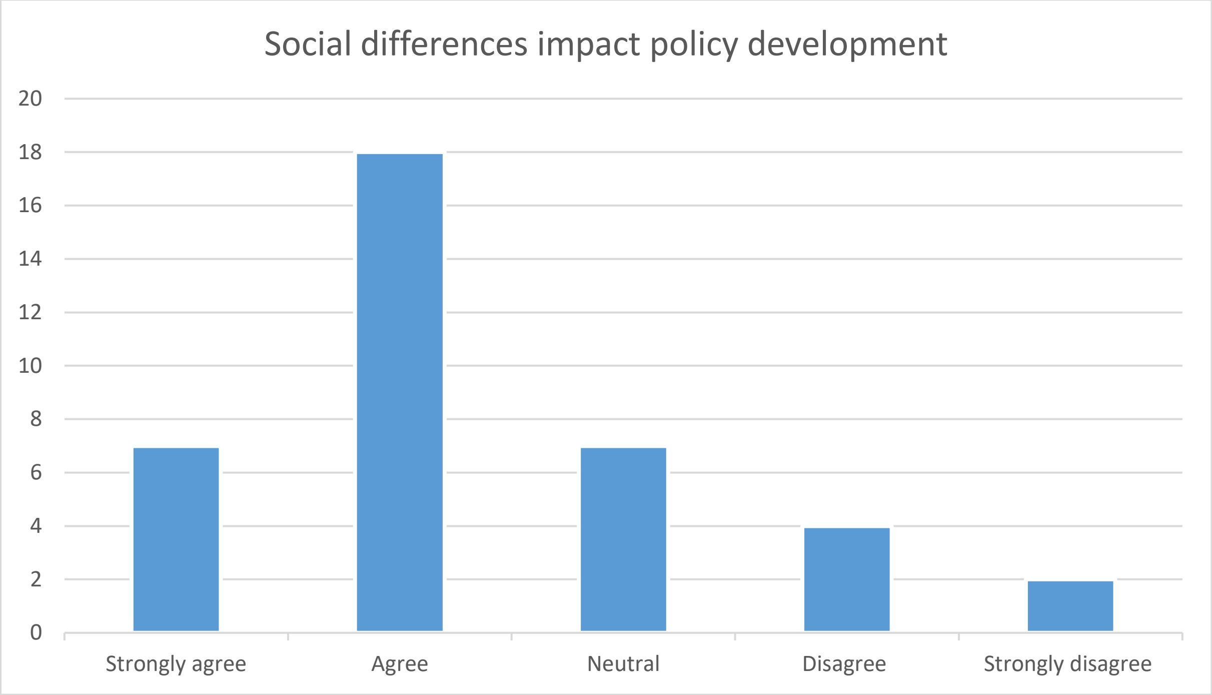


Figure E.270: Social differences impact policy development (Less than a year-UK)

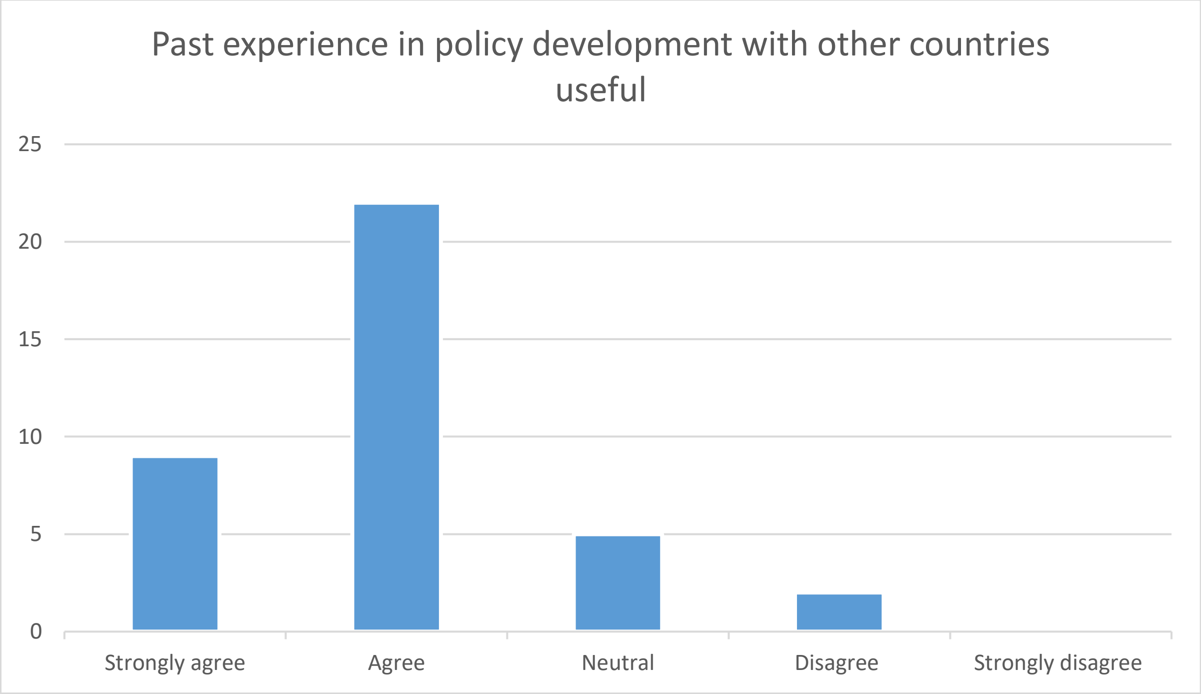


Figure E.271: Past experience in policy development with other countries useful (Less than a year-UK)

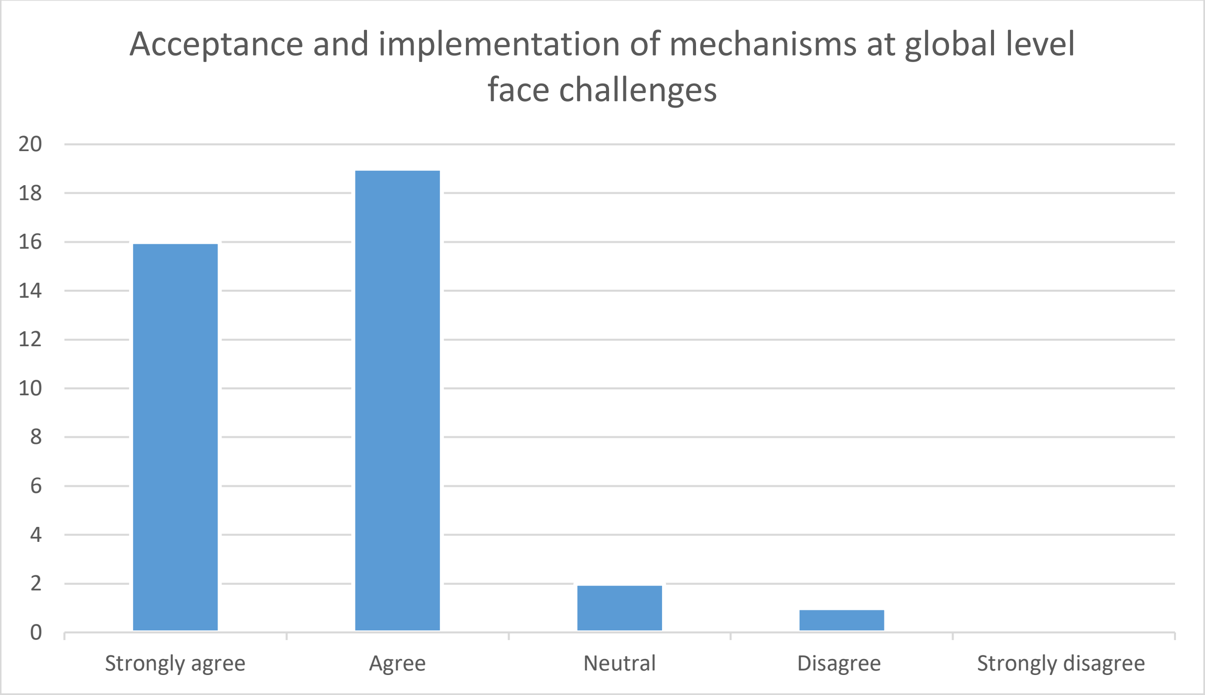


Figure E.272: Acceptance and implementation of mechanisms at global level face challenges (Less than a year-UK)

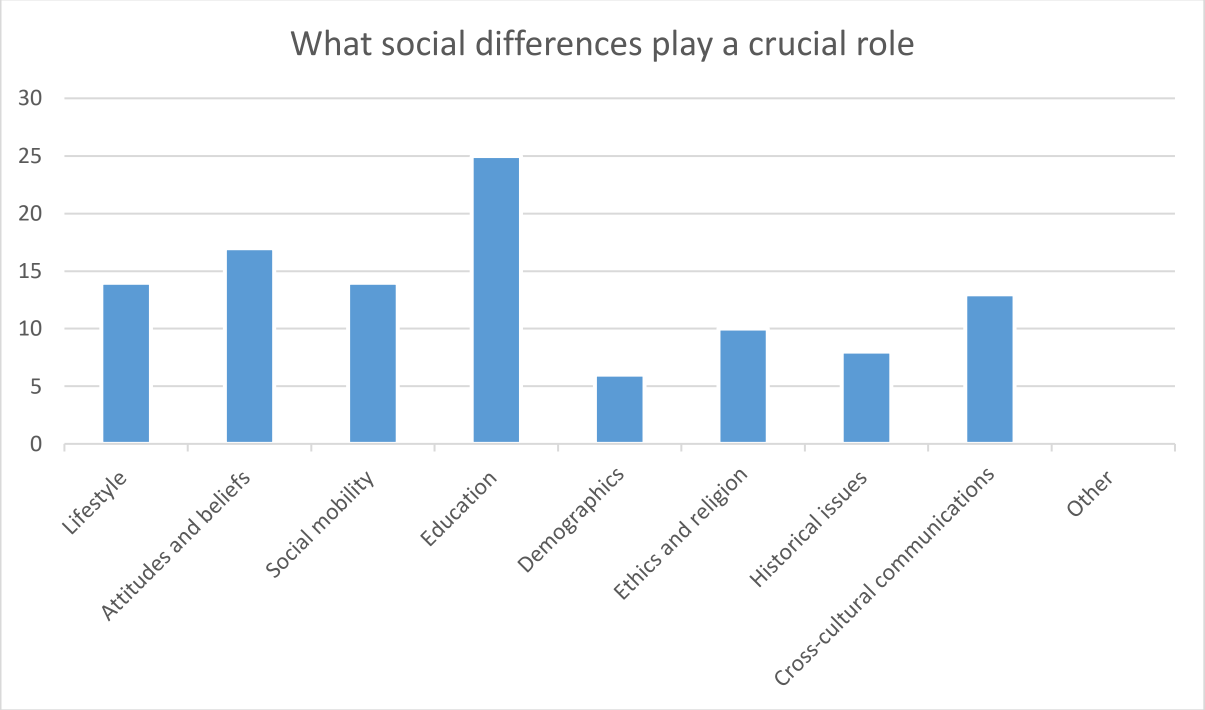


Figure E.273: What social differences play a crucial role (Less than a year-UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education (See figure E.273). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level.

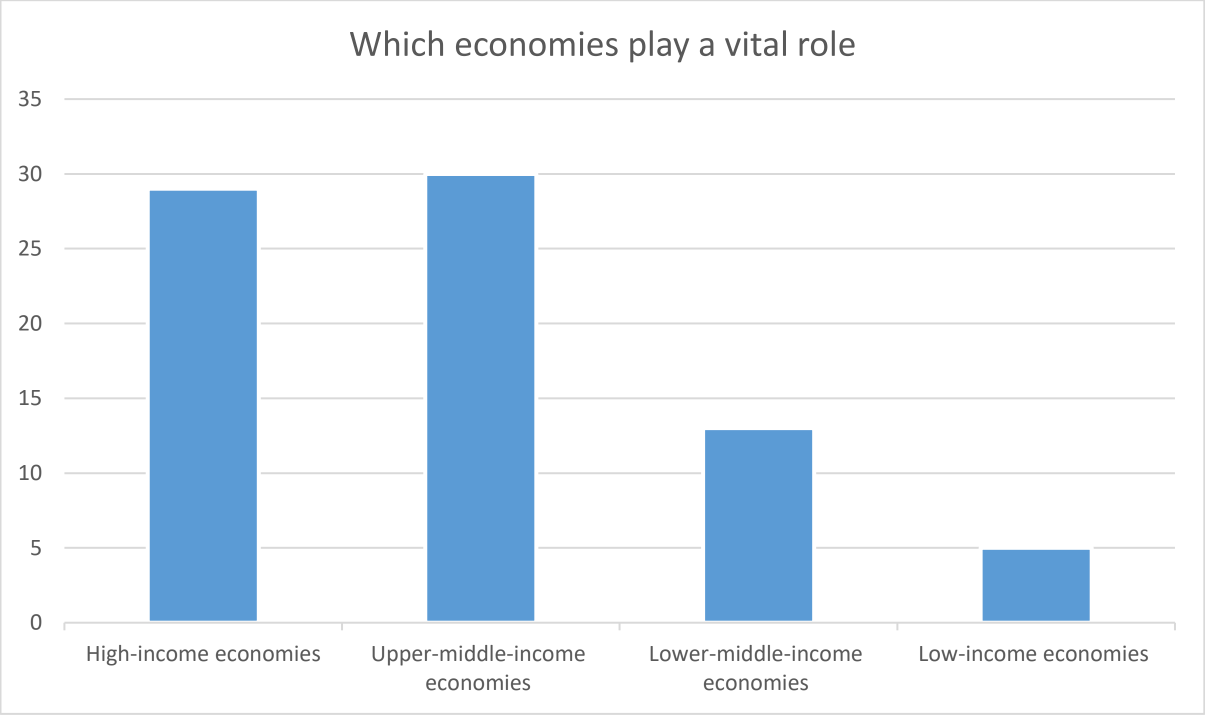


Figure E.274: Which economies play a vital role (Less than a year-UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.274). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

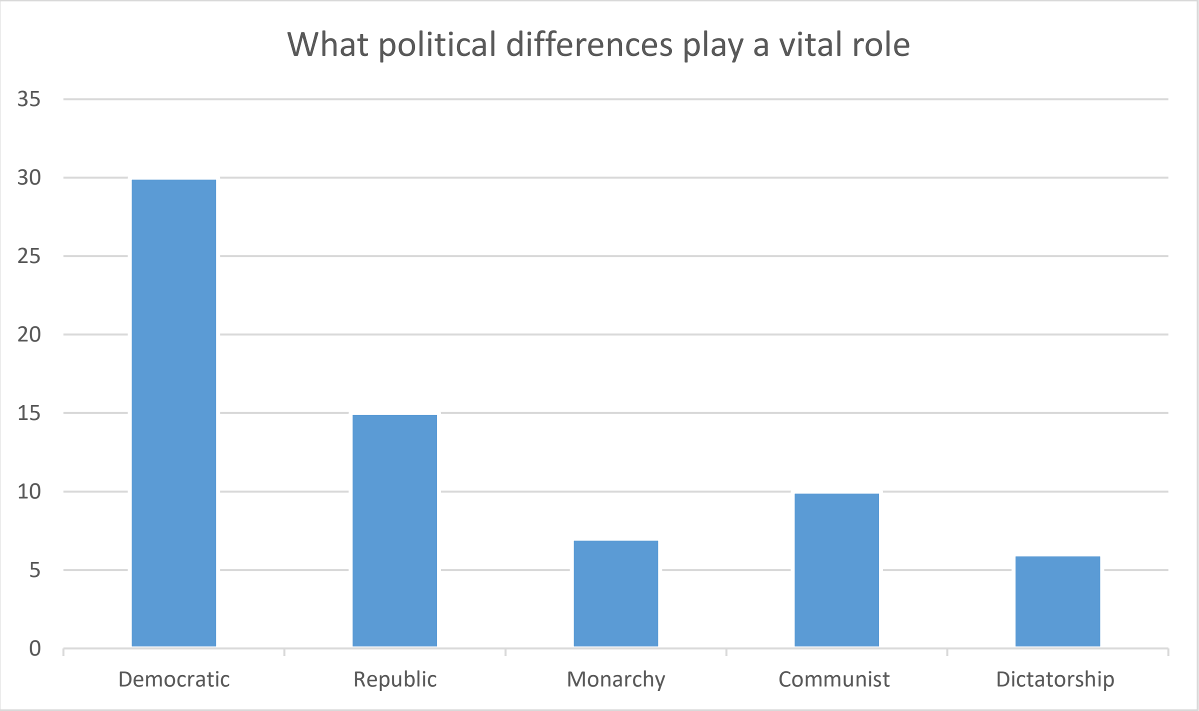


Figure E.275: What political differences play a vital role (Less than a year-UK)

The majority have chosen a democratic political system (See figure E.275), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

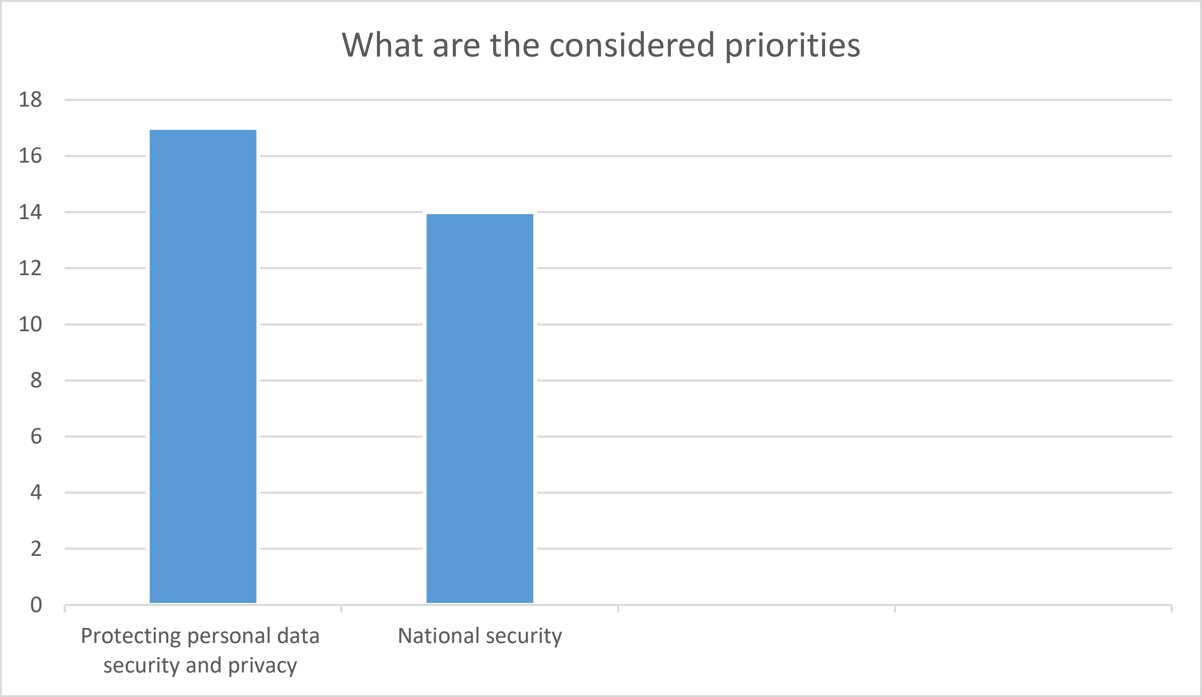


Figure E.276: What are the considered priorities (Less than a year-UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security, which is a significant factor (See figure E.276). In an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

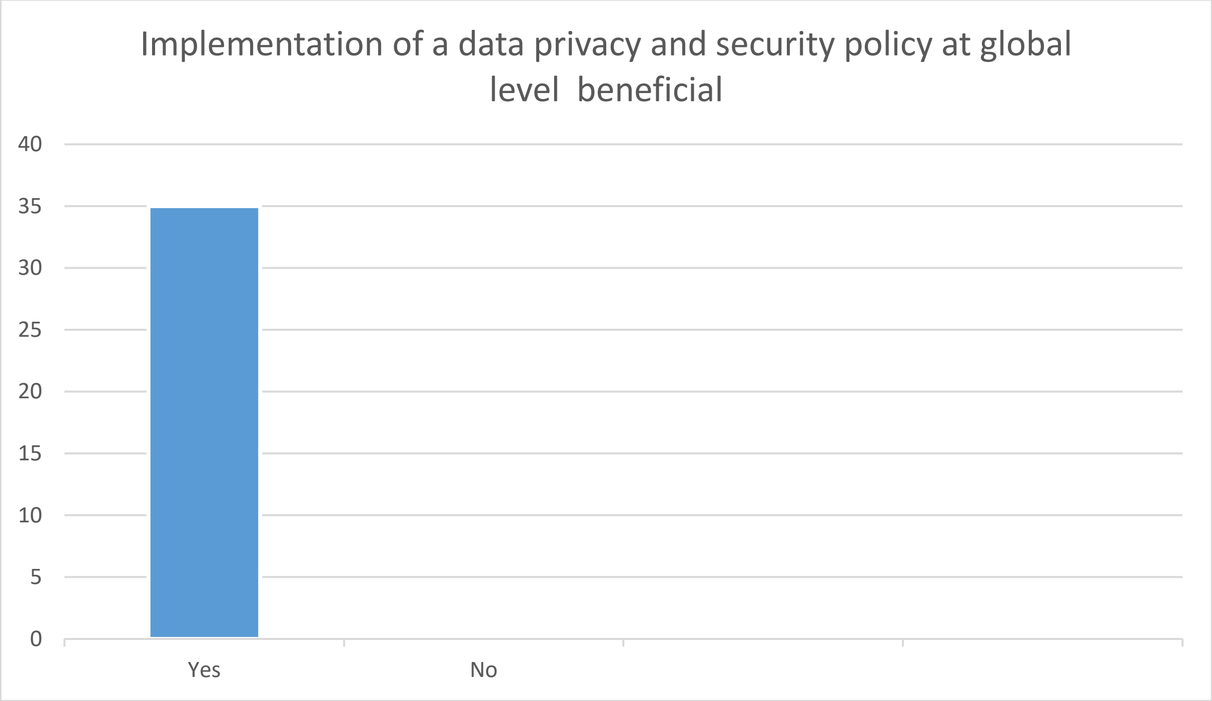


Figure E.277: Implementation of a data privacy and security policy at global level beneficial (Less than a year-UK)

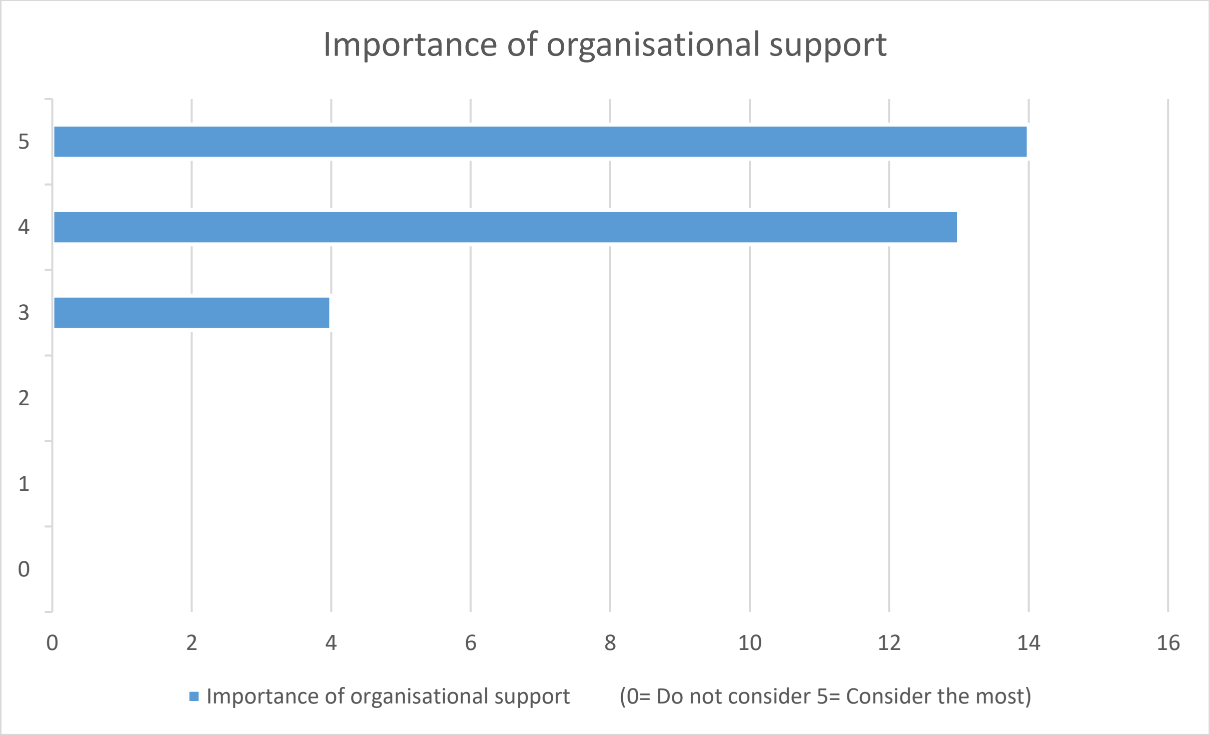


Figure E.278: Importance of organisational support (Less than a year-UK)

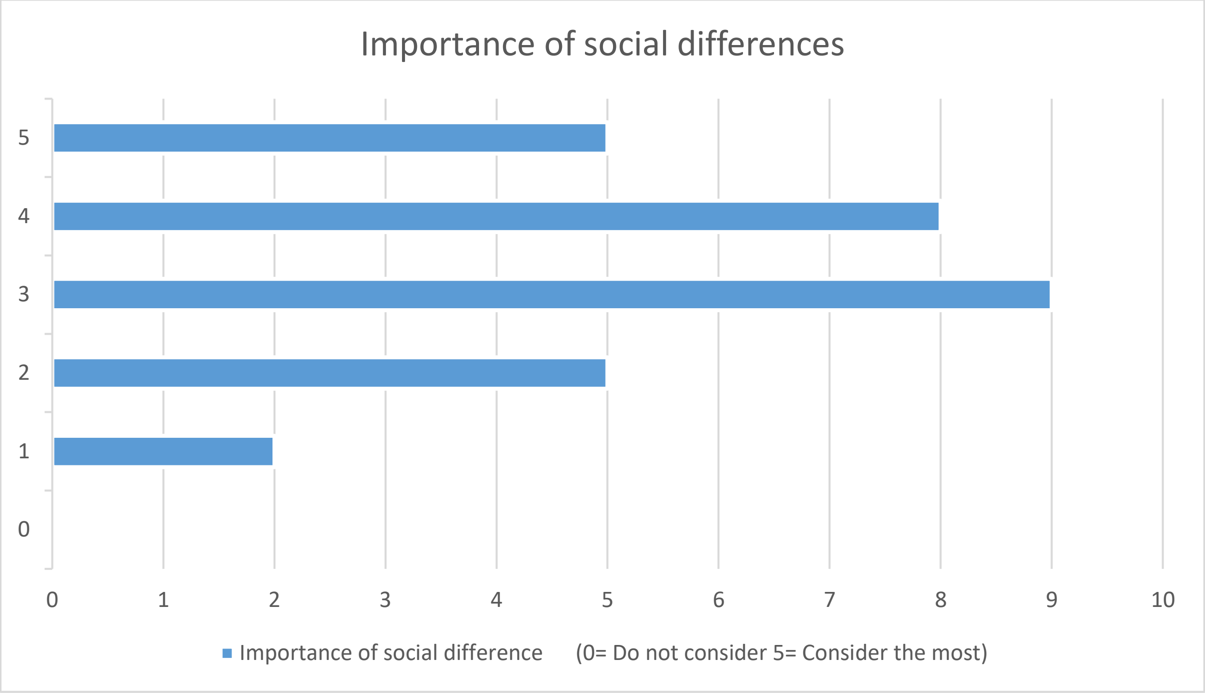


Figure E.279: Importance of social differences (Less than a year-UK)

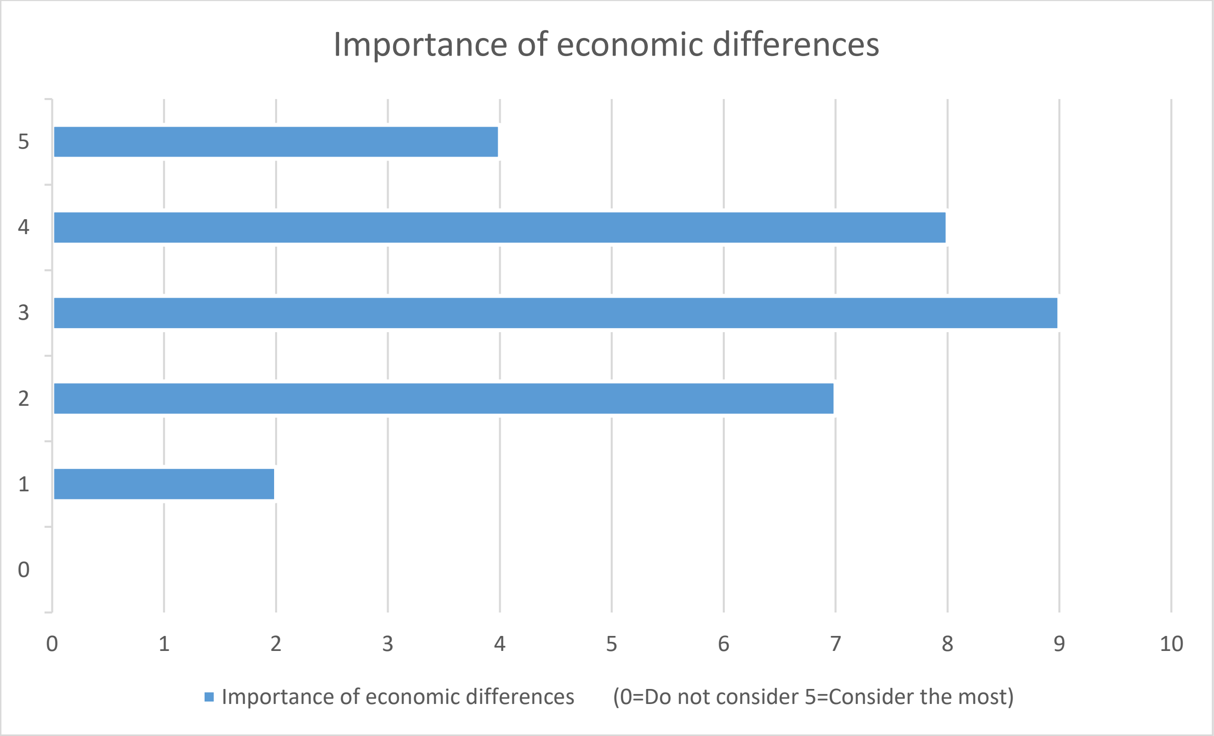


Figure E.280: Importance of economic differences (Less than a year-UK)

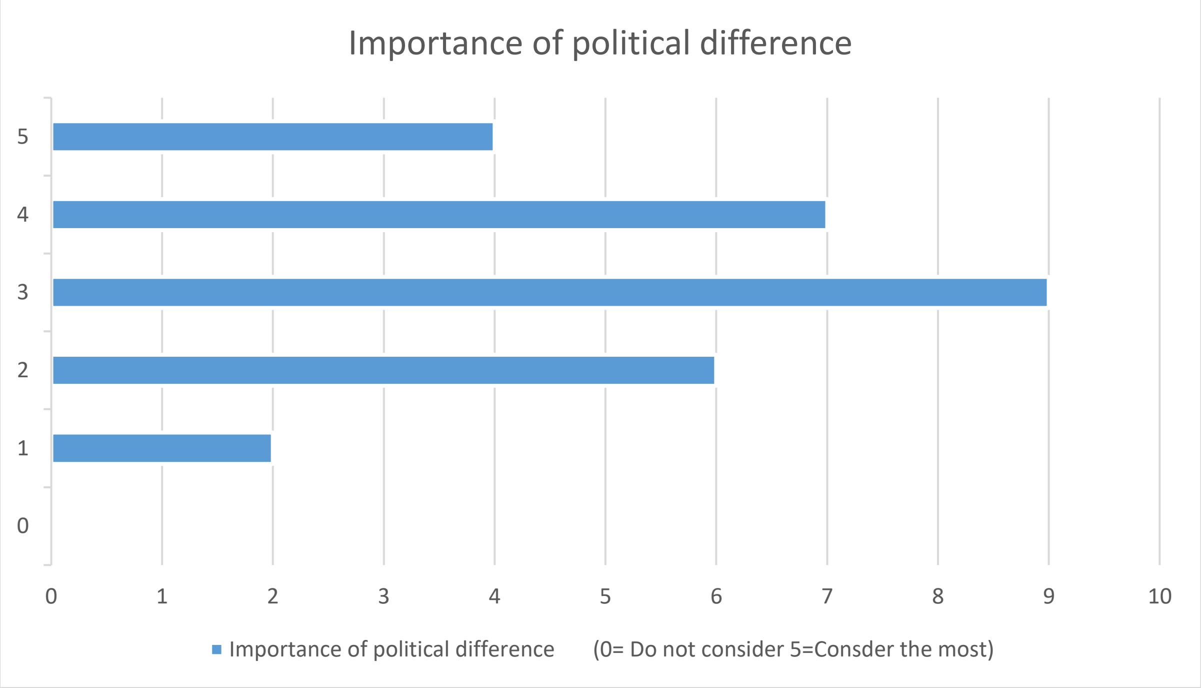


Figure E.281: Importance of political difference (Less than a year-UK)

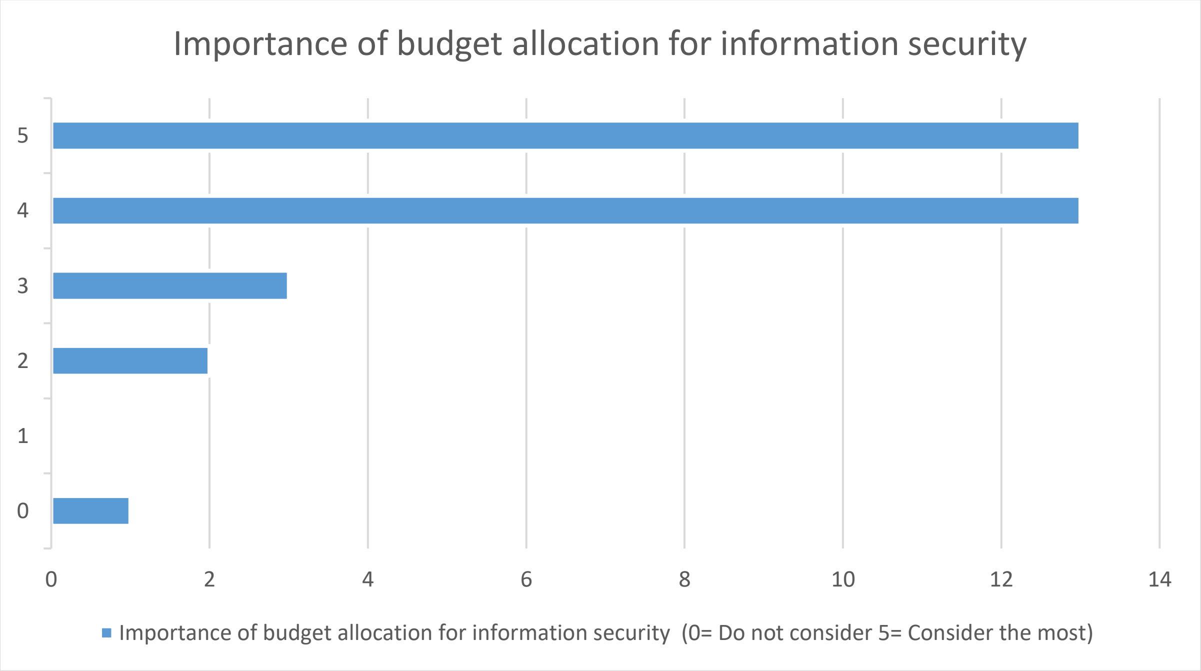


Figure E.282: Importance of budget allocation for information security (Less than a year-UK)

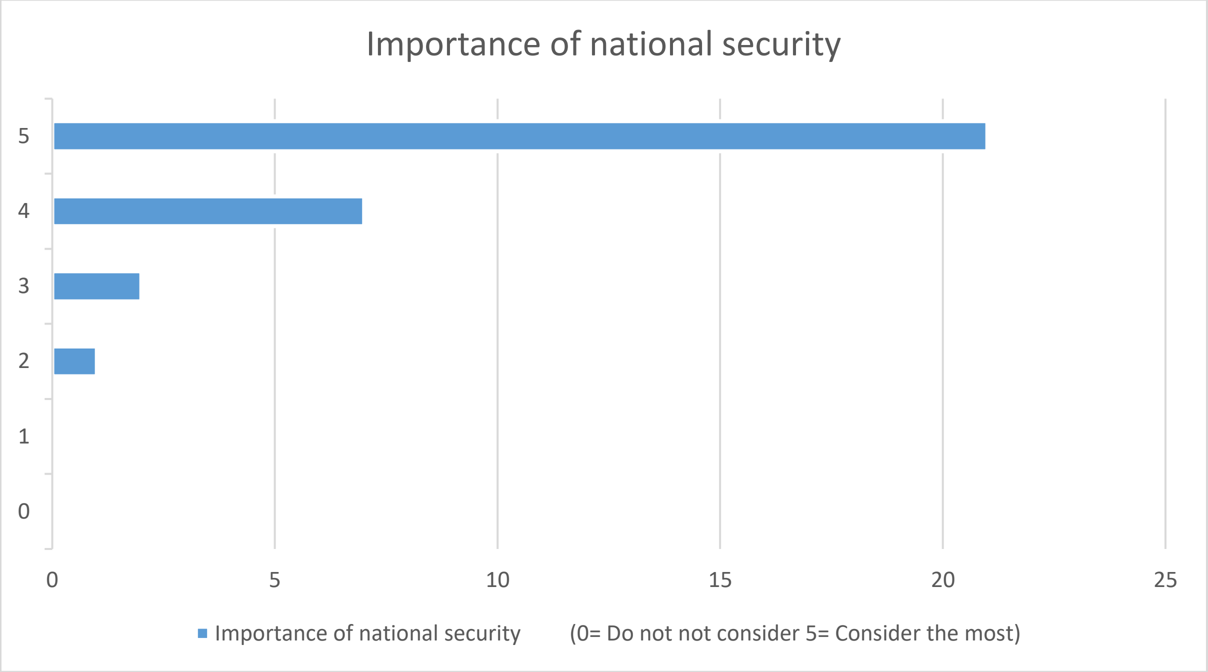


Figure E.283: Importance of national security (Less than a year-UK)

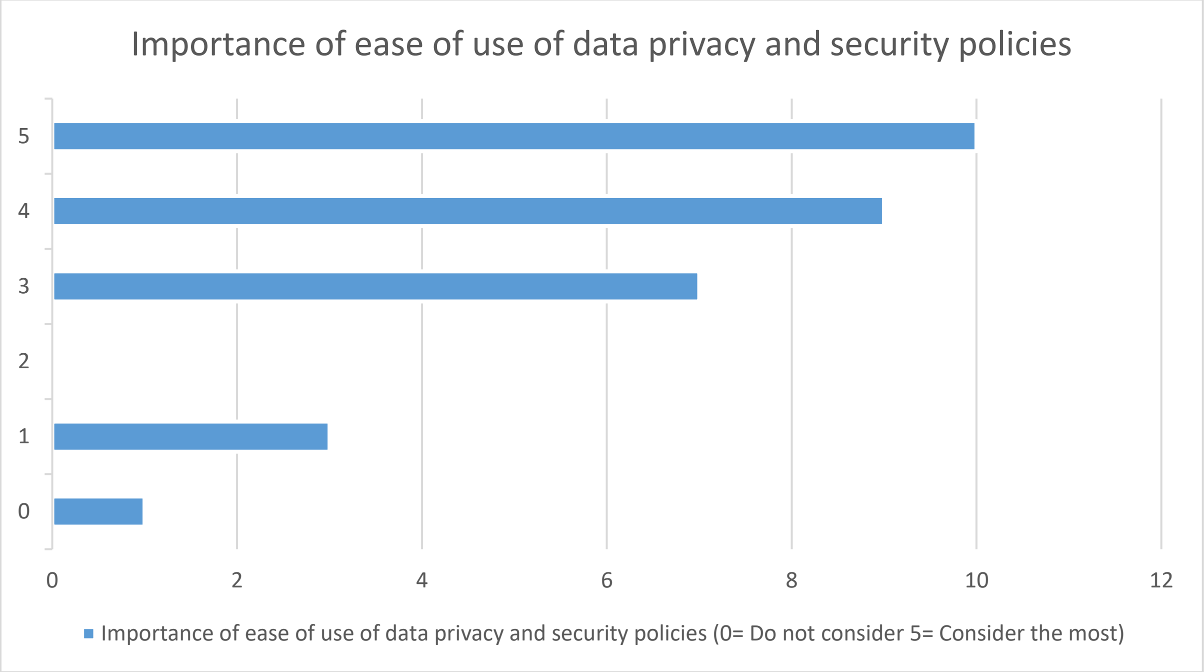


Figure E.284: Importance of ease of use of data privacy and security policies (Less than a year-UK)

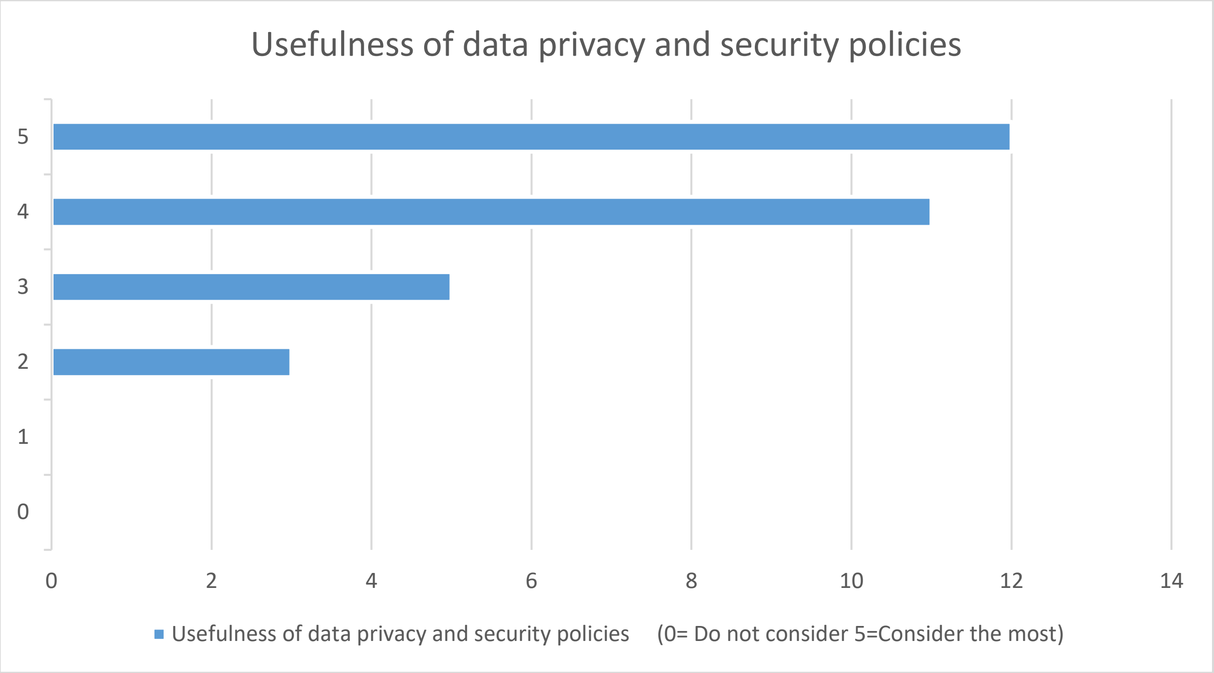


Figure E.285: Usefulness of data privacy and security policies (Less than a year-UK)

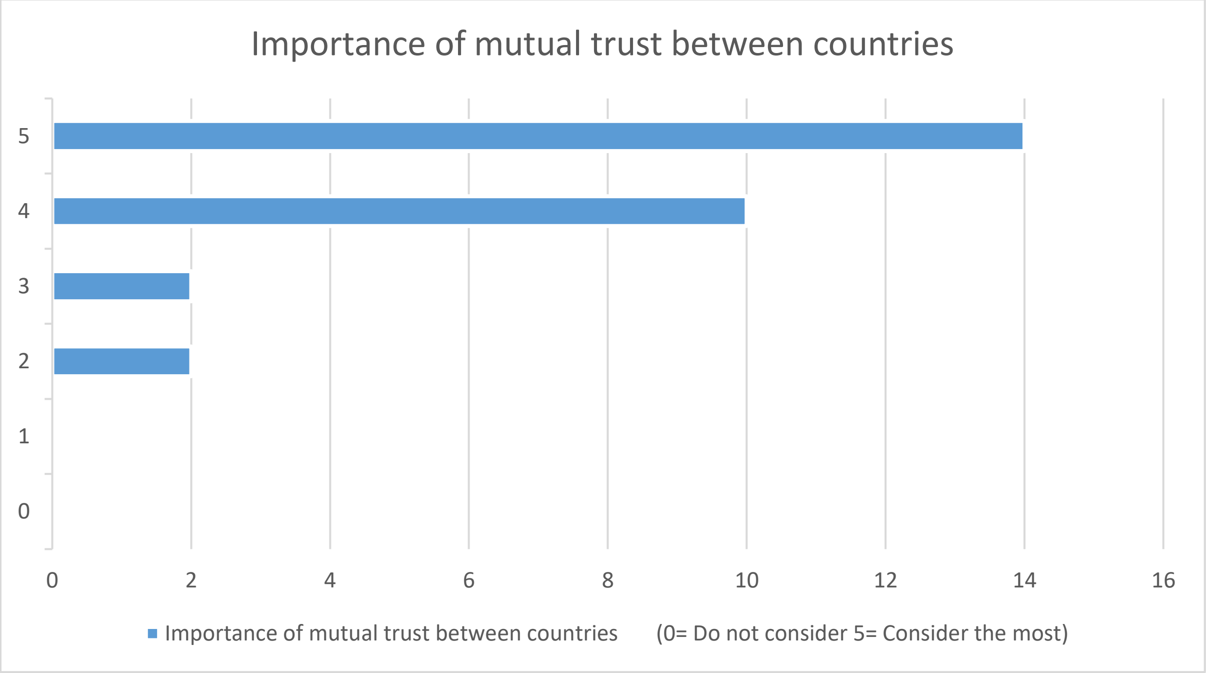


Figure E.286: Importance of mutual trust between countries (Less than a year-UK)

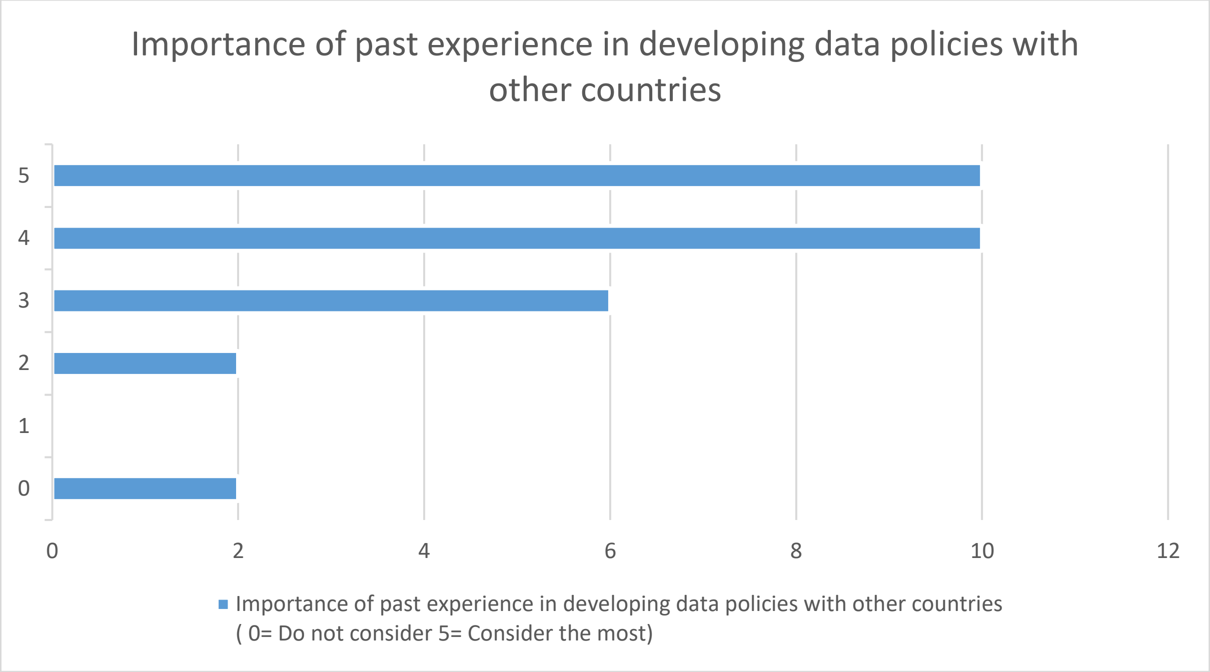


Figure E.287: Importance of past experience in developing data policies with other counties (Less than a year-UK)

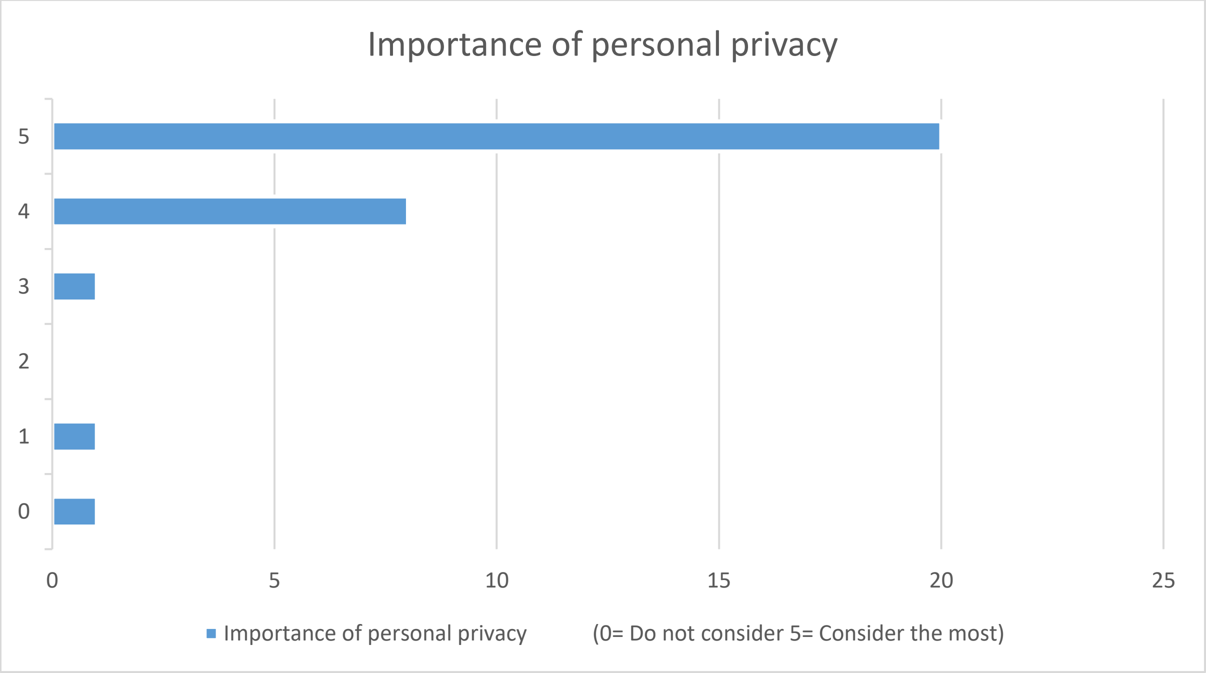


Figure E. 288: Importance of personal privacy (Less than a year-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 78 percent of the respondents have endorsed (See figure E.277). The other notable factors that have come out of the survey are organisational support, budget allocation, political differences, social differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure E.266-276) (See figure E.278-288).

United Kingdom – 1-5 years

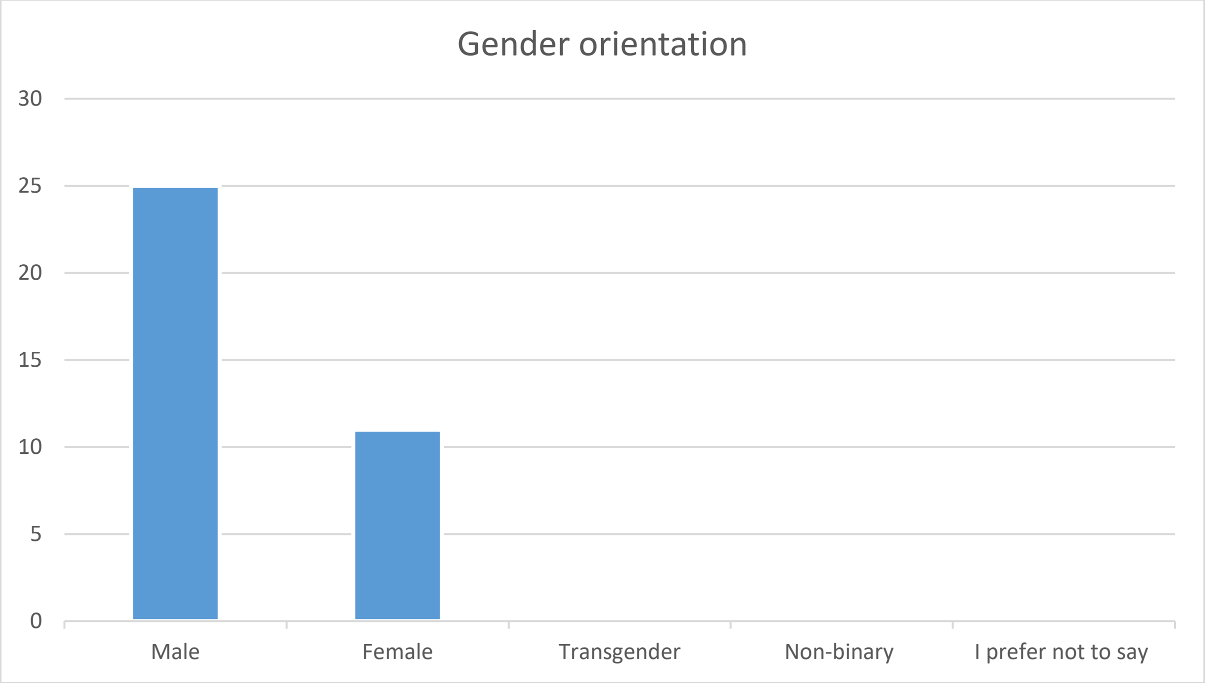


Figure E.289: Gender orientation (1-5 years UK)

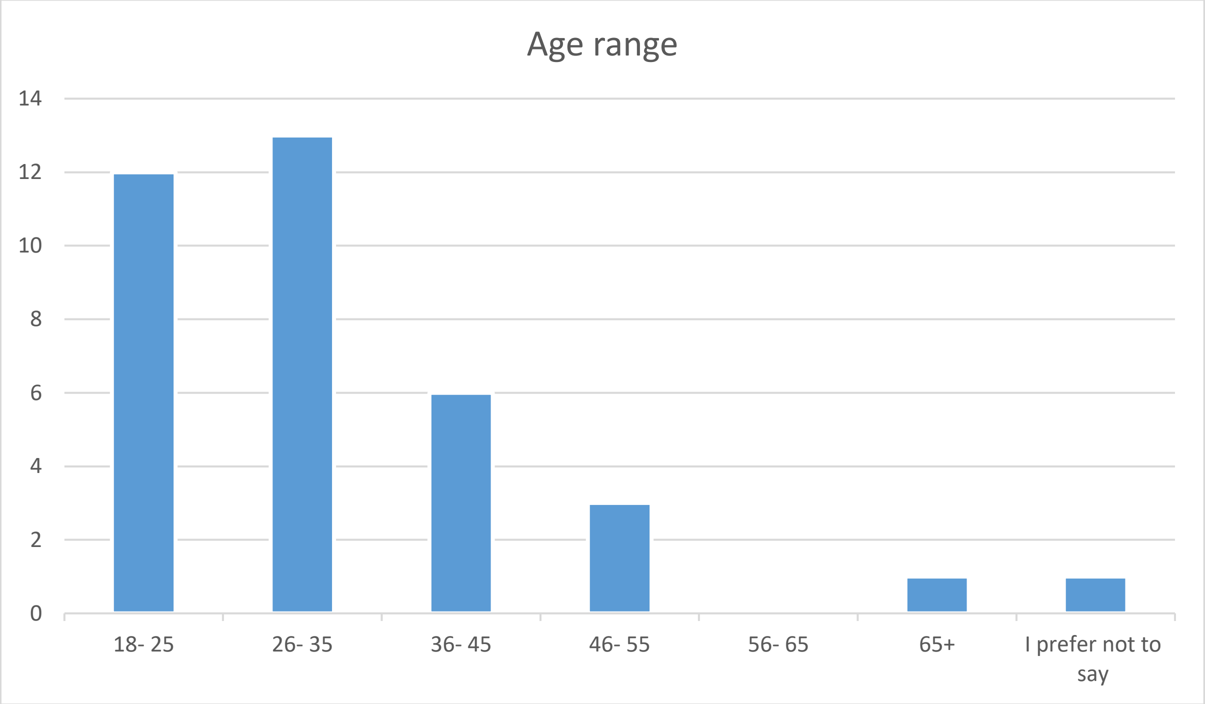


Figure E.290: Age range (1-5 years UK)

This analysis is based on the responses received from United Kingdom participants with 1 to 5 years of employment in the industry. There were 36 participants and 25 out of them were males and 11 females (See figure E.289). They were within the 18-65+ age range, and 1 participant has not revealed the age. 12 in the 18-25, 13 in the 26-35, 6 in the 36-45, 3 in the 46-55, and 1 over 65 range (See figure E.290).

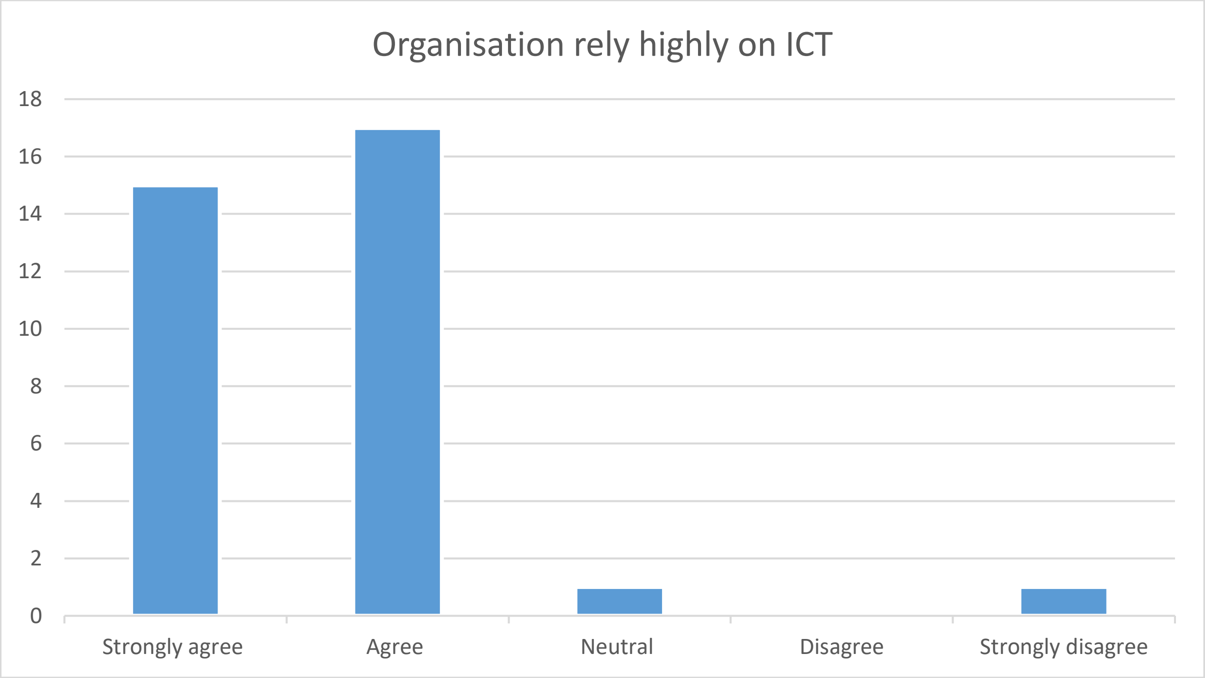


Figure E.291: Organisation rely highly on ICT (1-5 years UK)

Out of the 36 respondents, 32 have worked in a technology reliance working environment, 1 unaware of reliance on technology because of the nature of the work assigned to them, 1 have marked ‘disagree’ on ICT (See figure E.291). This indicates a majority of those who have been working in an organisation for 1-5 years have a high reliance on ICT.

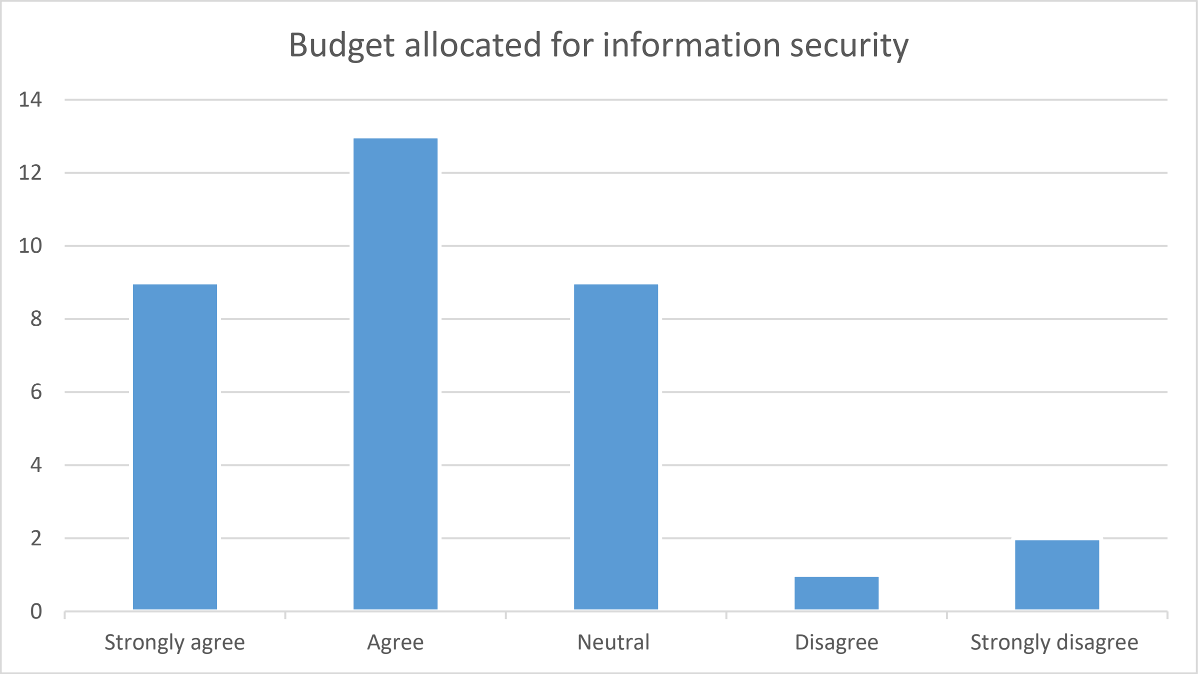


Figure E.292: Budget allocated for information security (1-5 years UK)

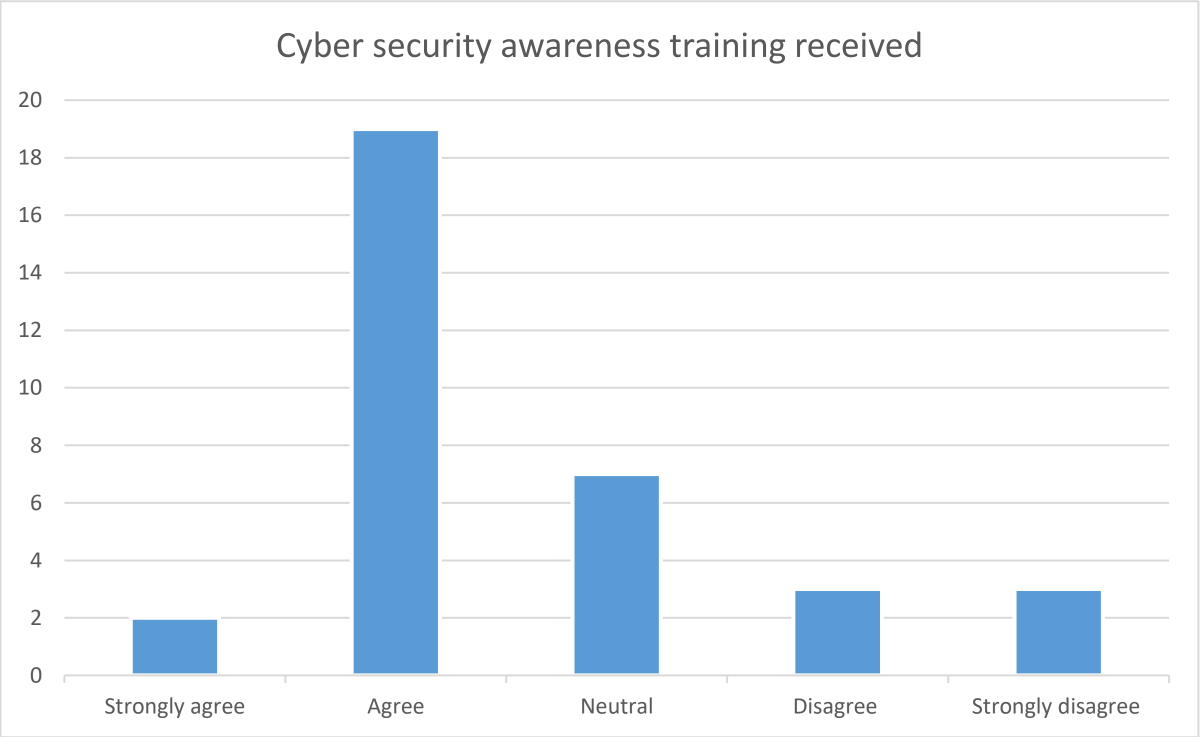


Figure E.293: Cyber security awareness training received (1-5 years UK)

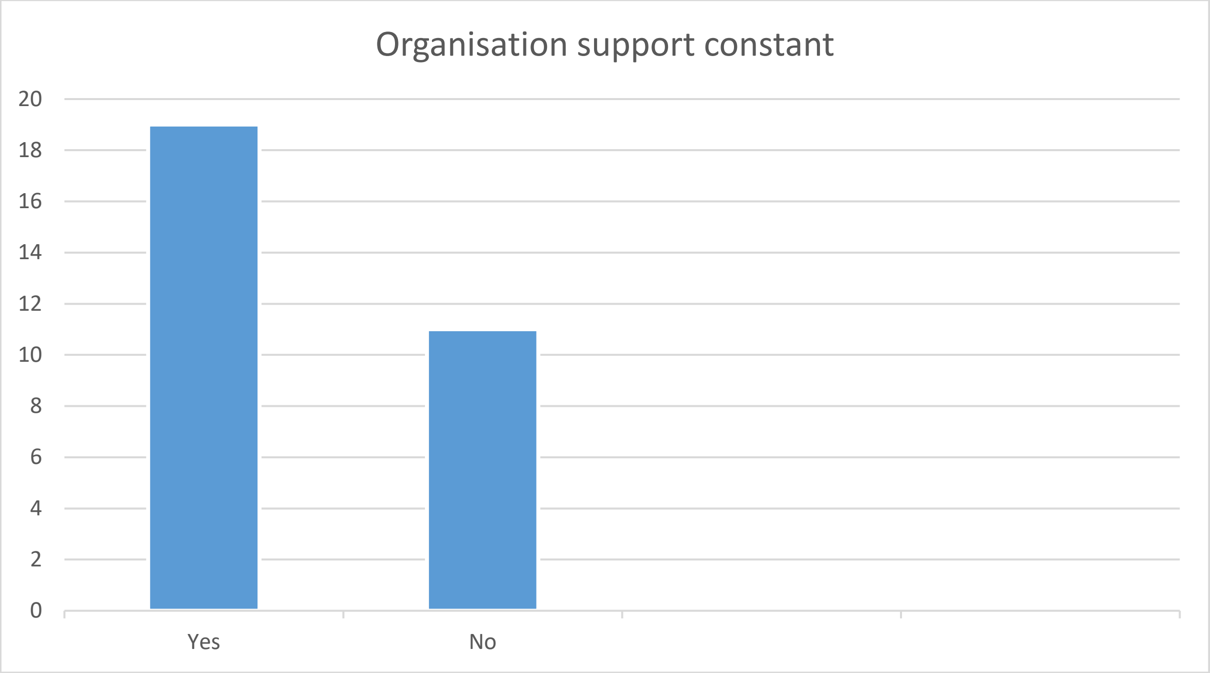


Figure E.294: Organisation support constant (1-5 years UK)

Funding has been sketchy. 22 out of the 36 have indicated that their organisations had an allocated budget for information security, whilst 9 had not expressed an opinion either way and notably according to the 3 disagreed, their organisations had no budget allocation for information security (See figure E.292). According to some of the participants, regular security awareness training received was adequate despite the satisfactory level of resources allocated for information security. 21 participants have received regular cybersecurity awareness training, whilst 7 neither agreed nor disagreed, and 6 participants had not regularly received security awareness training (See figure E.293). In addition, only 11 participants had not received support from the organisation to protect personal information, whilst only 19 did (See figure E.294). This suggest that organisations understand the importance of data protection, and provide funding for training and support.

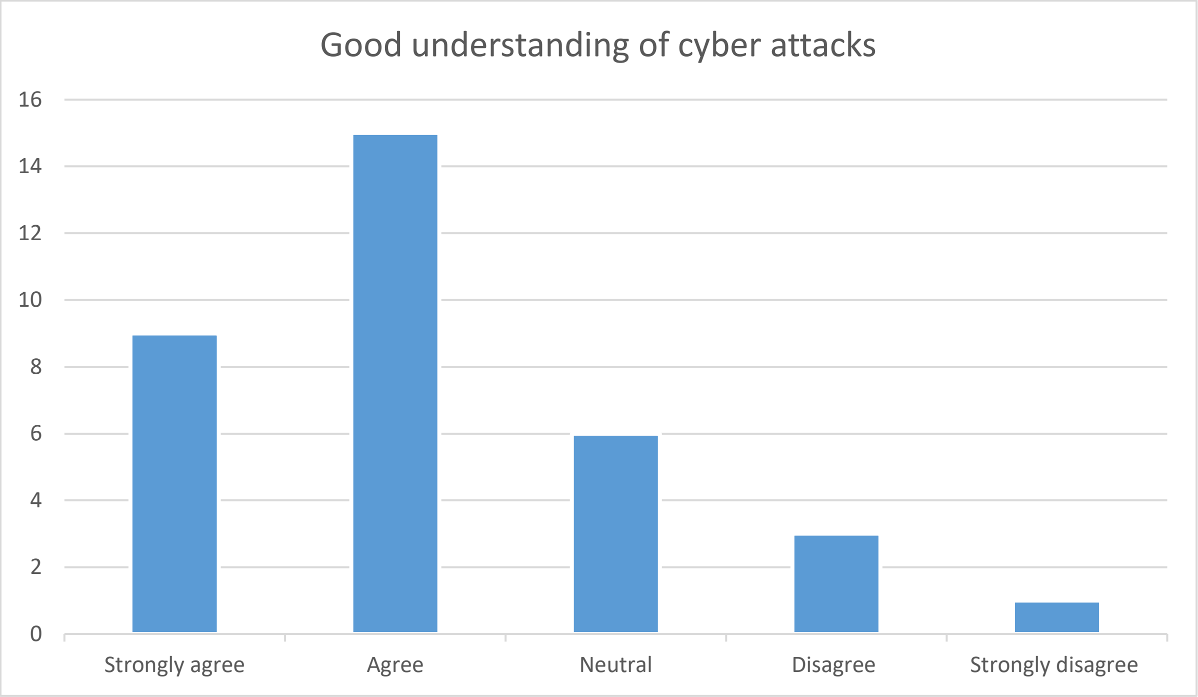


Figure E.295: Good understanding of cyberattacks (1-5 years UK)

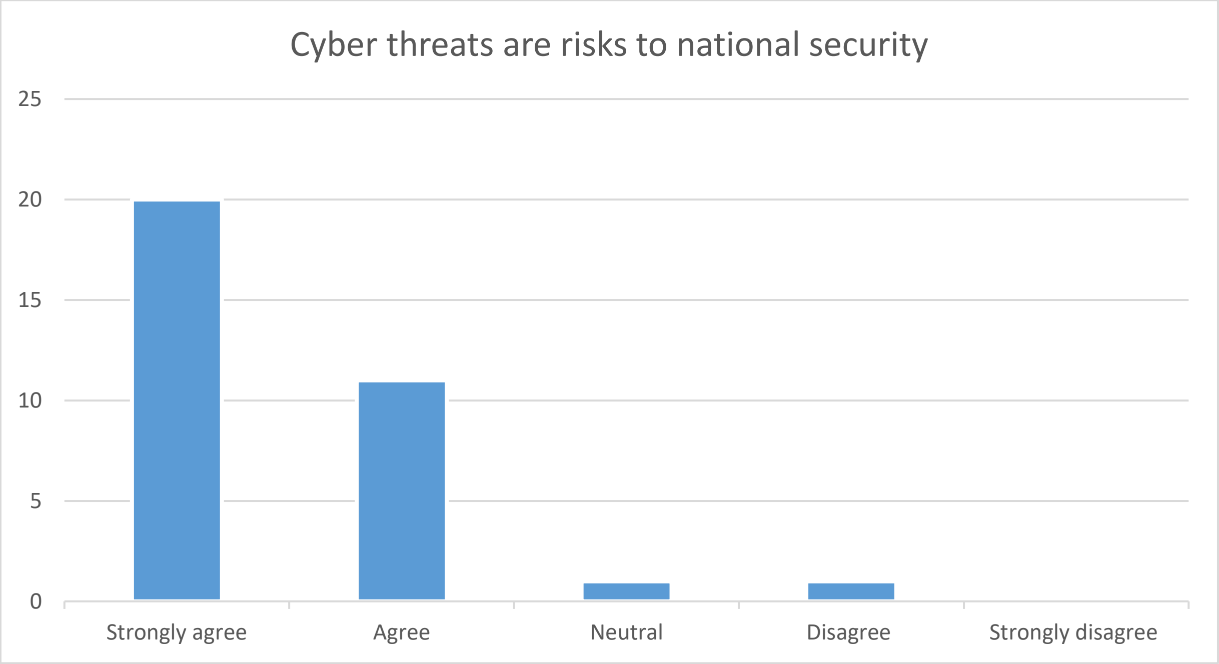


Figure E.296: Cyber threats are risks to national security (1-5 years UK)

Despite the security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 24 participants do have, 6 have not expressed opinion either way, and only 4 participants had no understanding (See figure E.295). Furthermore, 86 percent of the participants also realises the potential threats to national security from cyber-attacks (See figure E.296). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

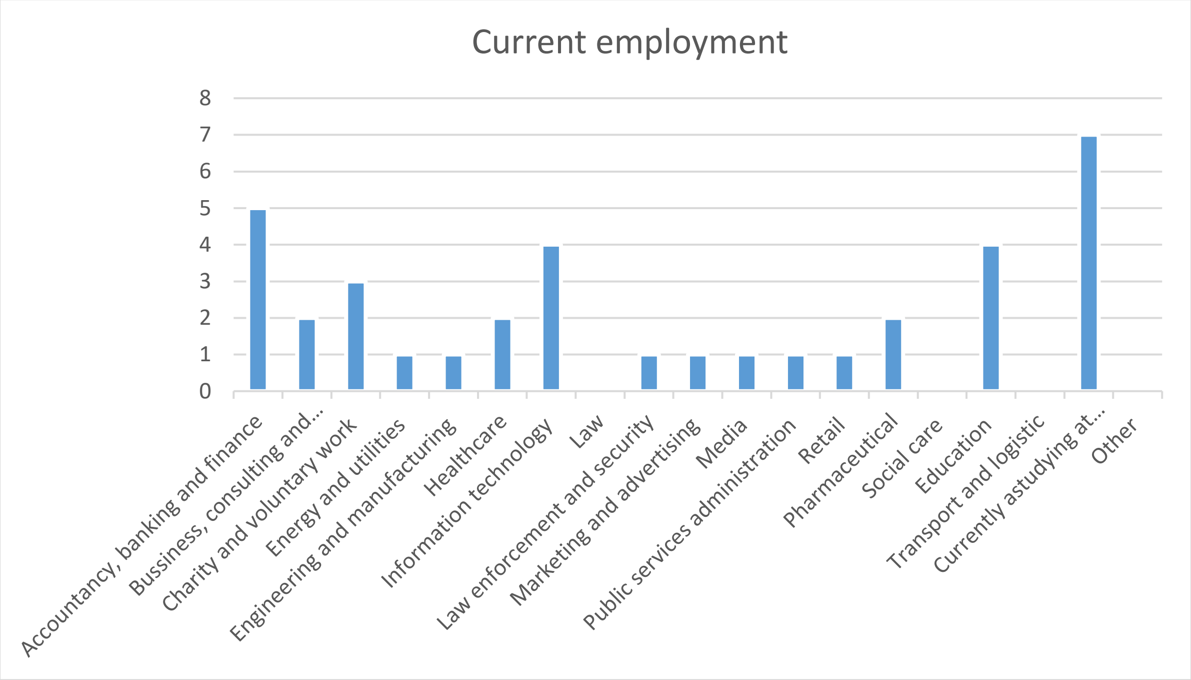


Figure E.297: Current employment (1-5 years UK)

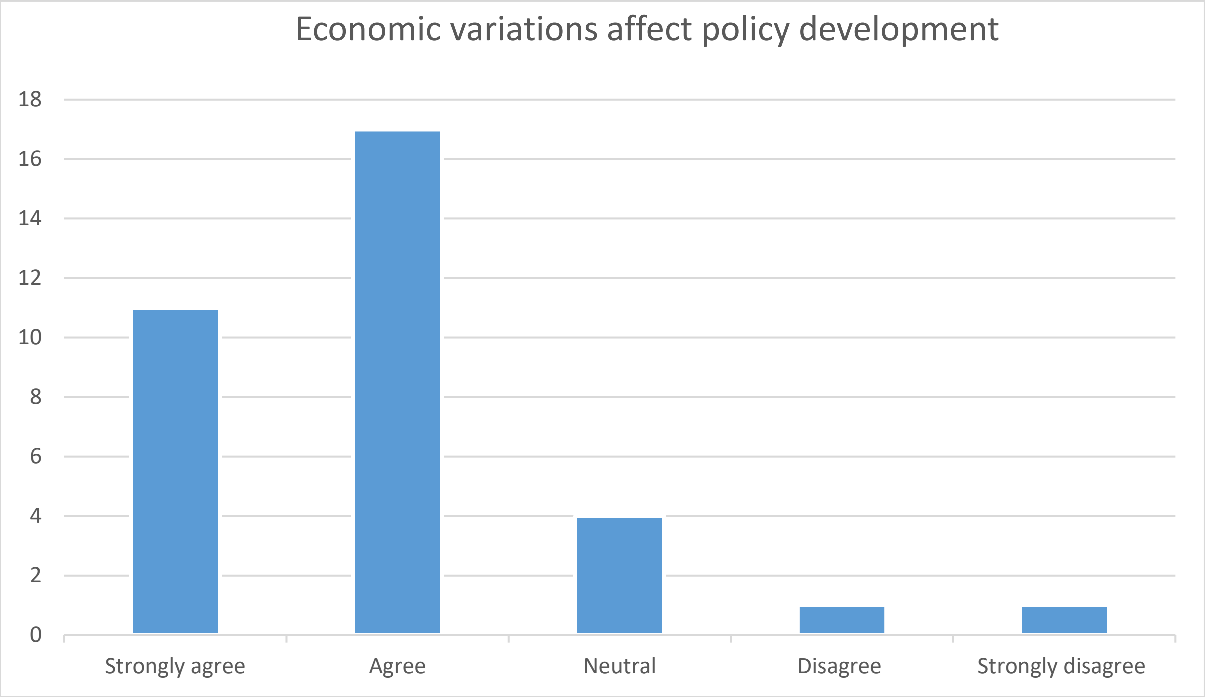


Figure E.298: Economic variations affect policy development (1-5 years UK)

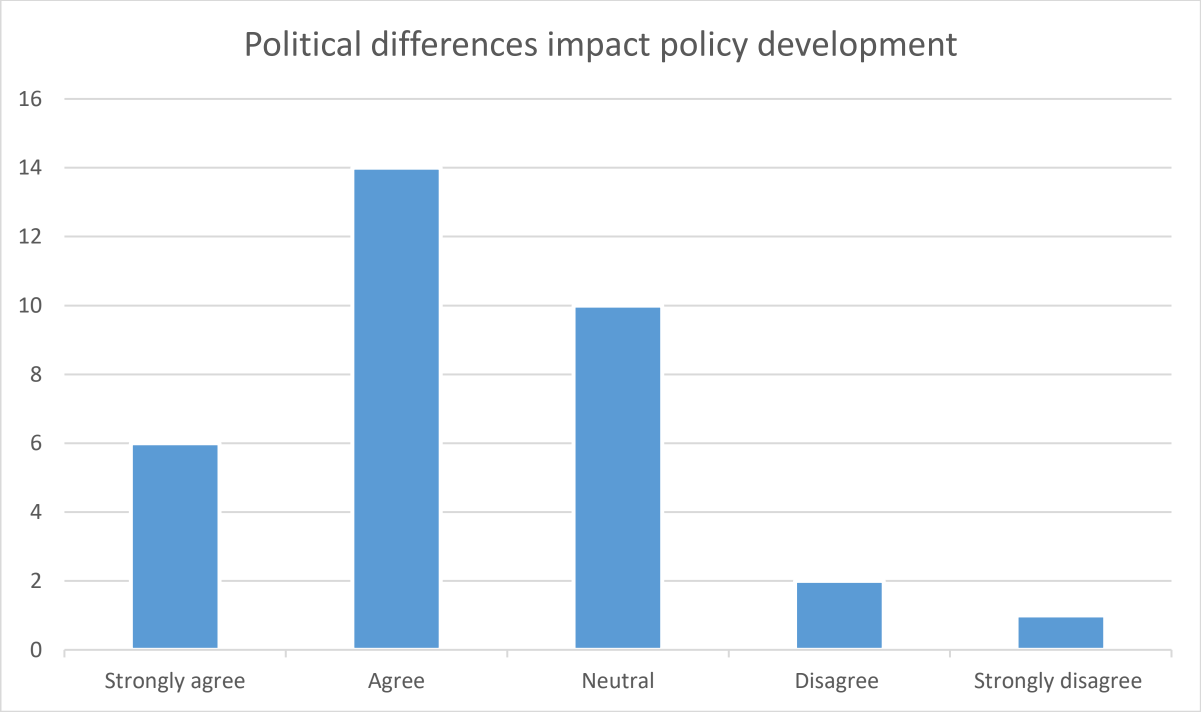


Figure E.299: Political differences impact policy development (1-5 years UK)

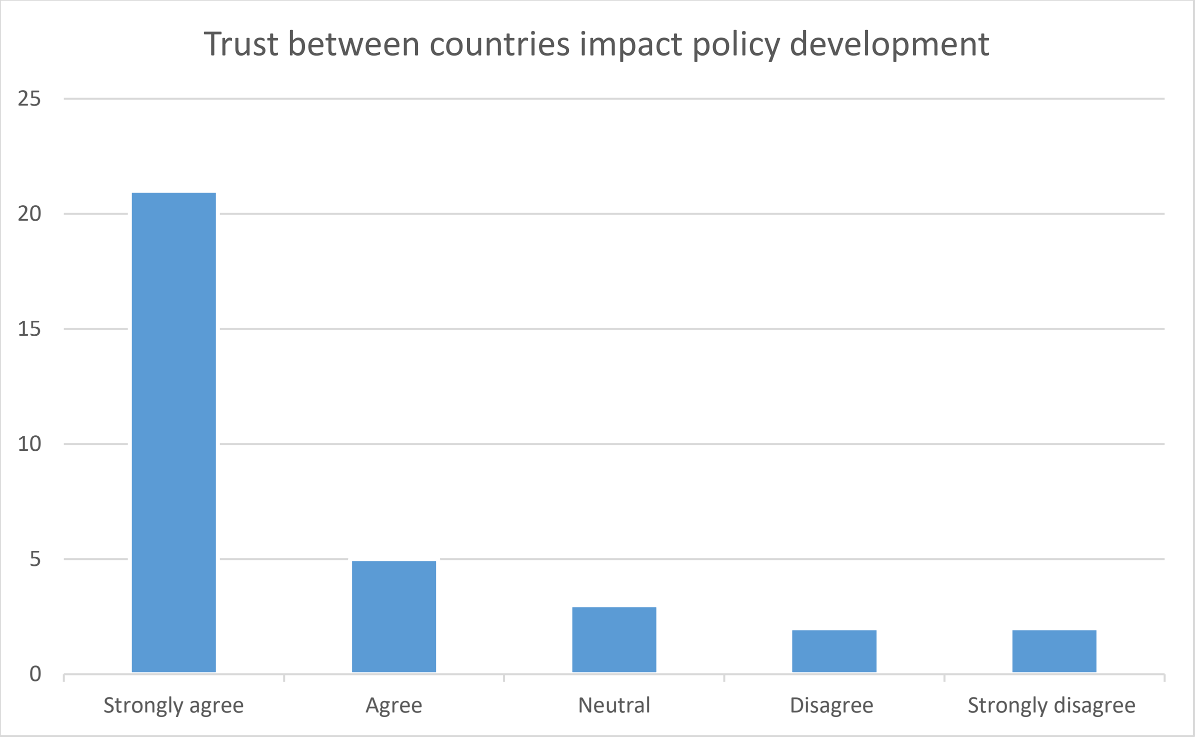


Figure E.300: Trust between countries impact policy development (1-5 years UK)

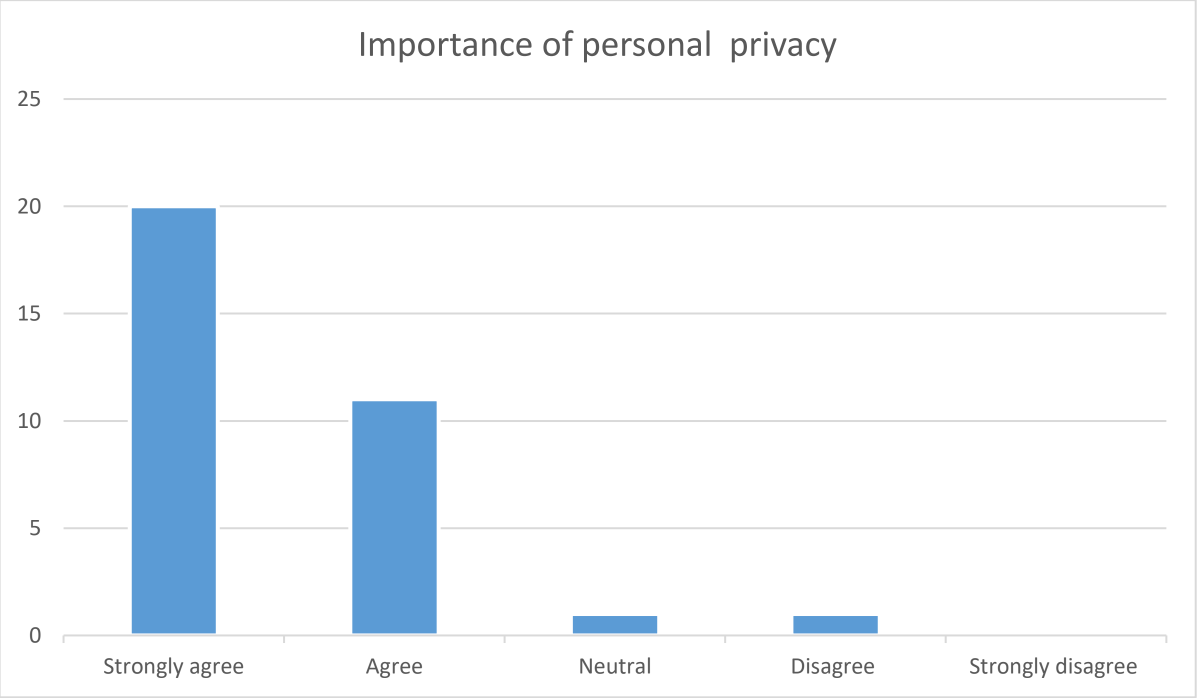


Figure E.301: Importance of personal privacy (1-5 years UK)

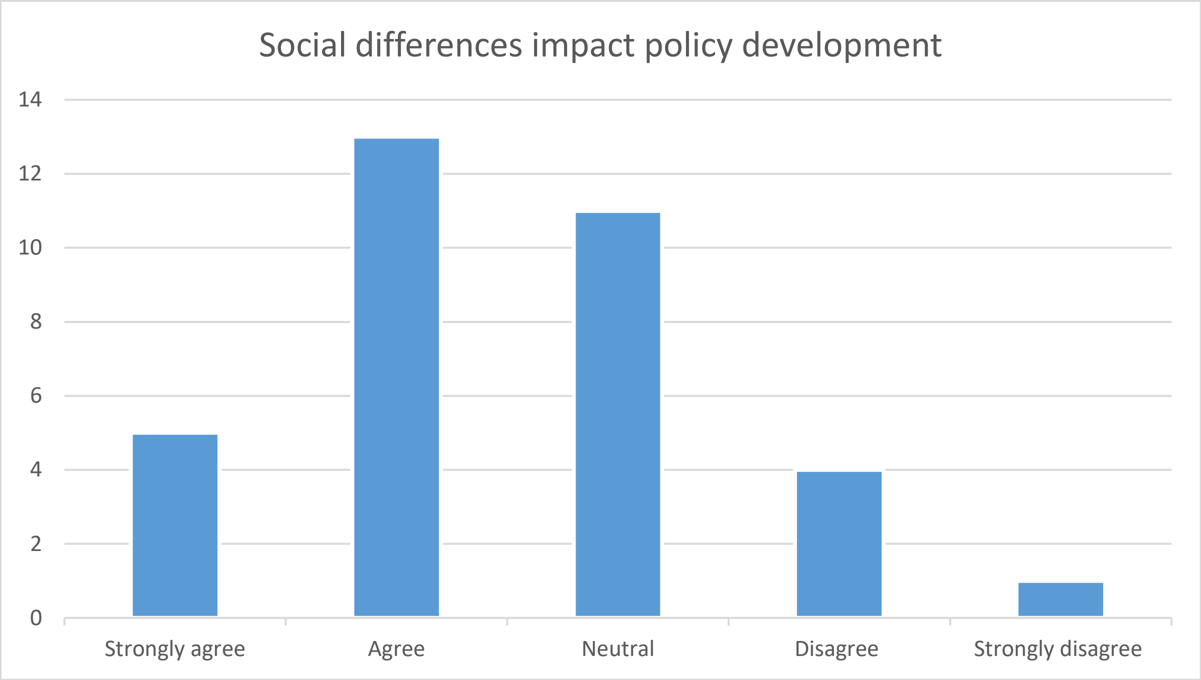


Figure E.302: Social differences impact policy development (1-5 years UK)

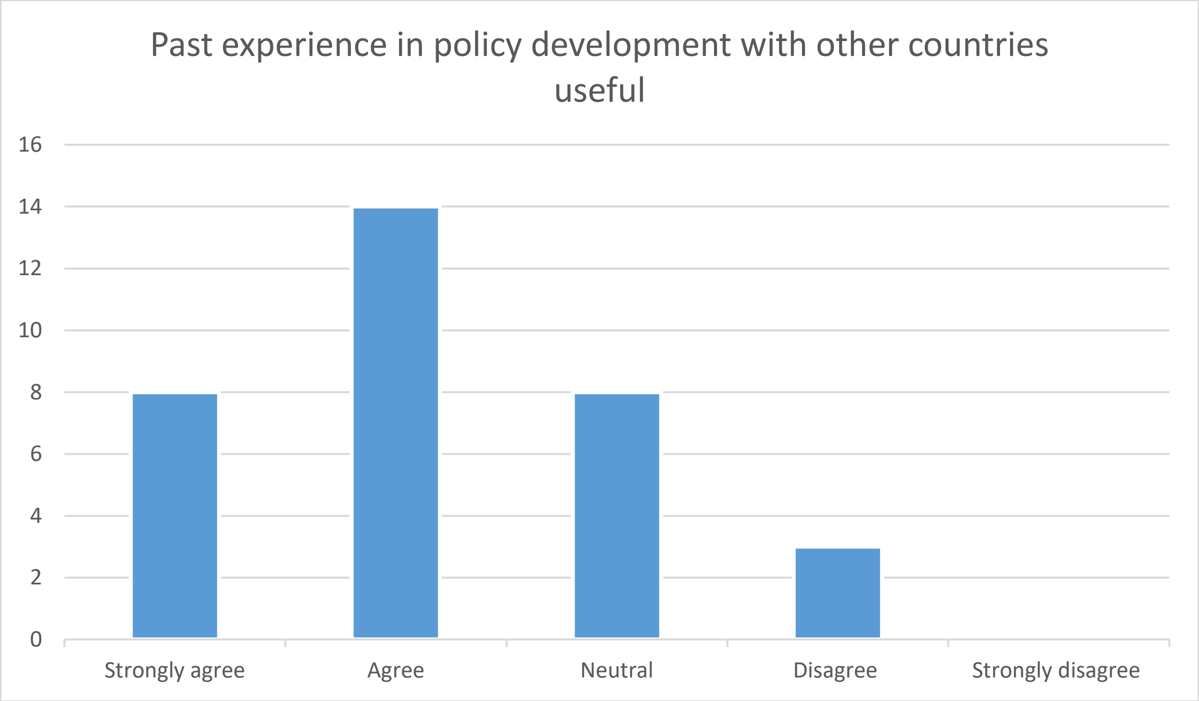


Figure E.303: Past experience in policy development with other countries useful (1-5 years UK)

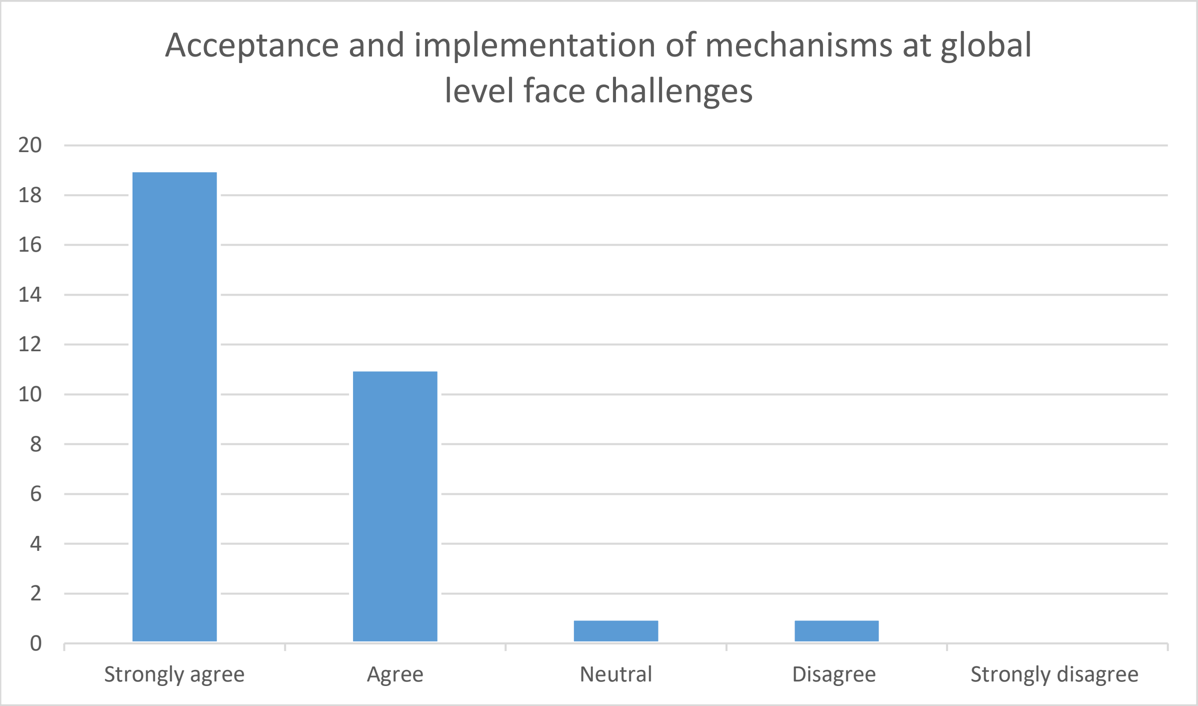


Figure E.304: Acceptance and implementation of mechanisms at global level face challenges (1-5 years UK)

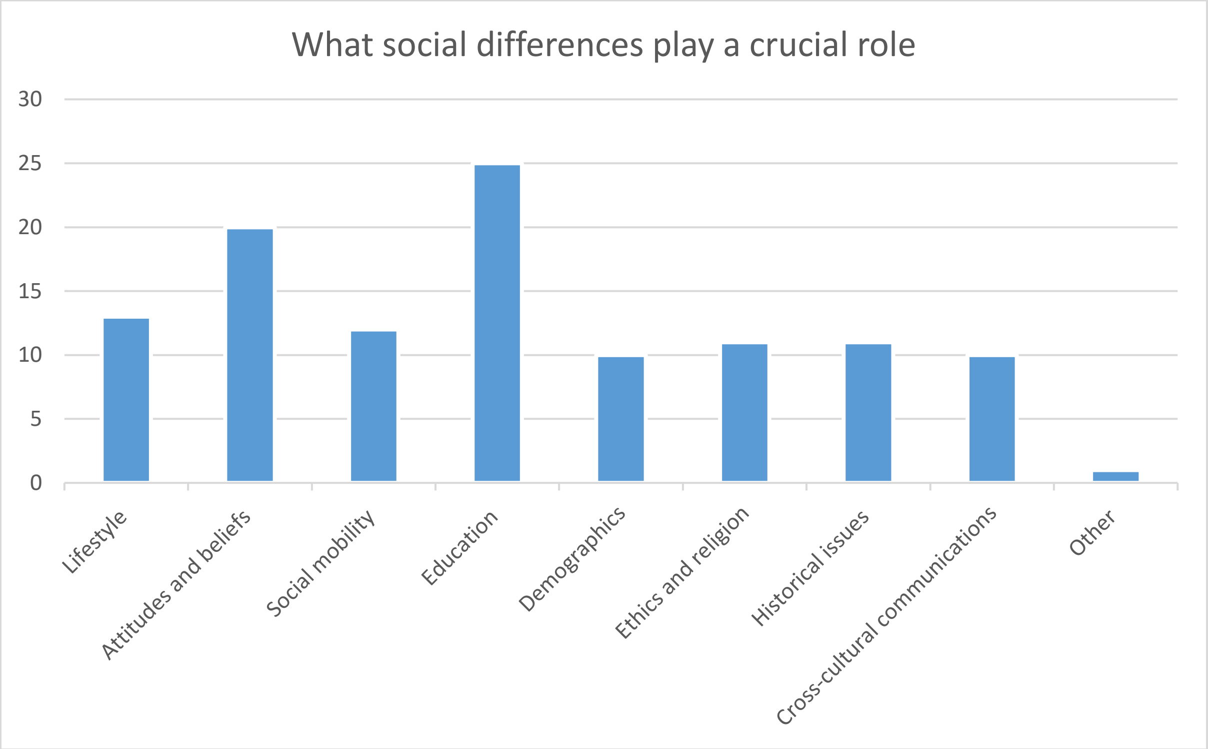


Figure E.305: What social differences play a crucial role (1-5 years UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure E.305). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

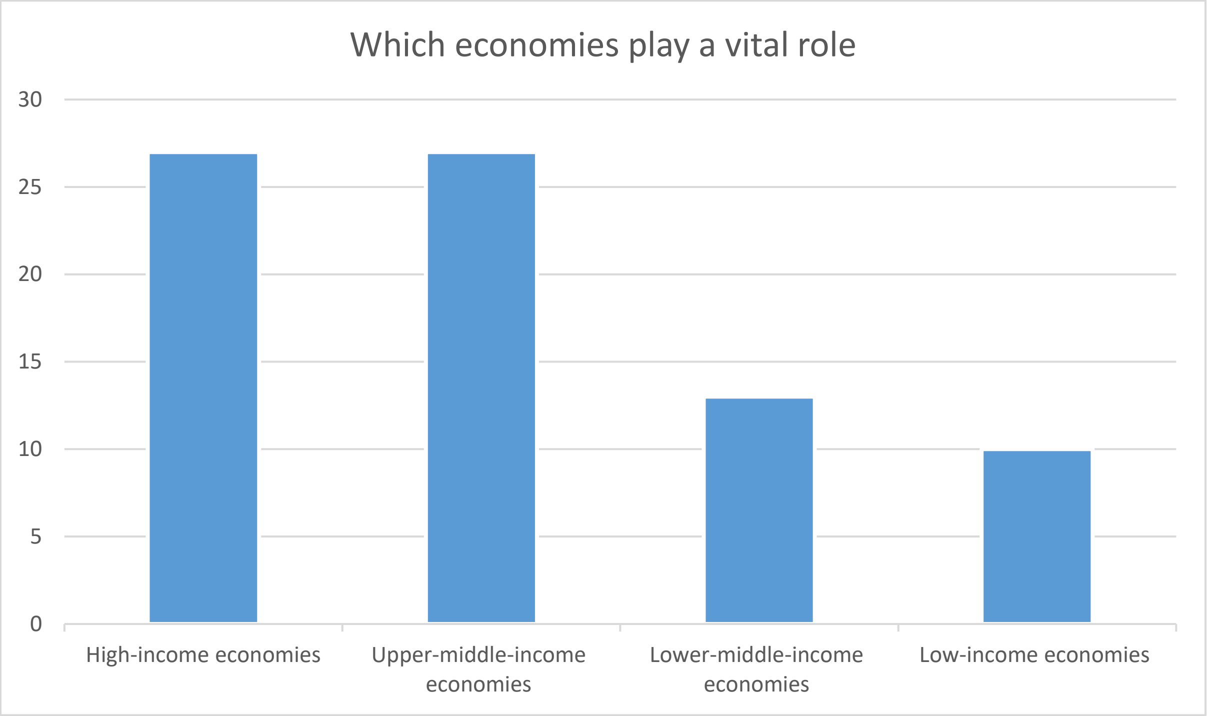


Figure E.306: Which economies play a vital role (1-5 years UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.306). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

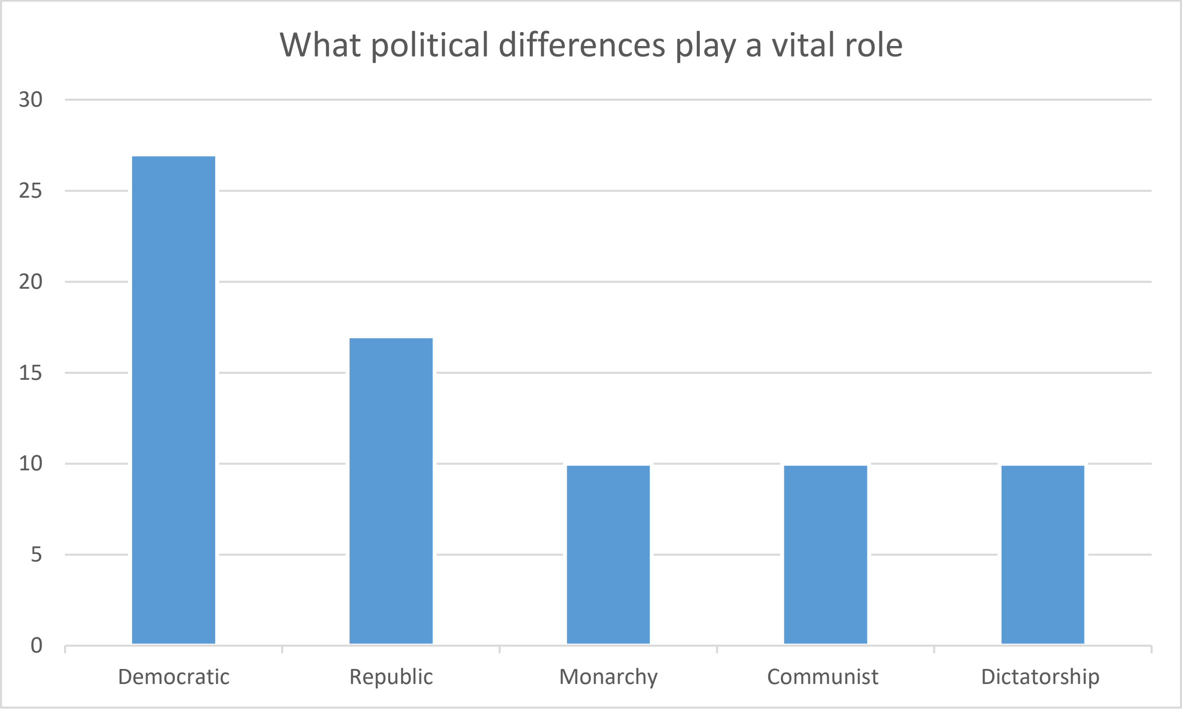


Figure E.307: What political differences play a vital role (1-5 years UK)

The majority have chosen a democratic political system (See figure E.307), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

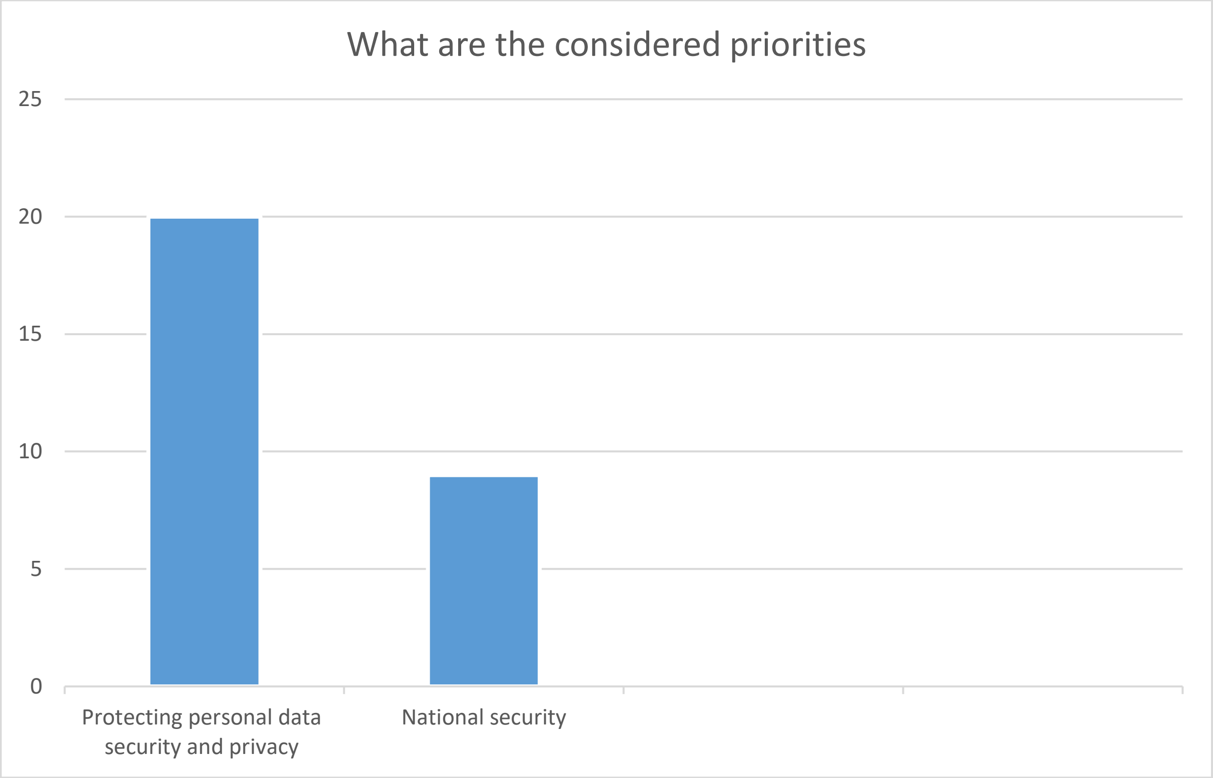


Figure E.308: What are the considered priorities (1-5 years UK)

In accepting and implementing global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security (See figure E.308), which is a significant factor. However, in an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

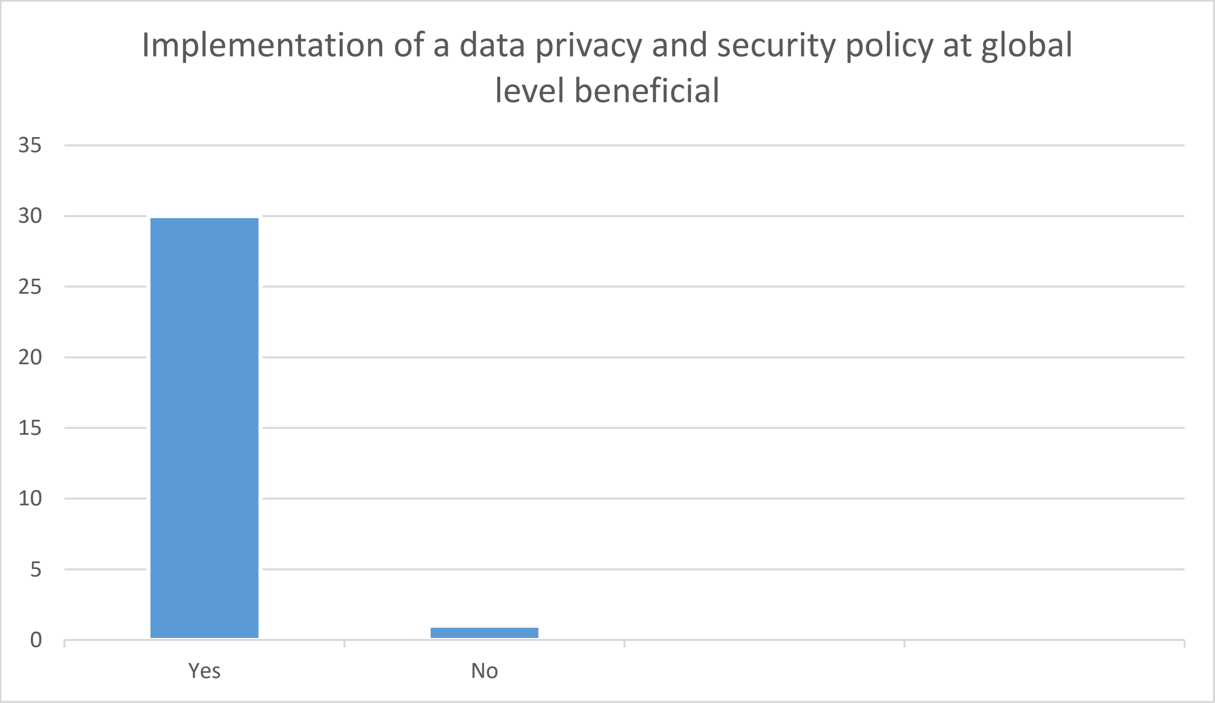


Figure E.309: Implementation of a data privacy and security policy at global level beneficial (1-5 years UK)

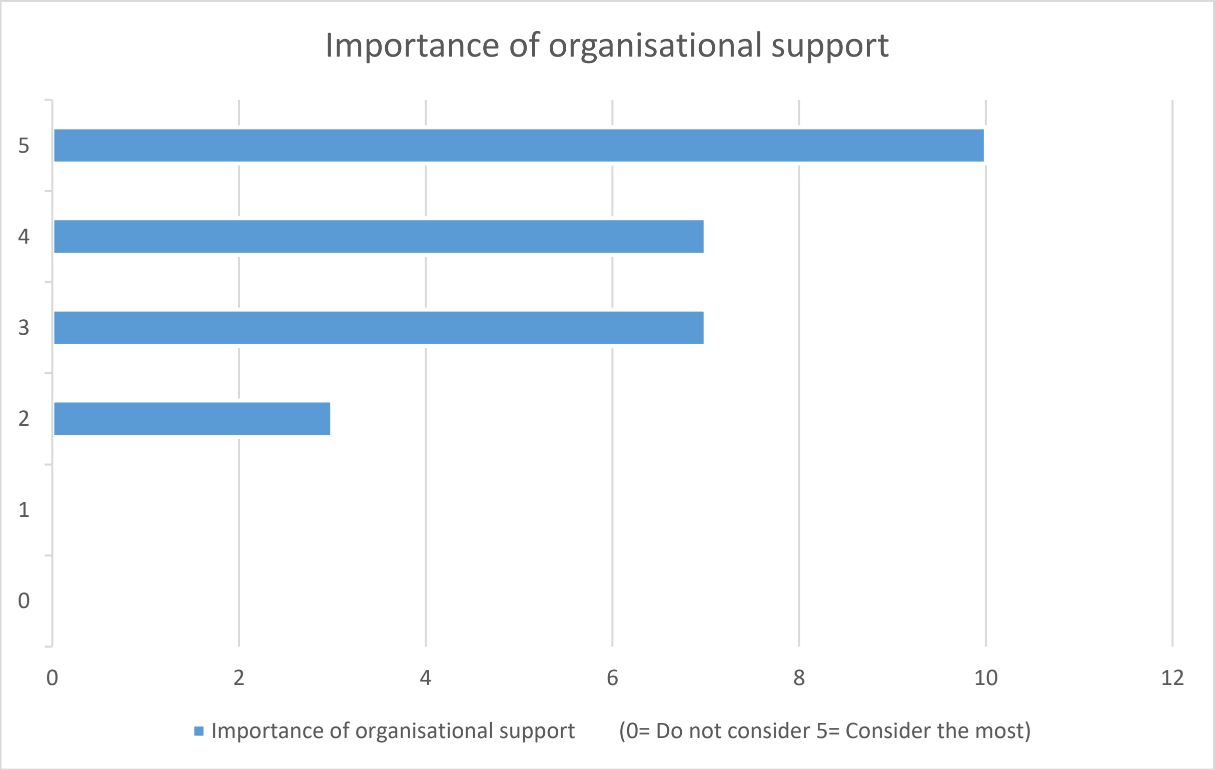


Figure E.310: Importance of organisational support (1-5 years UK)

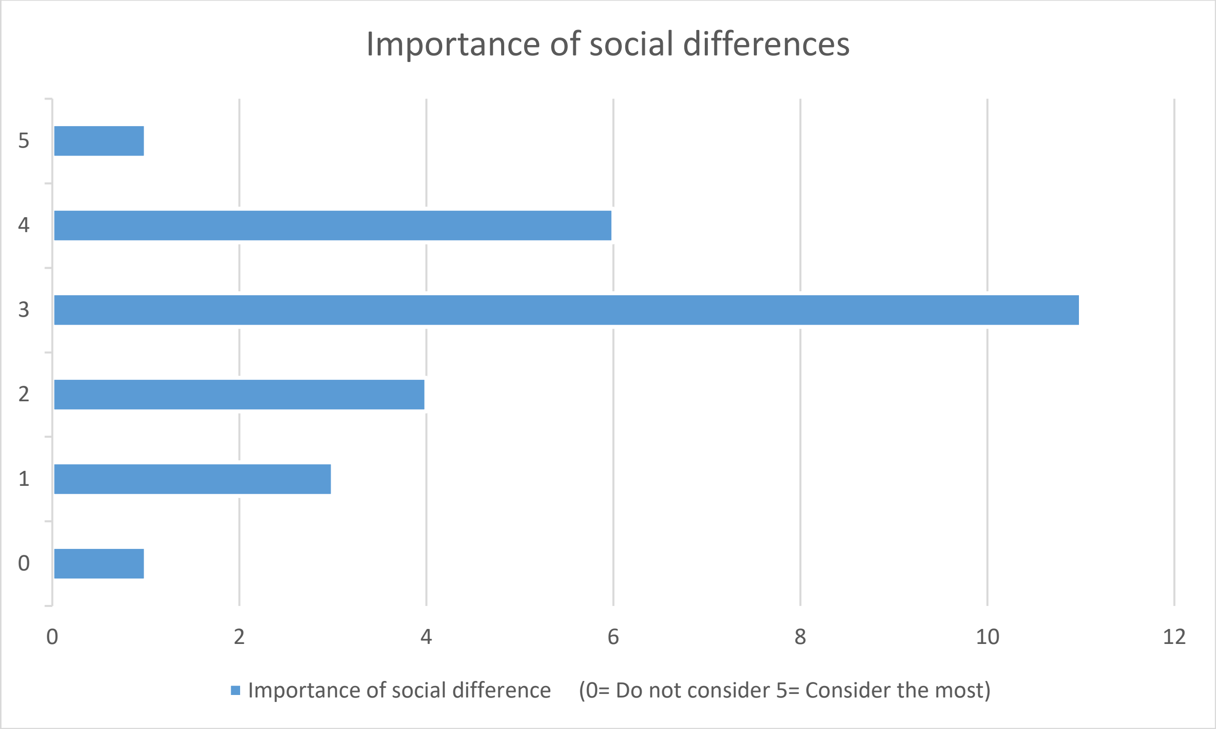


Figure E.311: Importance of social differences (1-5 years UK)

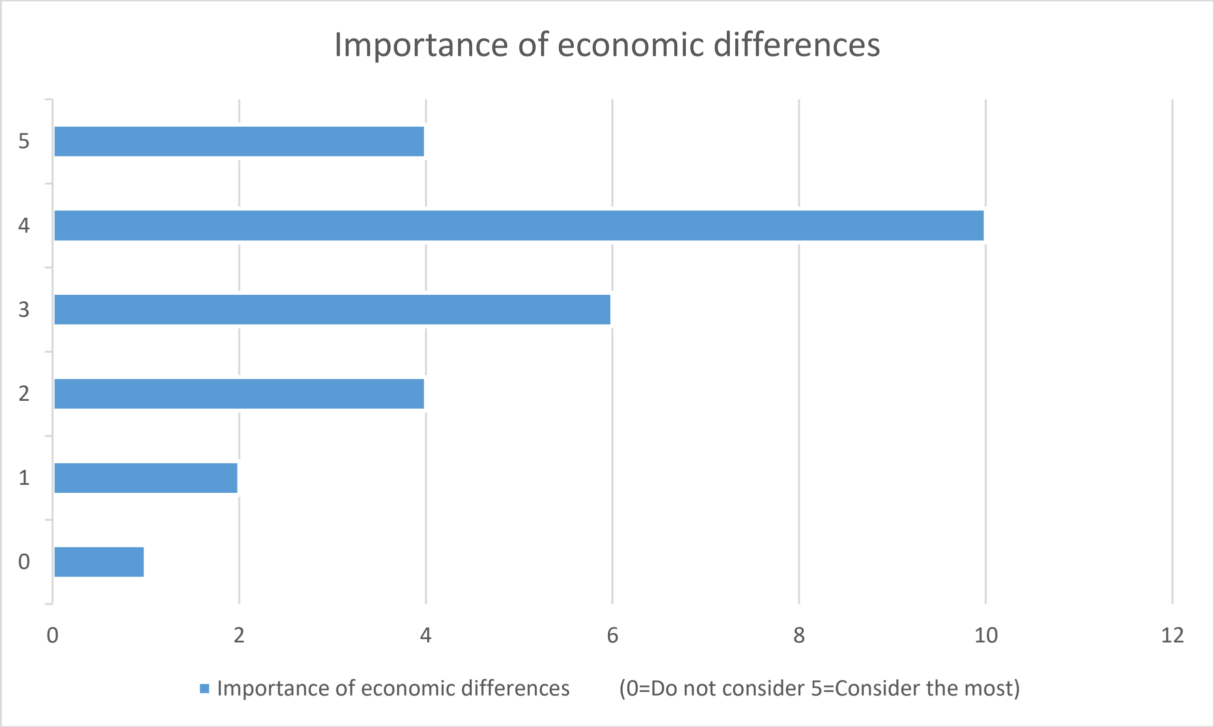


Figure E.312: Importance of economic differences (1-5 years UK)

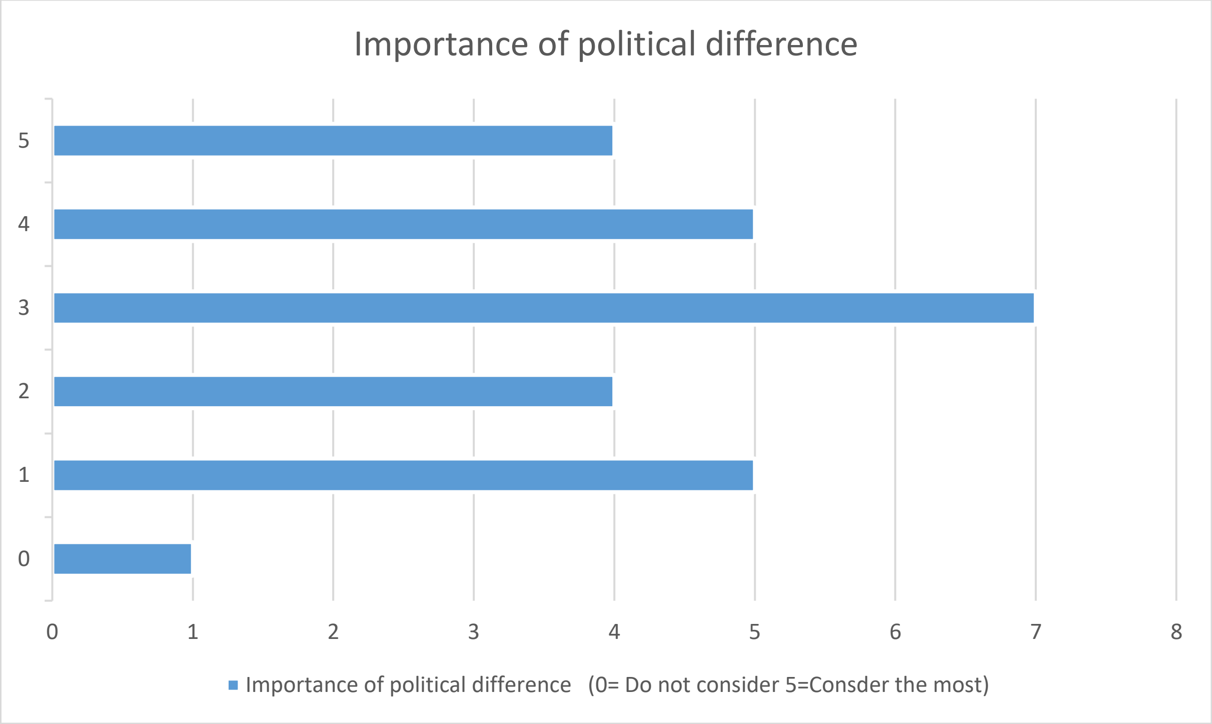


Figure E.313: Importance of political difference (1-5 years UK)

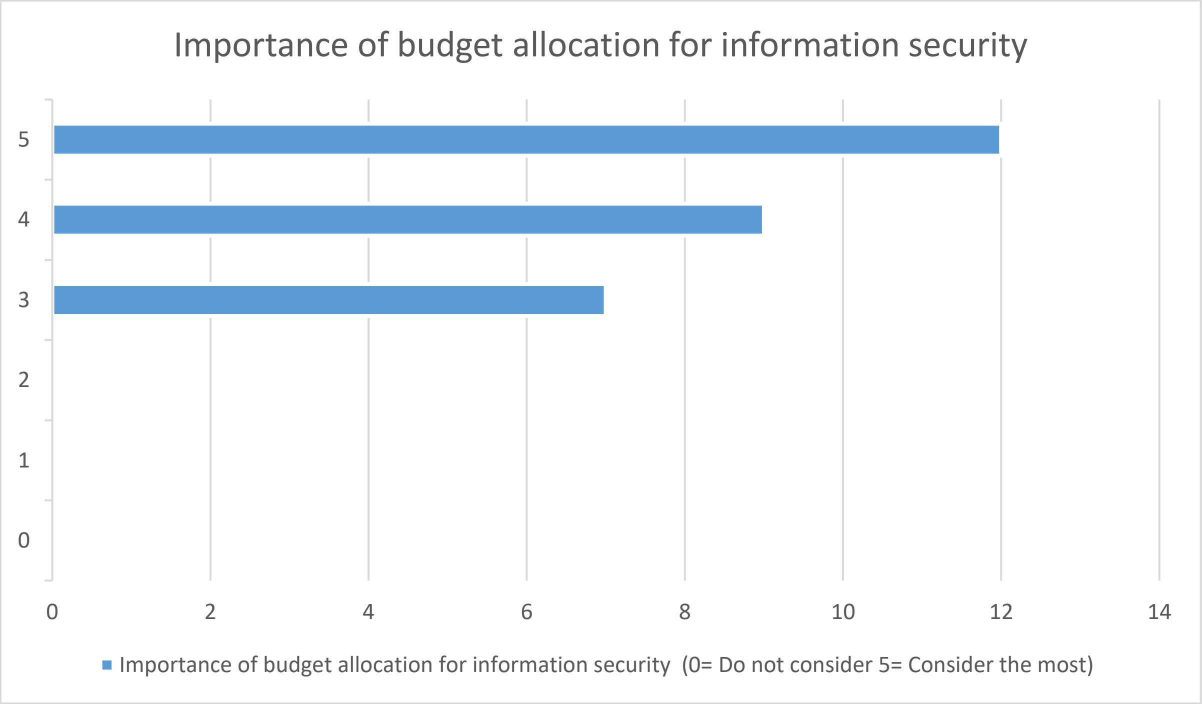


Figure E.314: Importance of budget allocation for information security (1-5 years UK)

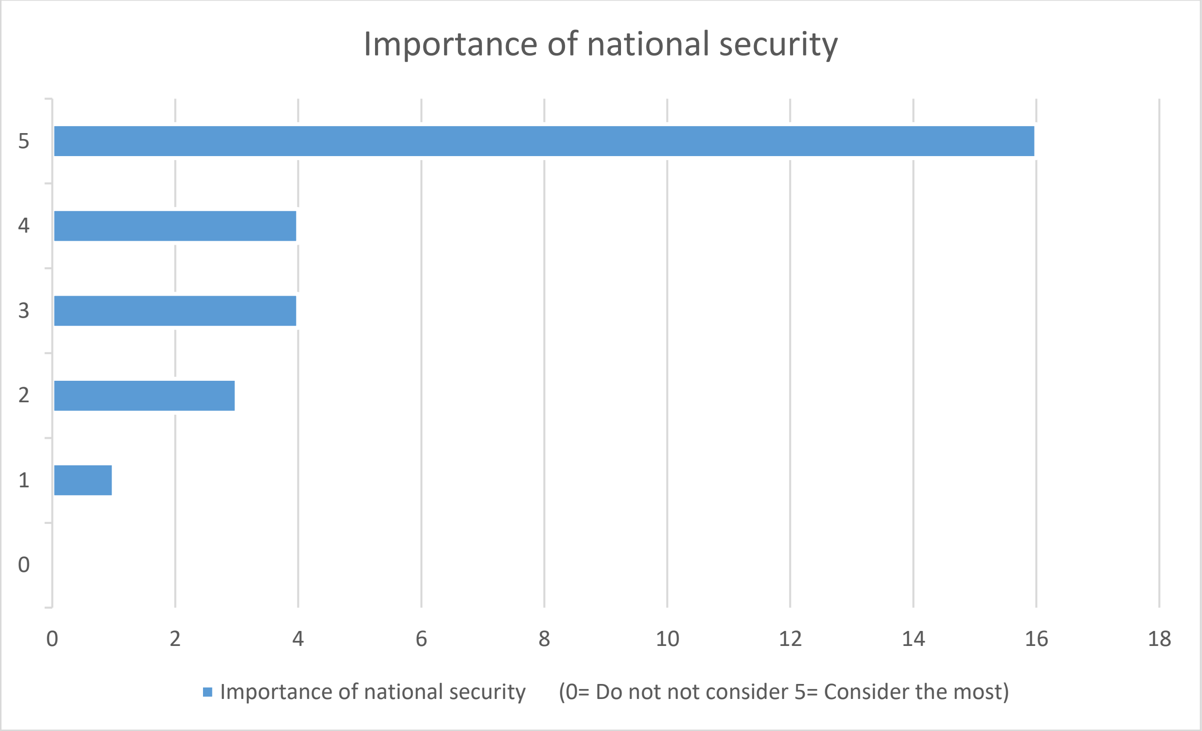


Figure E.315: Importance of national security (1-5 years UK)

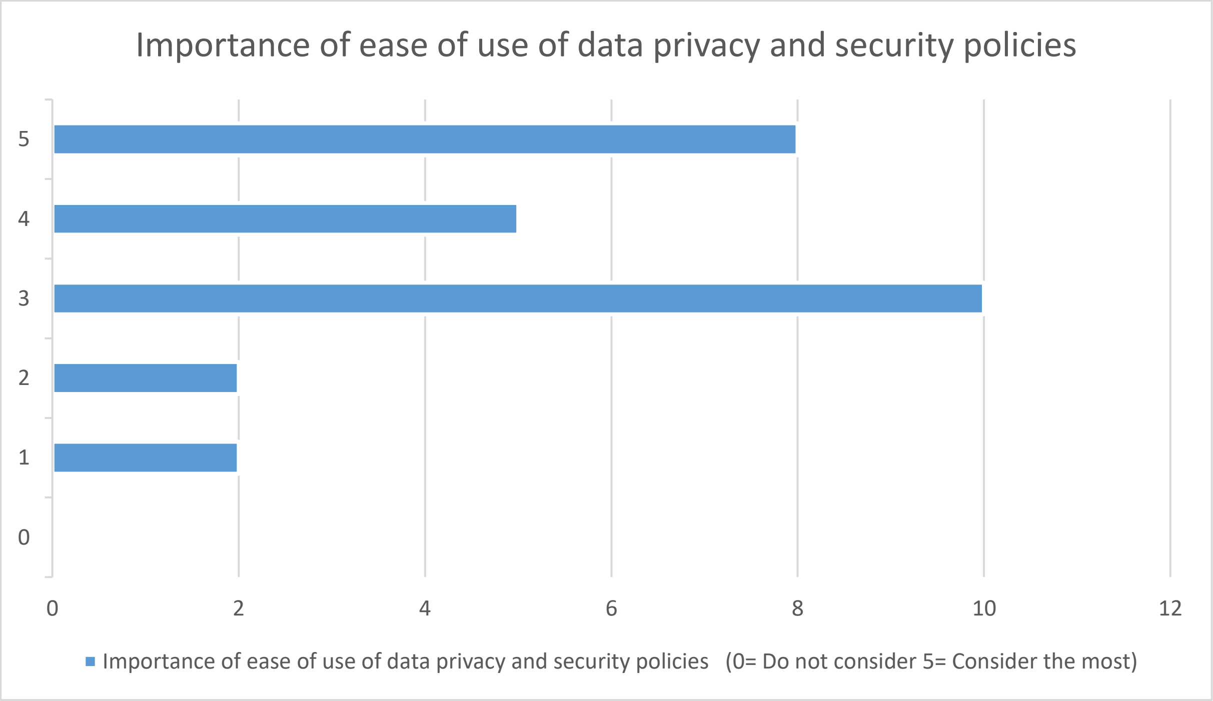


Figure E.316: Importance of ease of use of data privacy and security policies (1-5 years UK)

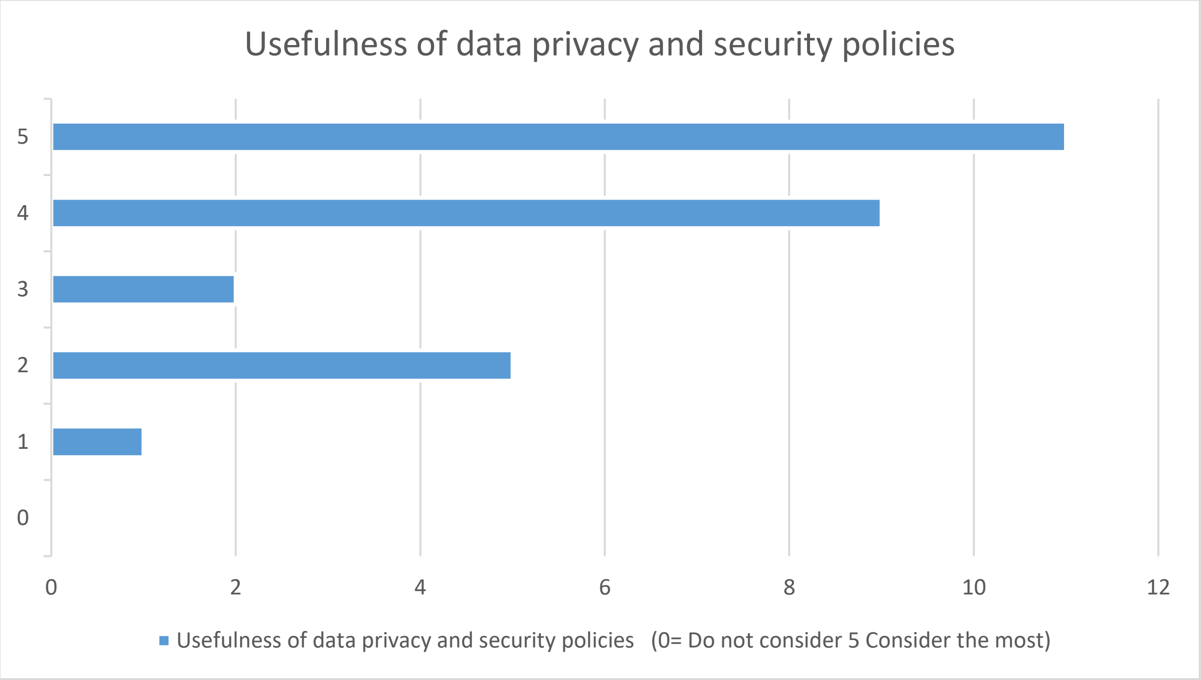


Figure E.317: Usefulness of data privacy and security policies (1-5 years UK)

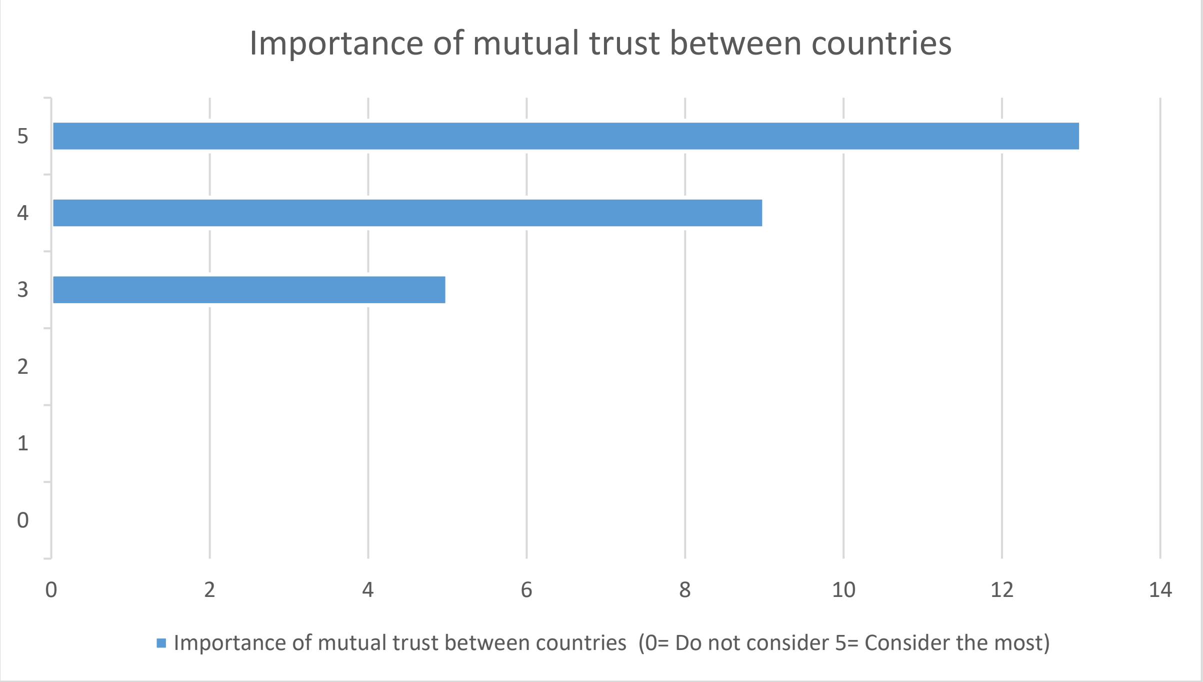


Figure E.318: Importance of mutual trust between countries (1-5 years UK)

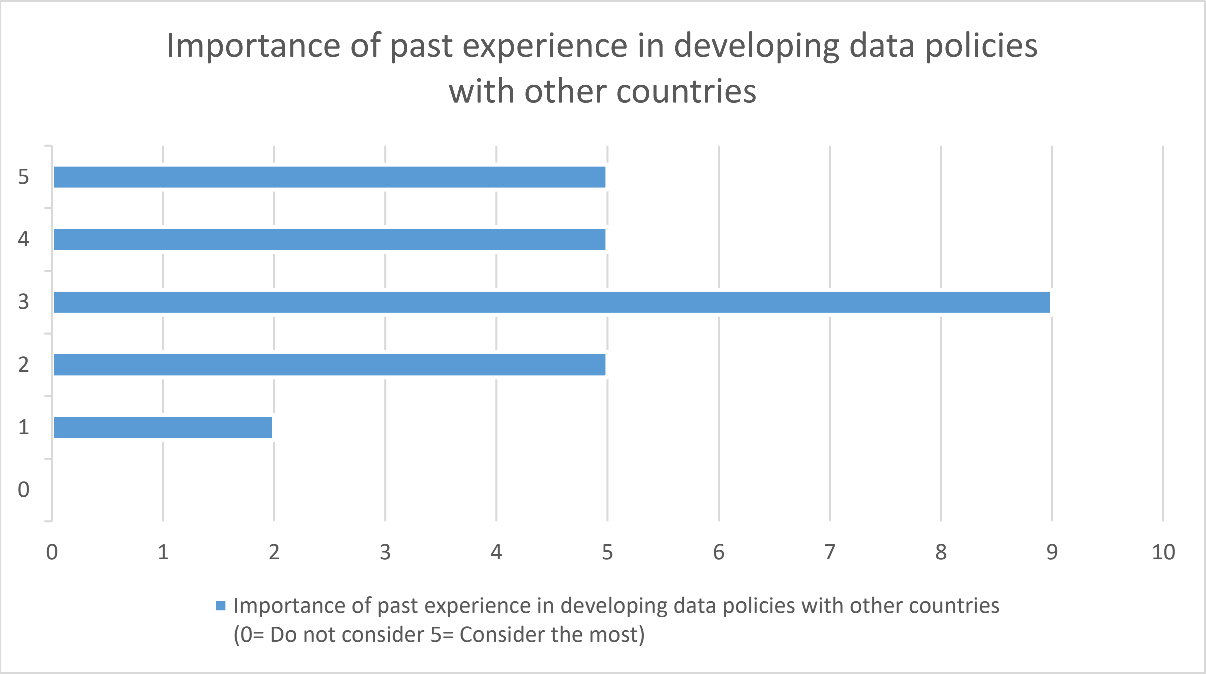


Figure E.319: Importance of past experience in developing data policies with other counties (1-5 years UK)

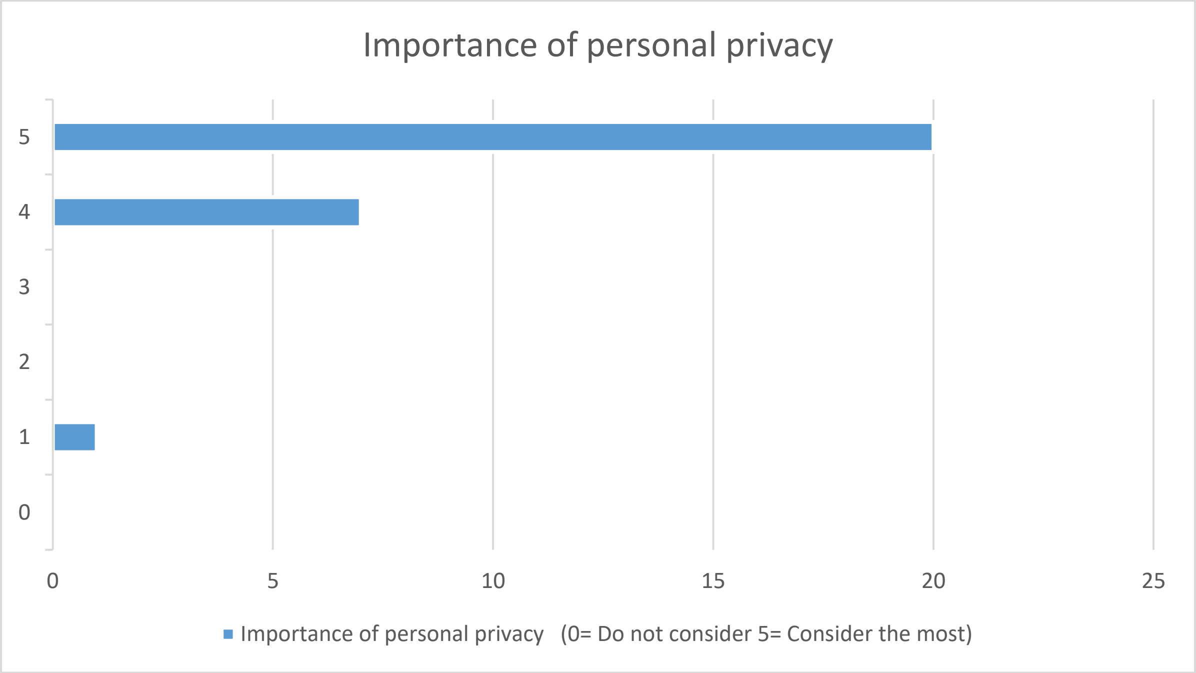


Figure E.320: Importance of personal privacy (1-5 years UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 83 percent of the respondents have endorsed (See figure E.309). The other notable factors that have come out of the survey are organisational support, budget allocation, political differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure E.298-308) (See figure E.310-320).

United Kingdom – 6-10 years

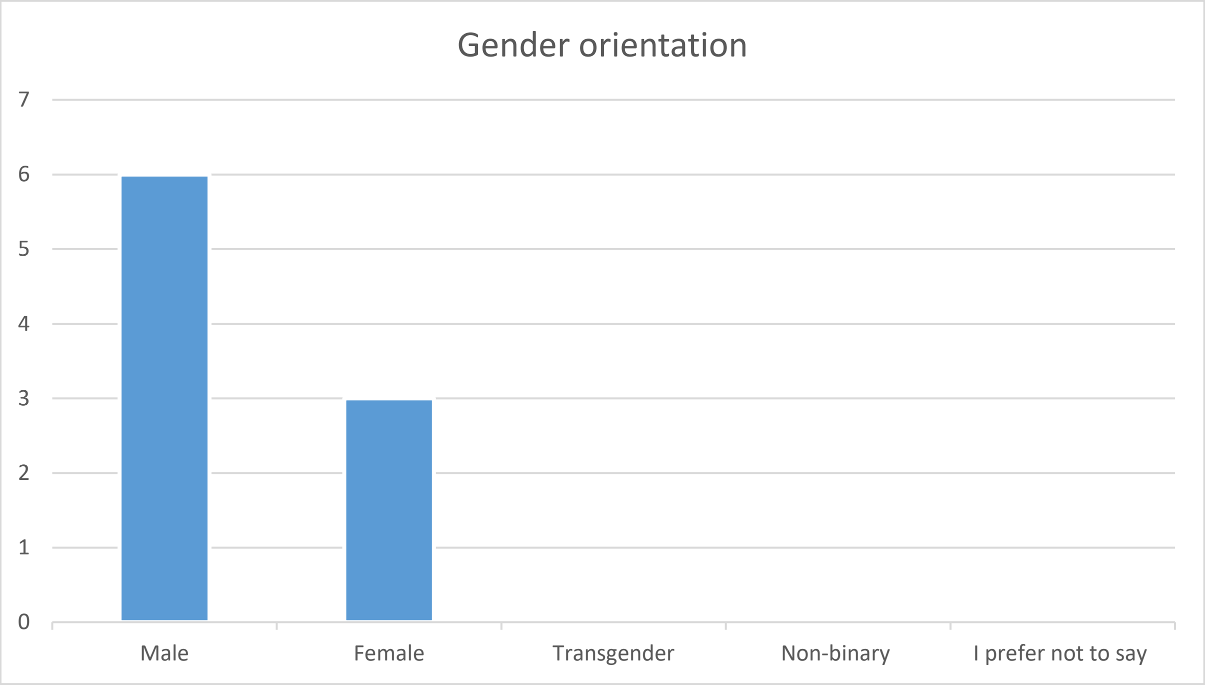


Figure E.321: Gender orientation (**6-10** years UK)

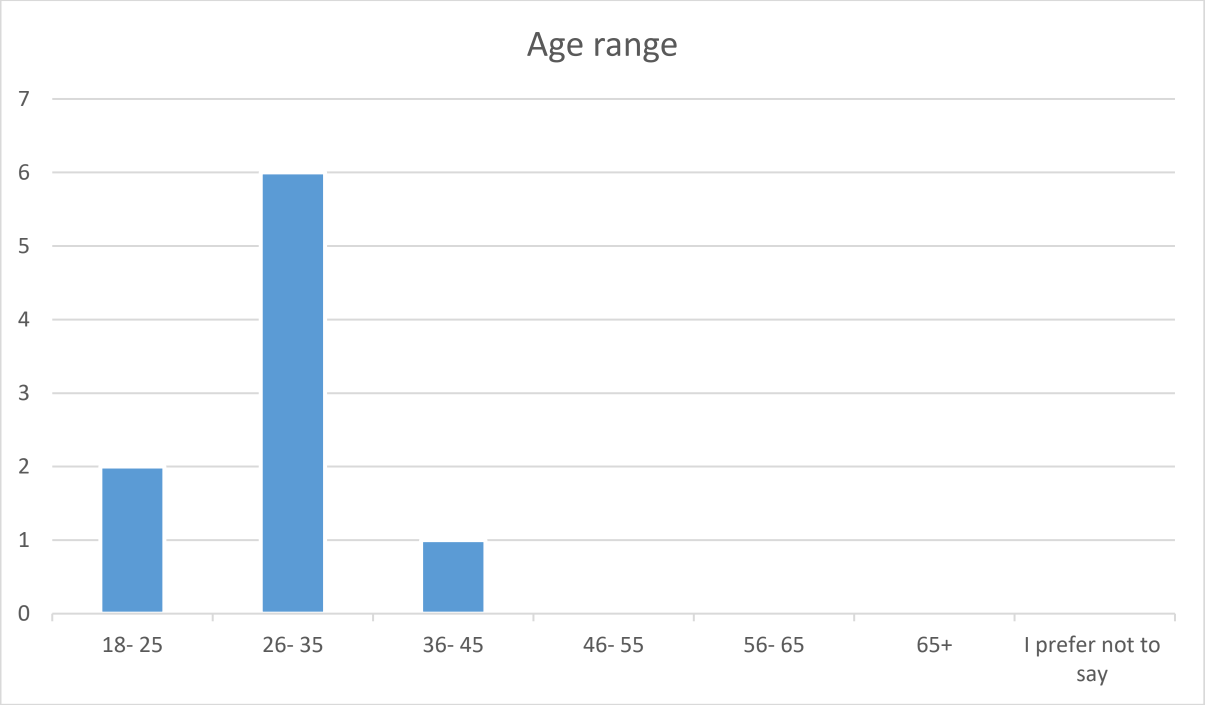


Figure E.322: Age range (**6-10** years UK)

This analysis is based on the responses received from United Kingdom participants with 6 to 10 years of employment in the industry. There were 9 participants and 6 out of them were males and 3 females (See figure E.321). They were within the 18-45 age range out of which 2 in the 18-25, 6 in the 26-35, and 1 in the 36-45 range (See figure E.322). This indicates that the age range of the majority of employees with 5-10 years of service is between 26-35 years.

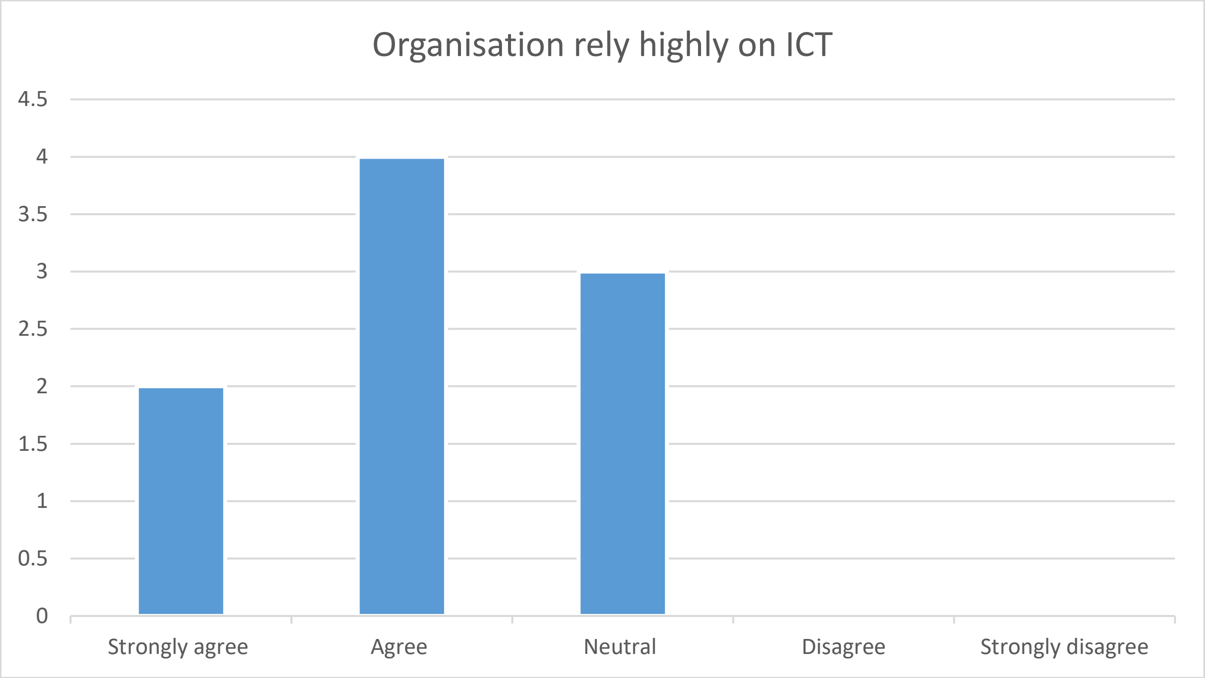


Figure E.323: Organisation rely highly on ICT (**6-10** years UK)

Out of the 9 respondents, 6 have worked in a technology reliance working environment, 3 unaware of reliance on technology because of the nature of the work assigned to them, and no one marked ‘disagree’ on ICT (See figure E.323). This indicates a majority of those who have been working in an organisation for 5-10 years have had a high reliance on ICT.

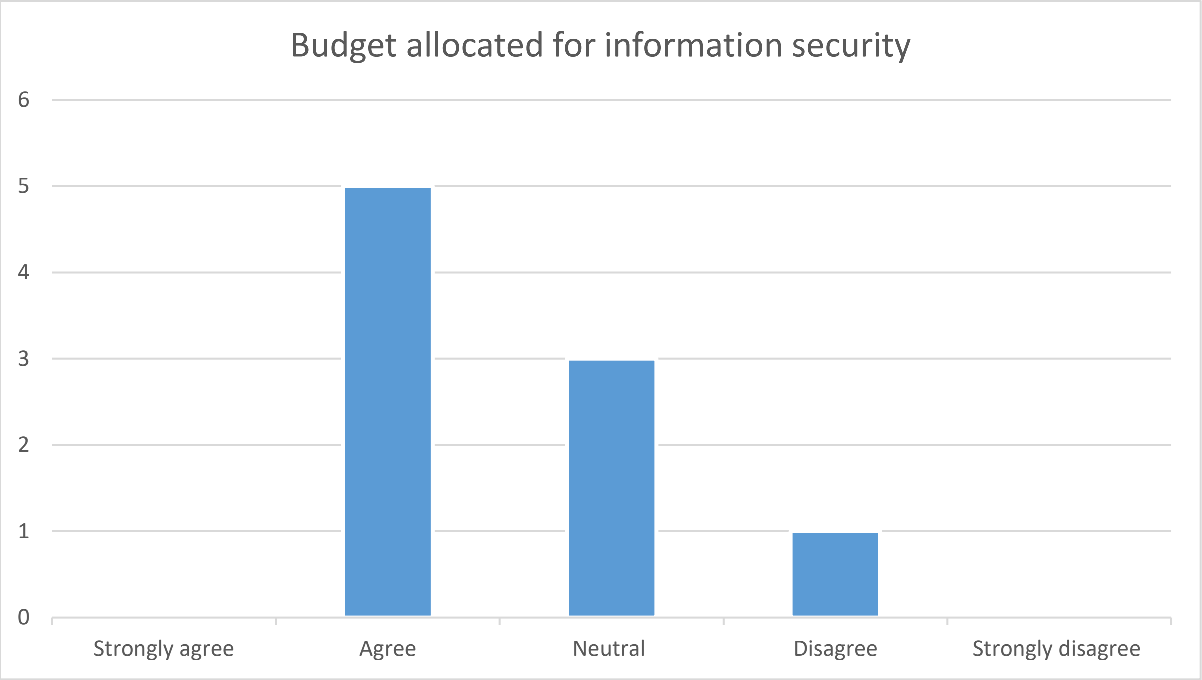


Figure E.324: Budget allocated for information security (**6-10** years UK)

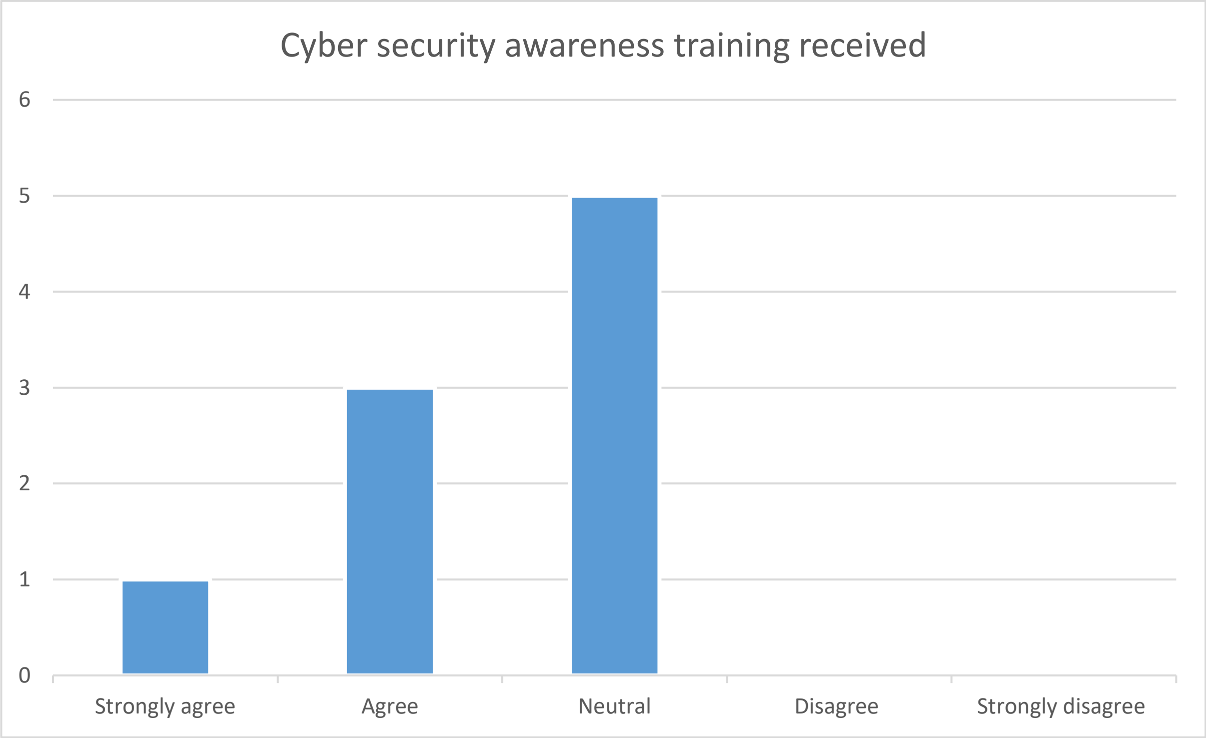


Figure E.325: Cyber security awareness training received (**6-10** years UK)

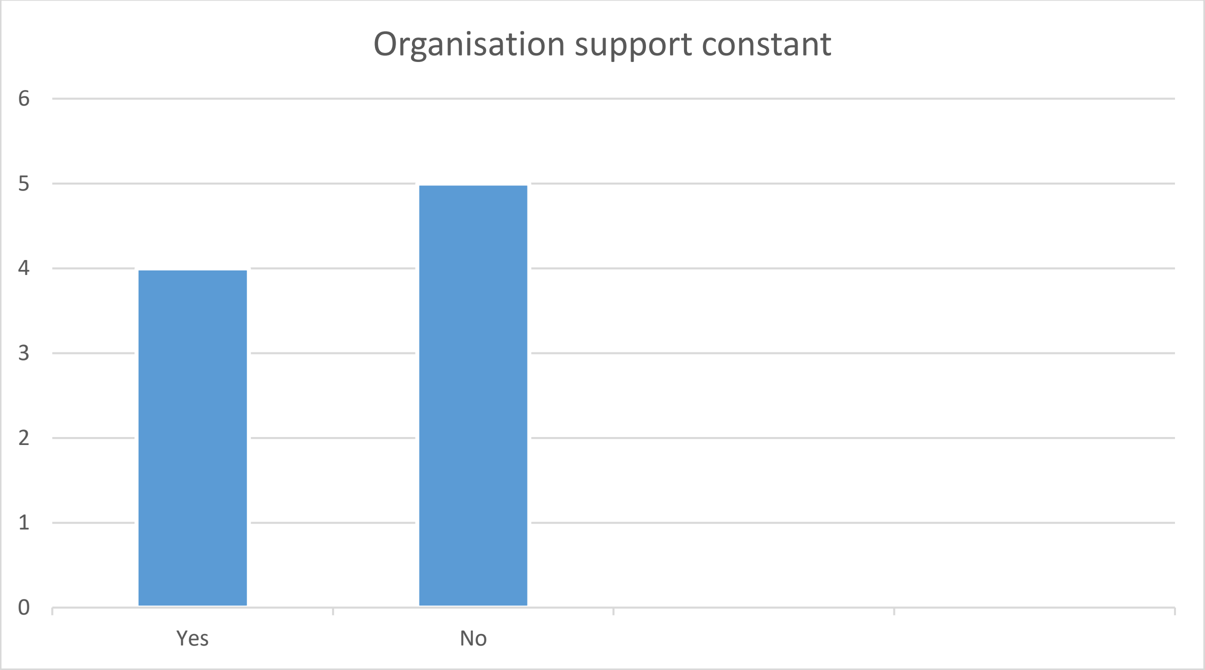


Figure E.326 Organisation support constant (**6-10** years UK)

Funding has been sketchy. 5 out of the 9 have indicated that their organisations had an allocated budget for information security, whilst 3 had not expressed an opinion either way and notably according to the 1 disagreed, their organisations had no budget allocation for information security (See figure E.324). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 4 participants have received regular cybersecurity awareness training, whilst 5 neither agreed nor disagreed (See figure E.325). In addition, 5 participants had not received support from the organisation to protect personal information, whilst only 4 did (See figure E.326). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

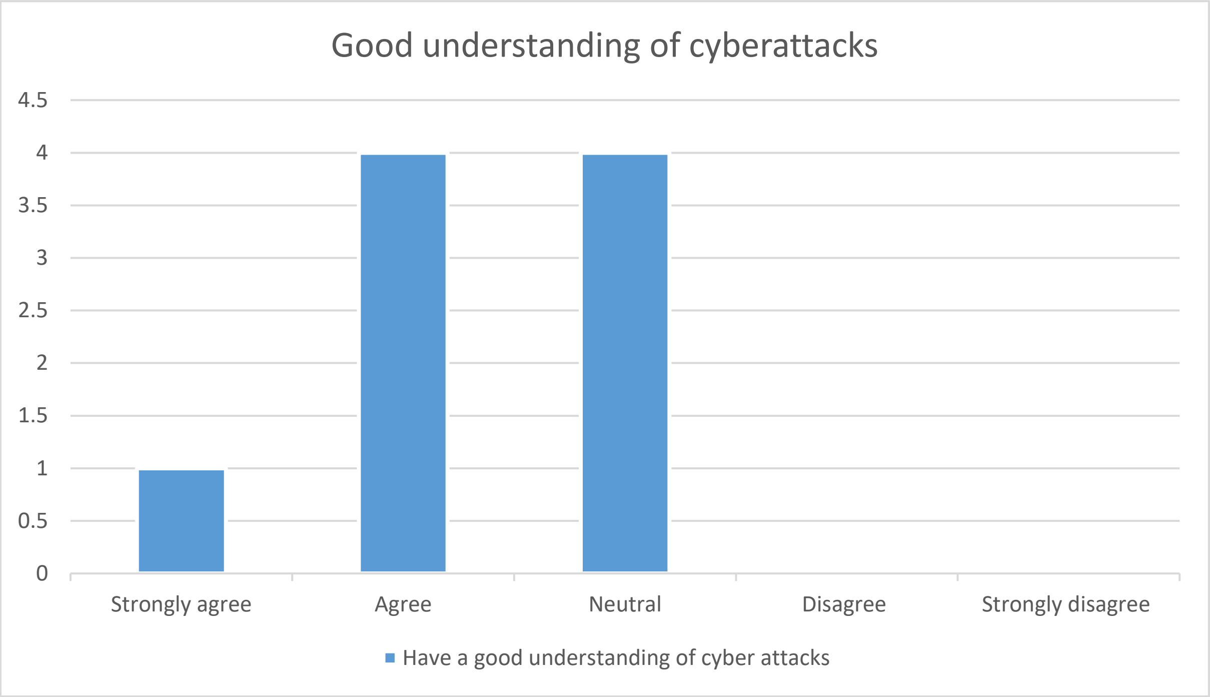


Figure E.327: Good understanding of cyberattacks (**6-10** years UK)

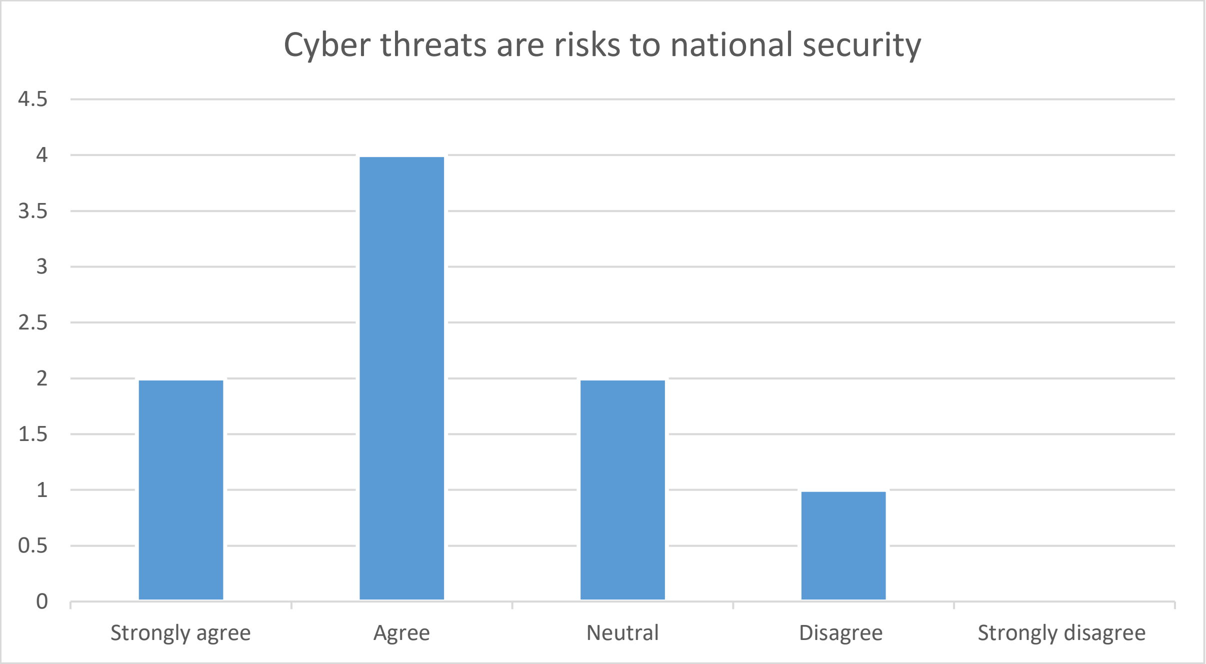


Figure E.328: Cyber threats are risks to national security (**6-10** years UK)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 5 participants do have, 4 have not expressed opinion either way (See figure E.327). Furthermore, 67 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure E.328). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

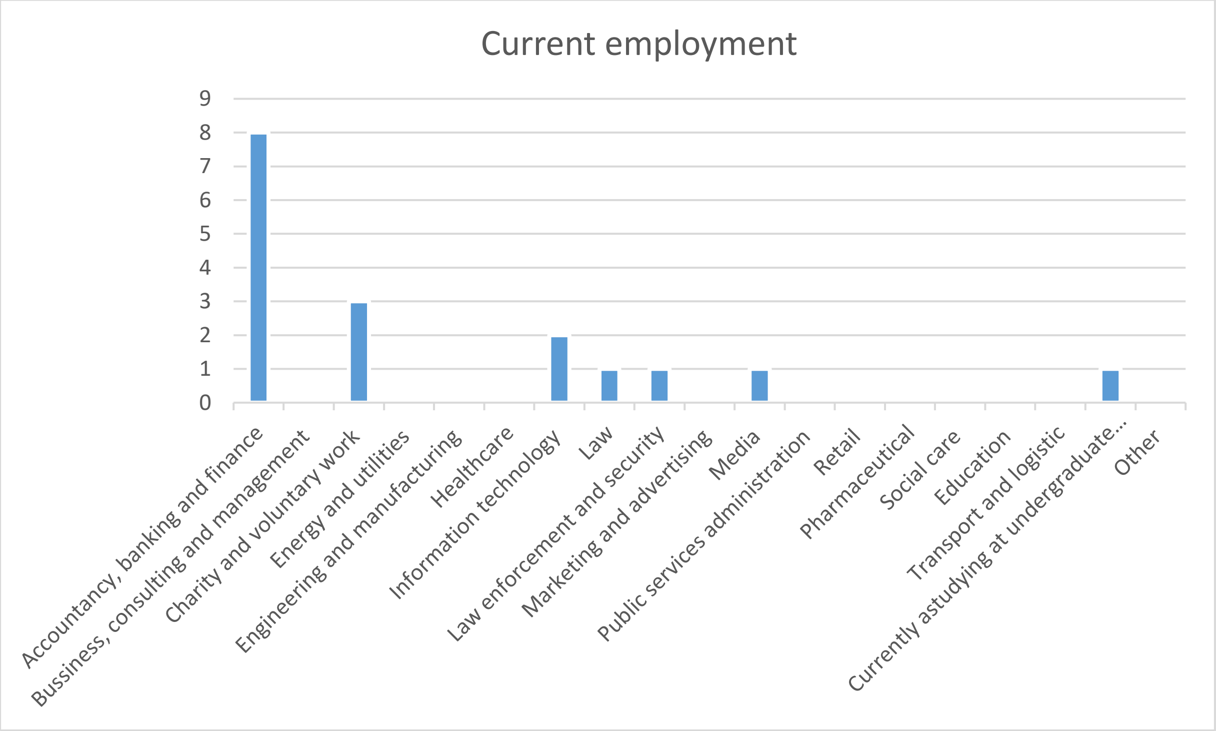


Figure E.329: Current employment (**6-10** years UK)

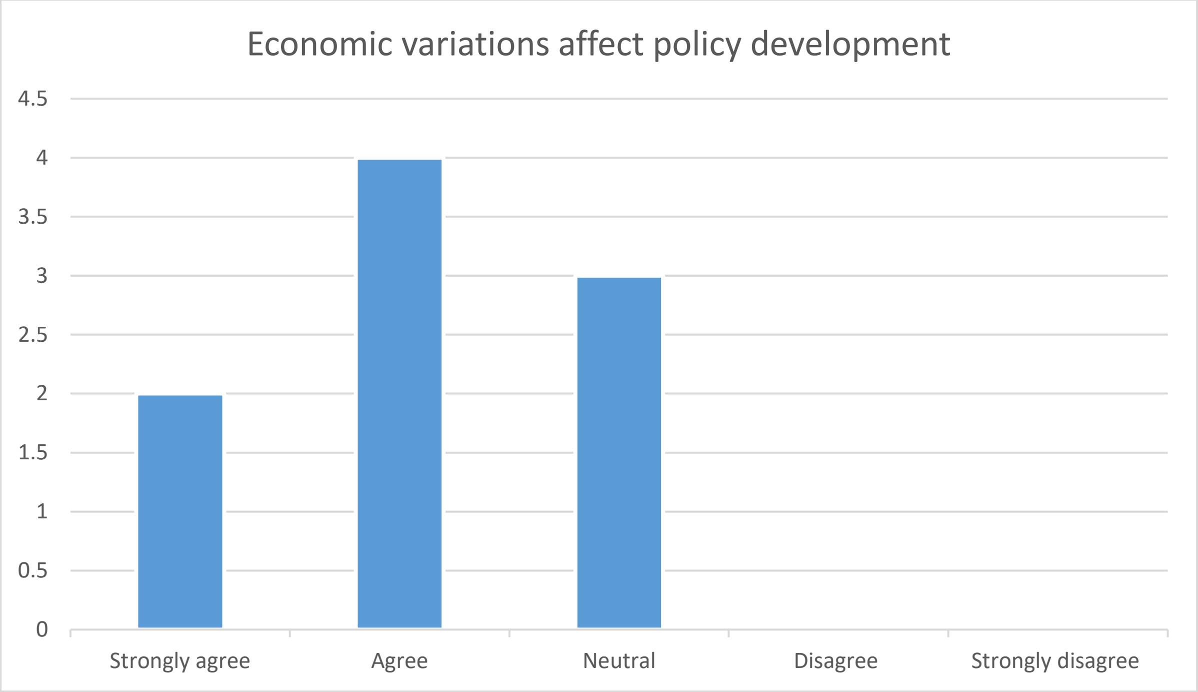


Figure E.330: Economic variations affect policy development (**6-10** years UK)

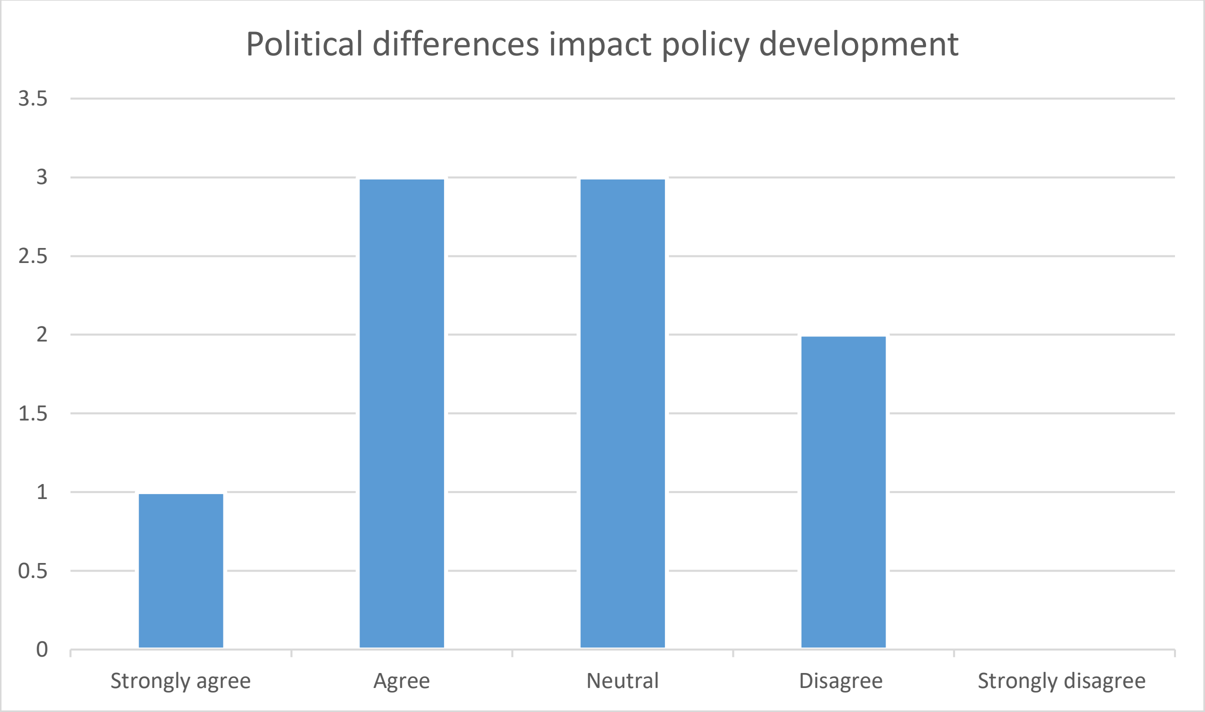


Figure E.331: Political differences impact policy development (**6-10** years UK)

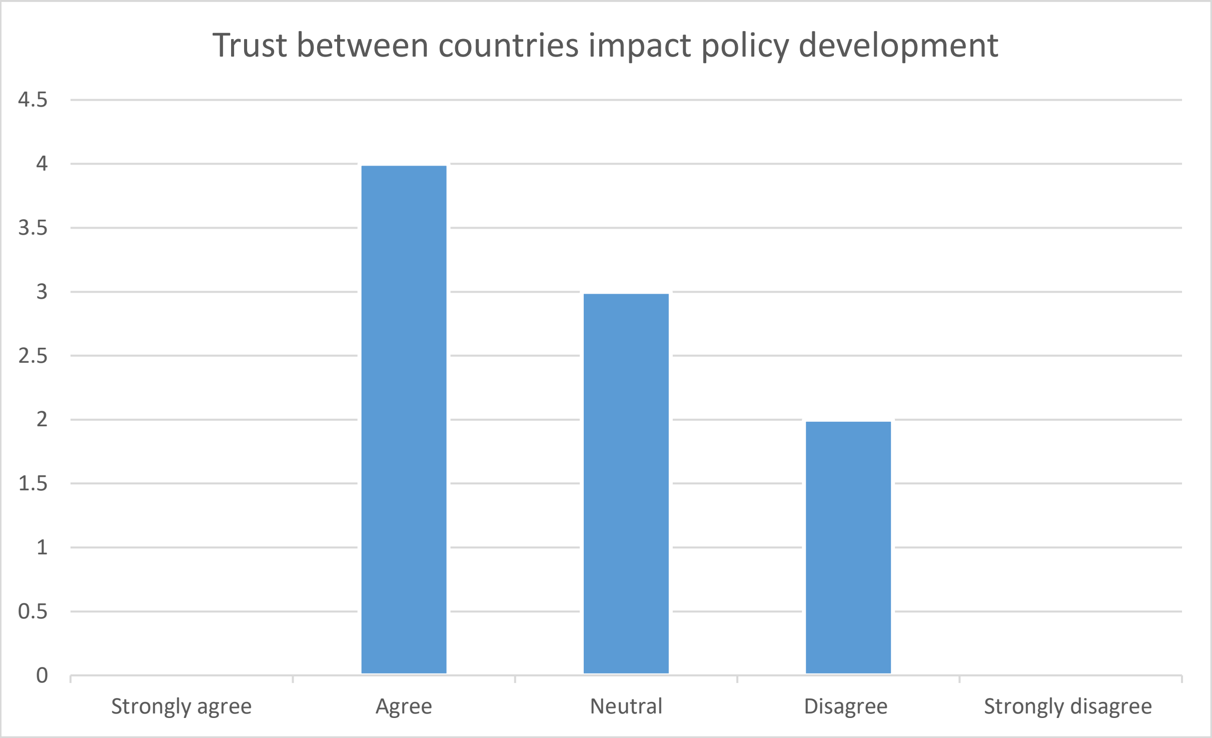


Figure E.332: Trust between countries impact policy development (**6-10** years UK)

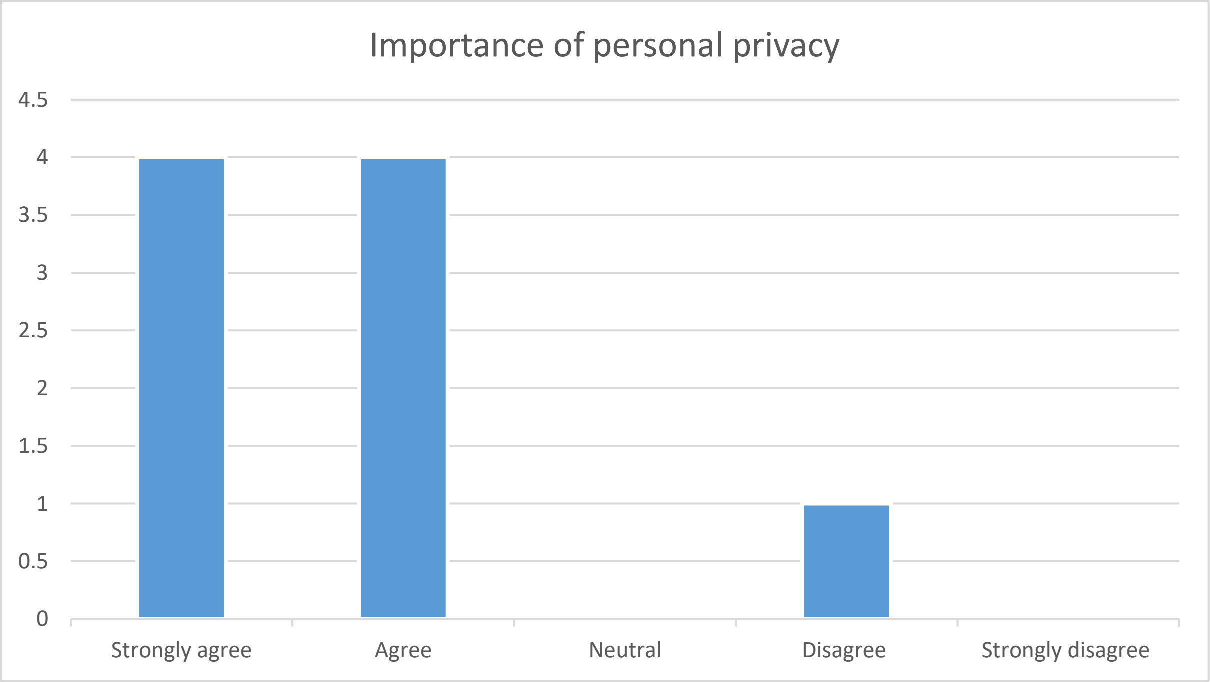


Figure E.333: Importance of personal privacy (**6-10** years UK)

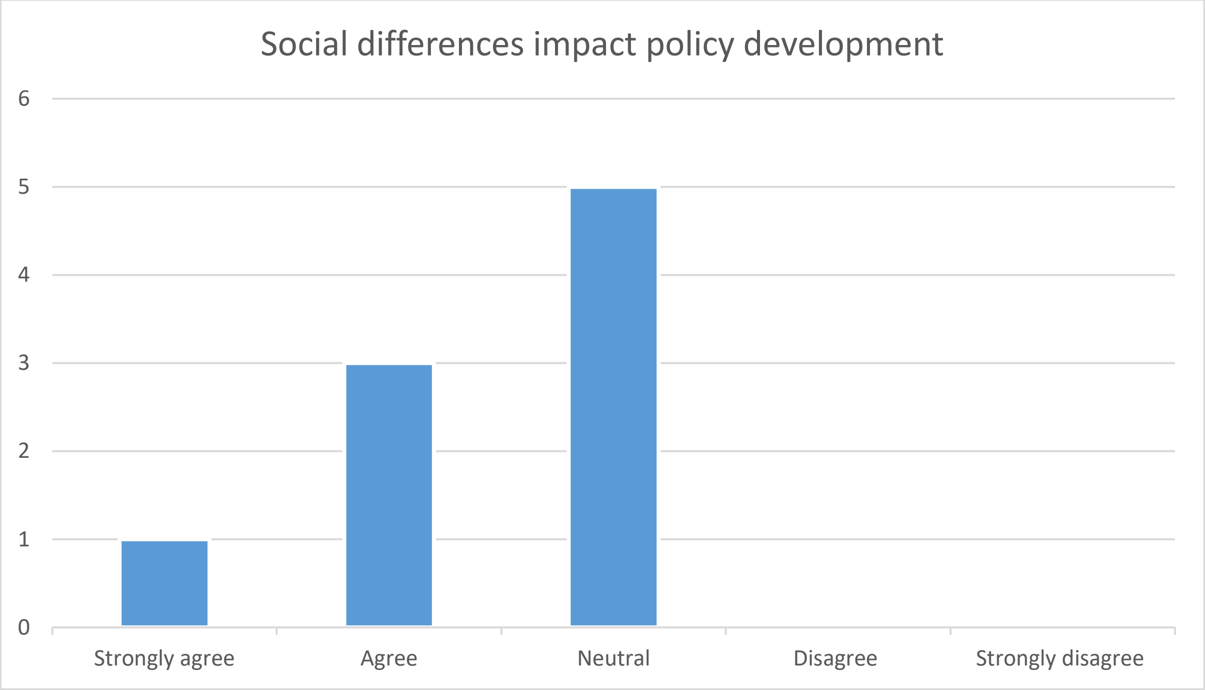


Figure E.334: Social differences impact policy development (**6-10** years UK)

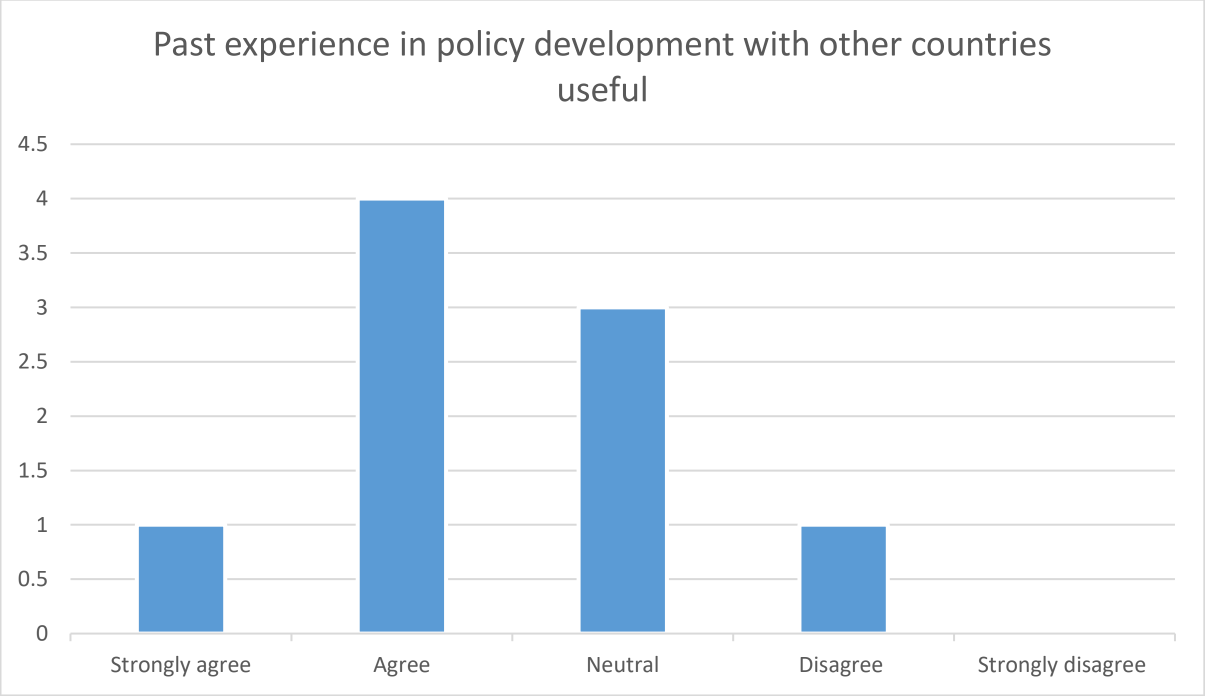


Figure E.335: Past experience in policy development with other countries useful (**6-10** years UK)

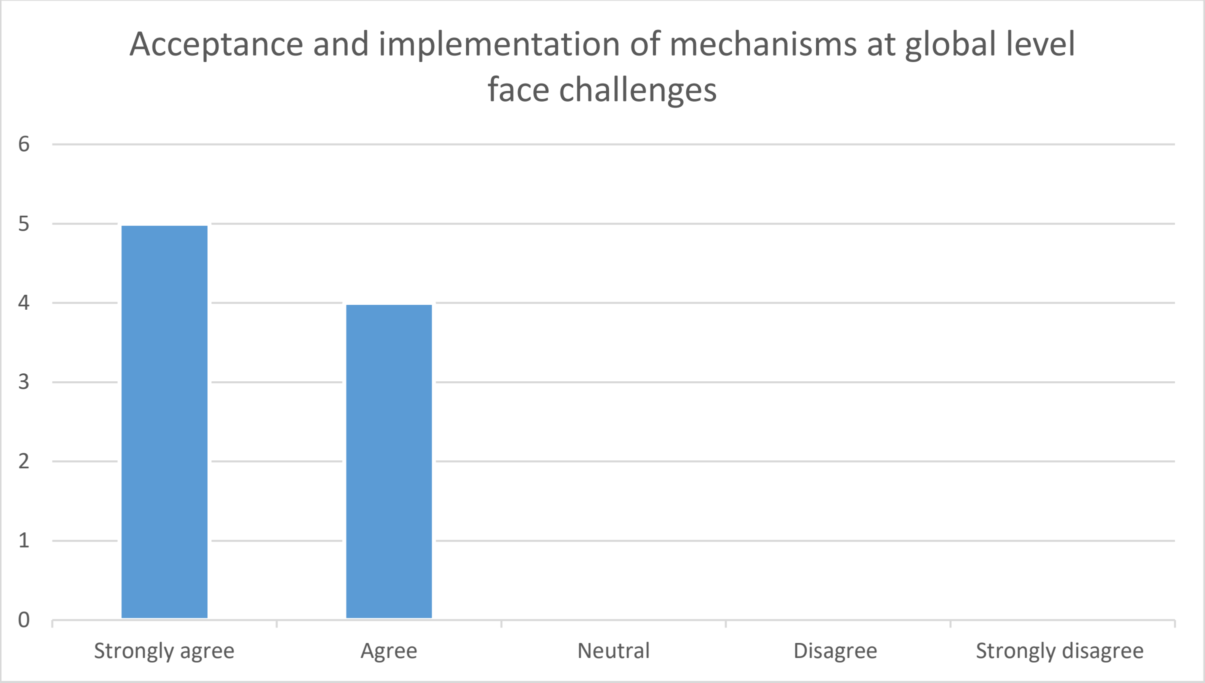


Figure E.336: Acceptance and implementation of mechanisms at global level face challenges (**6-10** years UK)

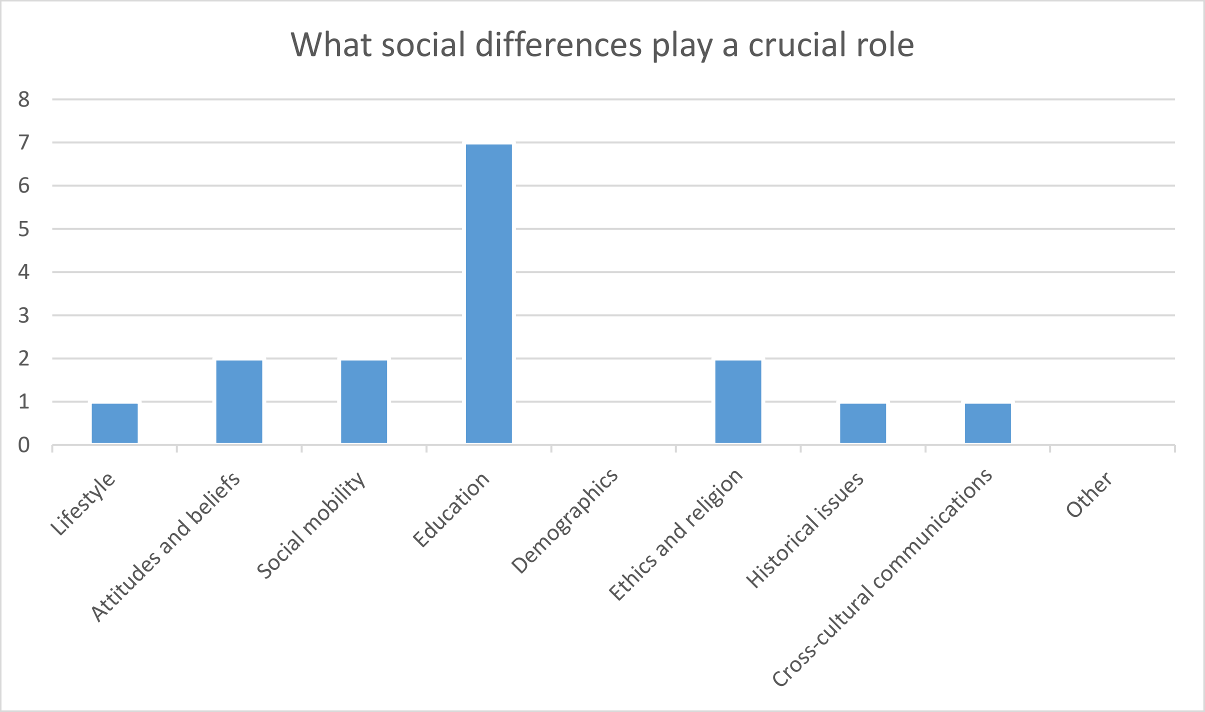


Figure E.337: What social differences play a crucial role (**6-10** years UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education (See figure E.337). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level.

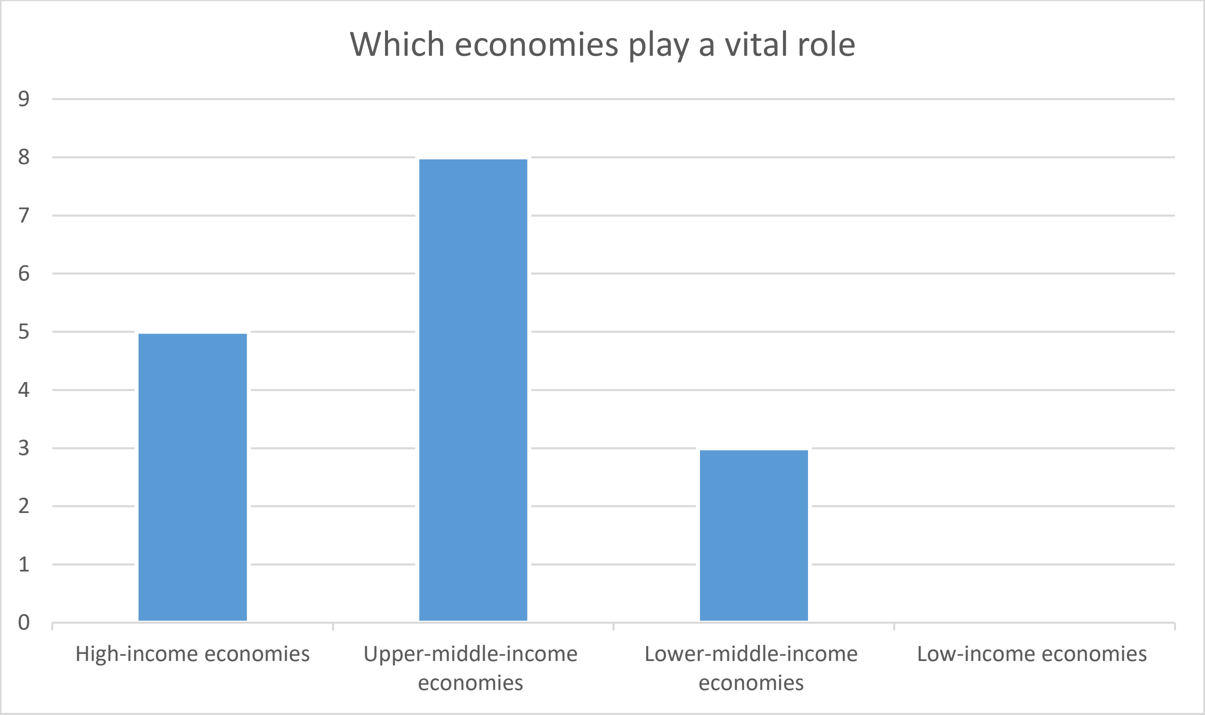


Figure E.338: Which economies play a vital role (**6-10** years UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role. There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

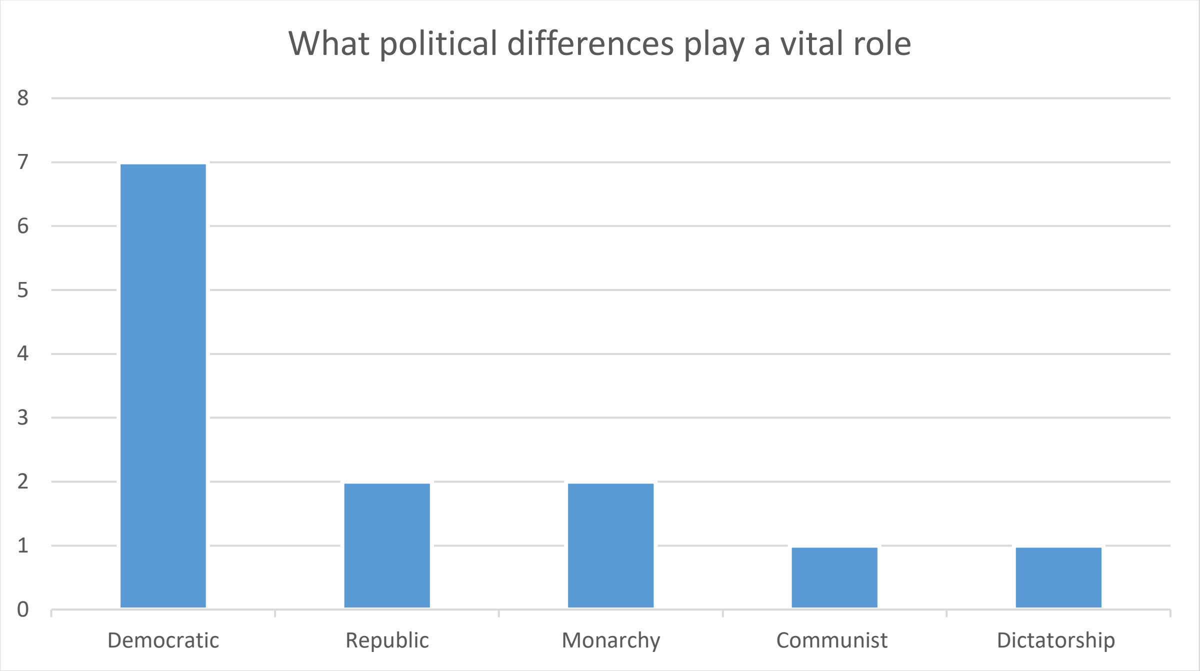


Figure E.339: What political differences play a vital role (**6-10** years UK)

The majority have chosen a democratic political system (See figure E.339), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

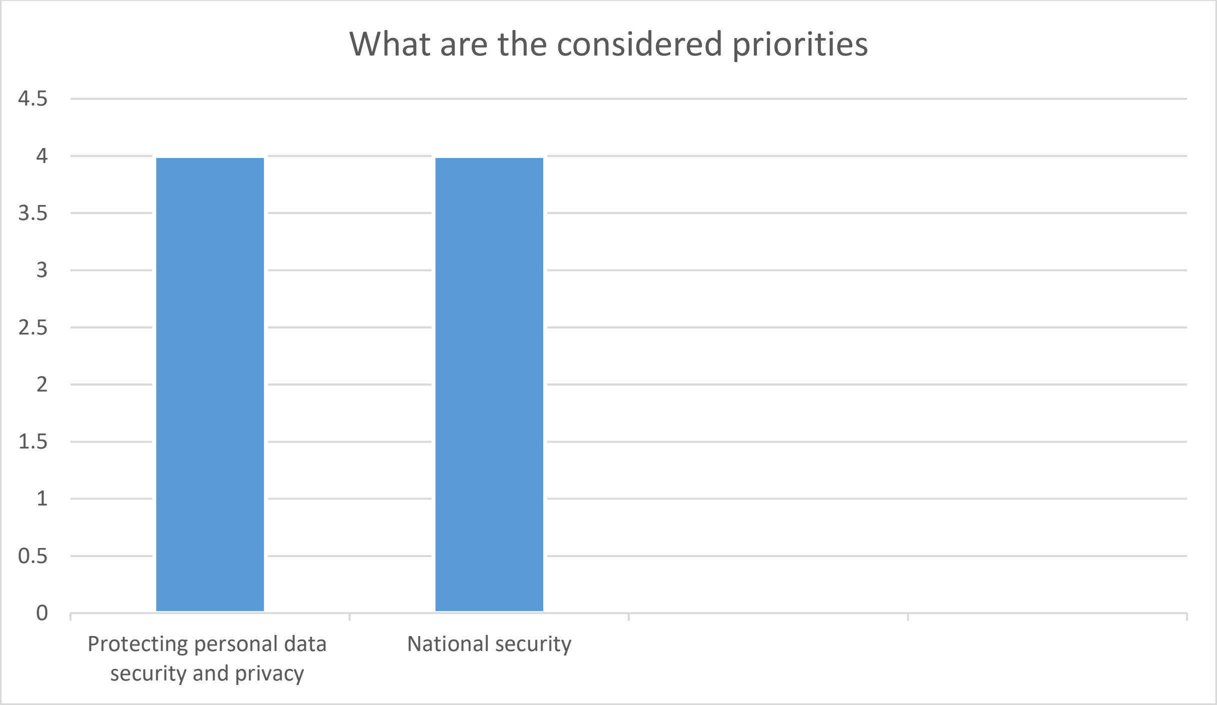


Figure E.340: What are the considered priorities (**6-10** years UK)

The majority not considered either the importance of protection of personal data security and privacy or protection of national security, in accepting and implementing a global data privacy and security policies (See figure E.340).

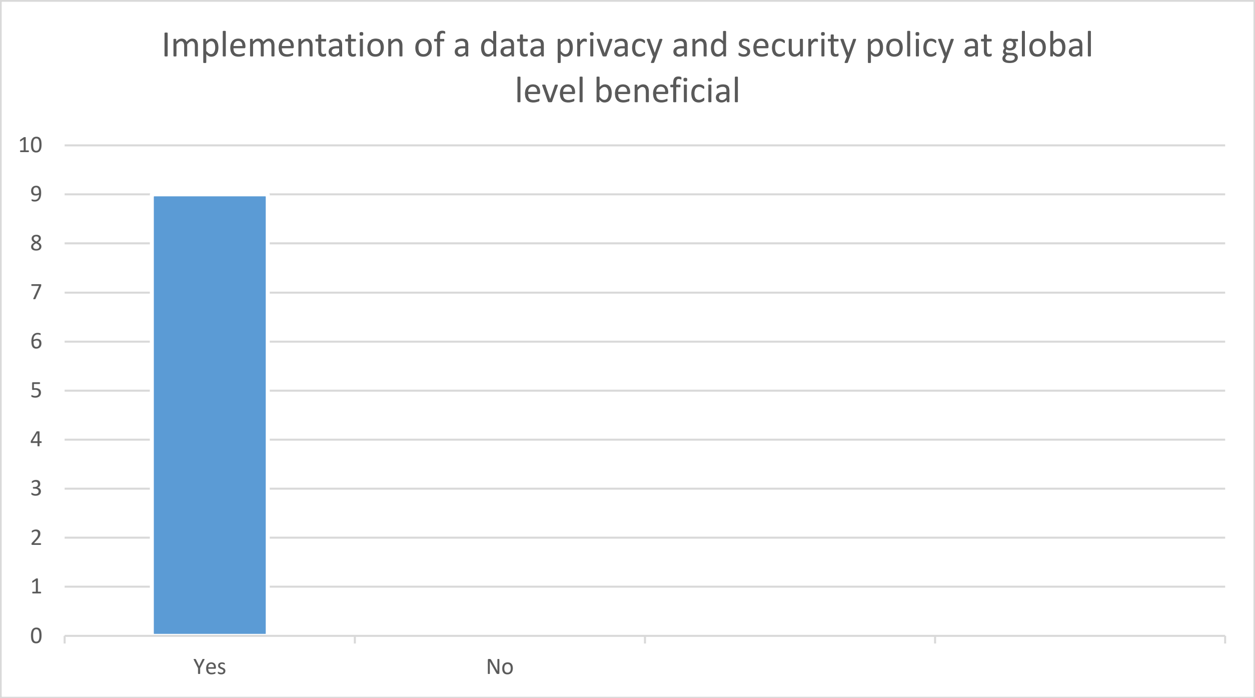


Figure E.341: Implementation of a data privacy and security policy at global level beneficial (**6-10** years UK)

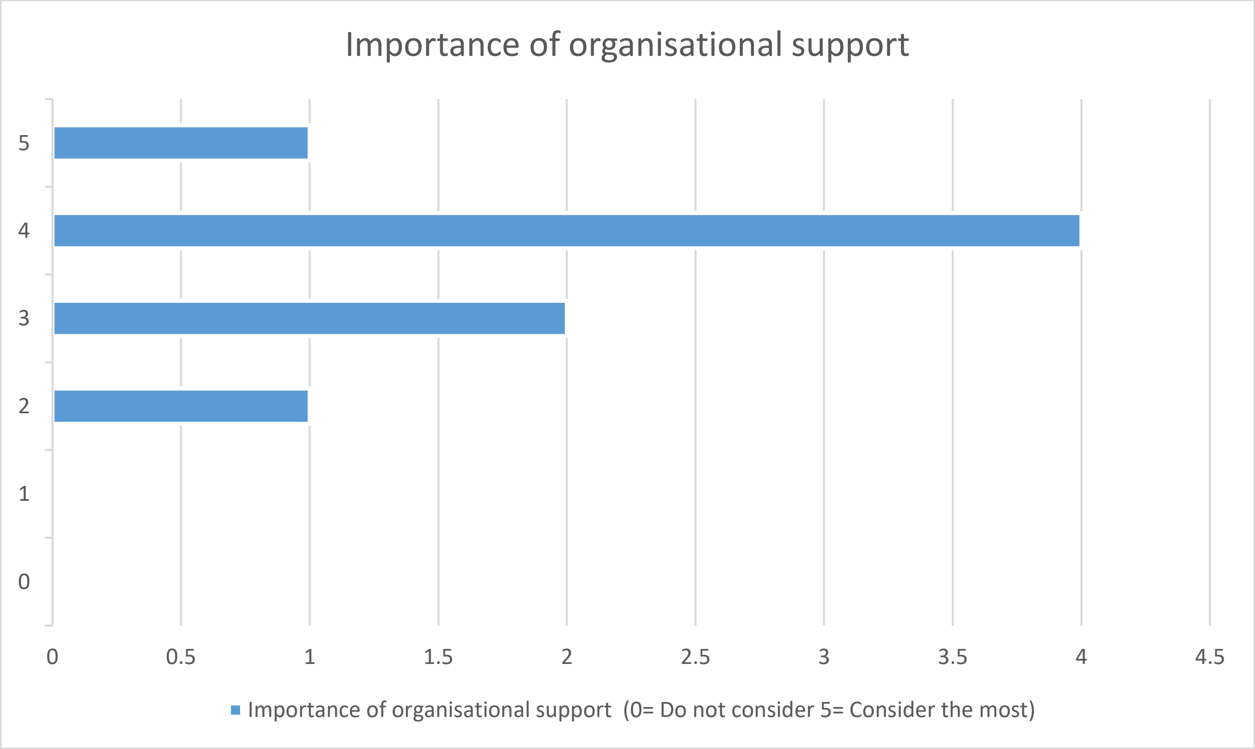


Figure E.342: Importance of organisational support (**6-10** years UK)

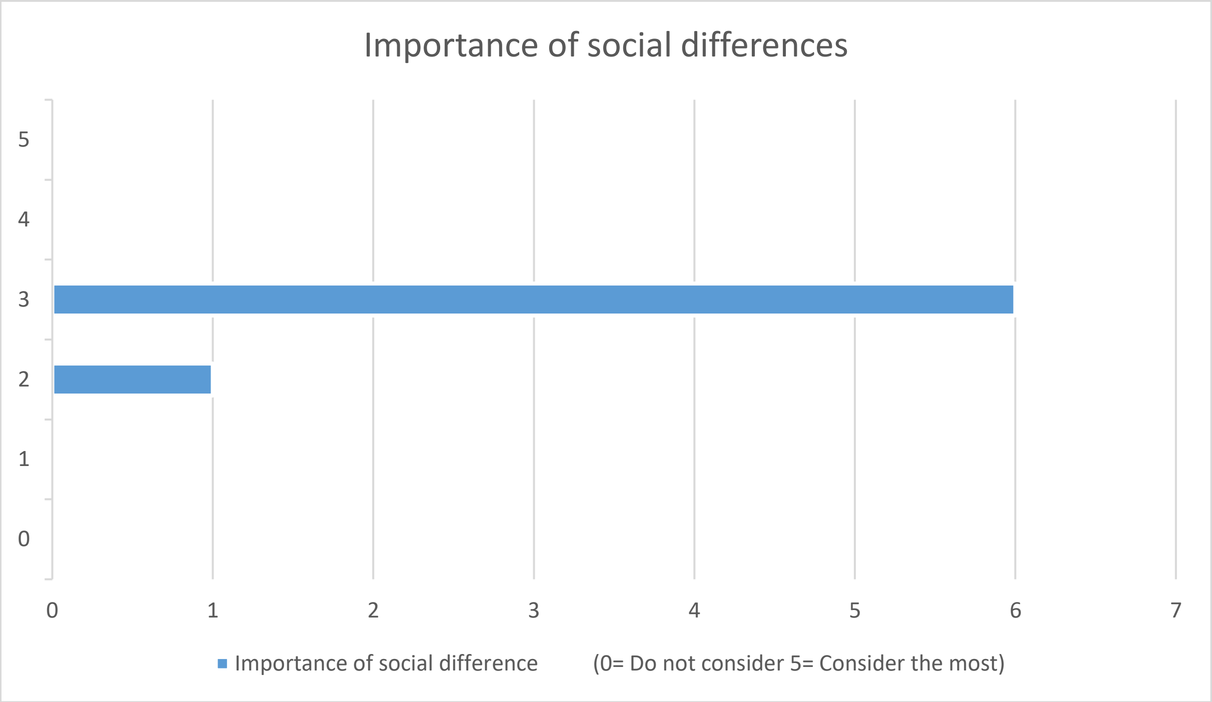


Figure E.343: Importance of social differences (**6-10** years UK)

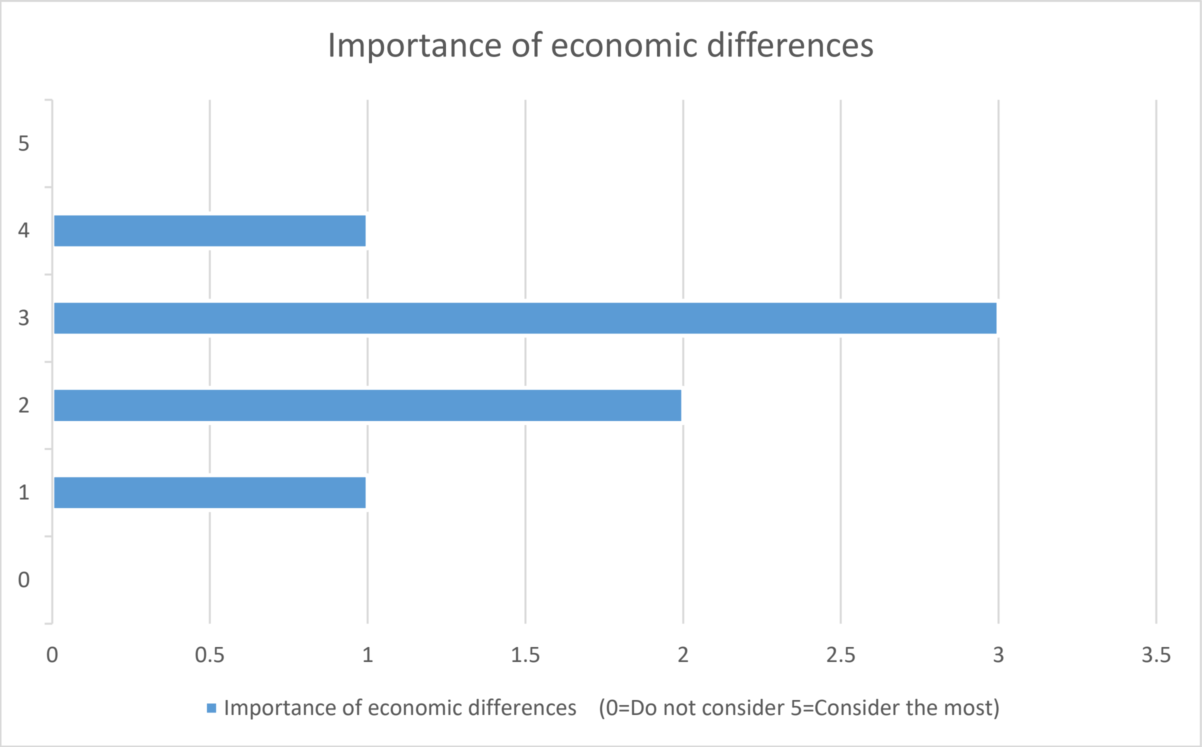


Figure E.344: Importance of economic differences (**6-10** years UK)

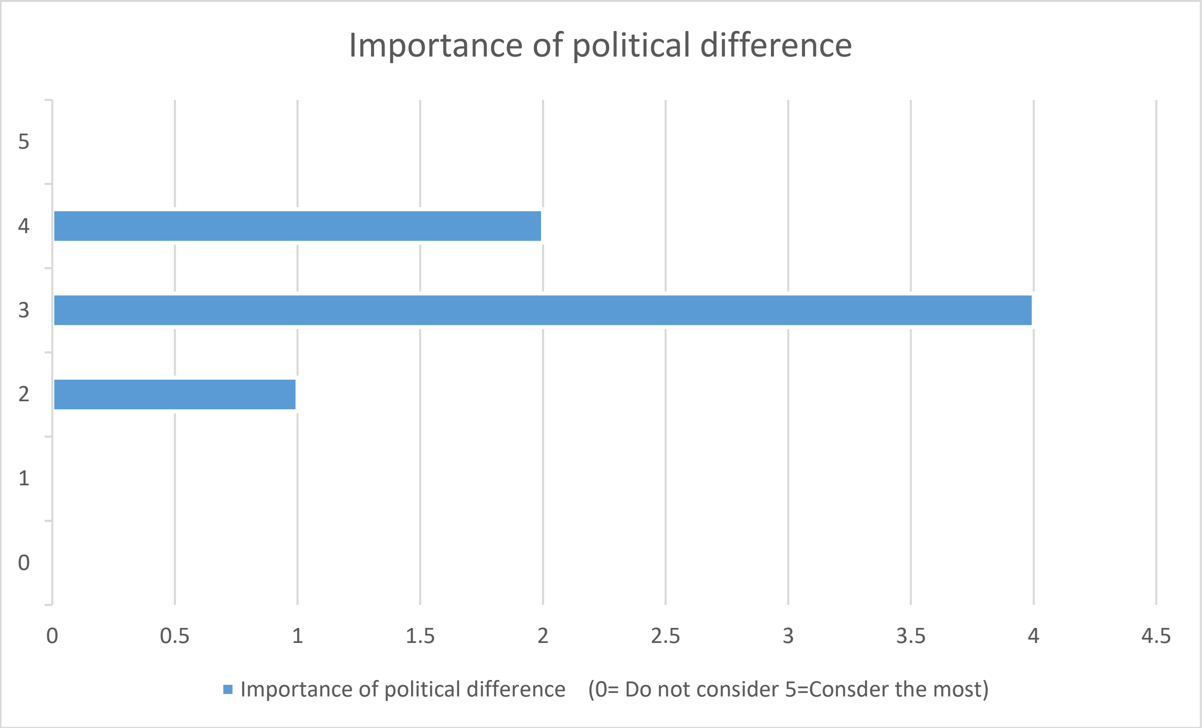


Figure E.345: Importance of political difference (**6-10** years UK)

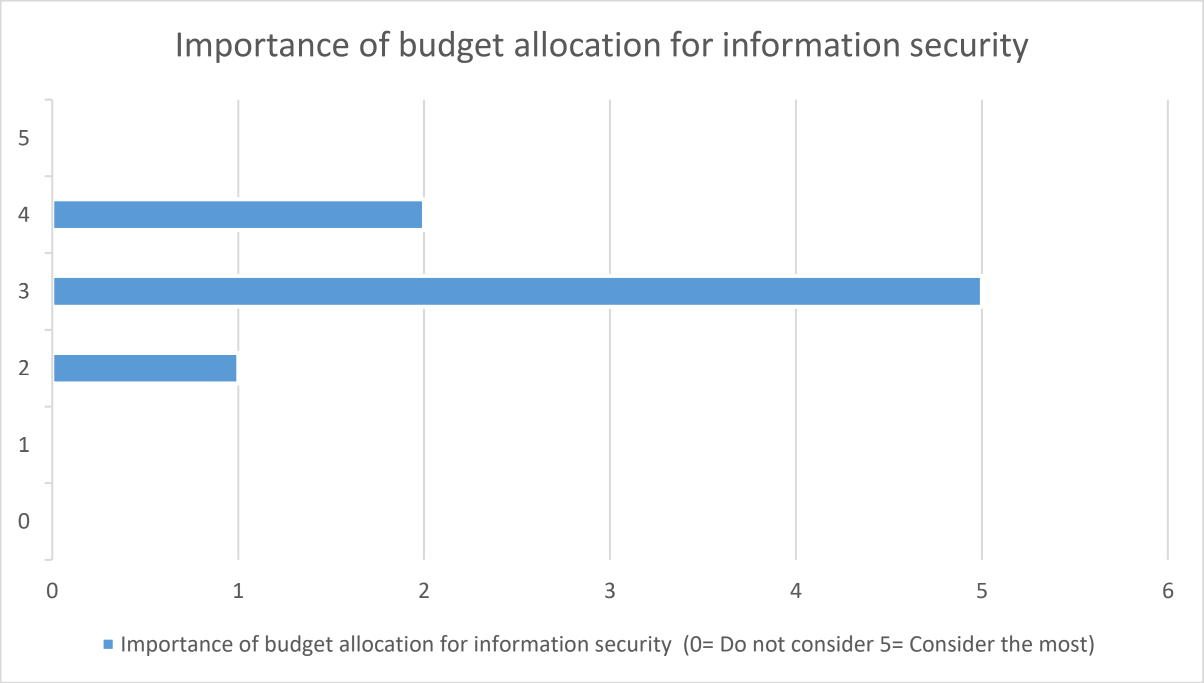


Figure E.346: Importance of budget allocation for information security (**6-10** years UK)

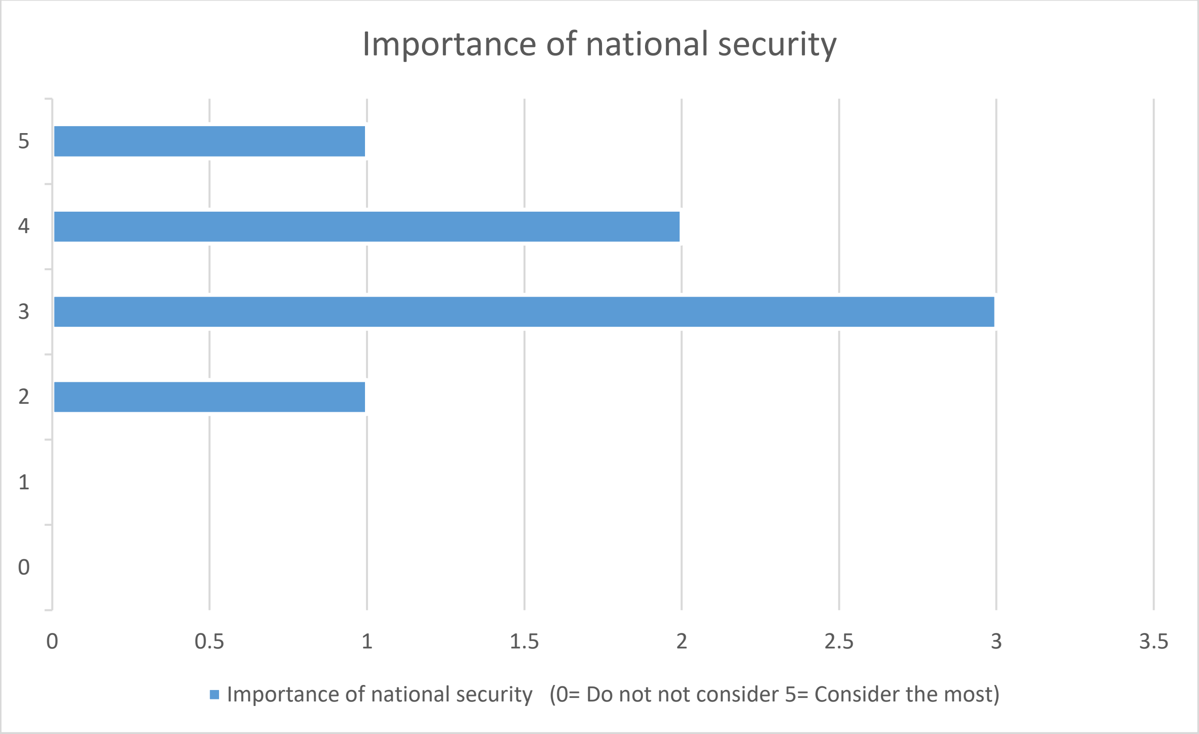


Figure E.347: Importance of national security (**6-10** years UK)

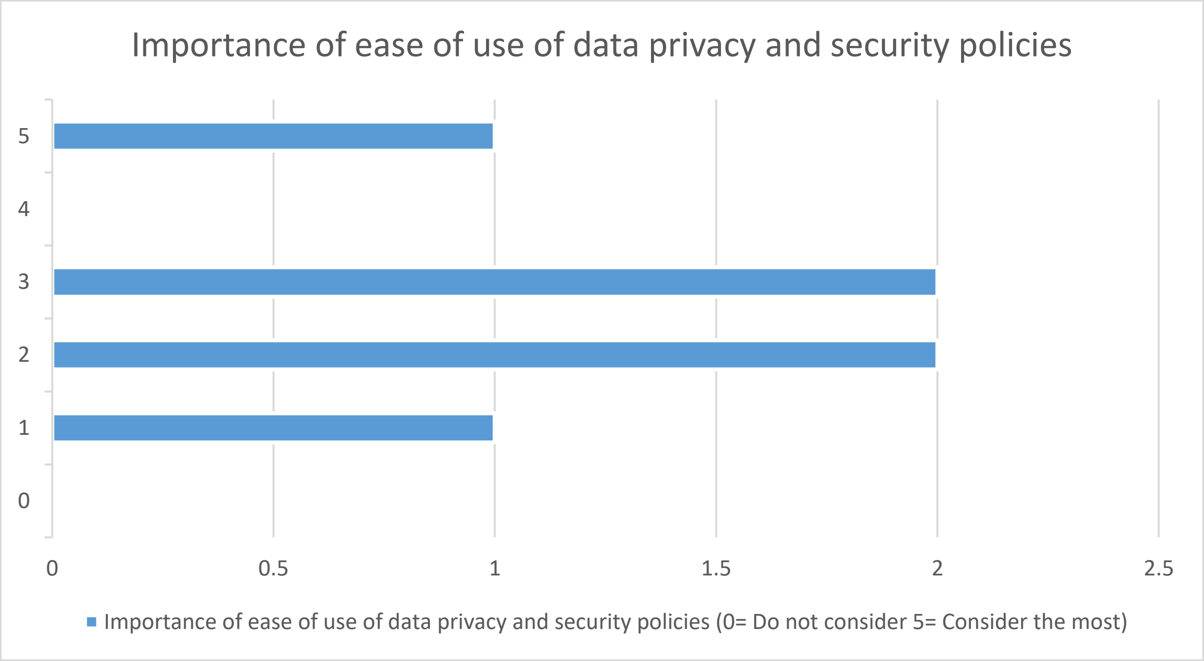


Figure E.348: Importance of ease of use of data privacy and security policies (**6-10** years UK)

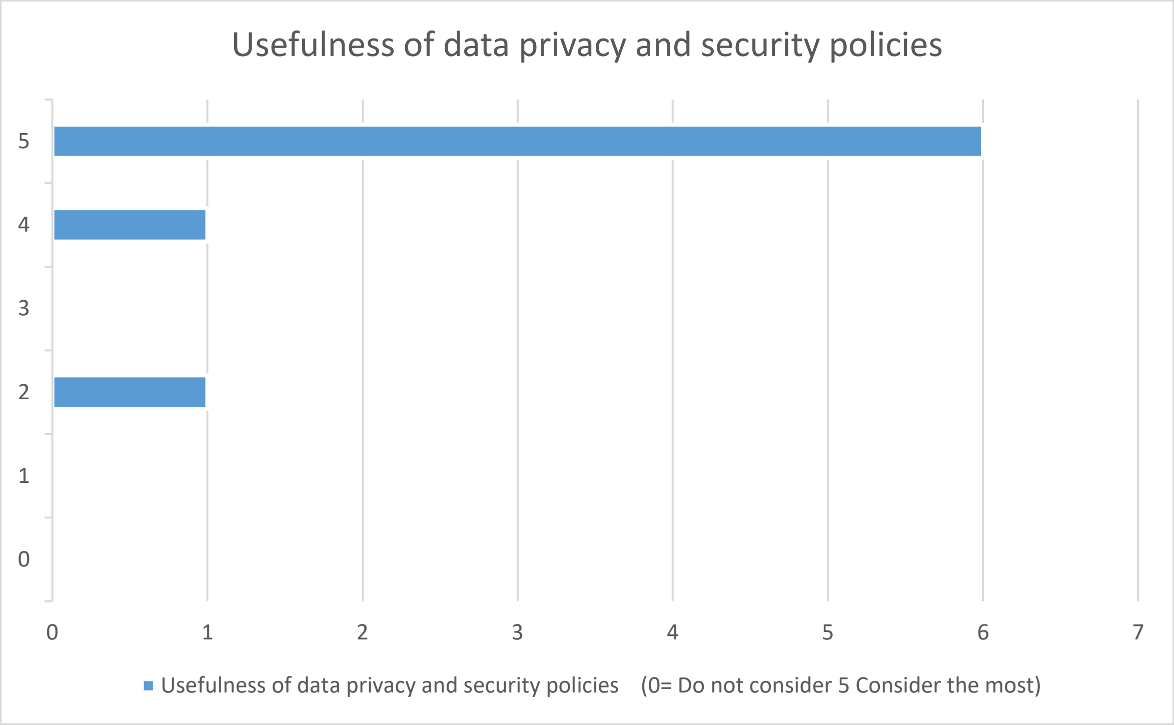


Figure E.349: Usefulness of data privacy and security policies (**6-10** years UK)

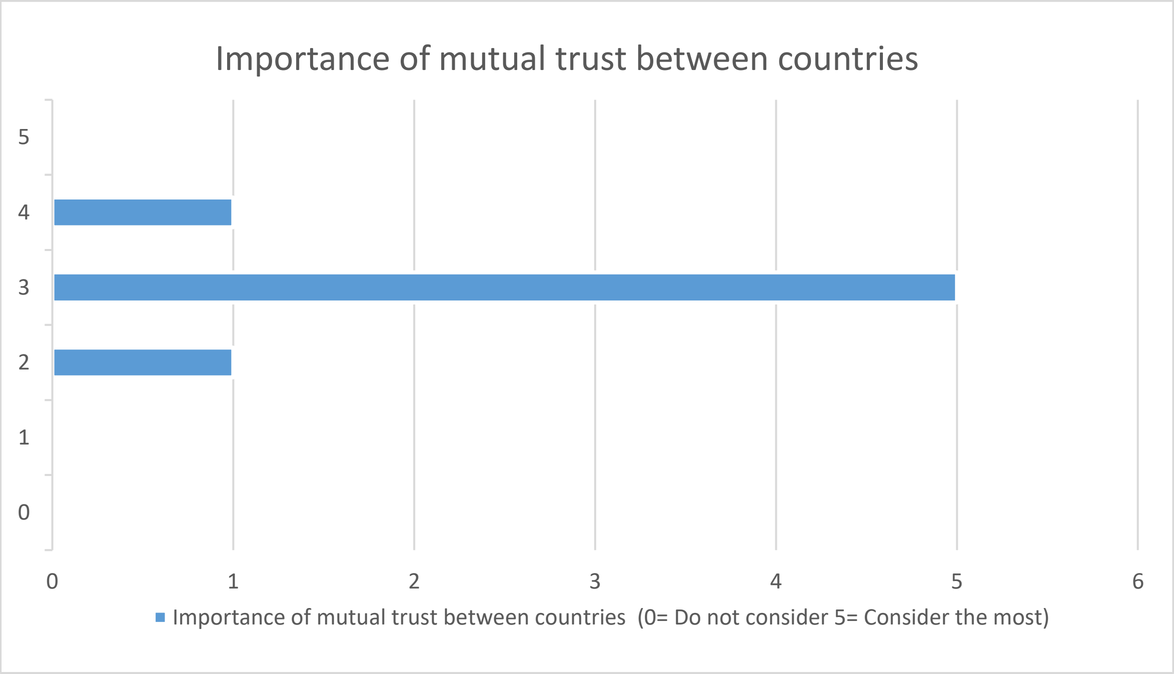


Figure E.350: Importance of mutual trust between countries (**6-10** years UK)

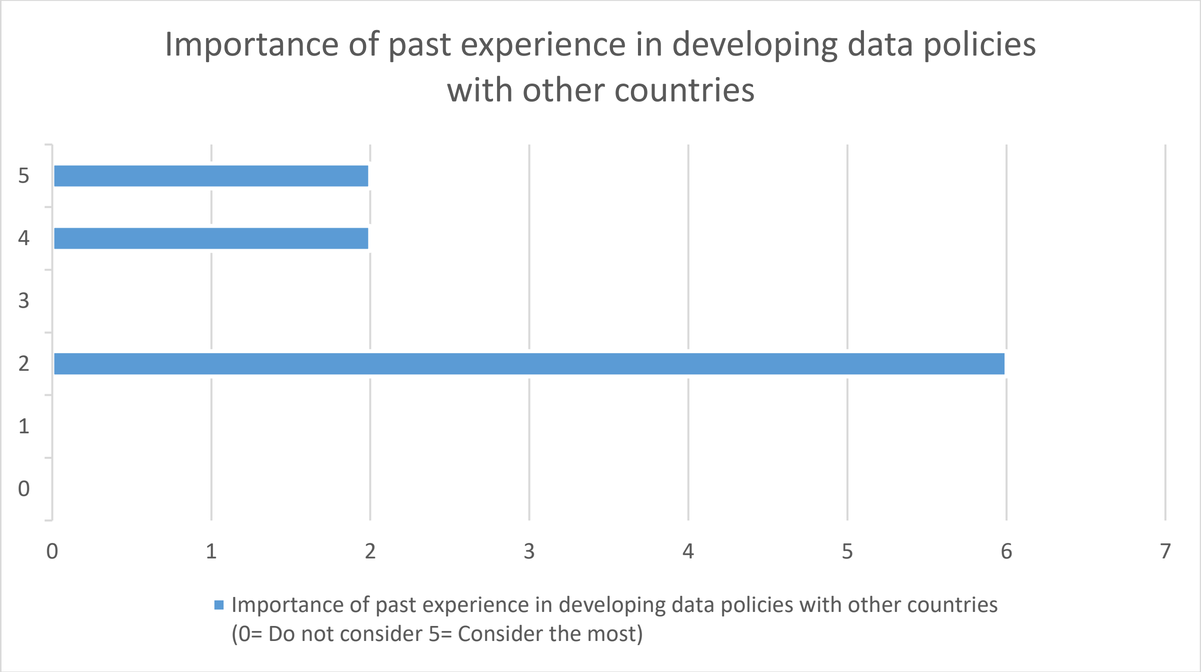


Figure E.351: Importance of past experience in developing data policies with other counties (**6-10** years UK)

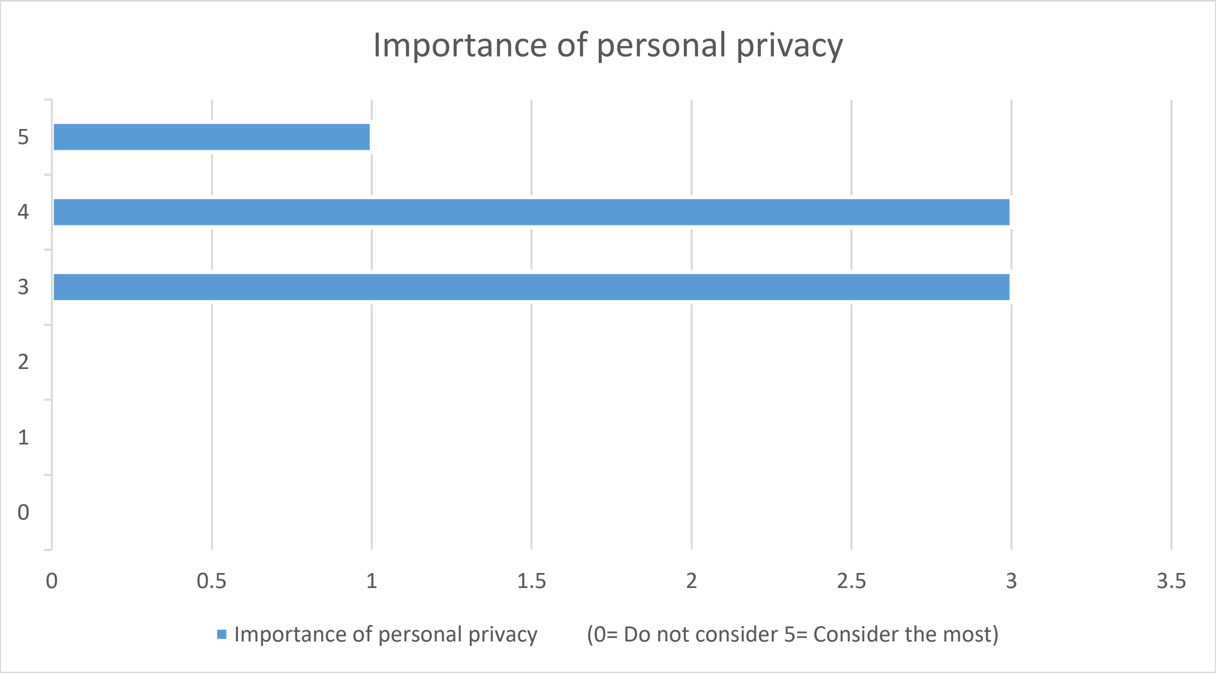


Figure E.352: Importance of personal privacy (**6-10** years UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 100 percent of the respondents have endorsed (See figure E.341). The other notable factors that have come out of the survey are organisational support, budget allocation, political differences, social differences, personal privacy, national security, the usefulness of data privacy and security policies and mutual trust between countries (See figure E.330-340) (See figure E.342-352) (See figure E.330-340) (See figure E.342-352). Most importantly, the participants have not highlighted the importance of economic differences (See figure E.344).

United Kingdom – Over 10 years

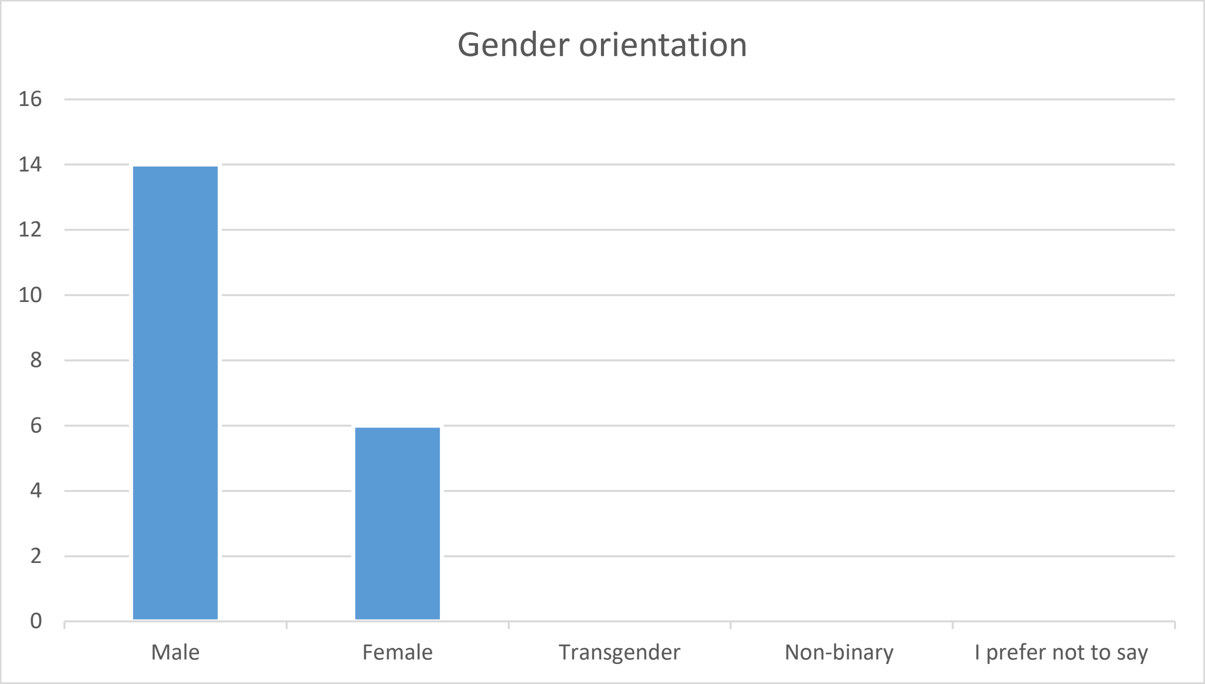


Figure E.353: Gender orientation (Over 10 years UK)

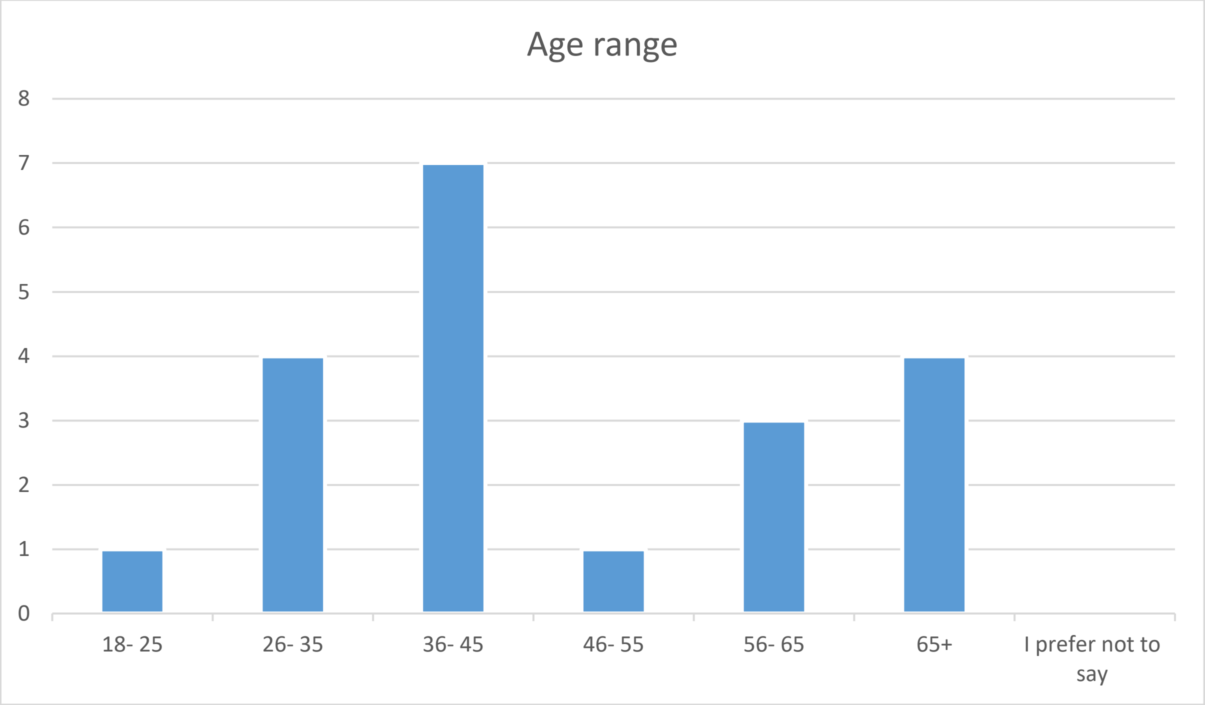


Figure E.354: Age range (Over 10 years UK)

This analysis is based on the responses received from United Kingdom participants with over 10 years of employment in the industry. There were 20 participants and 14 out of them were males and 6 females (See figure E.353). They were within the 18-65+ age range out of which 1 in the 18-25, 4 in the 26-35, 7 in the 36-45, 1 in the 46-55, 3 in the 56-65, and 4 in the 65+ range (See figure E.354).

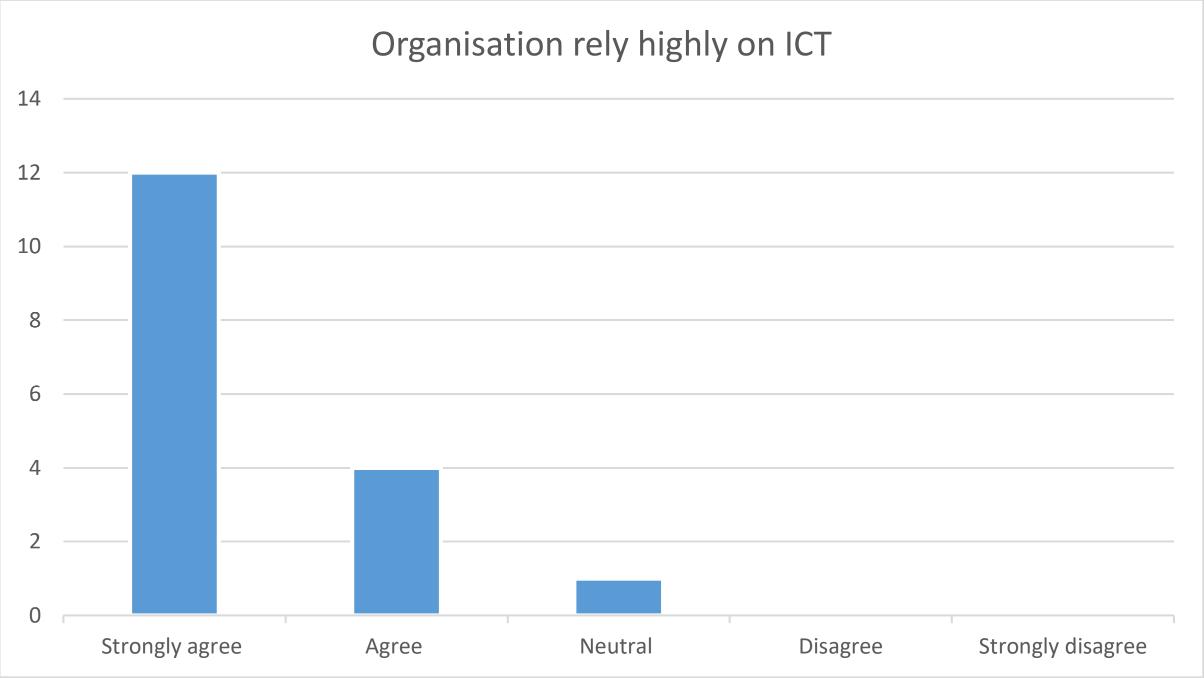


Figure E.355: Organisation rely highly on ICT (Over 10 years UK)

Out of the 20 respondents, 16 have worked in a technology reliance working environment, 1 unaware of reliance on technology because of the nature of the work assigned to them (See figure E.355). This indicates a majority of those who have been working in an organisation for over 10 years do have a high reliance on ICT.

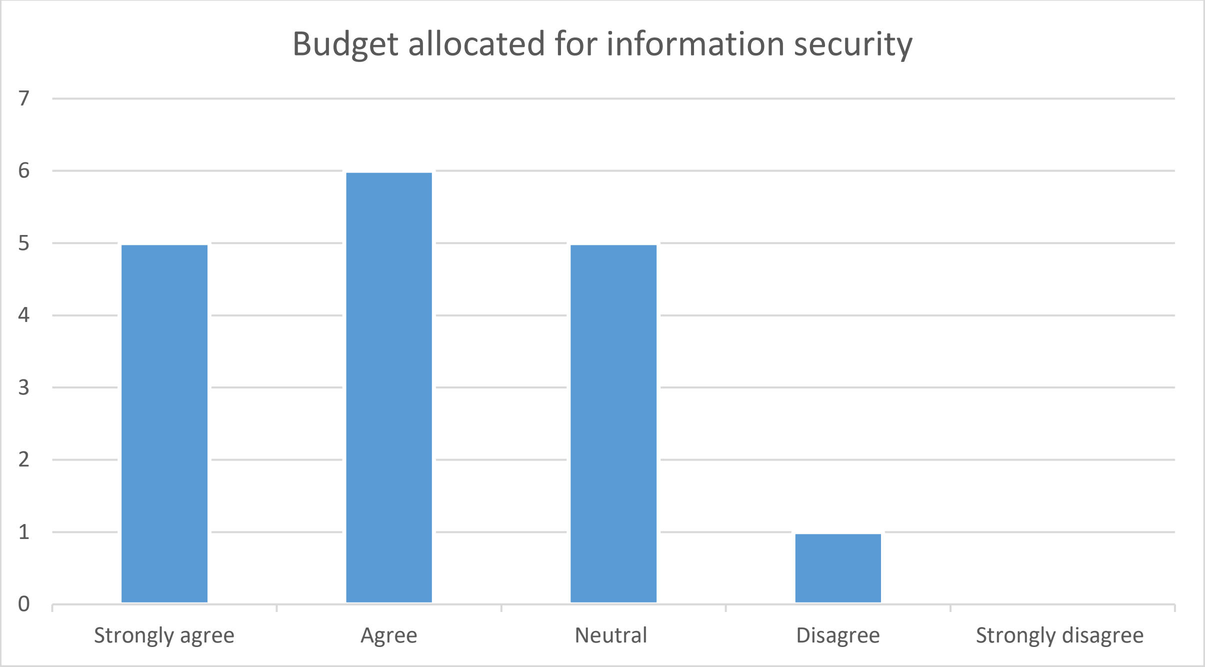


Figure E.356: Budget allocated for information security (Over 10 years UK)

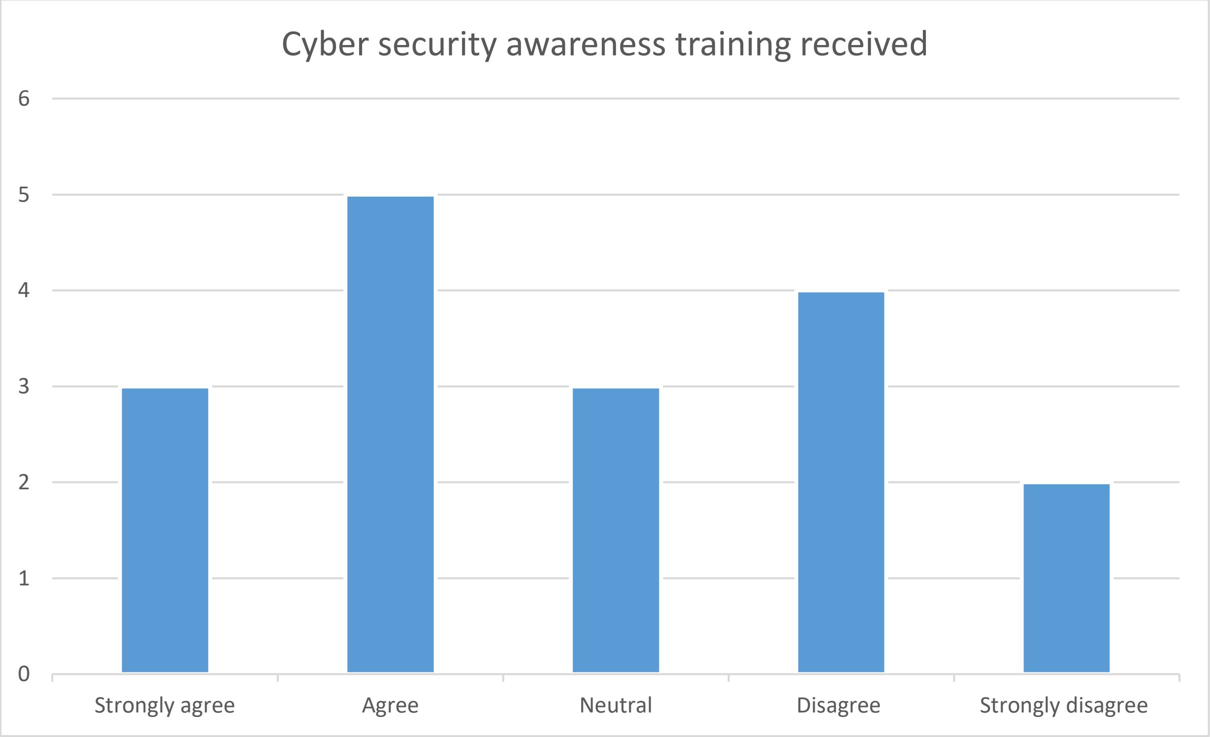


Figure E.357: Cyber security awareness training received (Over 10 years UK)

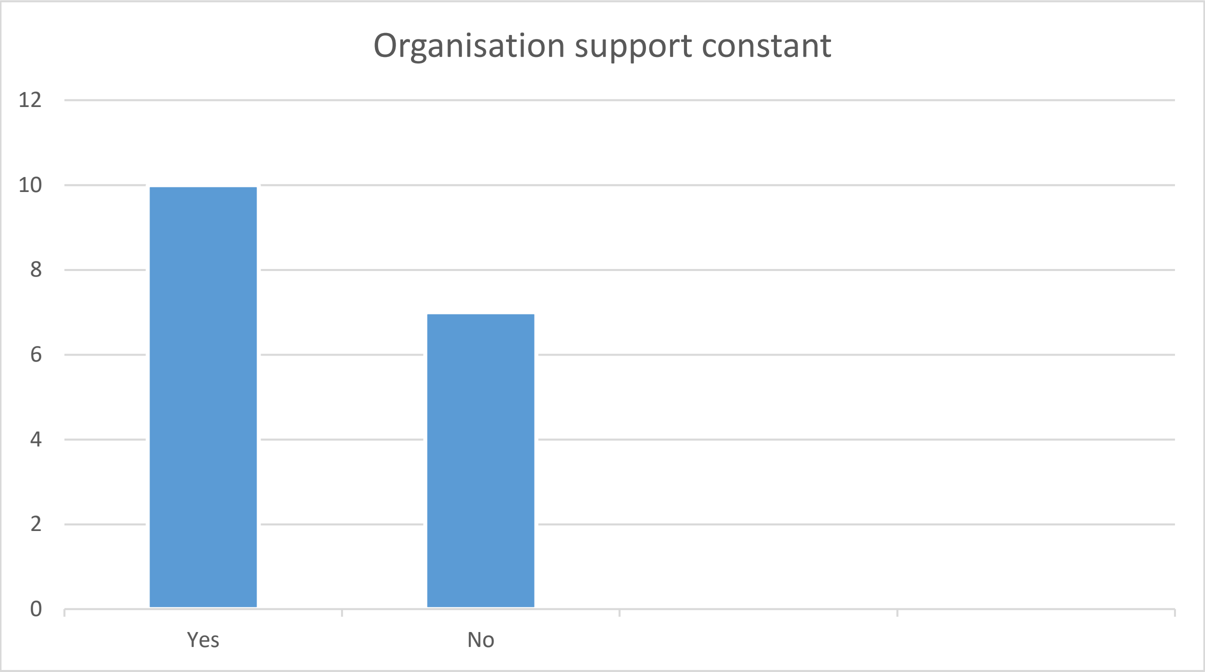


Figure E.358: Organisation support constant (Over 10 years UK)

Funding has been sketchy. 11 out of the 20 have indicated that their organisations had an allocated budget for information security, whilst 5 had not expressed an opinion either way and notably according to the 1 disagreed, their organisations had no budget allocation for information security (See figure E.356). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 8 participants have received regular cybersecurity awareness training, whilst 3 neither agreed nor disagreed, and 6 participants had not regularly received security awareness training (See figure E.357). However, 10 participants received support from the organisation to protect personal information, and 7 did not (See figure E.358). In this specific case, even though the organisation has not provided necessary training to their staff, according to the participants, the organisations provided appropriate support to protect personal information. In the UK, organisations are bound by the Data protection act 2018, and in an instance of a data breach, the organisations will incur heavy fines. It appears that the organisations are actively supporting their staff to protect the reputation of the organisation and to maintain consumer trust in them, and to avoid breaches and penalties.

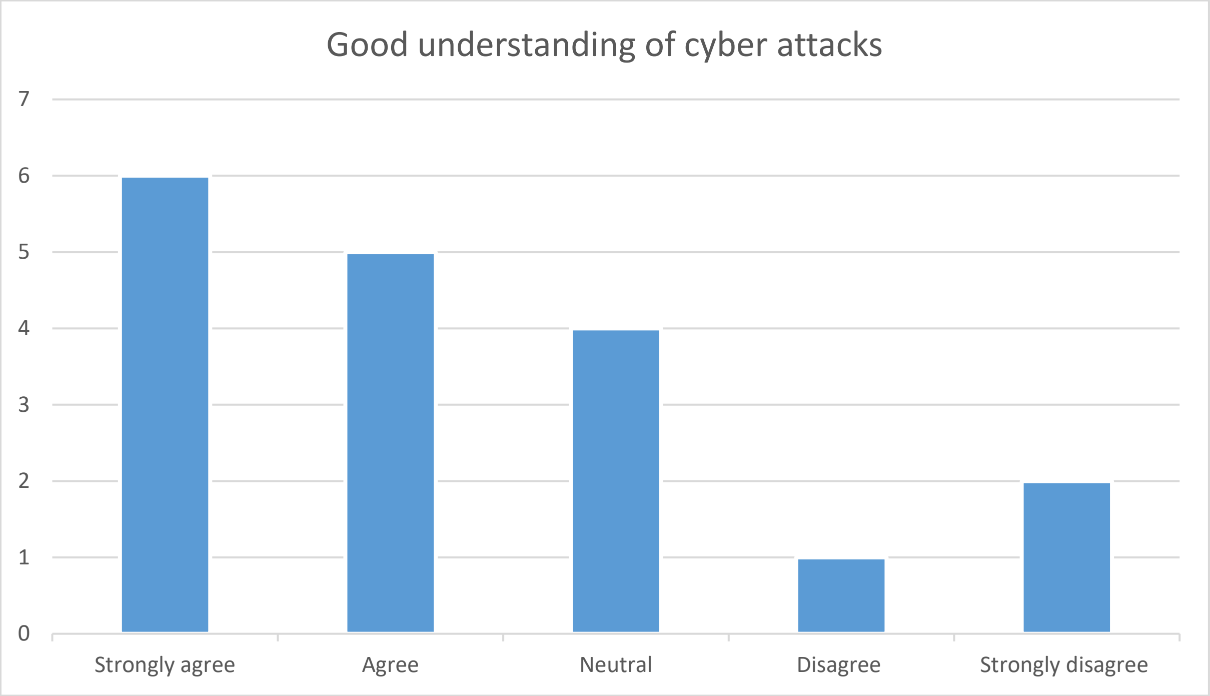


Figure E.359: Good understanding of cyberattacks (Over 10 years UK)

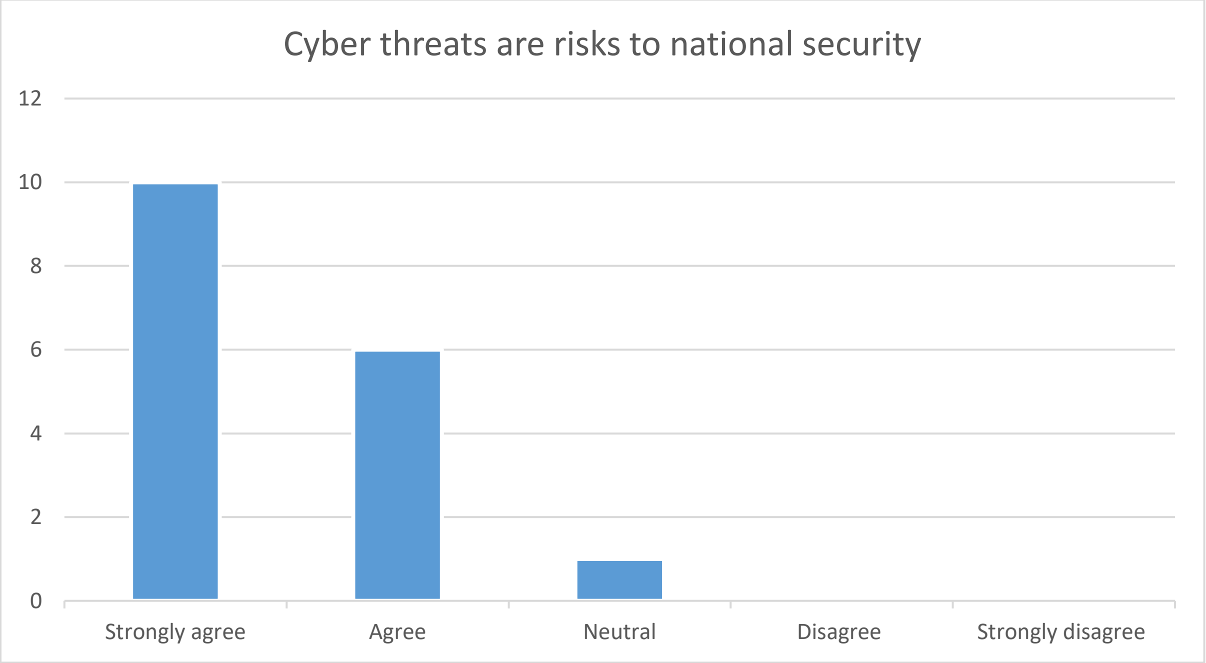


Figure E.360: Cyber threats are risks to national security (Over 10 years UK)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 11 participants do have, 4 have not expressed opinion either way, and only 3 participants had no understanding (See figure E.359). Furthermore,80 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure E.360). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

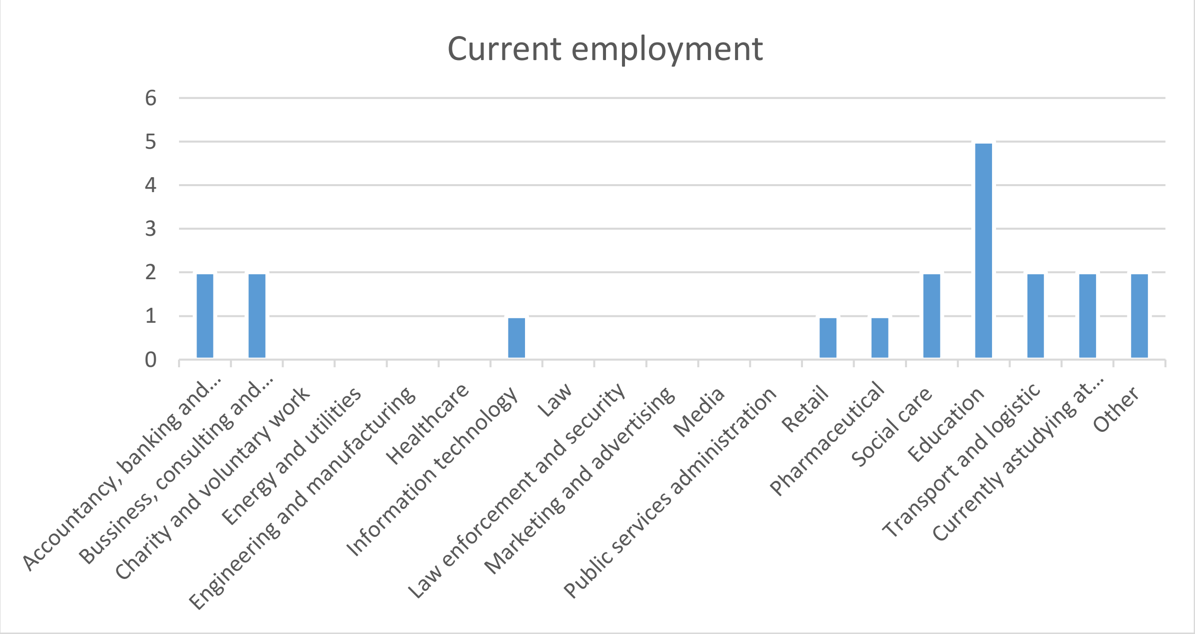


Figure E.361: Current employment (Over 10 years UK)

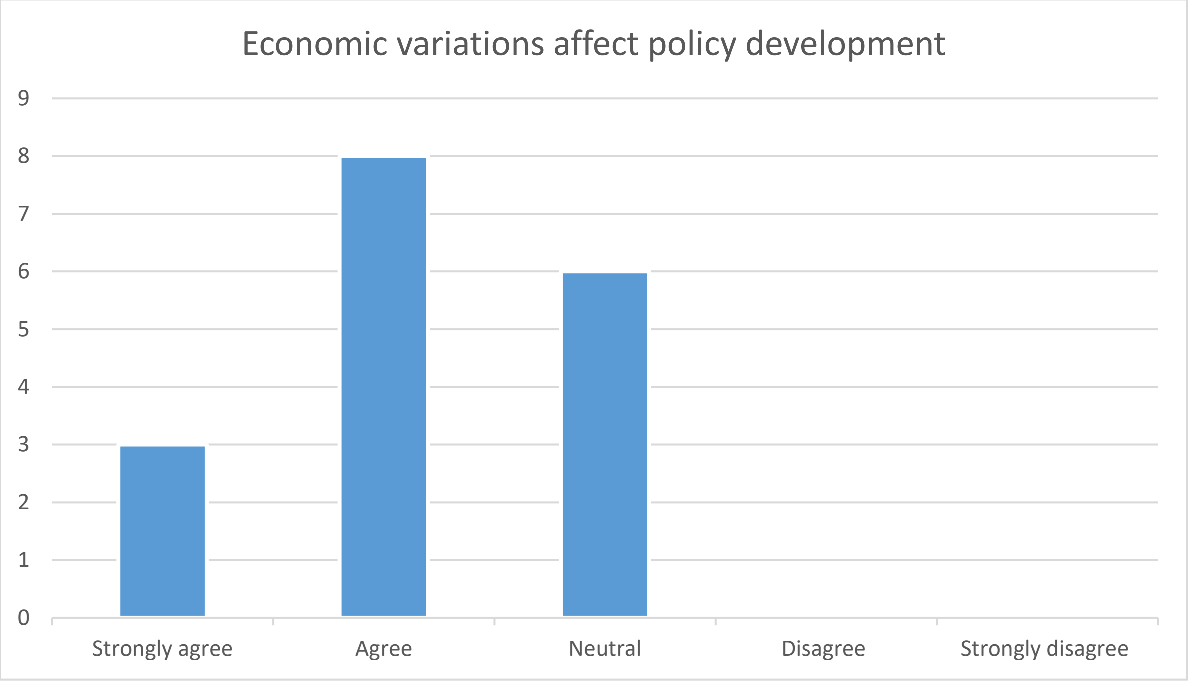


Figure E.362: Economic variations affect policy development (Over 10 years UK)

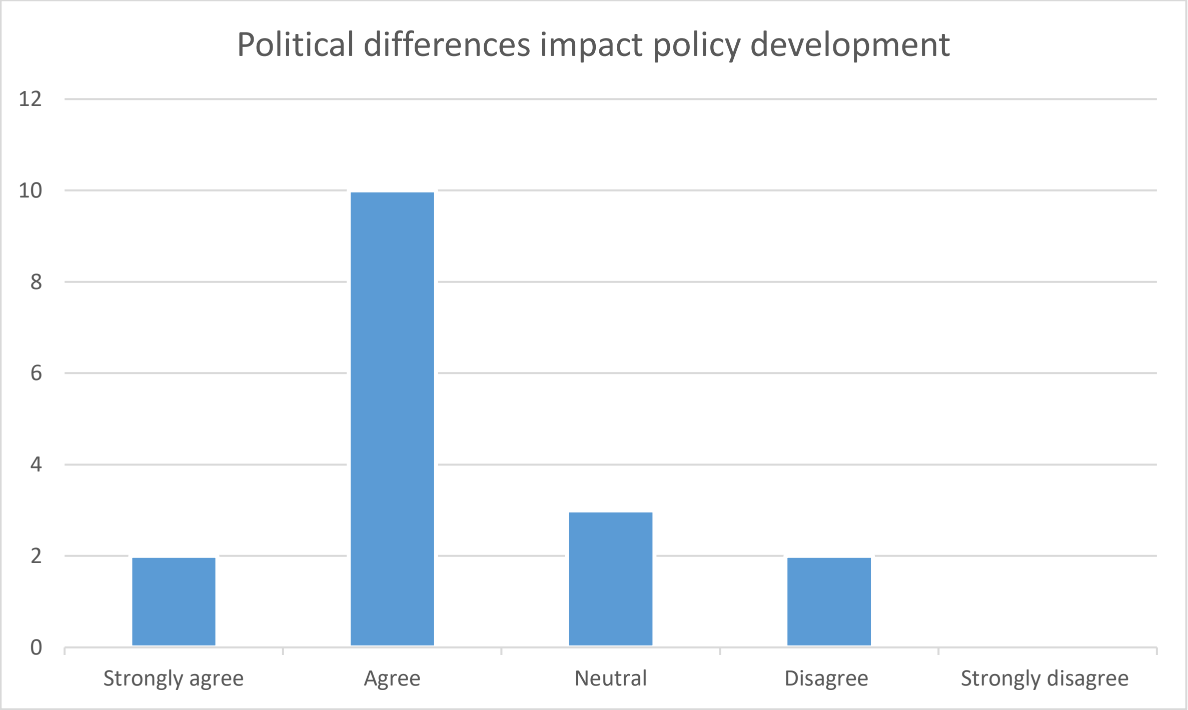


Figure E.363: Political differences impact policy development (Over 10 years UK)

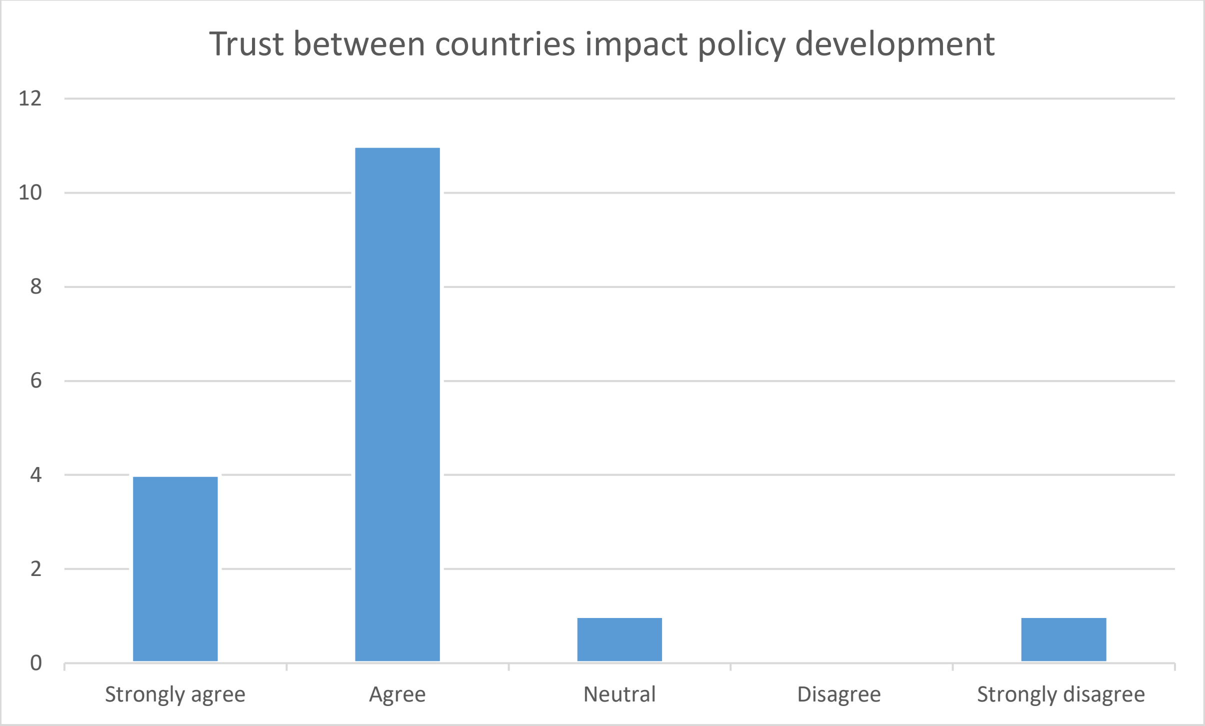


Figure E.364: Trust between countries impact policy development (Over 10 years UK)

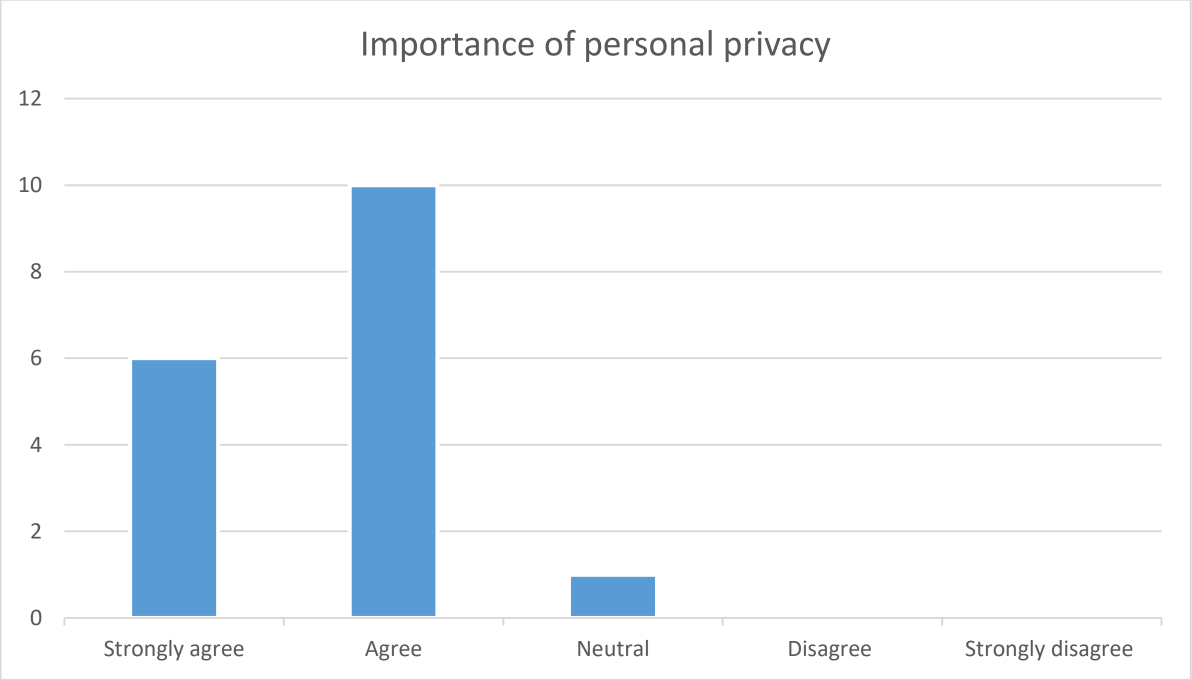


Figure E.365: Importance of personal privacy (Over 10 years UK)

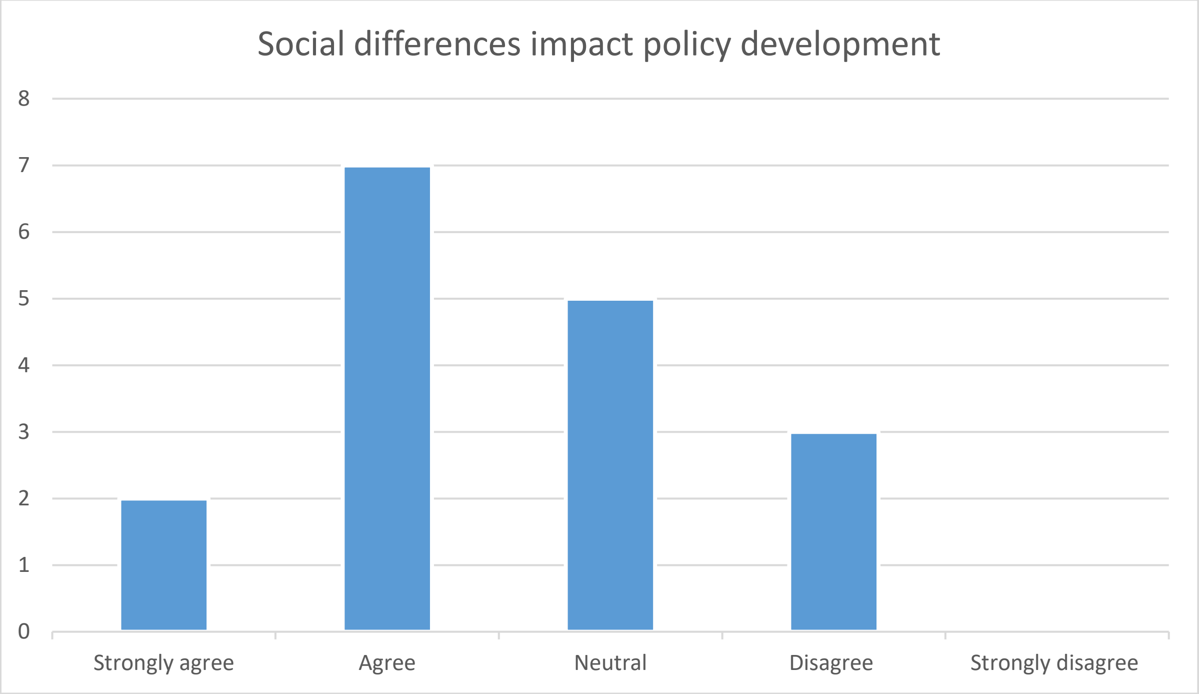


Figure E.366: Social differences impact policy development (Over 10 years UK)

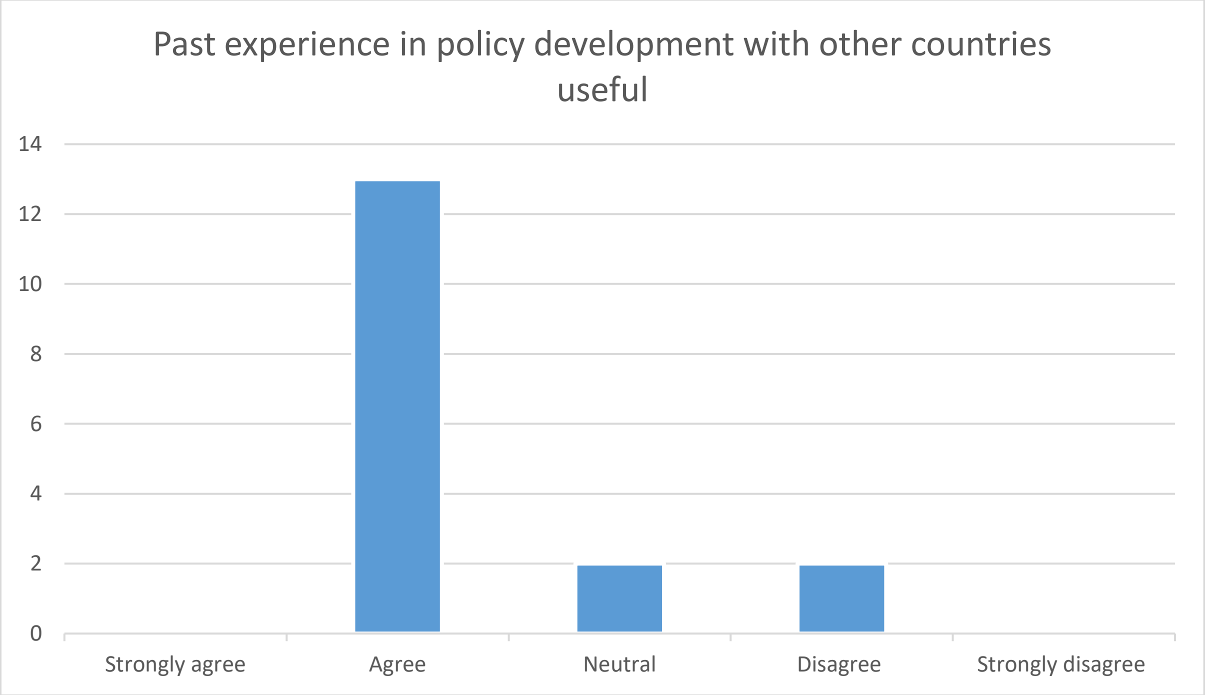


Figure E.367: Past experience in policy development with other countries useful (Over 10 years UK)

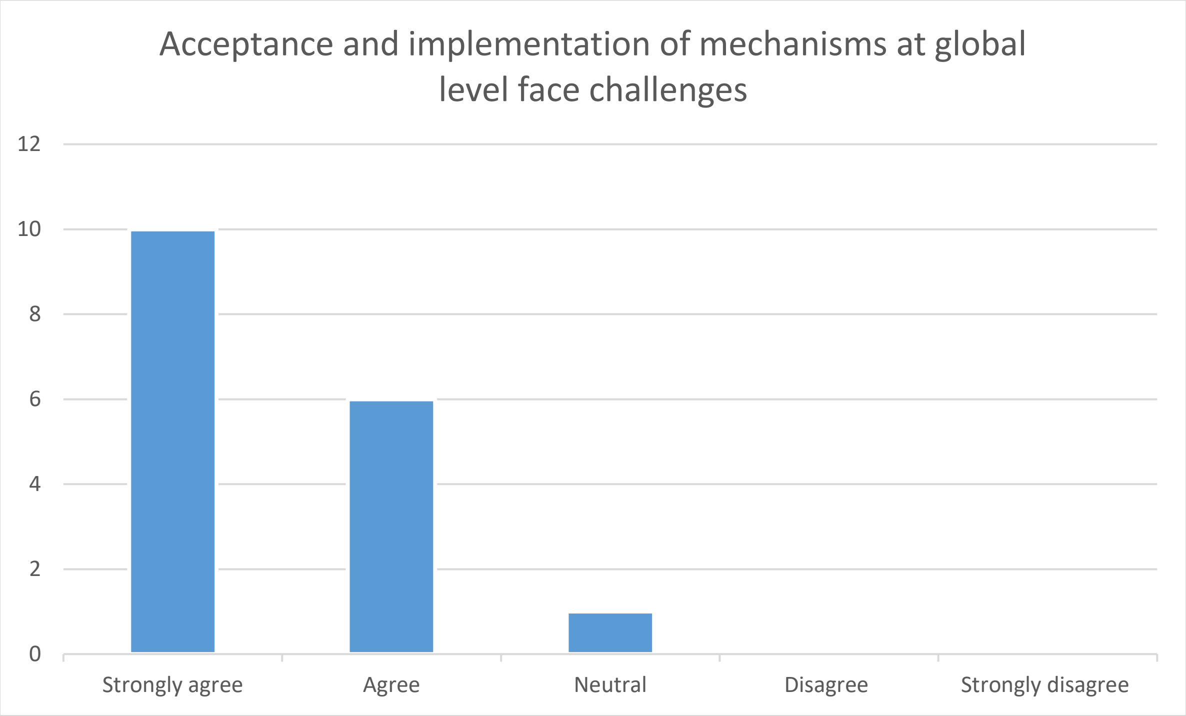


Figure E.368: Acceptance and implementation of mechanisms at global level face challenges (Over 10 years UK)

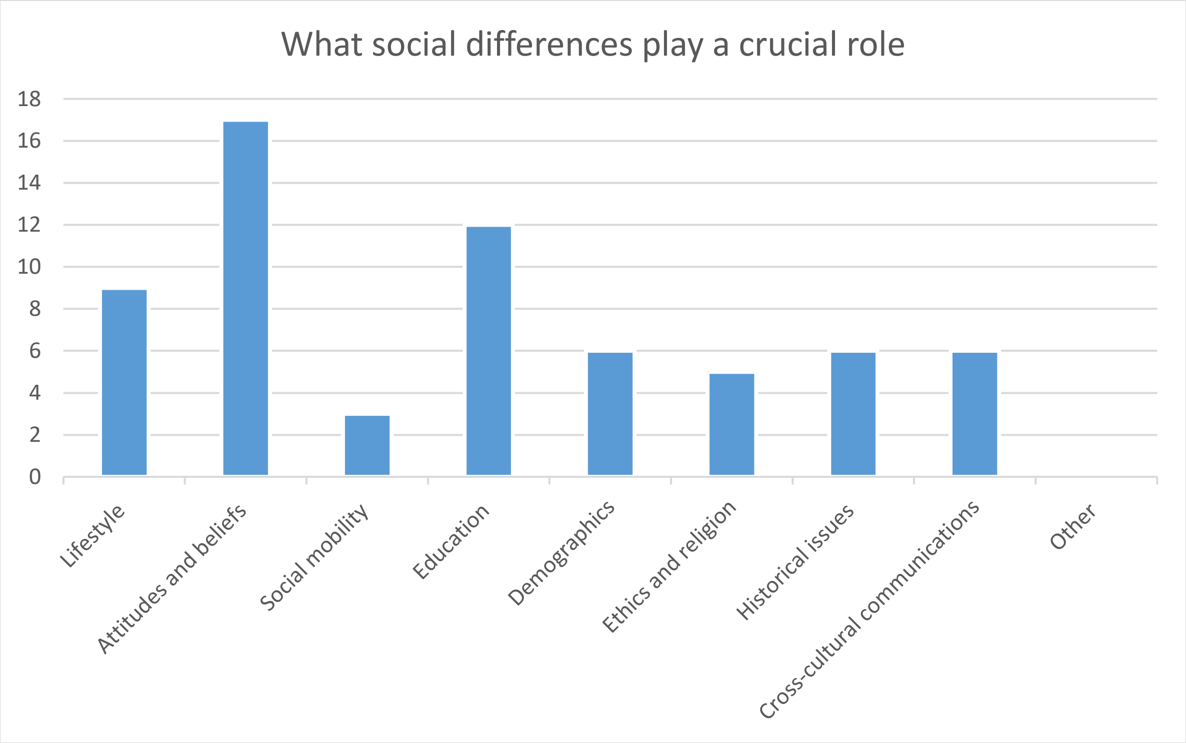


Figure E.369: What social differences play a crucial role (Over 10 years UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure E.369). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

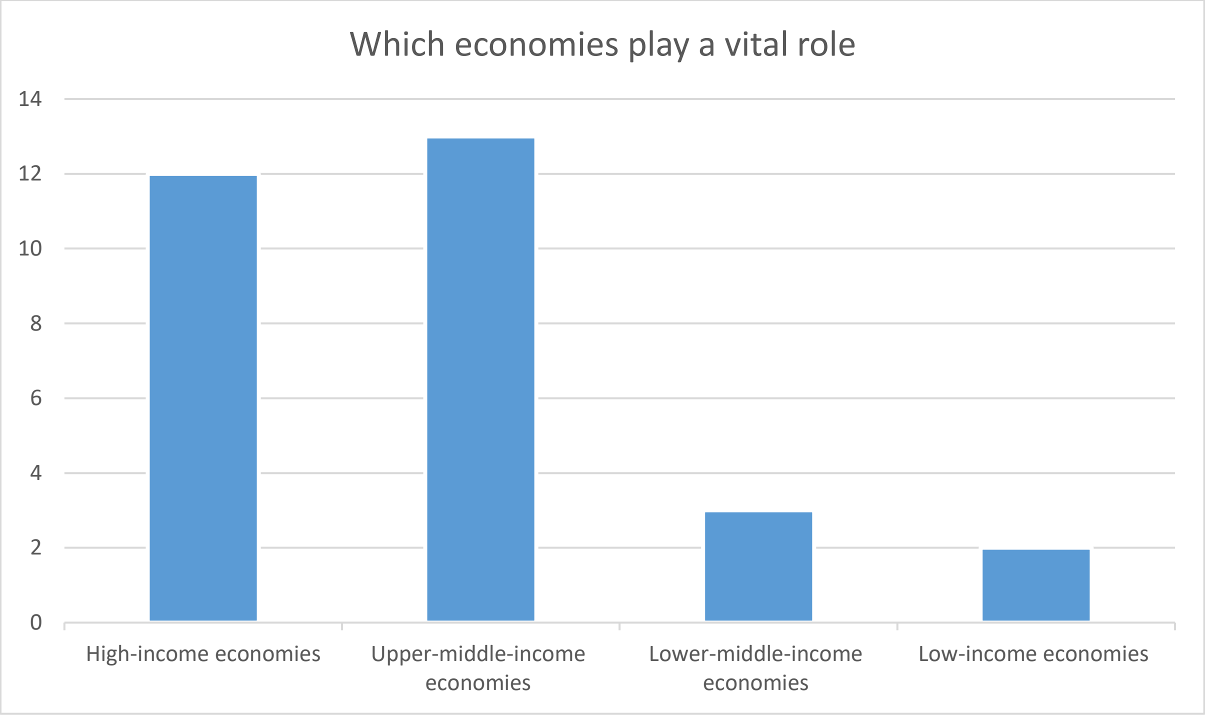


Figure E.370: Which economies play a vital role (Over 10 years UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.370). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

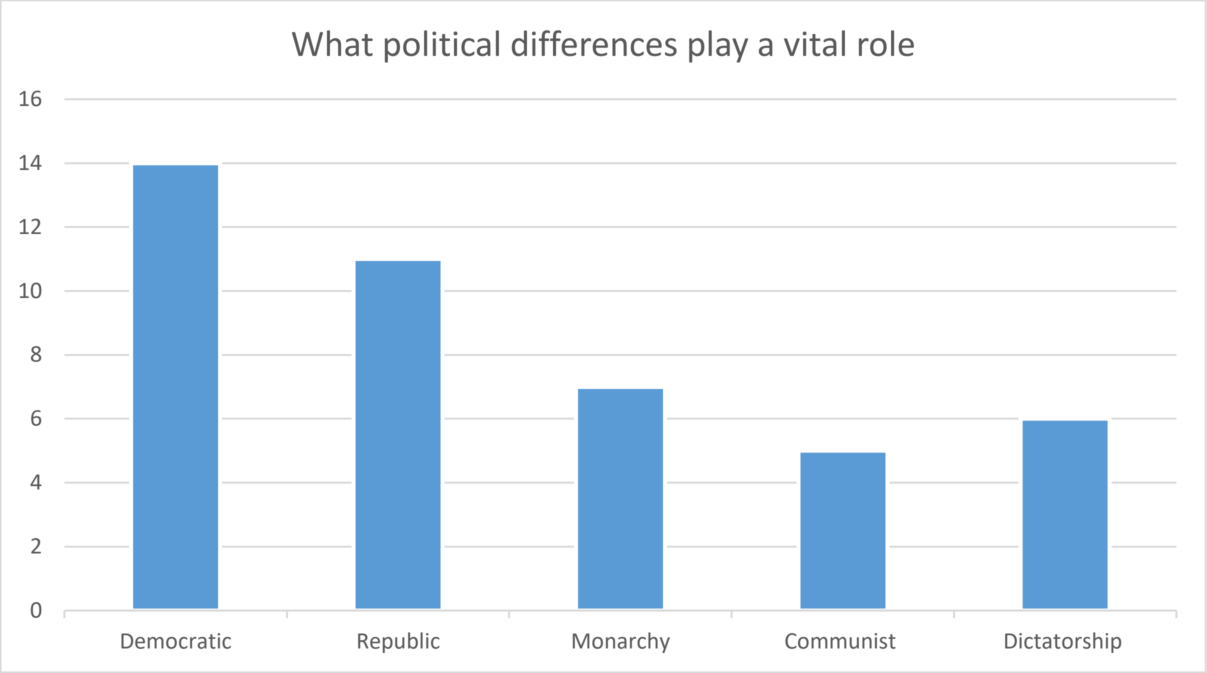


Figure E.371: What political differences play a vital role (Over 10 years UK)

The majority have chosen democratic and republic political systems (See figure E.371). In a democratic system, it allows a public voice to influence in the process of policy development and facilitates a consensus and collective responsibility for their actions. In a Republican system, the people and their elected representatives hold power and entrusted with taking decisions in accordance with the constitution. For those reasons, a reasonable assumption to make is the people look for legal assurances through the constitution to prevent the governments and organisations from compromising collected personal information. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

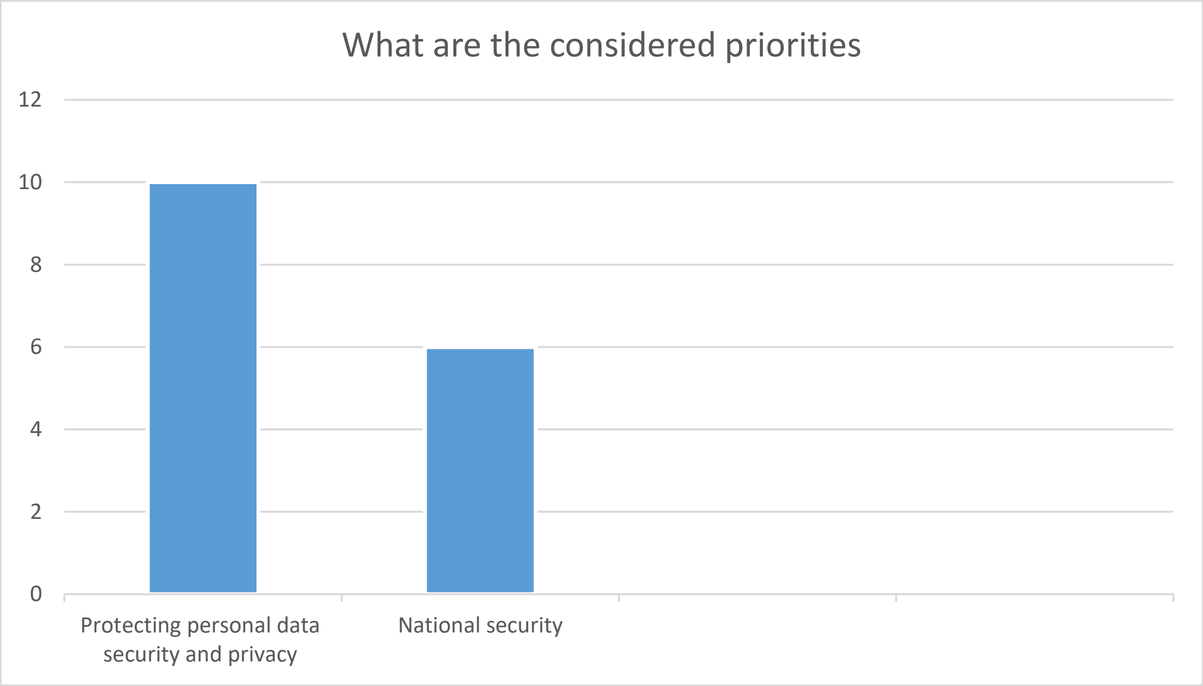


Figure E.372: What are the considered priorities (Over 10 years UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security (See figure E.372), which is a significant factor. However, in an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

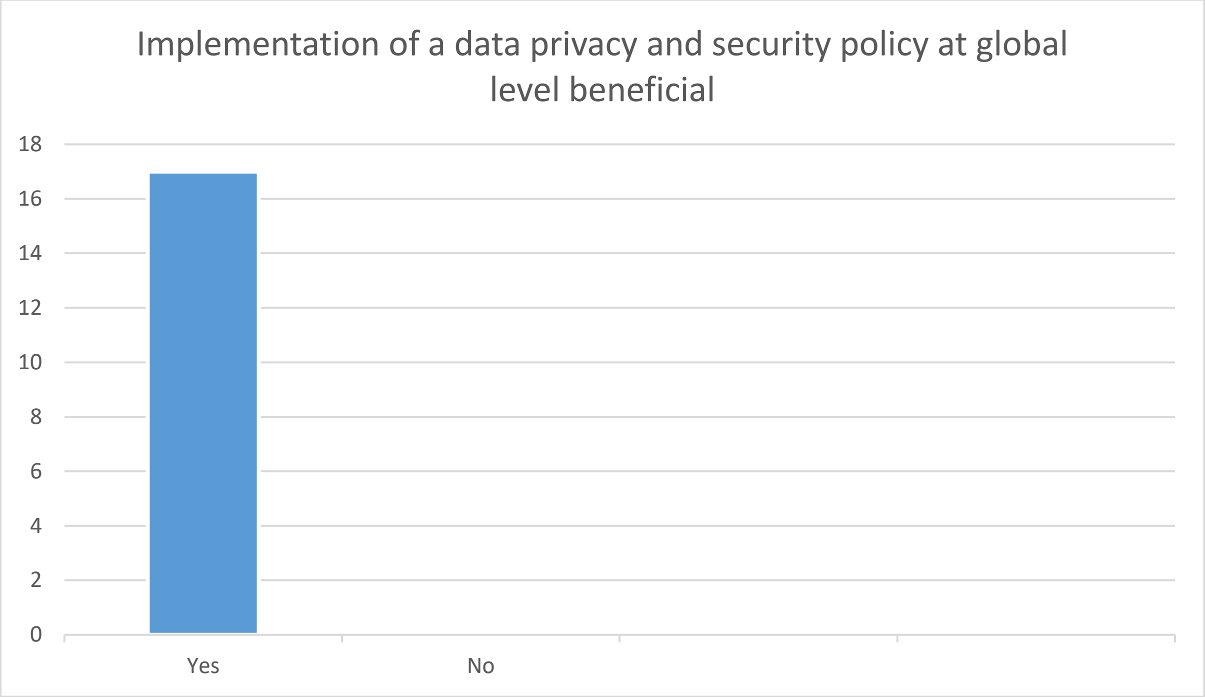


Figure E.373: Implementation of a data privacy and security policy at global level beneficial (Over 10 years UK)

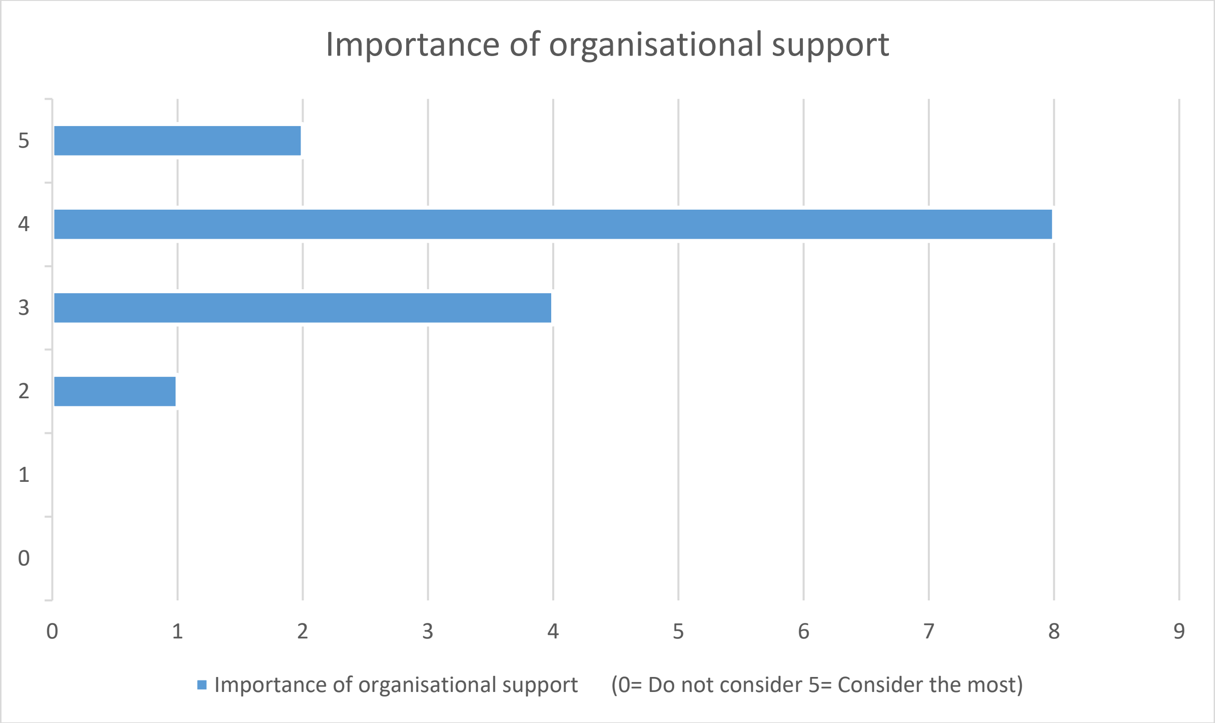


Figure E.374: Importance of organisational support (Over 10 years UK)

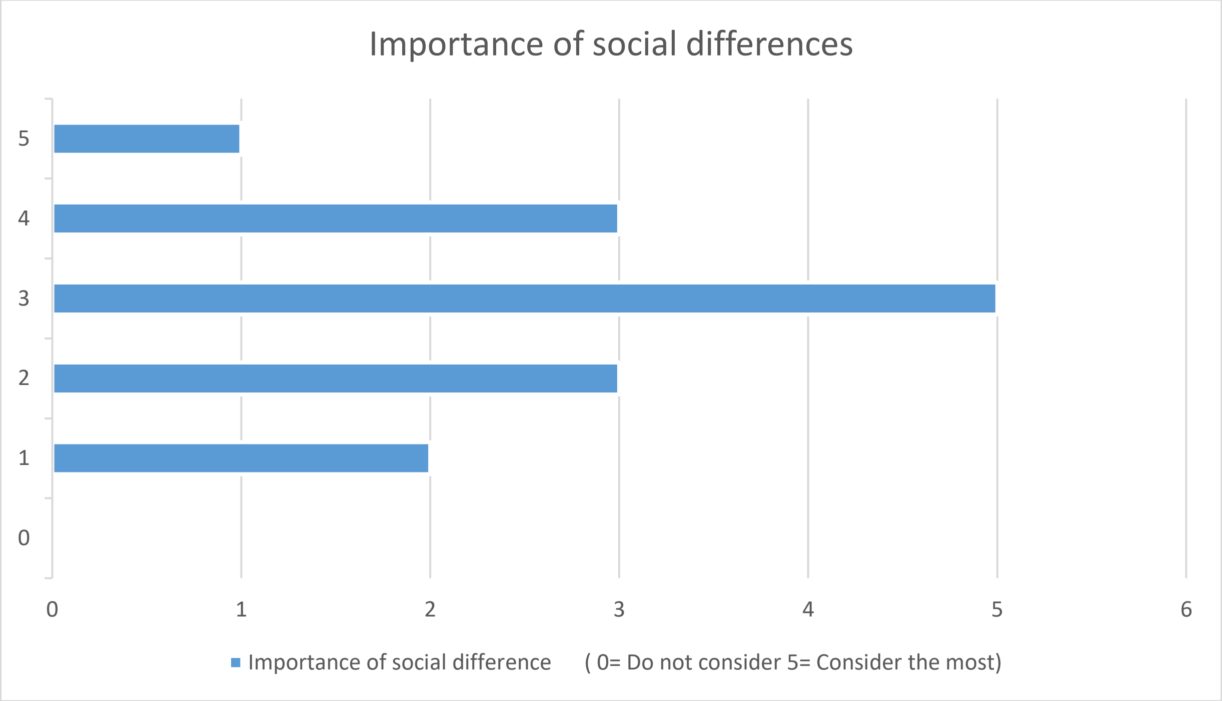


Figure E.375: Importance of social differences (Over 10 years UK)

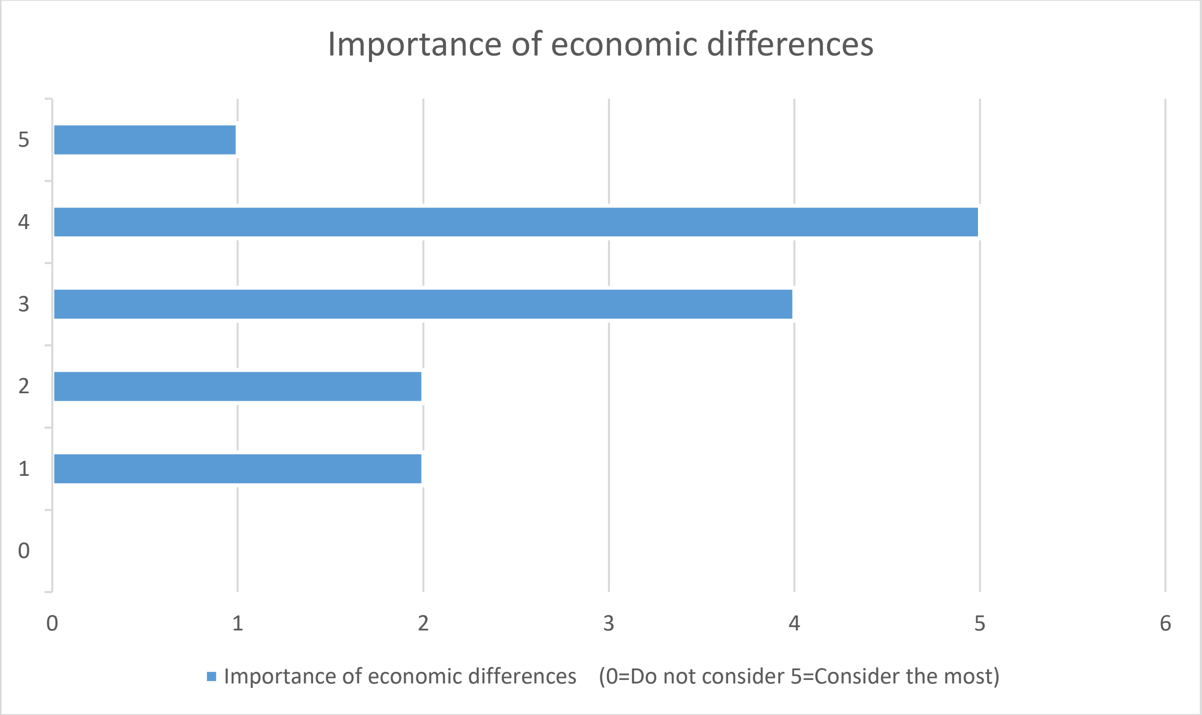


Figure E.376: Importance of economic differences (Over 10 years UK)

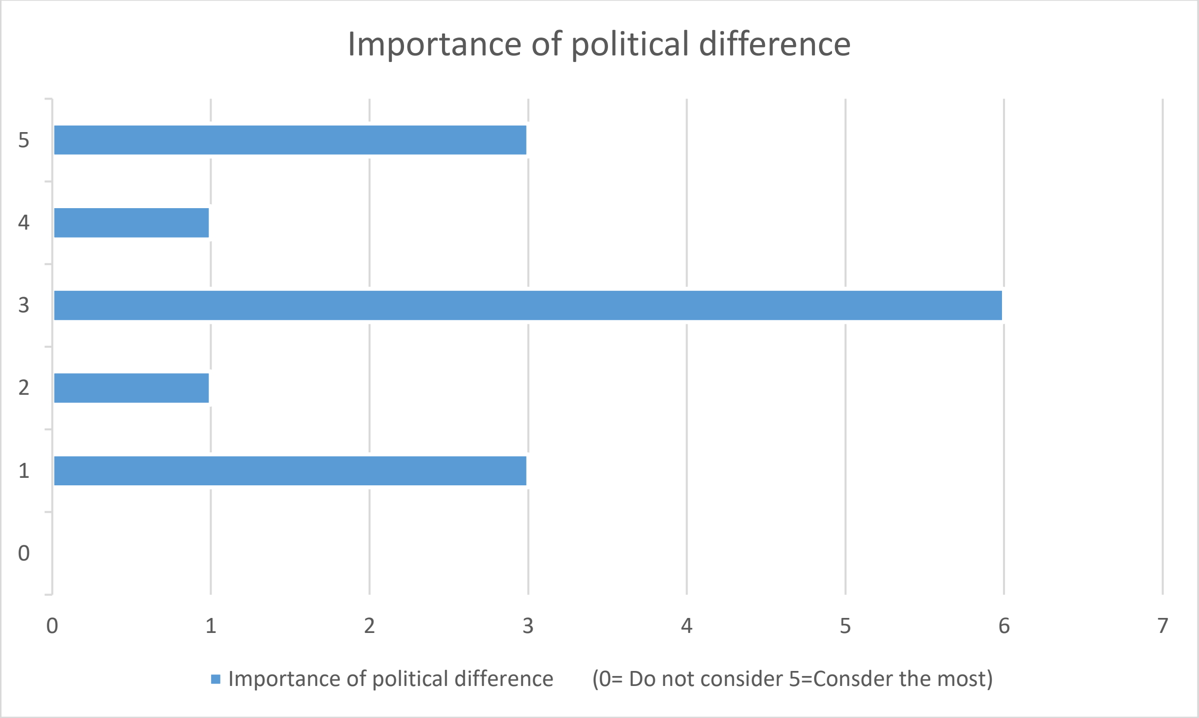


Figure E.377: Importance of political difference (Over 10 years UK)

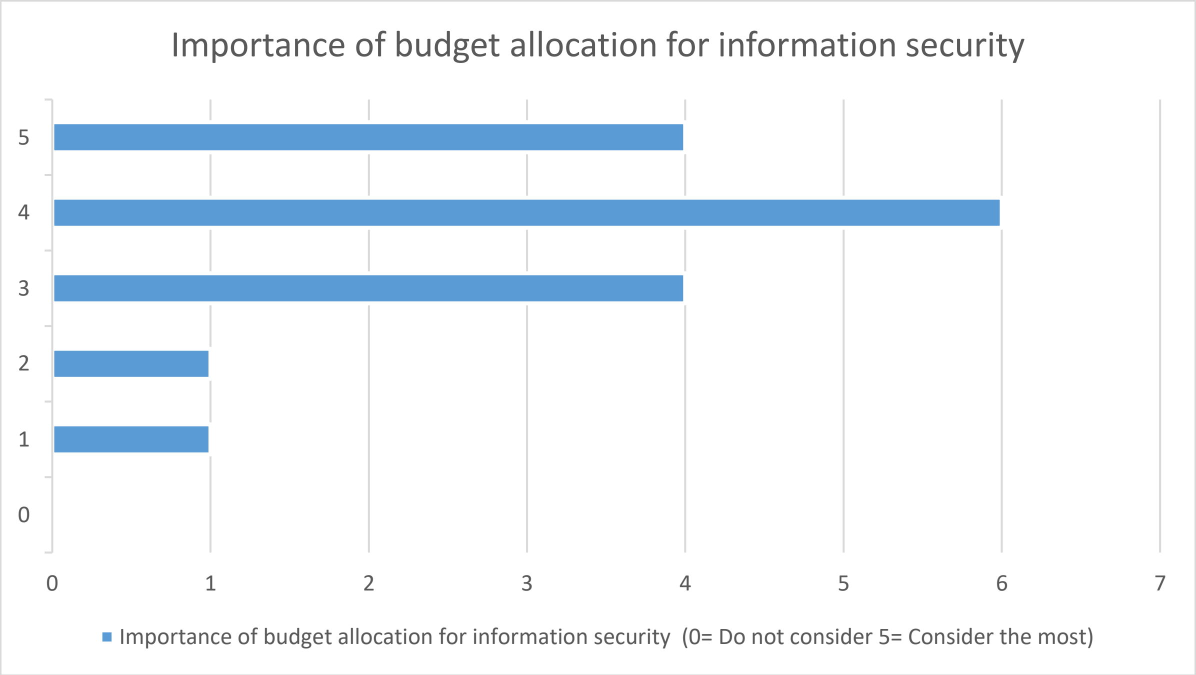


Figure E.378: Importance of budget allocation for information security (Over 10 years UK)

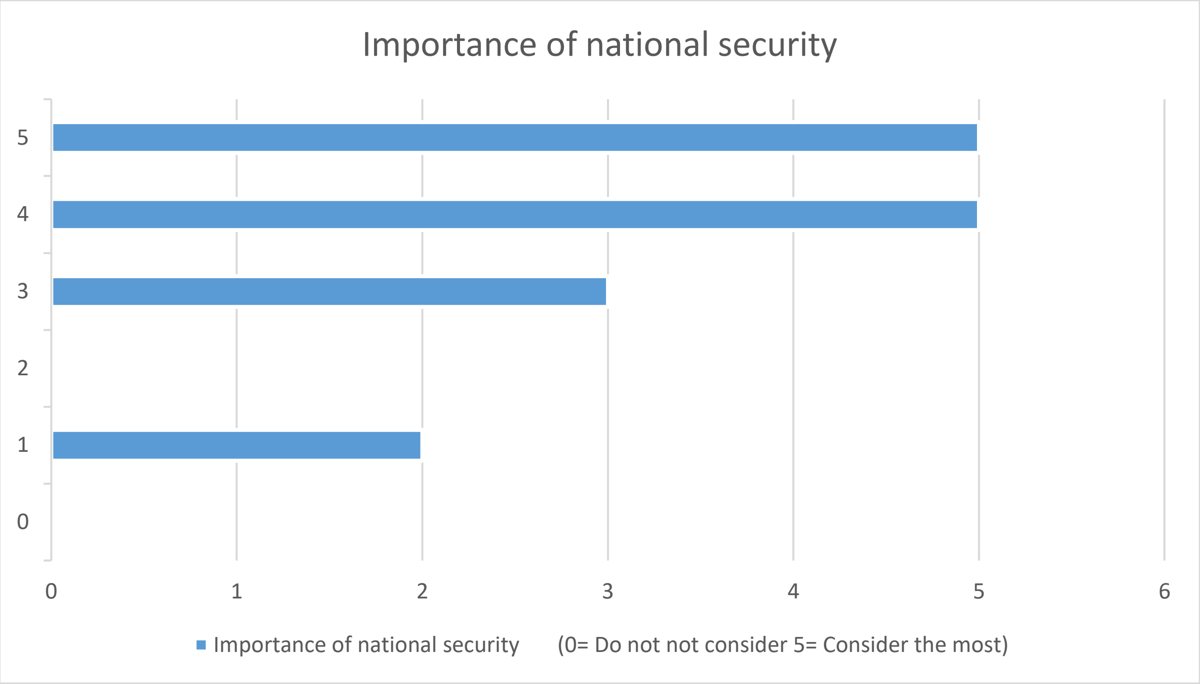


Figure E.379: Importance of national security (Over 10 years UK)

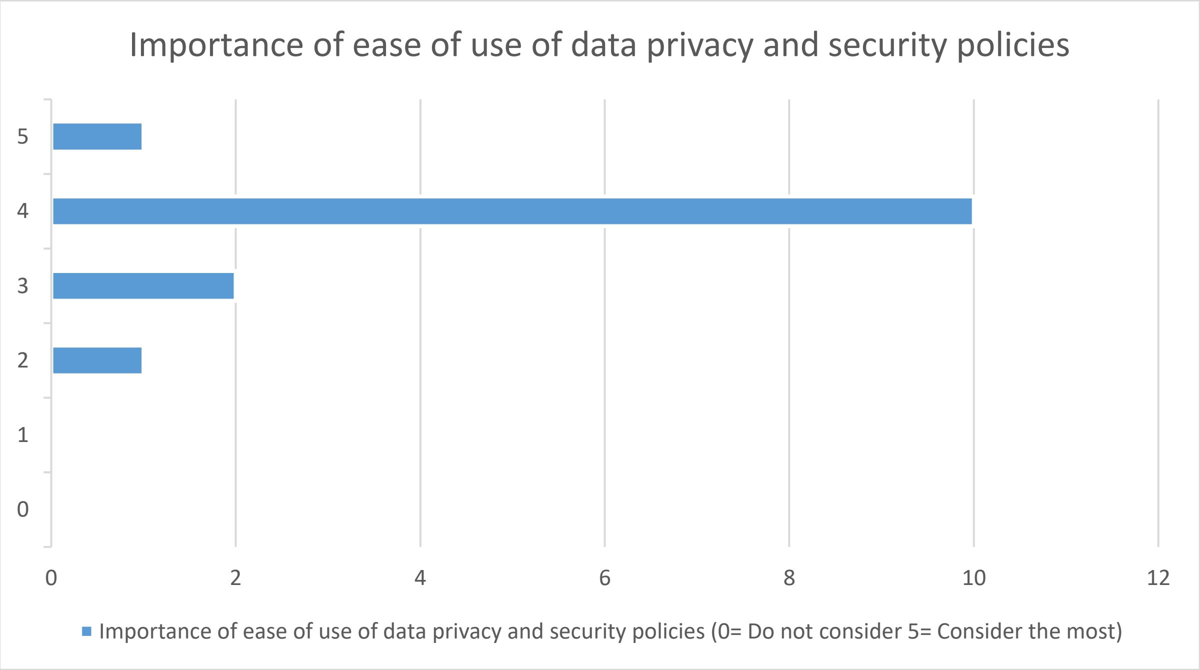


Figure E.380: Importance of ease of use of data privacy and security policies (Over 10 years UK)

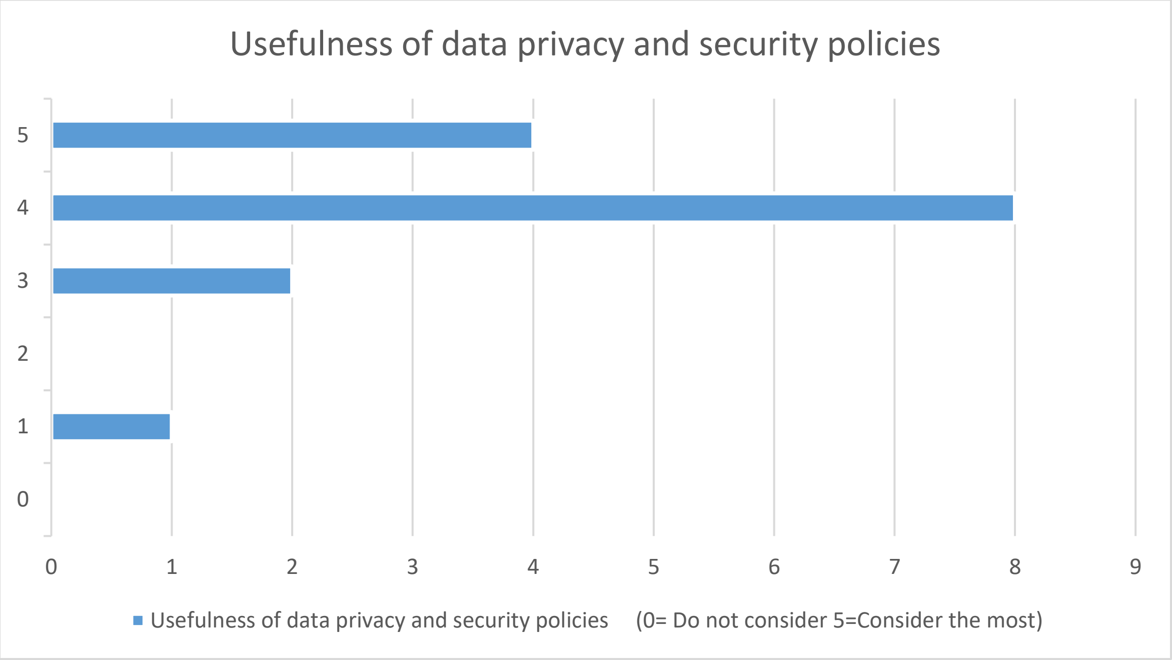


Figure E.381: Usefulness of data privacy and security policies (Over 10 years UK)

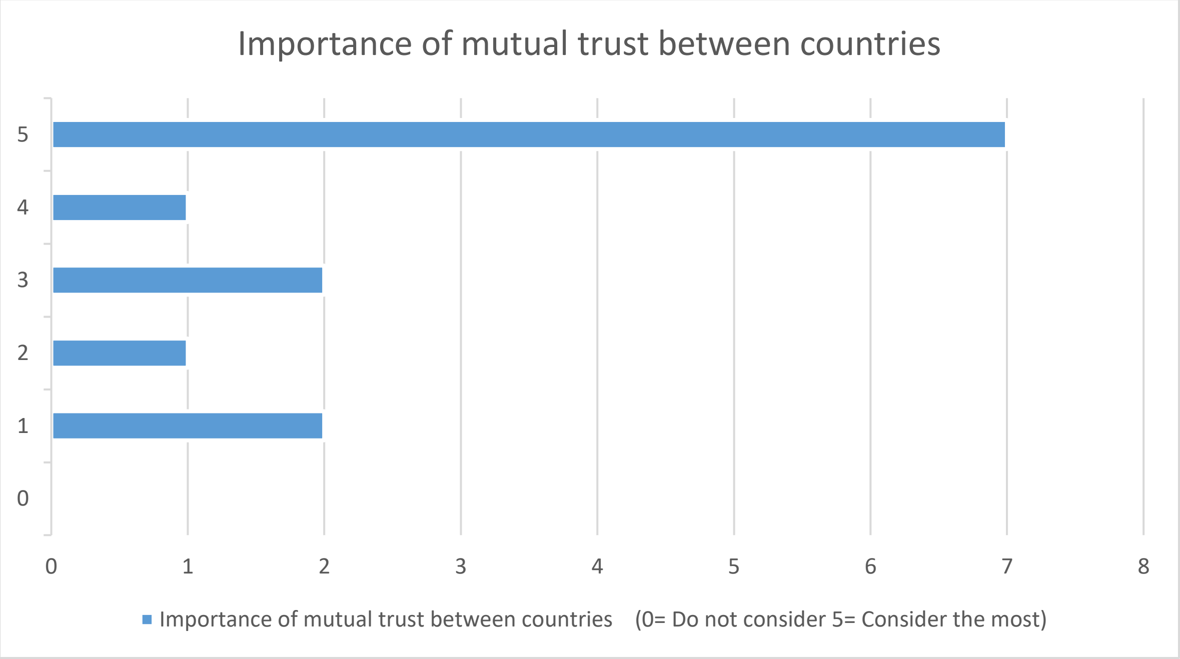


Figure E.382: Importance of mutual trust between countries (Over 10 years UK)

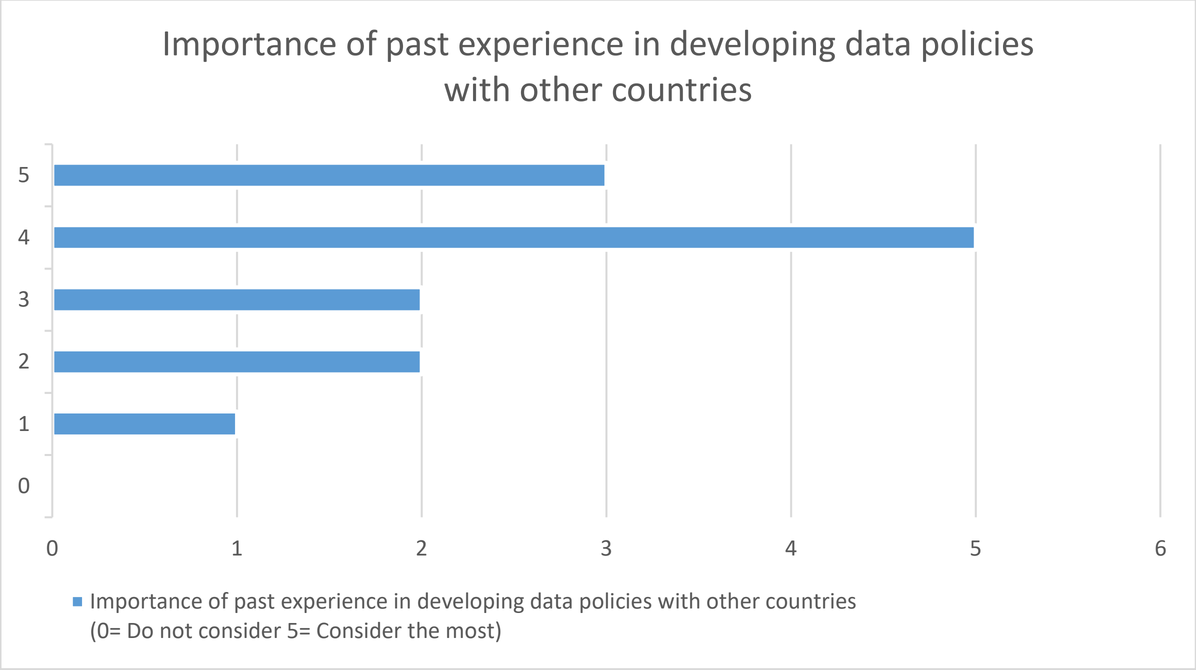


Figure E.383: Importance of past experience in developing data policies with other counties (Over 10 years UK)

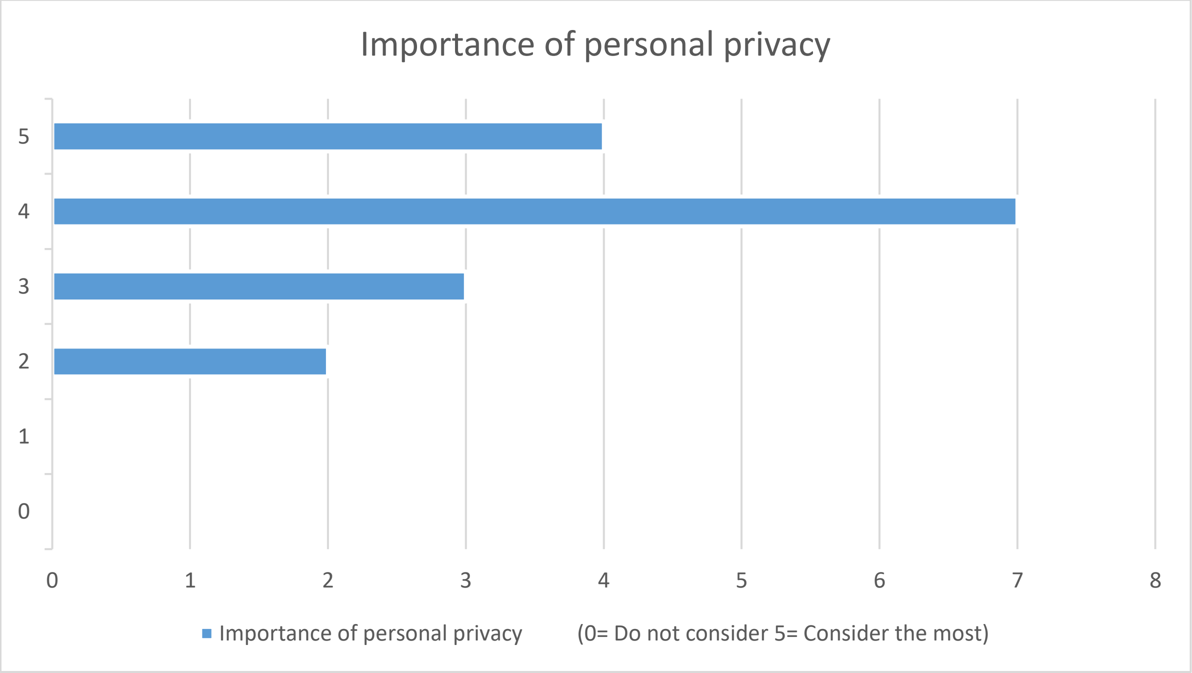


Figure E.384: Importance of personal privacy (Over 10 years UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 85 percent of the respondents have endorsed (See figure E.373). The other notable factors that have come out of the survey are organisational support, political differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure E.362-372) (See figure E.374-384). Interestingly, those employed in industry for more than 10 years do not see allocating funding as an important factor in accepting and implementing a global level data protection mechanism (See figure E.378).

United Kingdom – Accountancy, banking and finance

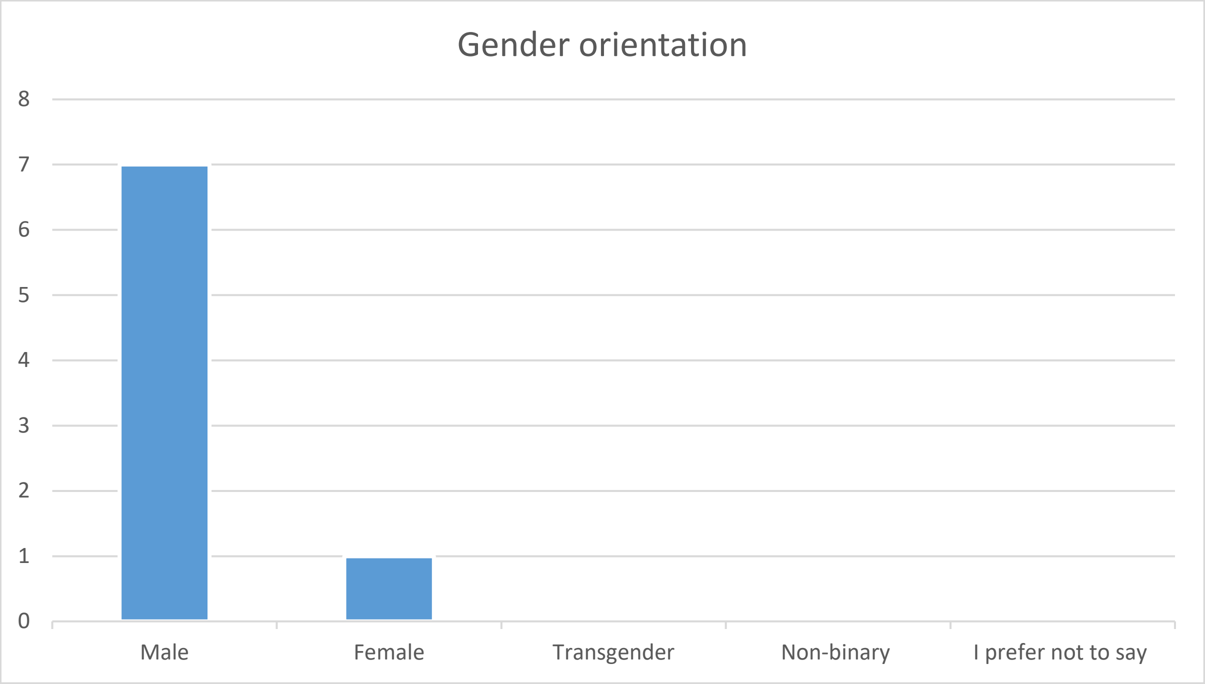


Figure E.385: Gender orientation (Accountancy, Banking, Finance- UK)

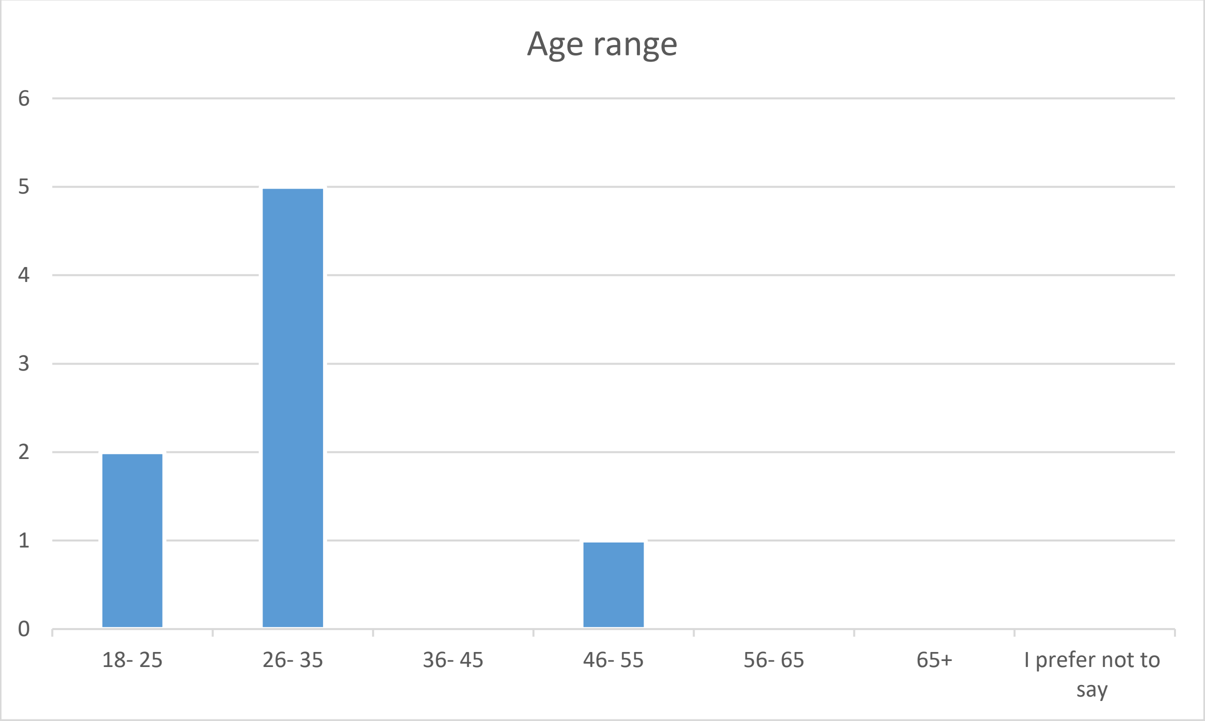


Figure E.386: Age range (Accountancy, Banking, Finance- UK)

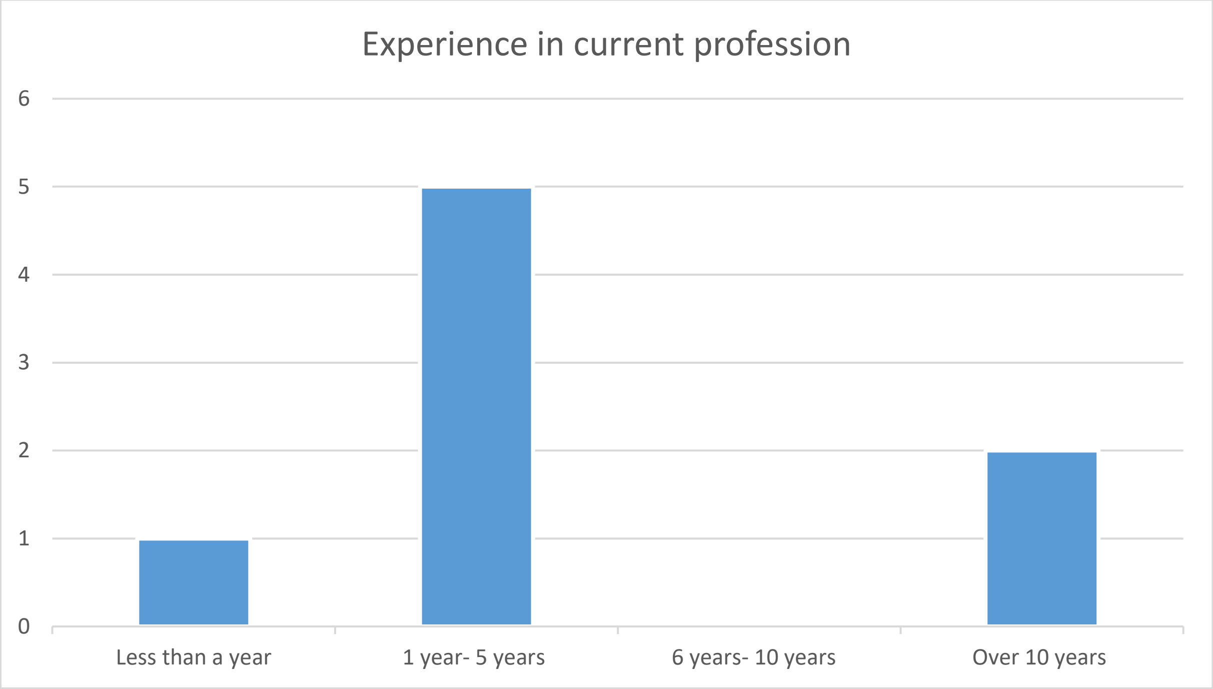


Figure E.387: Experience in current profession (Accountancy, Banking, Finance- UK)

This analysis is based on the responses received from United Kingdom participants employed in the accountancy, banking and finance sector. There were 8 participants and 7 out of them were males and 1 female (See figure E.385). They were within the 18-55 age range out of which 2 in the 18-25, 5 in the 26-35, and 1 in the 46-55 range (See figure E.386). The participants employed in the industry for less than a year and over 10 years (See figure E.387).

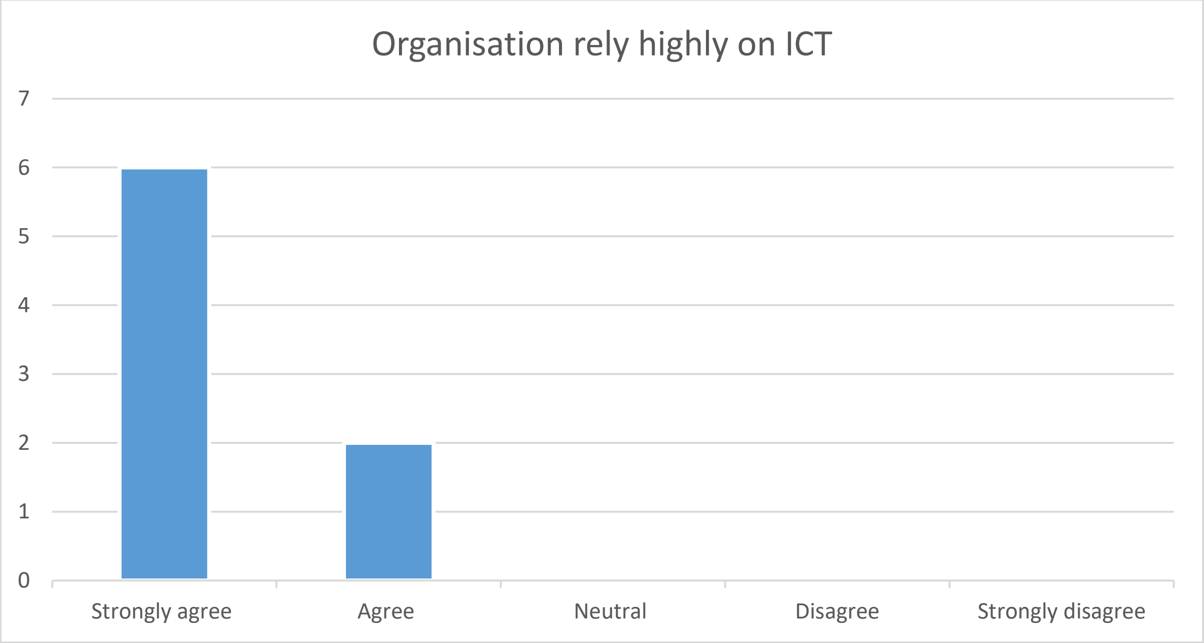


Figure E.388: Organisation rely highly on ICT (Accountancy, Banking, Finance- UK)

Out of the 8 respondents, all the participants have worked in a technology reliance working environment (See figure E.388).

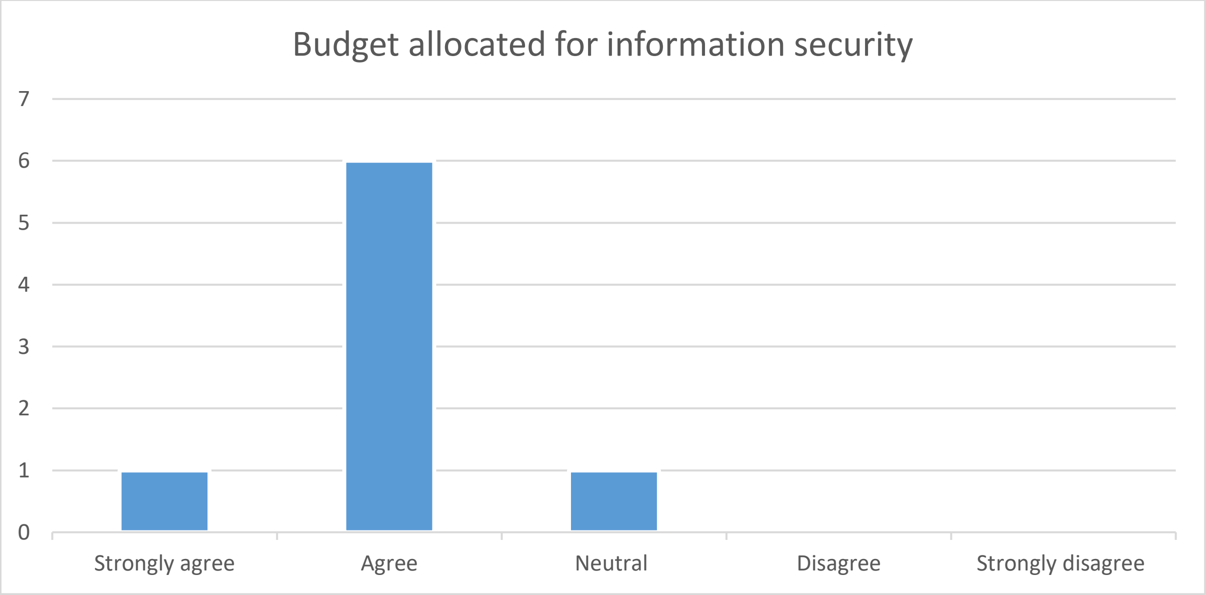


Figure E.389: Budget allocated for information security (Accountancy, Banking, Finance- UK)

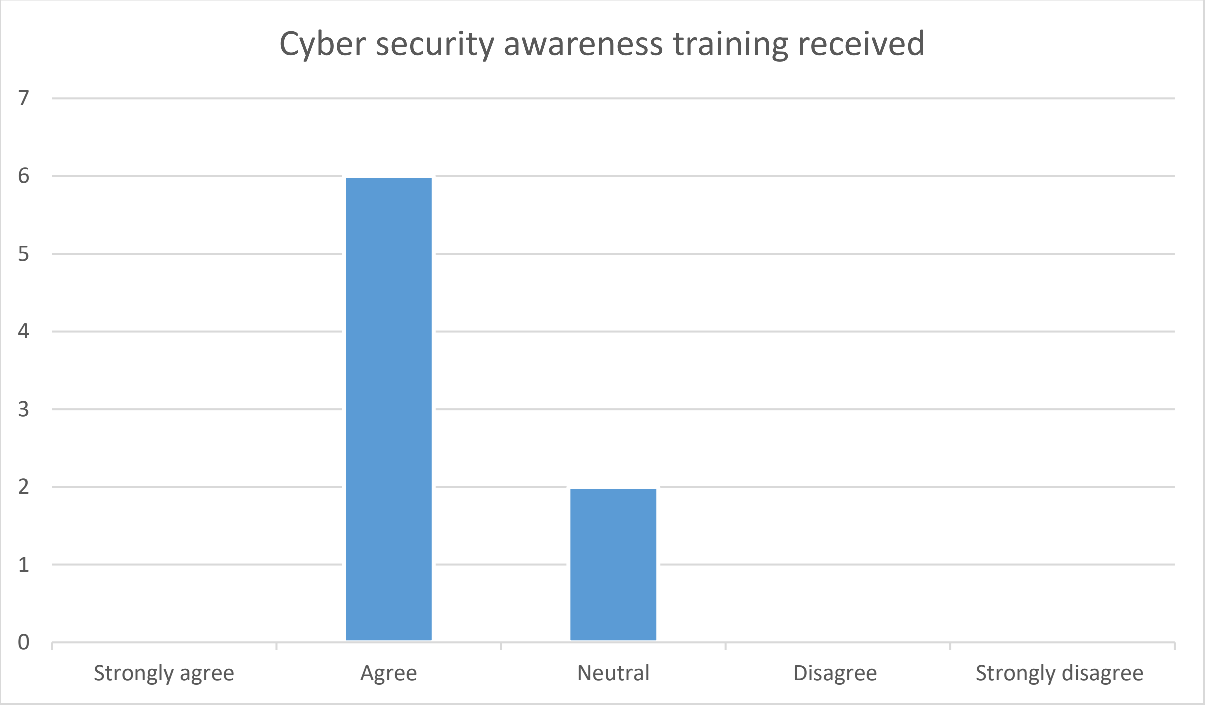


Figure E.390: Cyber security awareness training received (Accountancy, Banking, Finance- UK)

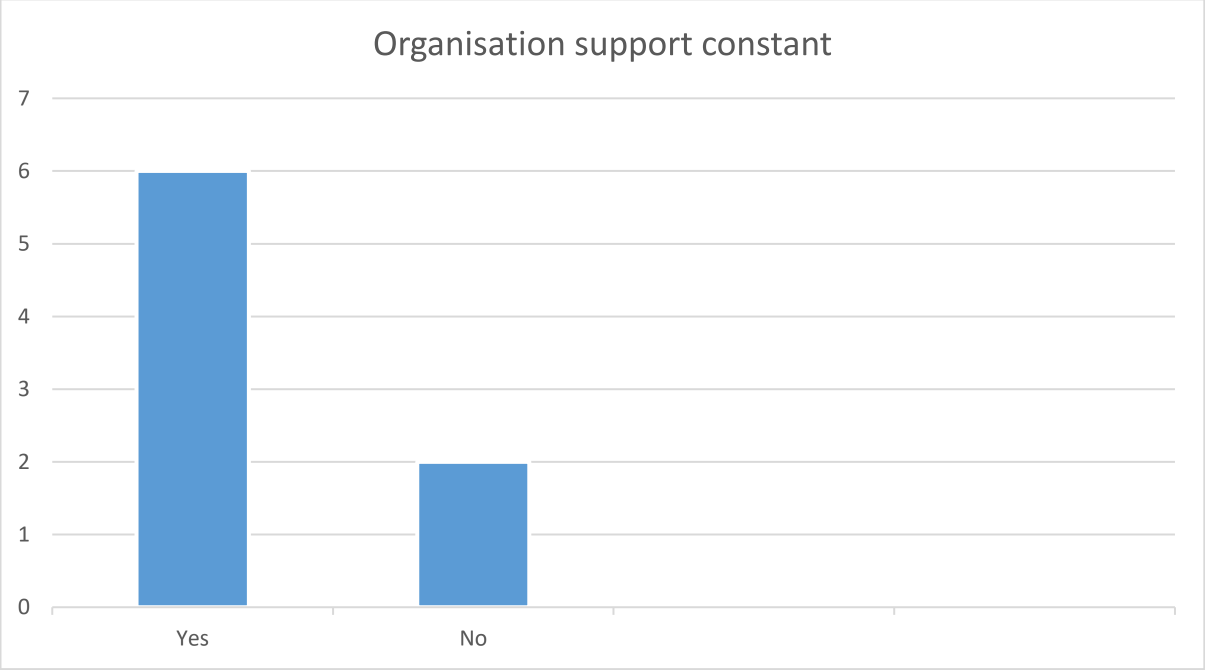


Figure E.391: Organisation support constant (Accountancy, Banking, Finance- UK)

Funding has been sketchy. 7 out of the 8 have indicated that their organisations had an allocated budget for information security, whilst 1 had not expressed an opinion either way (See figure E.389). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was also adequate. 6 participants have received regular cybersecurity awareness training, whilst 2 participants neither agreed nor disagreed (See figure E.390). In addition, 6 participants received support from the organisation to protect personal information, and 2 did not (See figure E.391). Given that the employees handle money and personal information, it is clear that the organisations allocate funding and provide regular awareness training, and support needed to protect personal information.

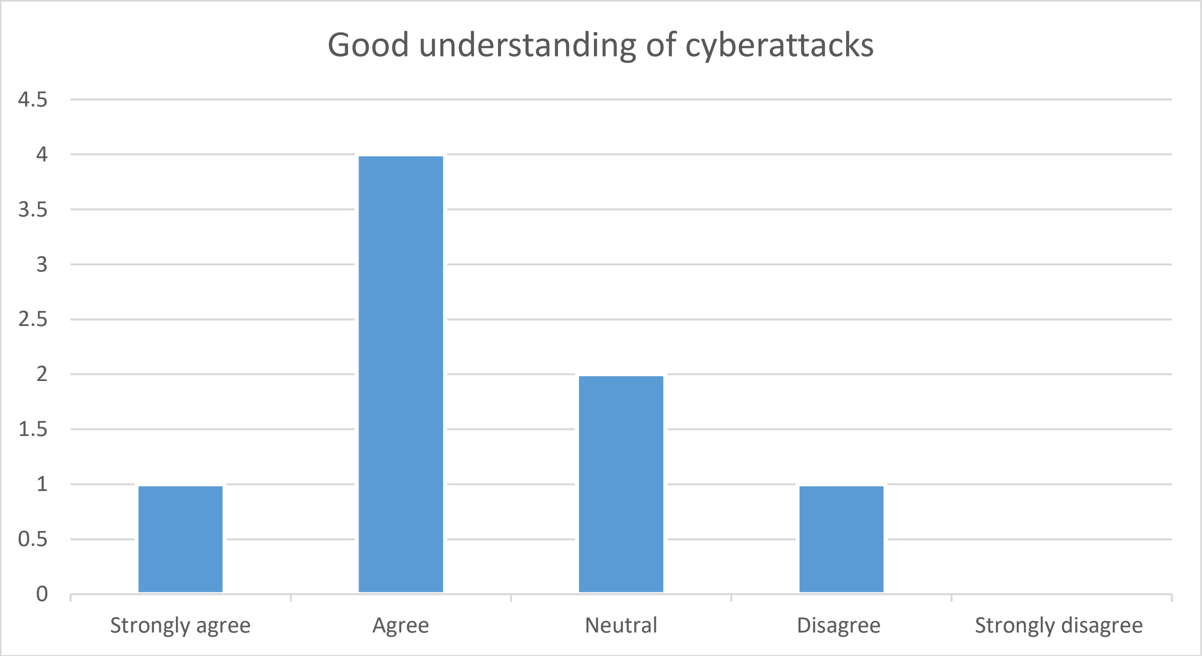


Figure E.392: Good understanding of cyberattacks (Accountancy, Banking, Finance-UK)

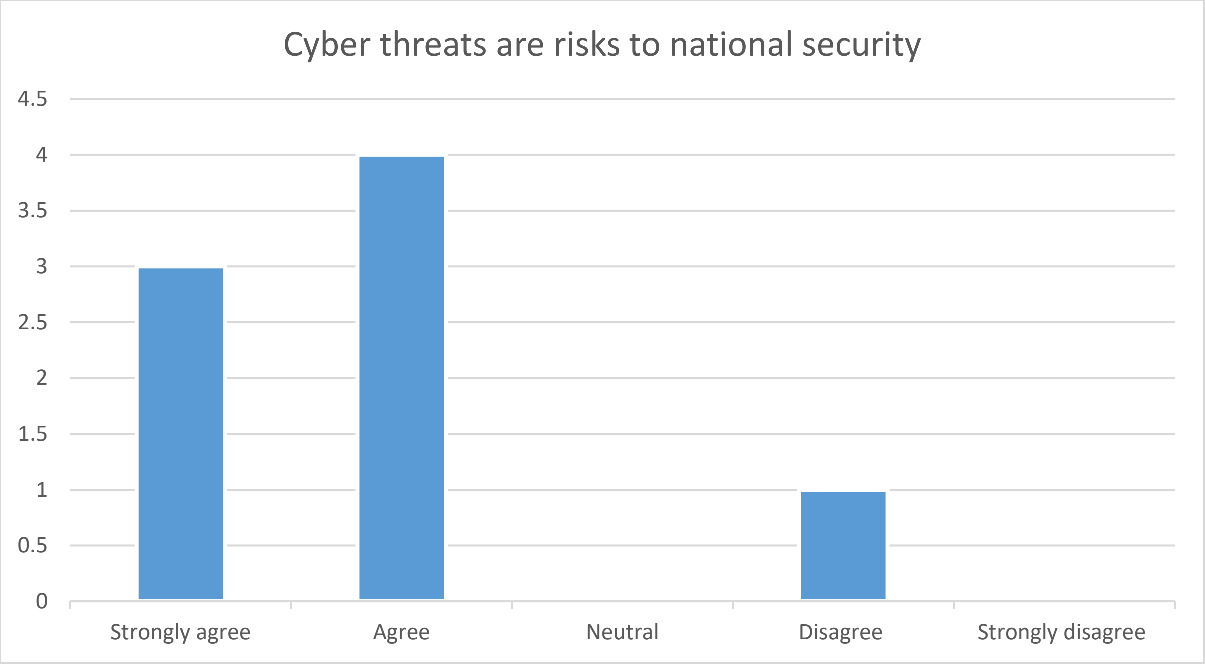


Figure E.393: Cyber threats are risks to national security (Accountancy, Banking, Finance- UK)

Despite the security awareness training, the participants appear to have a satisfactory level of understanding of the impact of cyber-attacks on the public and the organisation. 5 participants do have, 2 have not expressed opinion either way, and 1 participant had no understanding (See figure E.392). Furthermore, 88 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure E.393). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

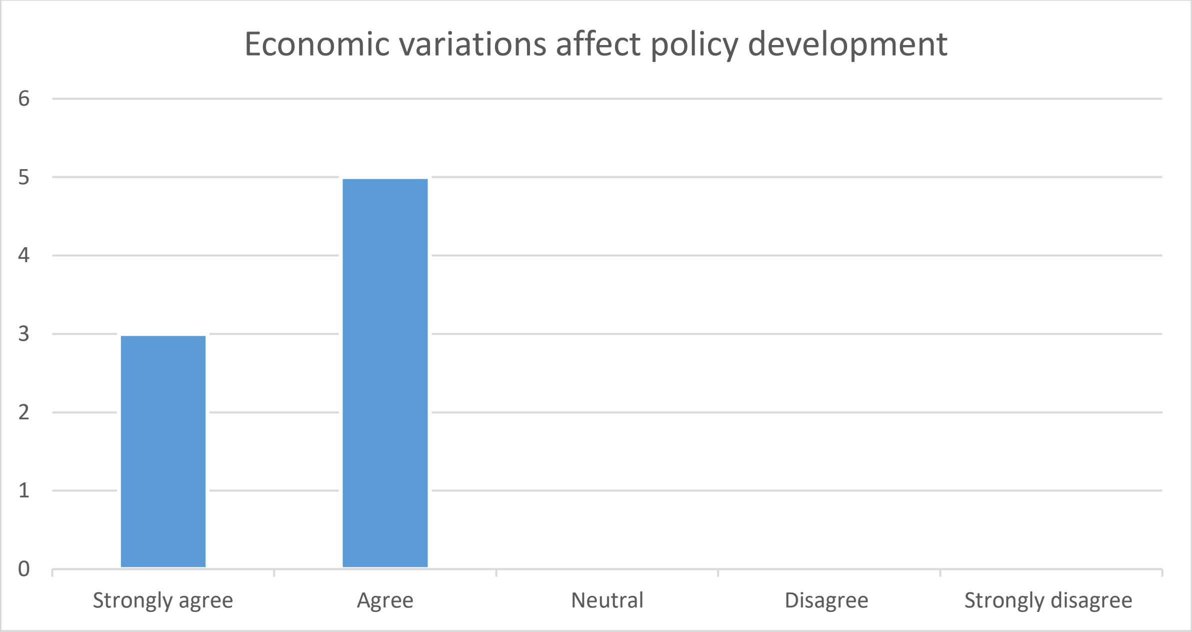


Figure E.394: Economic variations affect policy development (Accountancy, Banking, Finance- UK)

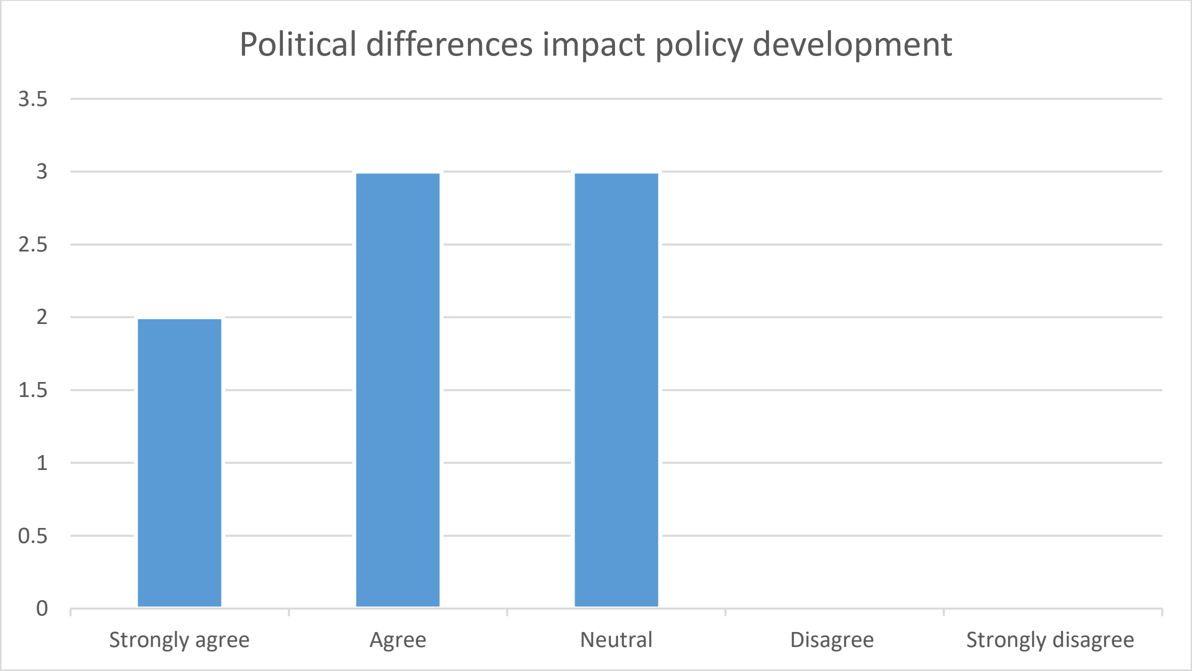


Figure E.395: Political differences impact policy development (Accountancy, Banking, Finance- UK)

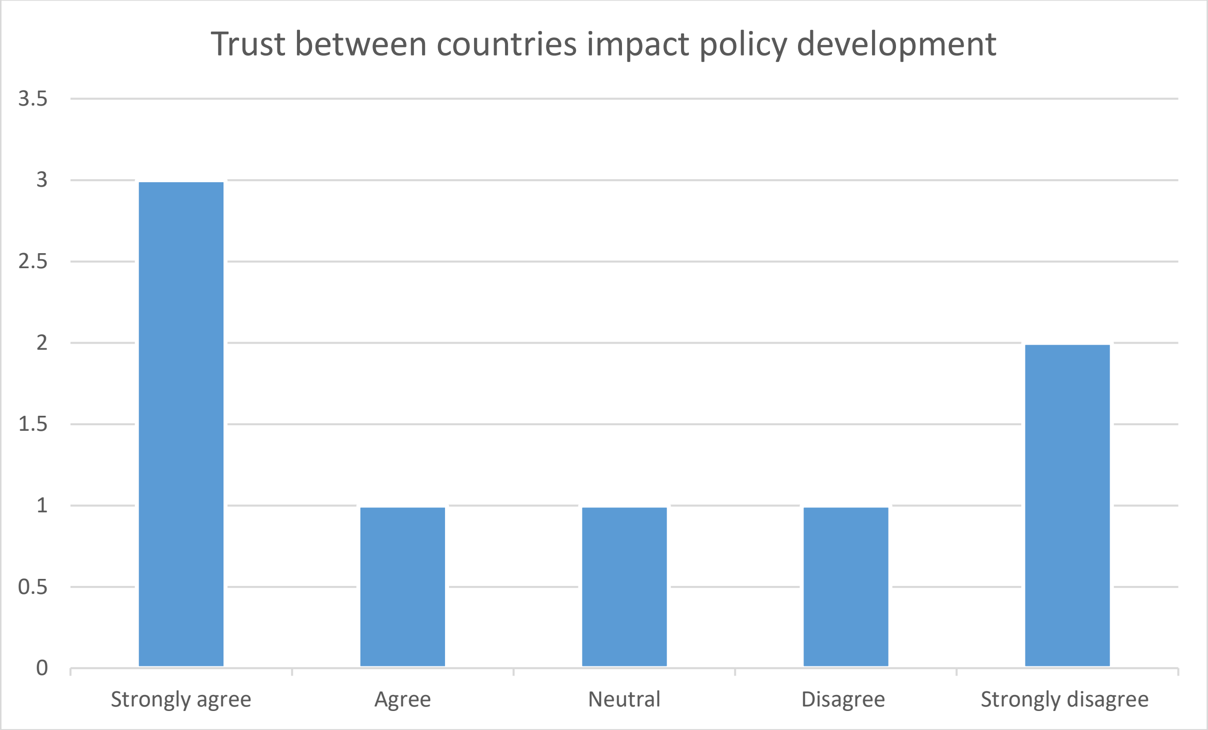


Figure E.396: Trust between countries impact policy development (Accountancy, Banking, Finance- UK)

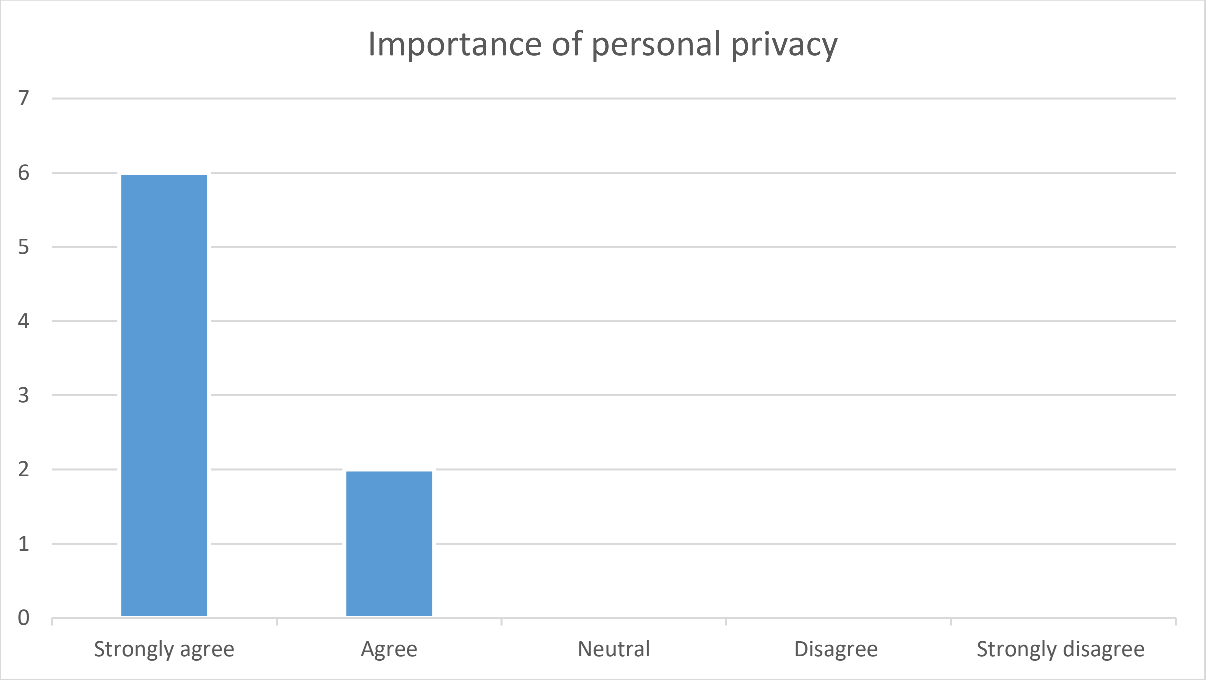


Figure E.397: Importance of personal privacy (Accountancy, Banking, Finance- UK)

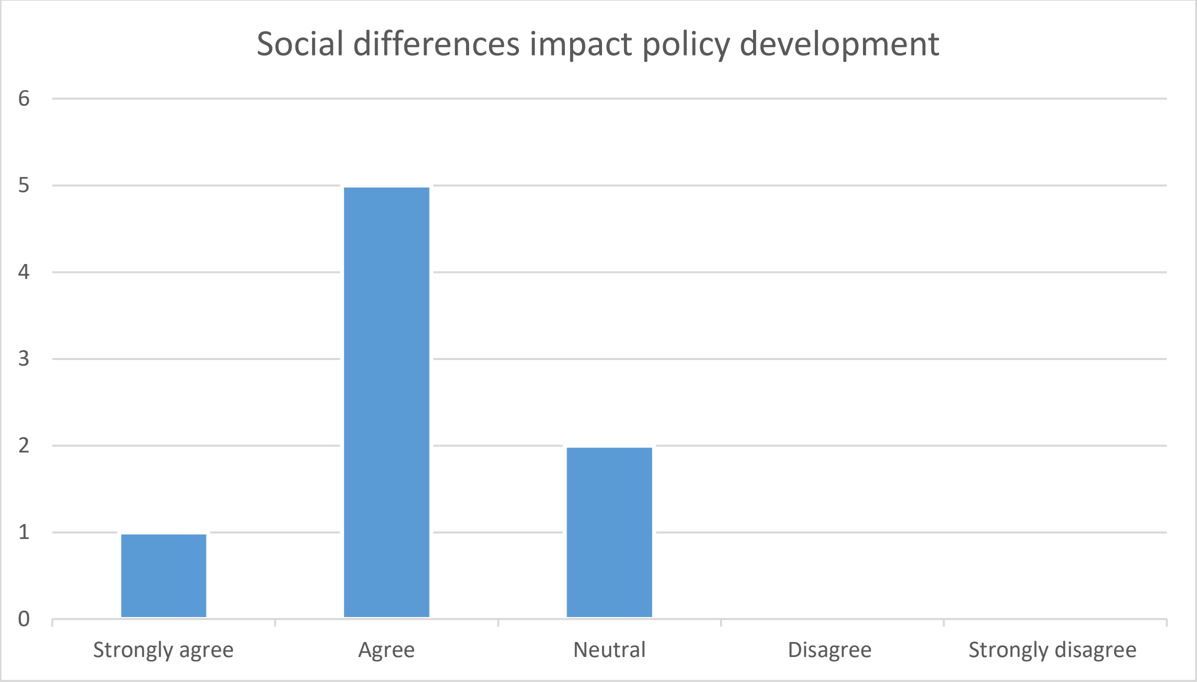


Figure E.398: Social differences impact policy development (Accountancy, Banking, Finance- UK)

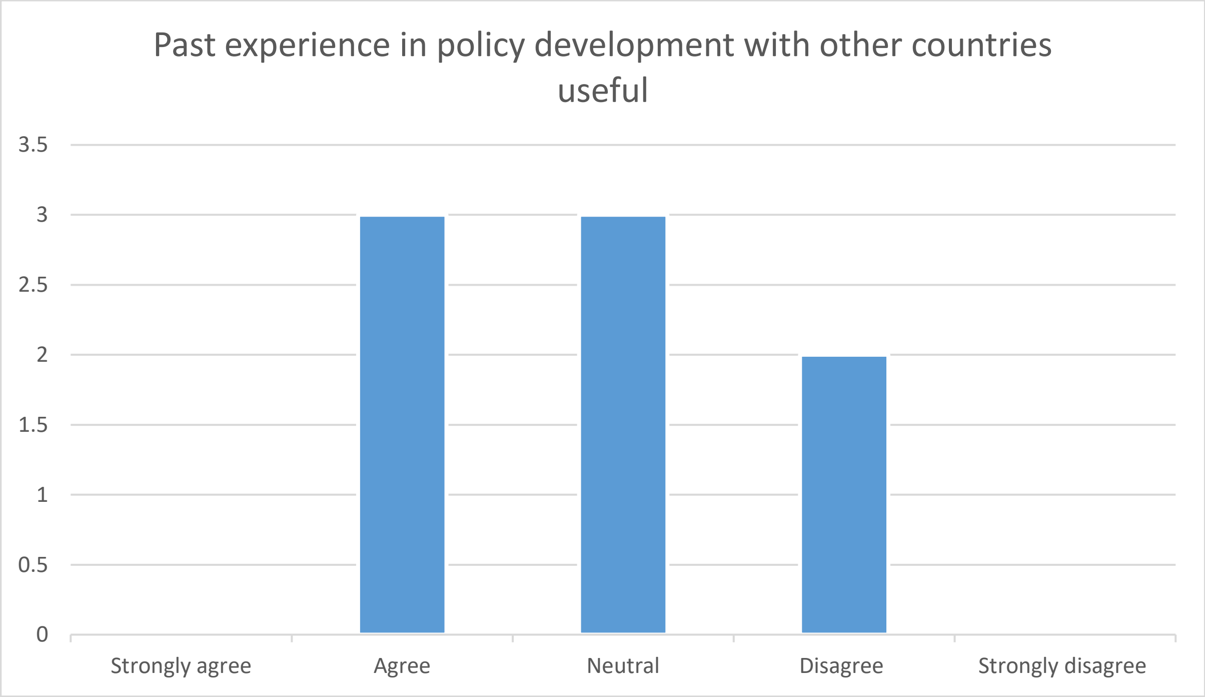


Figure E.399: Past experience in policy development with other countries useful (Accountancy, Banking, Finance- UK)

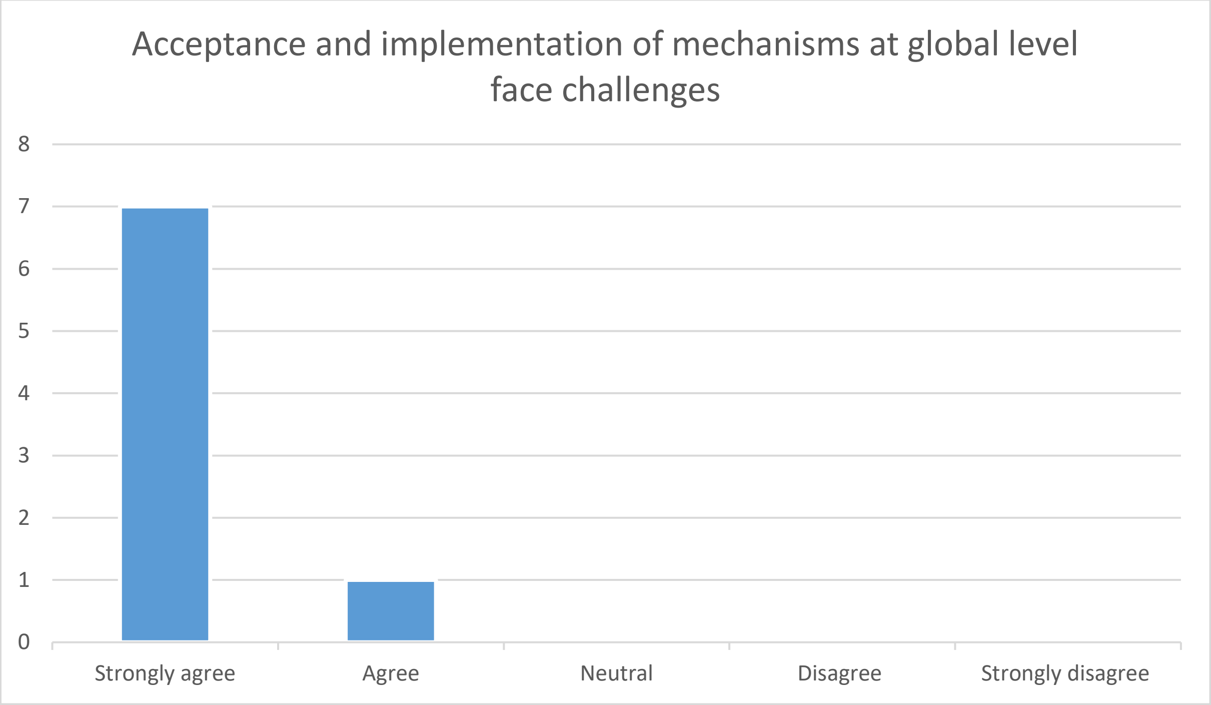


Figure E.400: Acceptance and implementation of mechanisms at global level face challenges (Accountancy, Banking, Finance- UK)

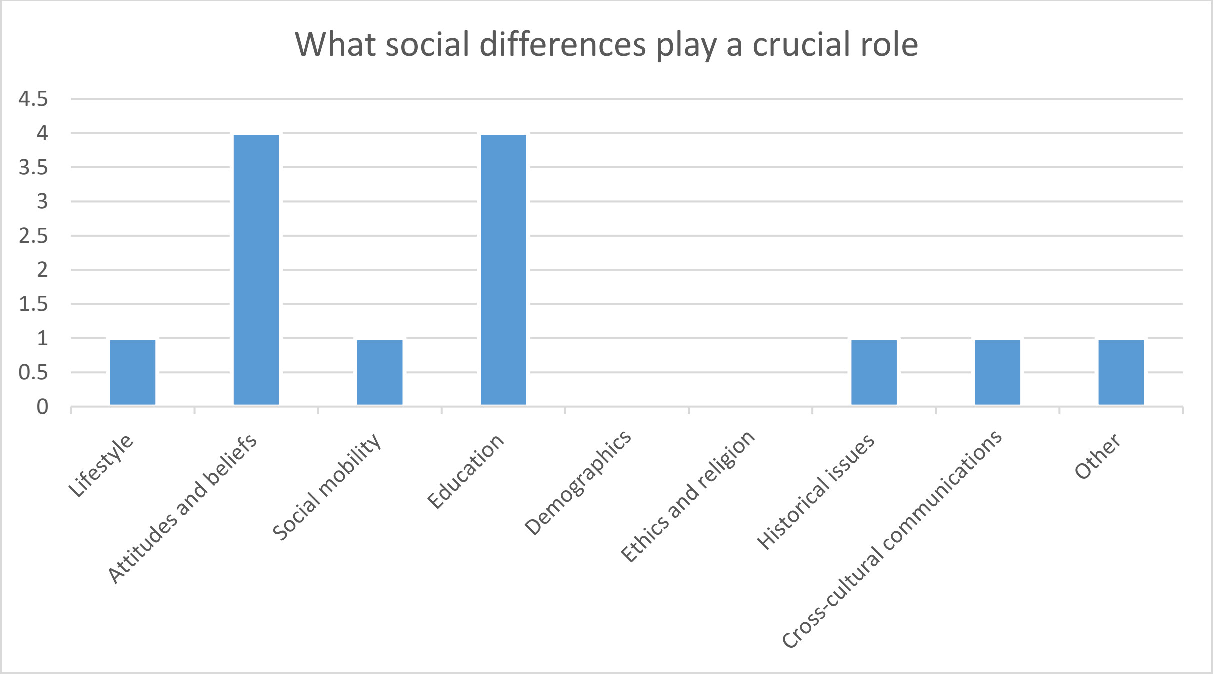


Figure E.401: What social differences play a crucial role (Accountancy, Banking, Finance-UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure E.401). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

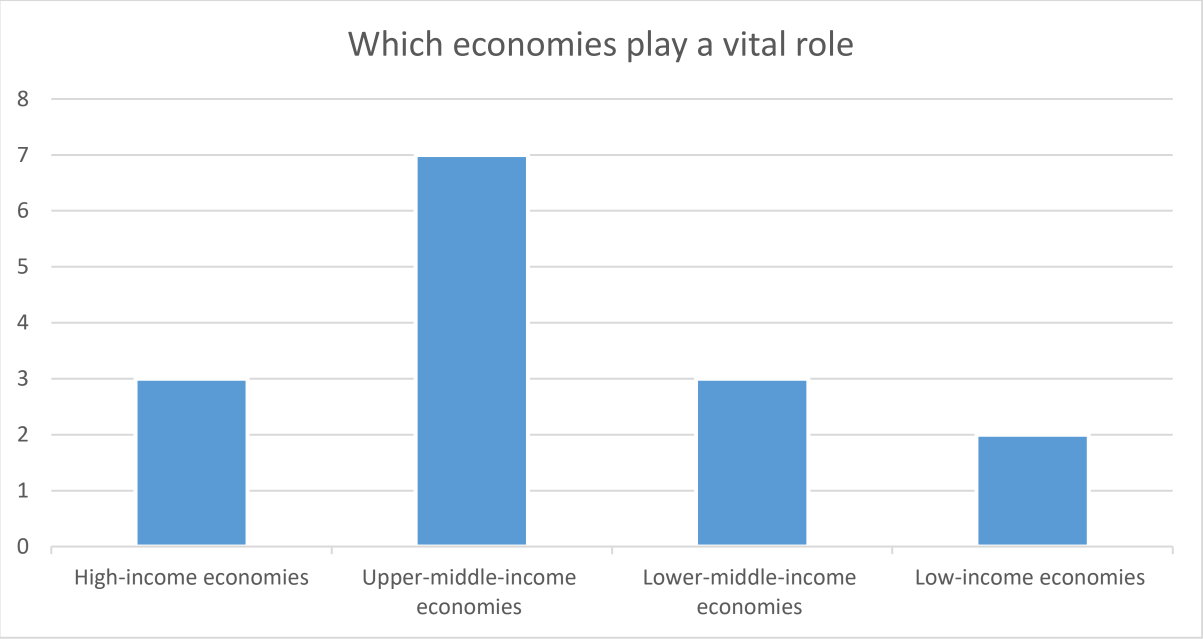


Figure E.402: Which economies play a vital role (Accountancy, Banking, Finance-UK)

In the questionnaire, majority has stated that the upper-middle-income countries play a vital role (See figure E.402). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

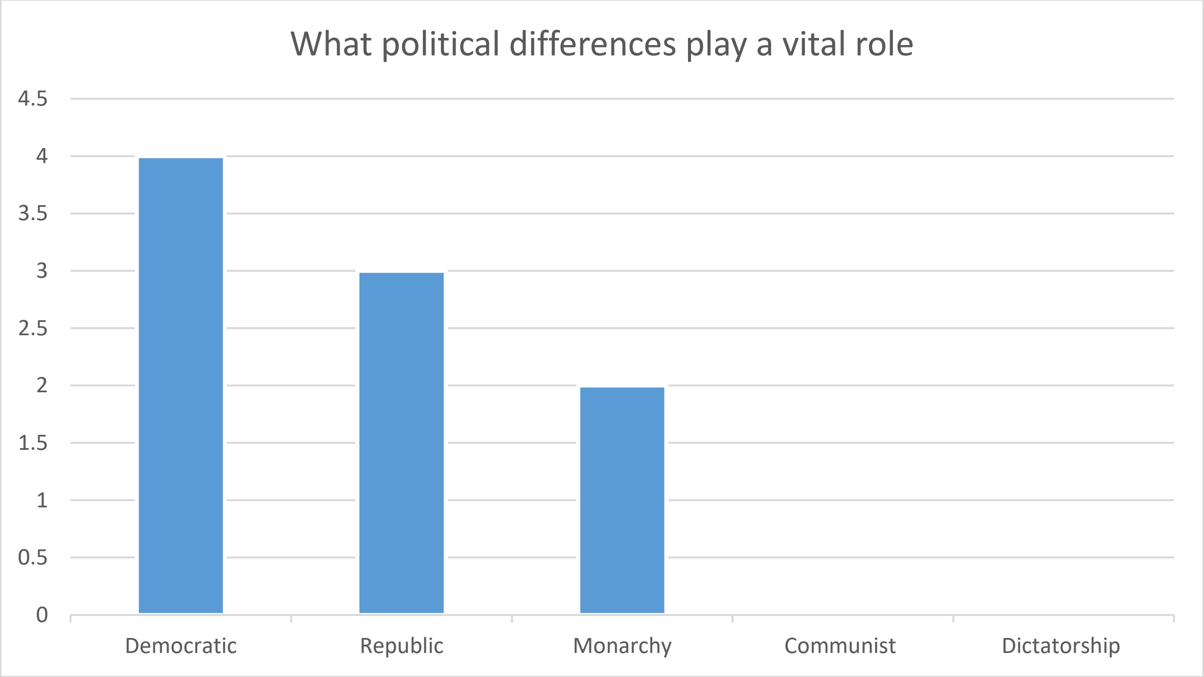


Figure E.403: What political differences play a vital role (Accountancy, Banking, Finance- UK)

The majority have chosen a democratic political system (See figure E.403), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

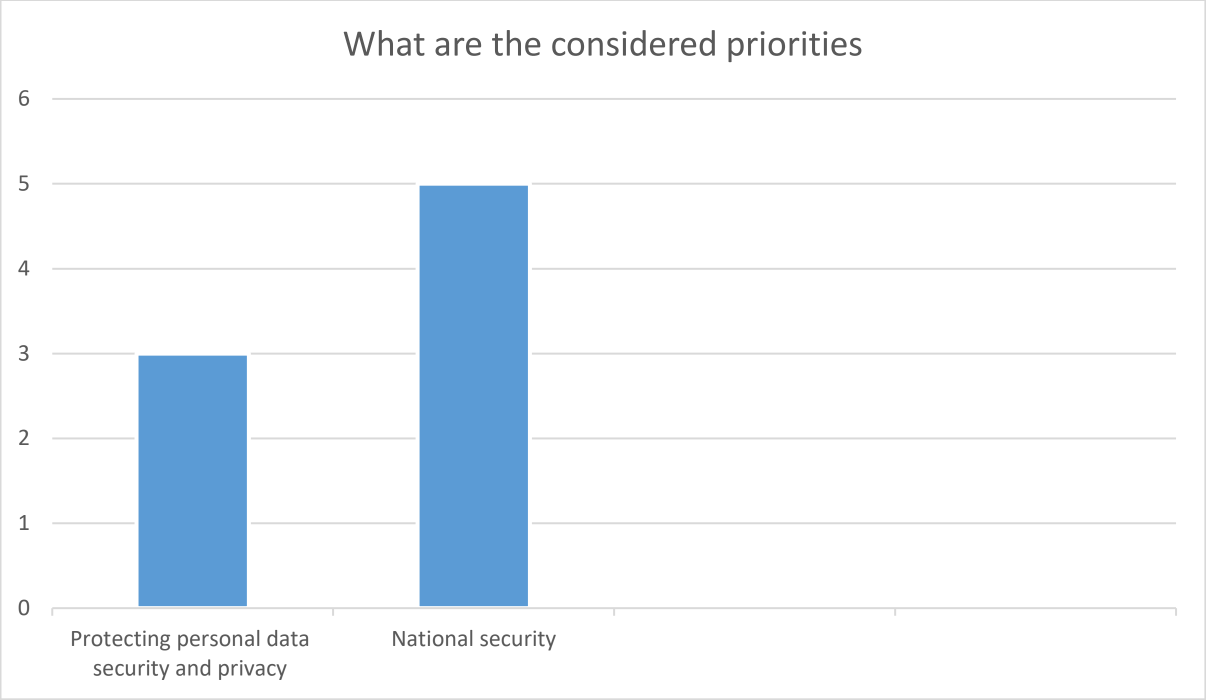


Figure E.404: What are the considered priorities (Accountancy, Banking, Finance- UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of national security is placed above the protection of personal data security and privacy (See figure E.404). However, in an incident of a personal data breach, there will potentially be a knock-on effect on personal data security and privacy as well, and it will also be felt right across the groups as well as the community alike.

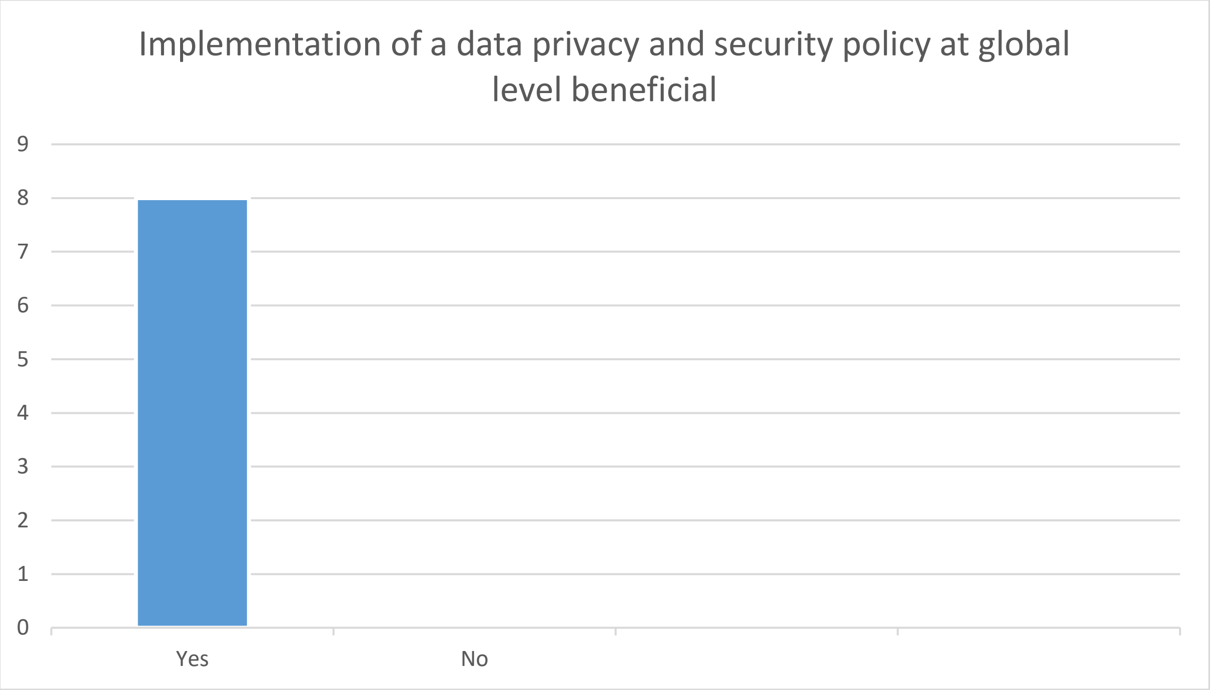


Figure E.405: Implementation of a data privacy and security policy at global level beneficial (Accountancy, Banking, Finance- UK)

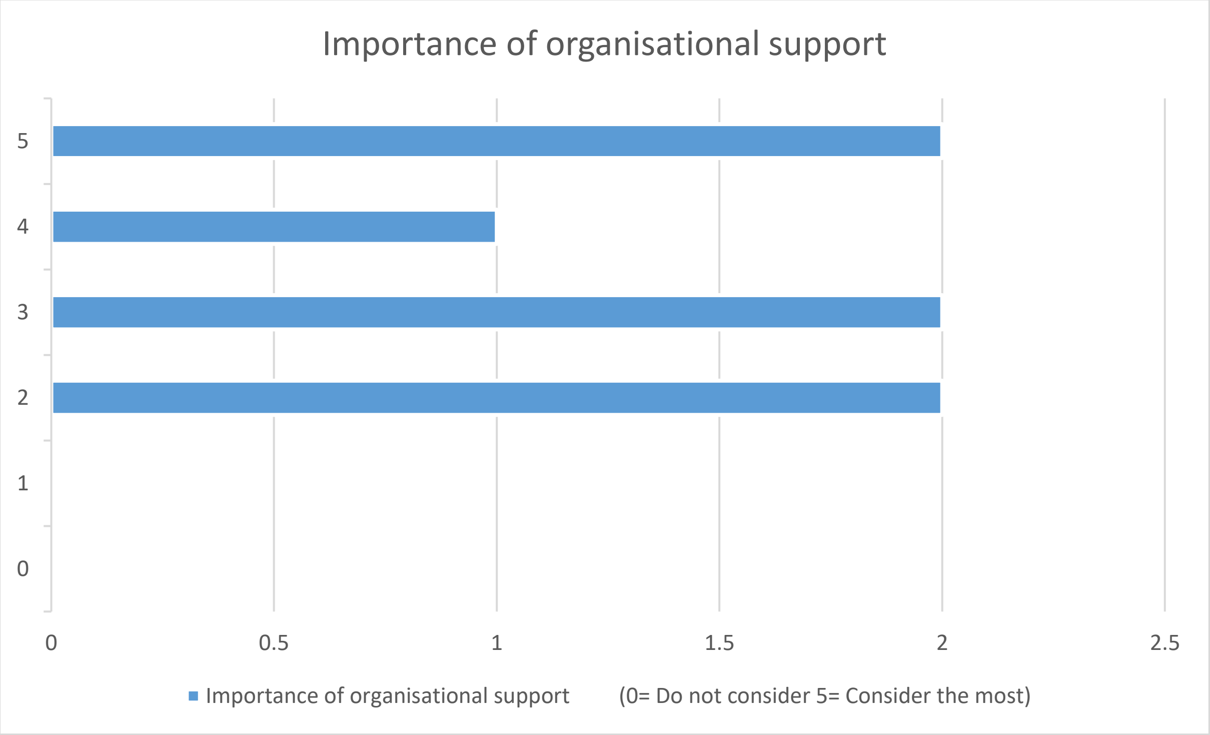


Figure E.406: Importance of organisational support (Accountancy, Banking, Finance- UK)

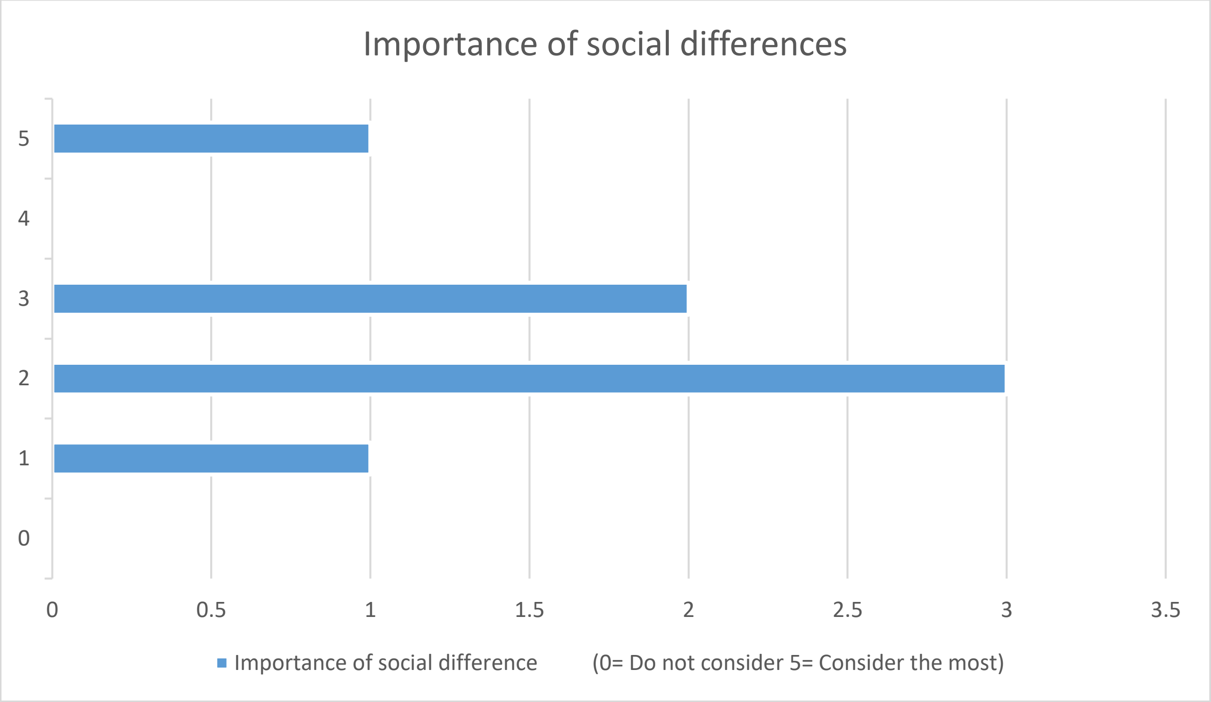


Figure E.407: Importance of social differences (Accountancy, Banking, Finance- UK)

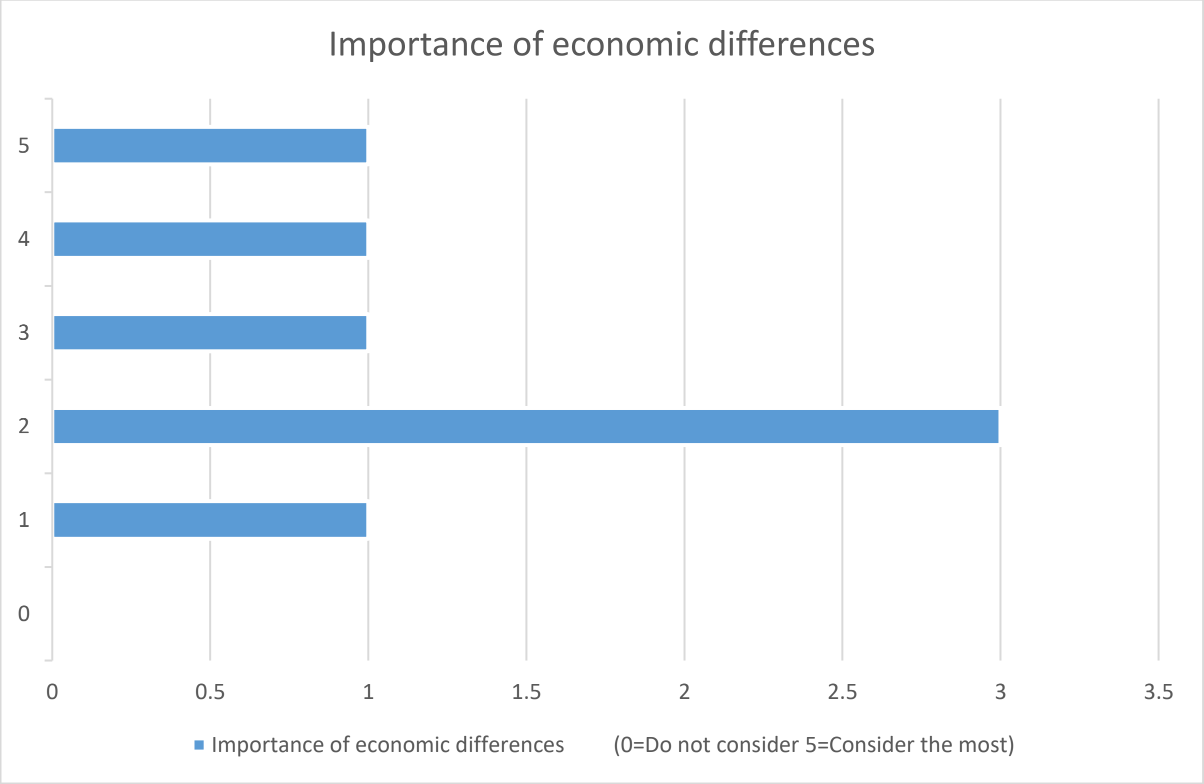


Figure E.408: Importance of economic differences (Accountancy, Banking, Finance- UK)

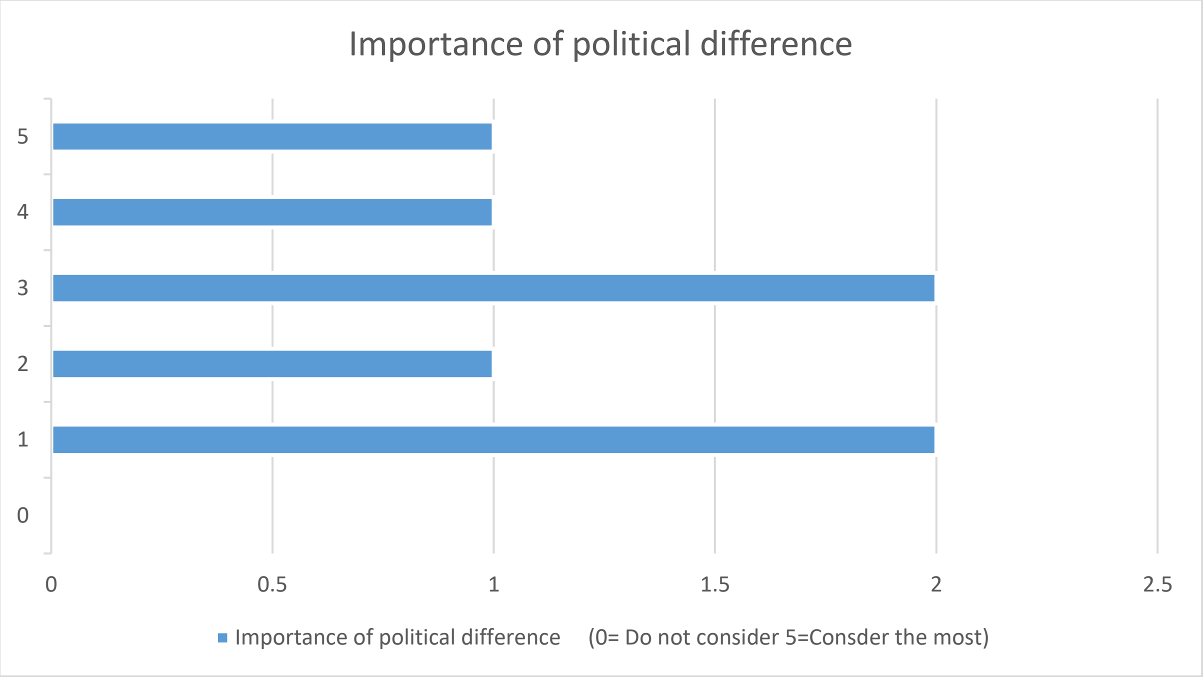


Figure E.409: Importance of political difference (Accountancy, Banking, Finance- UK)

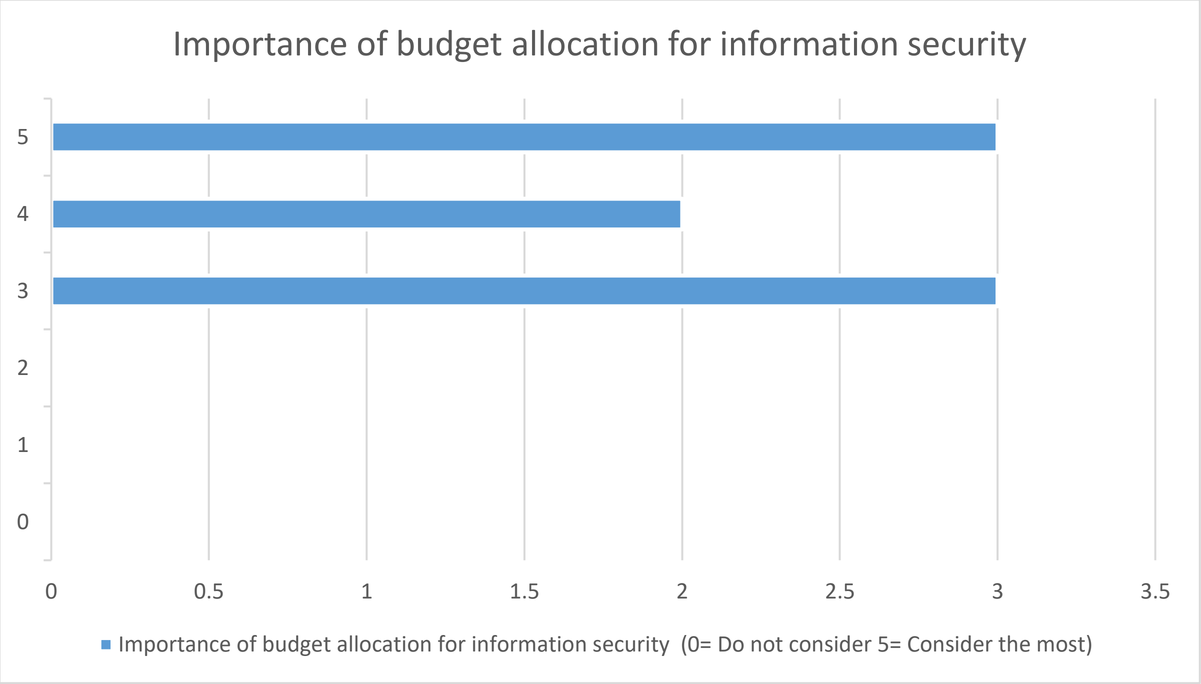


Figure E.410: Importance of budget allocation for information security (Accountancy, Banking, Finance- UK)

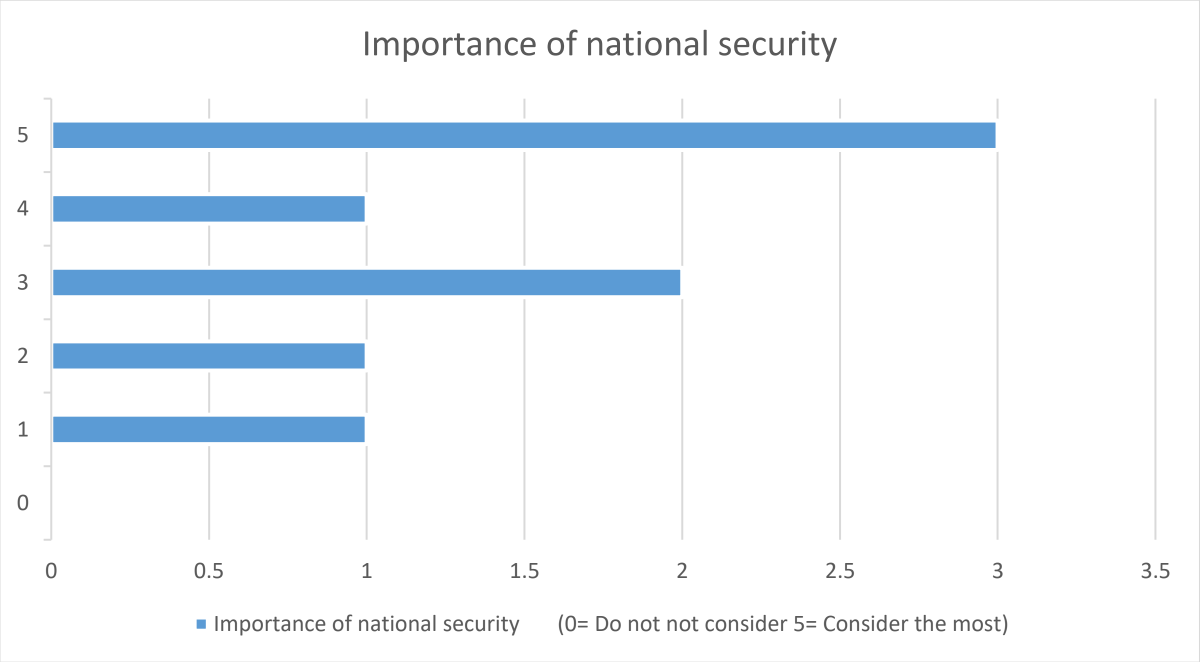


Figure E.411: Importance of national security (Accountancy, Banking, Finance-UK)

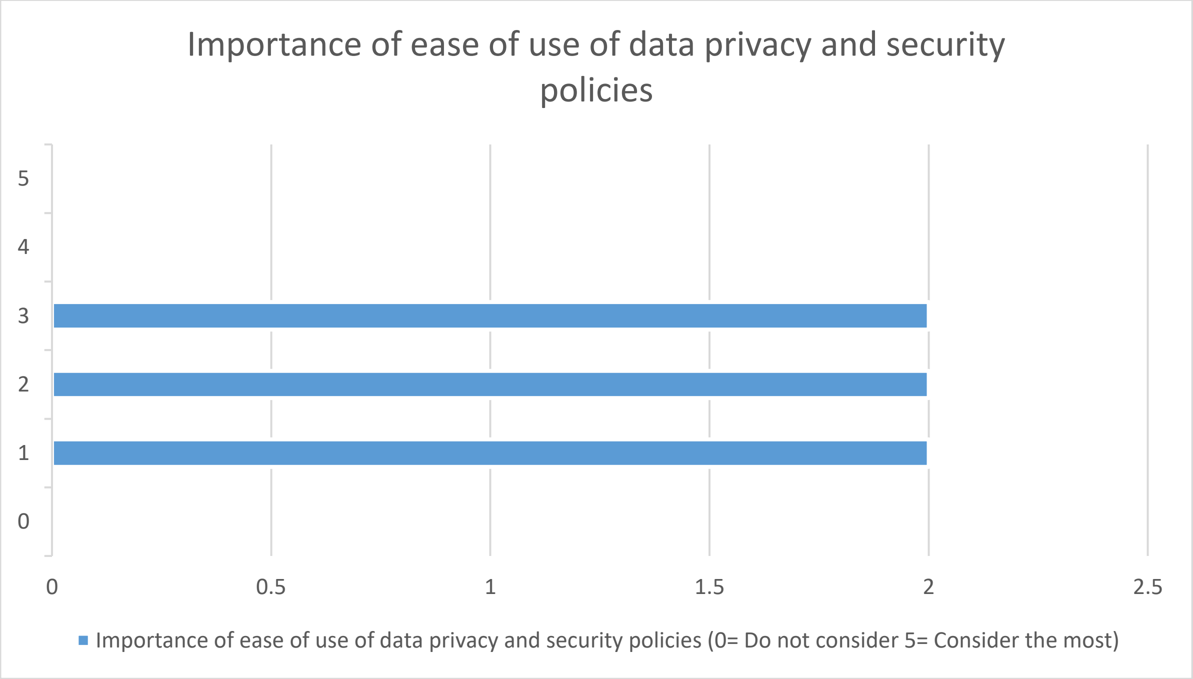


Figure E.412: Importance of ease of use of data privacy and security policies (Accountancy, Banking, Finance- UK)

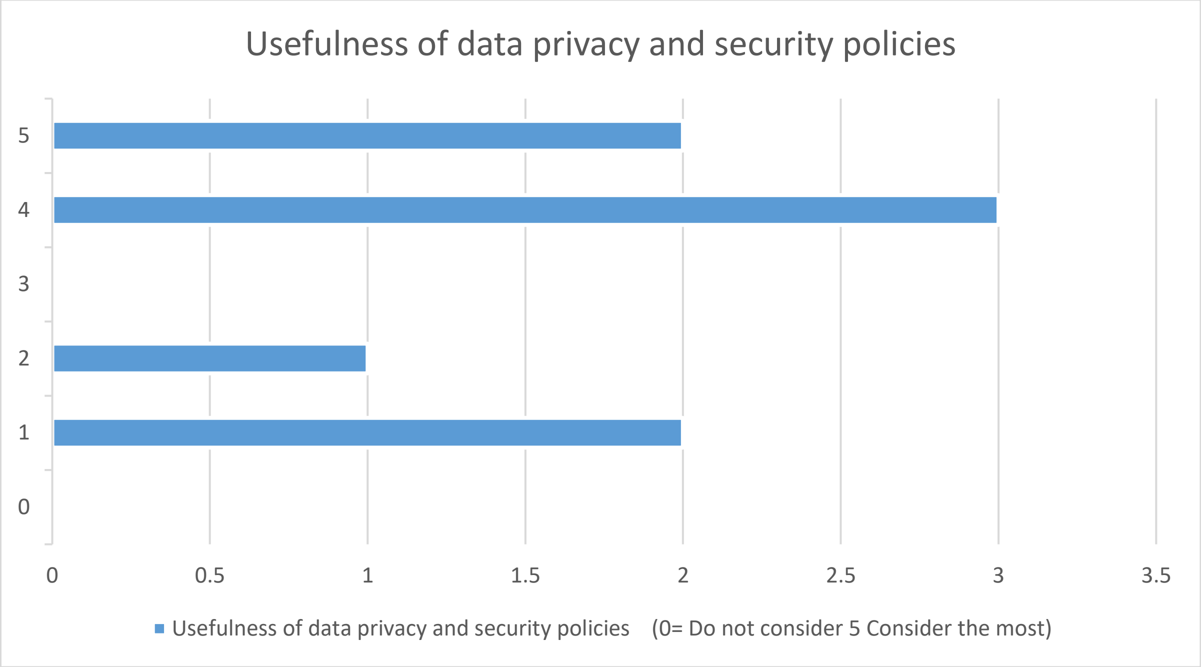


Figure E.413: Usefulness of data privacy and security policies (Accountancy, Banking, Finance- UK)

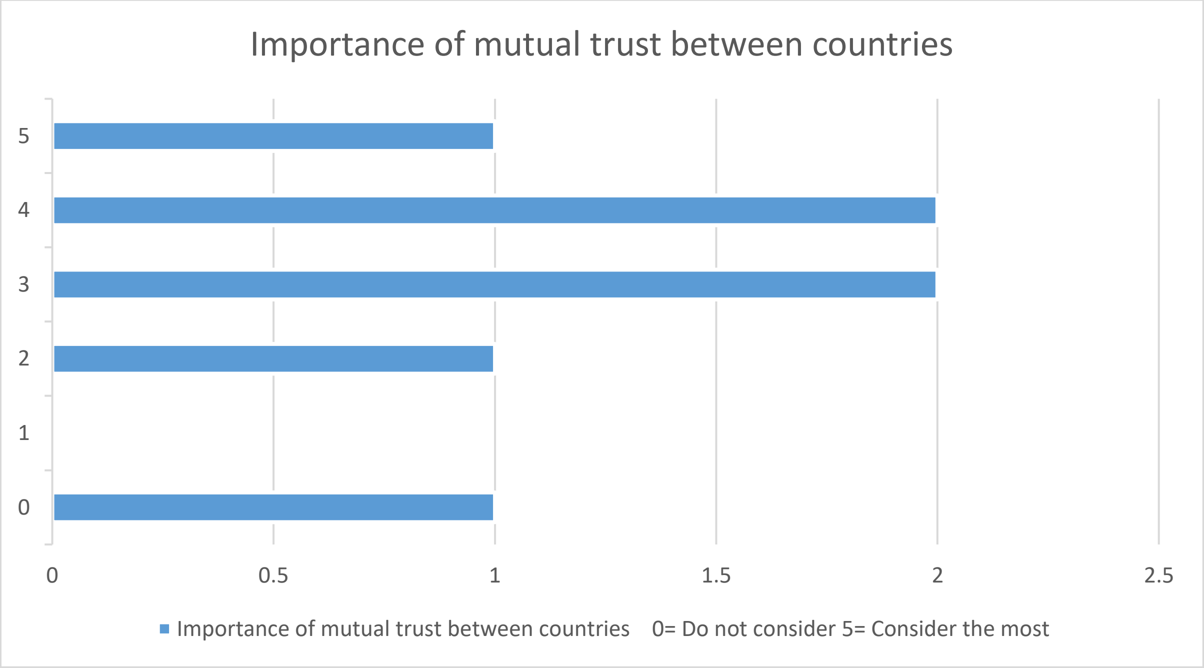


Figure E.414: Importance of mutual trust between countries (Accountancy, Banking, Finance- UK)

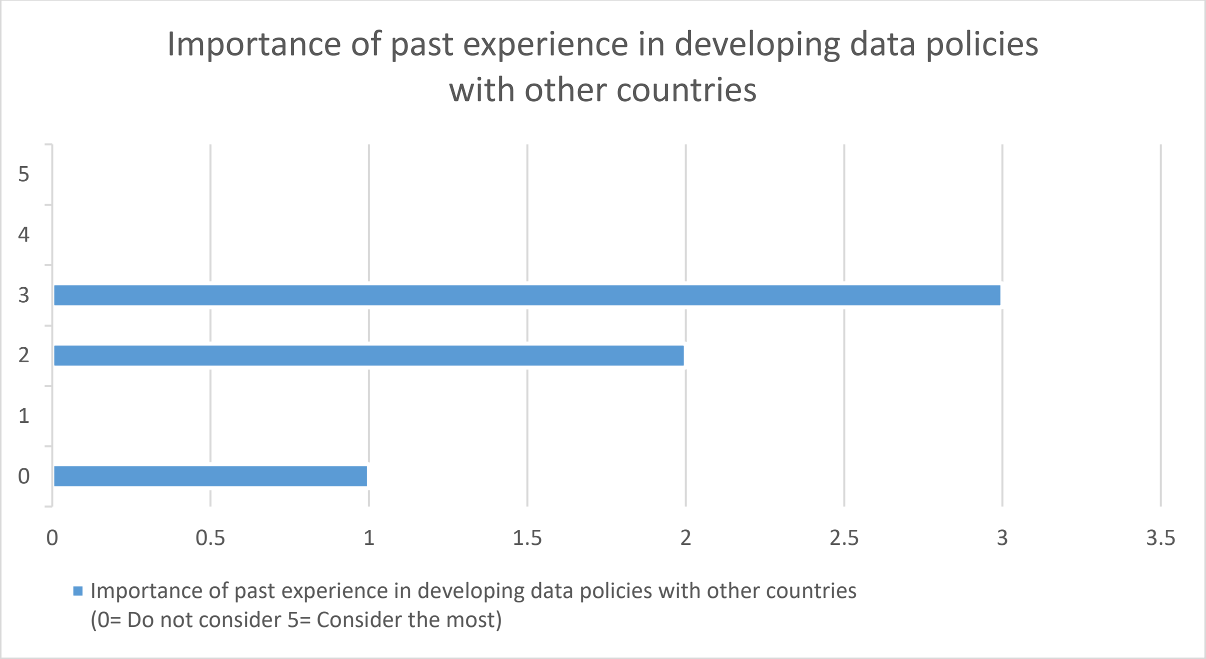


Figure E.415: Importance of past experience in developing data policies with other counties (Accountancy, Banking, Finance- UK)

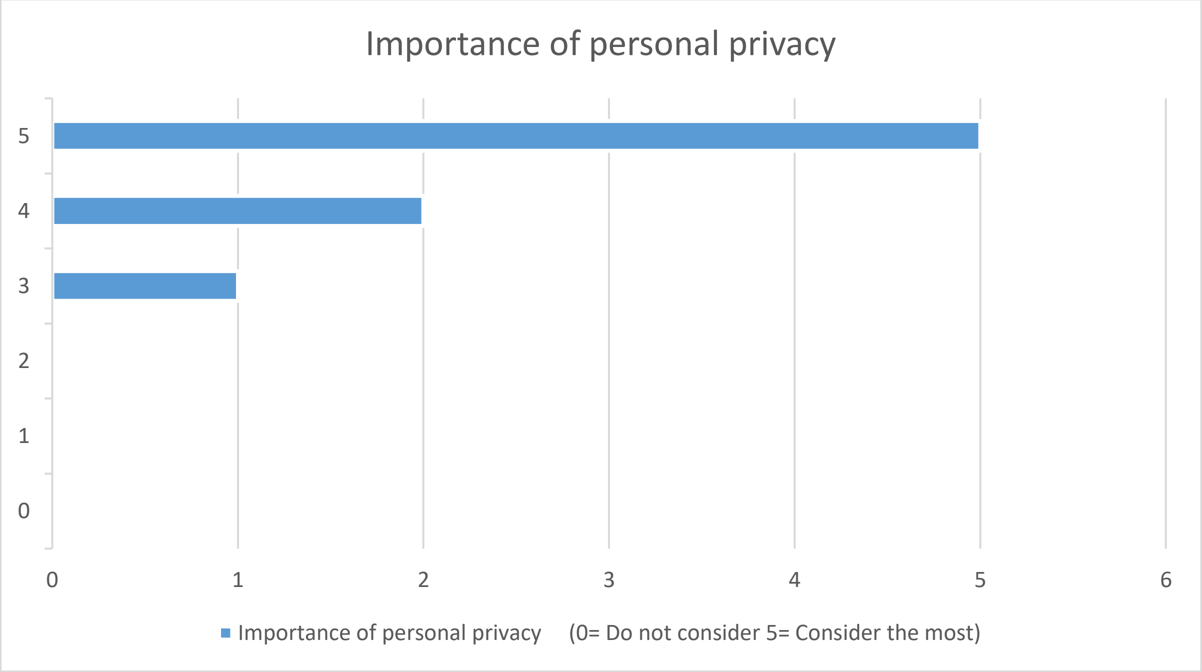


Figure E.416: Importance of personal privacy (Accountancy, Banking, Finance- UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 100 percent of the respondents have endorsed (See figure E.405). The other notable factors that have come out of the survey are organisational support, budget allocation, political differences, personal privacy, national security, the usefulness of data privacy and security policies, mutual trust between countries (See figure E.394-404) (See figure E.406-416).

United Kingdom – Business, consulting and management

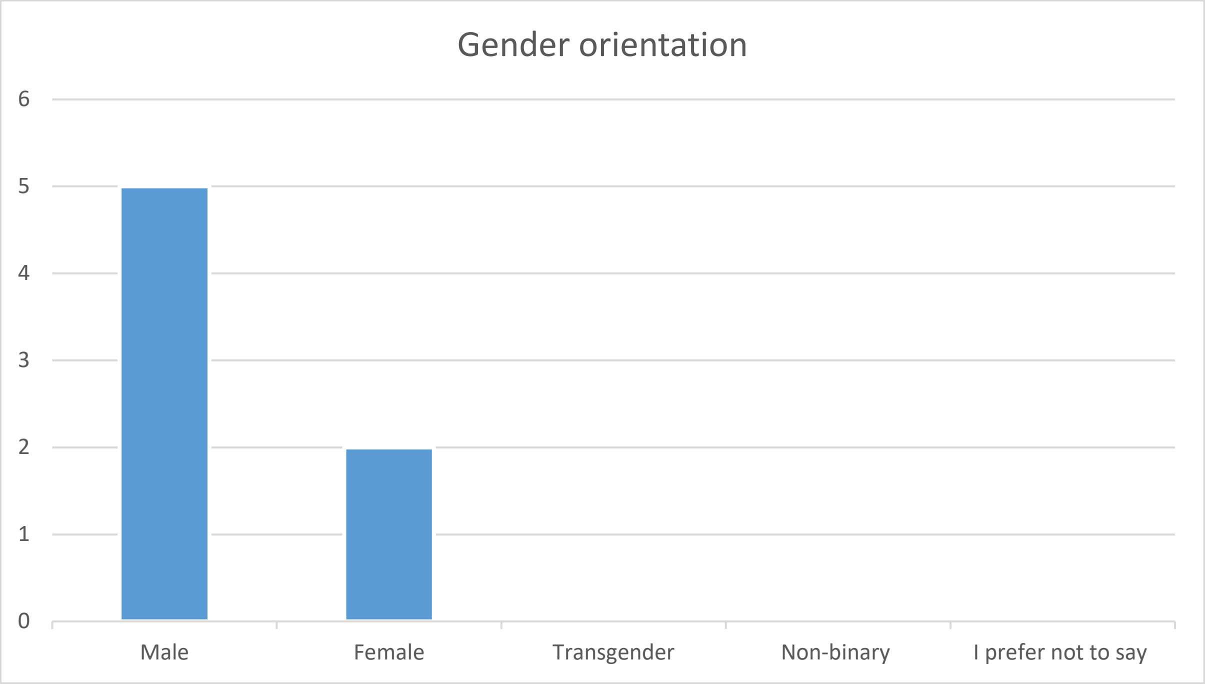


Figure E.417: Gender orientation (Business, consultancy and management- UK)

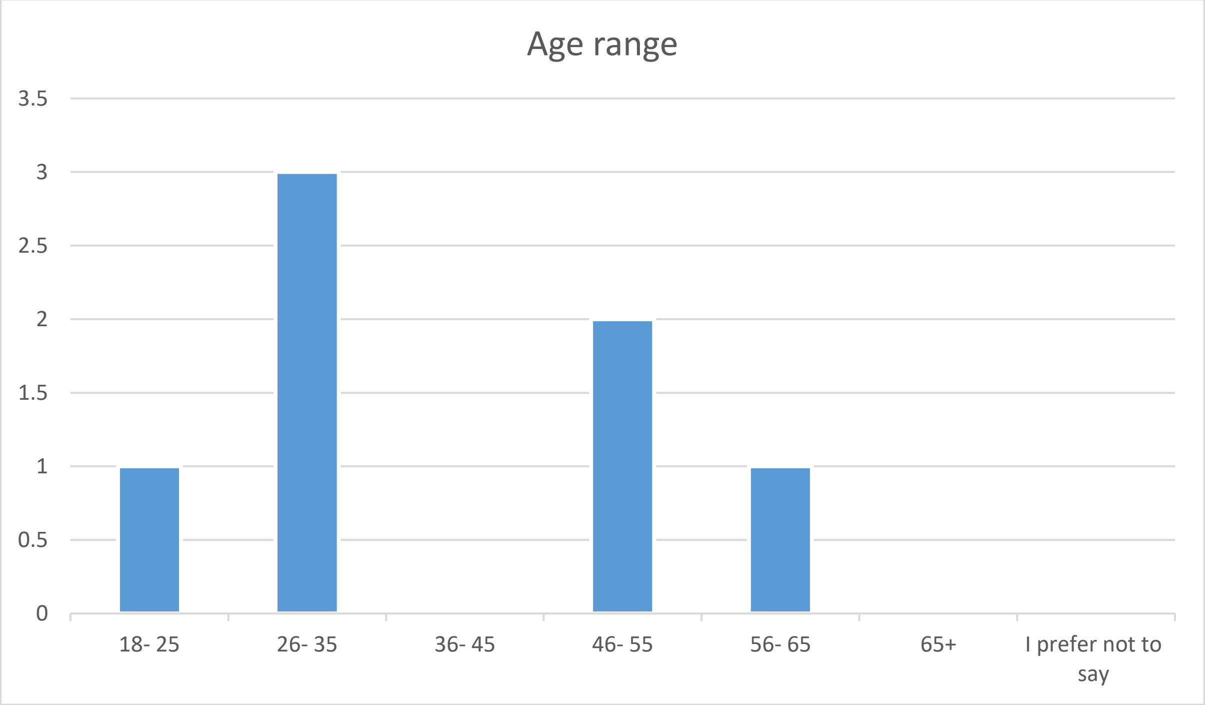


Figure E.418: Age range (Business, consultancy and management- UK)

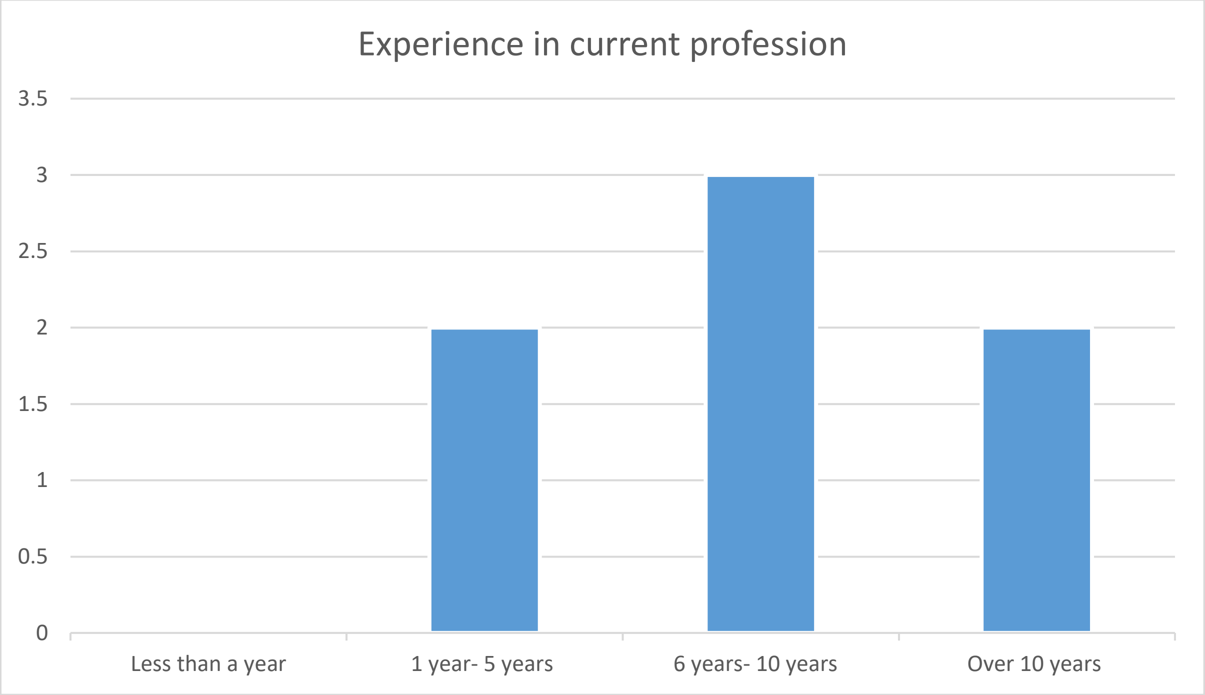


Figure E.419: Experience in current profession (Business, consultancy and management- UK)

This analysis is based on the responses received from United Kingdom participants employed in the Business, consulting and management sector. There were 7 participants and 5 out of them were males and 2 females (See figure E. 417). They were within the 18-65 age range out of which 1 in the 18-25, 3 in the 26-35, 2 in the 46-55, and 1 in the 56-65 range (See figure E. 418). The participants employed in industry between 1 and over 10 years (See figure E. 419).

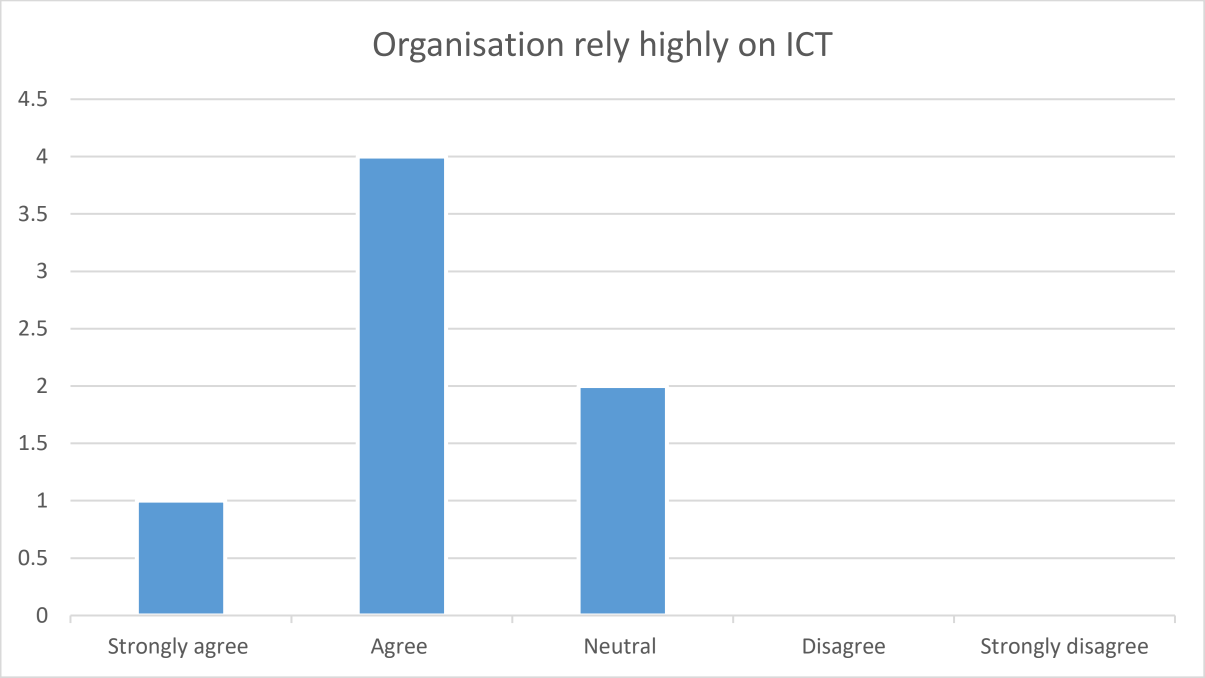


Figure E.420: Organisation rely highly on ICT (Business, consultancy and management- UK)

Out of the 7 respondents, 5 have worked in a technology reliance working environment, 2 unaware of reliance on technology because of the nature of the work assigned to them (See figure E.420). This indicates a majority of those who have been working in business, consultancy and management industry have had a high reliance on ICT.

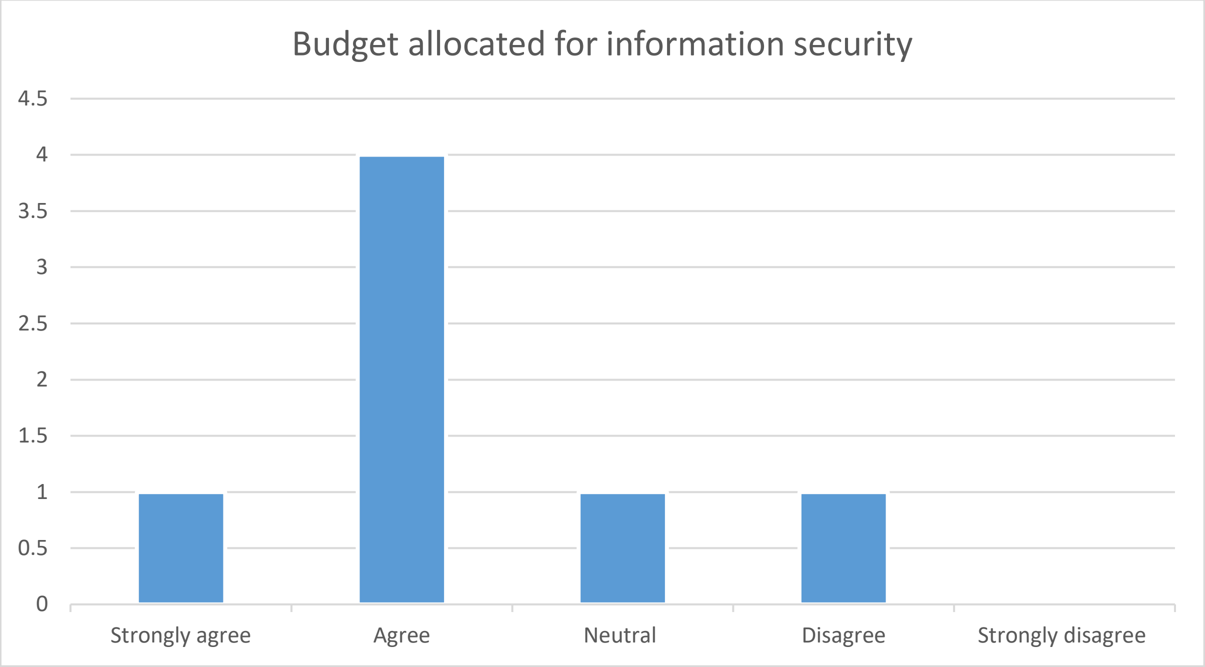


Figure E.421: Budget allocated for information security (Business, consultancy and management- UK)

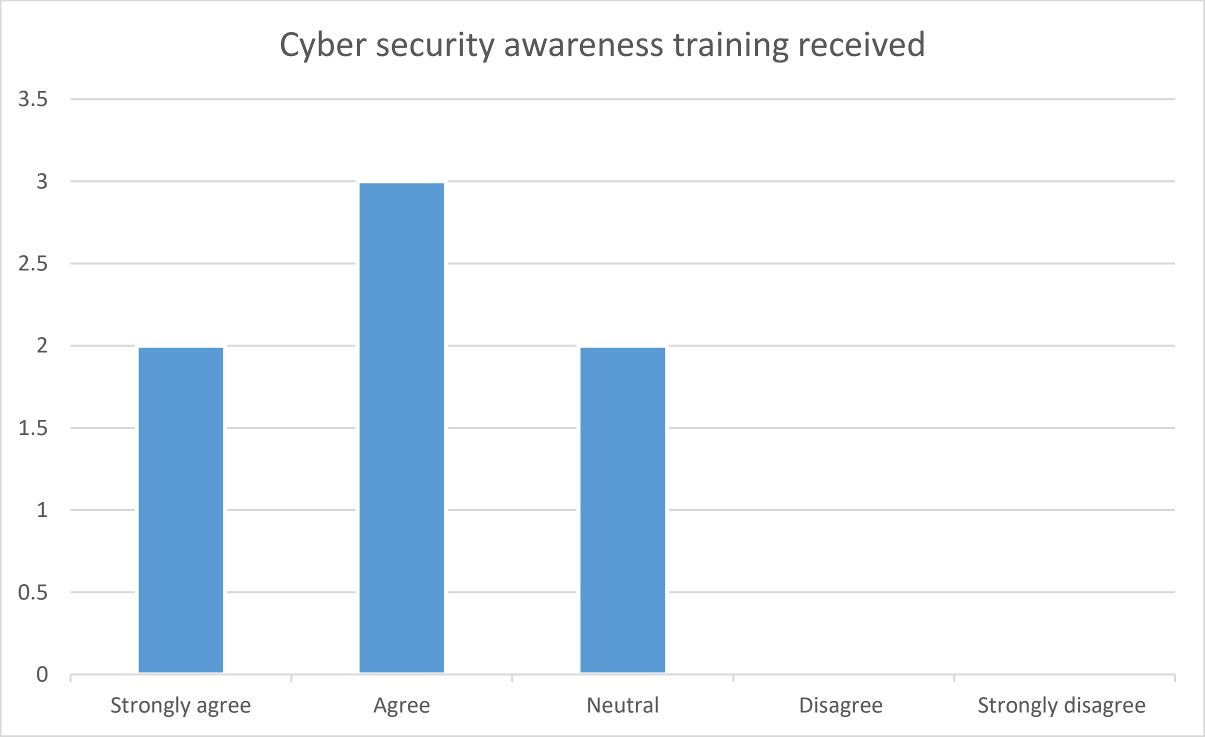


Figure E.422: Cyber security awareness training received (Business, consultancy and management- UK)

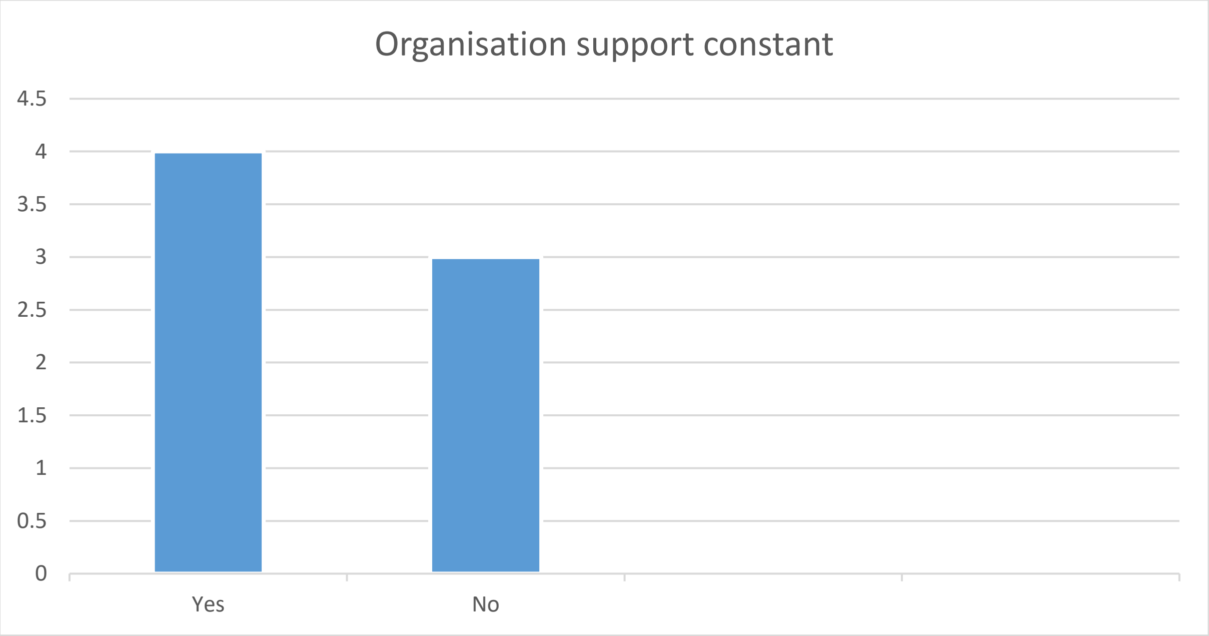


Figure E.423: Organisation support constant (Business, consultancy and management-UK)

Funding has been sketchy. 5 out of the 7 have indicated that their organisations had an allocated budget for information security, whilst 1 had not expressed an opinion either way and notably according to the 1 disagreed, their organisations had no budget allocation for information security (See figure E. 421). According to some of the participants, regular security awareness training received was adequate despite the satisfactory level of resources allocated for information security.5 participants have received regular cybersecurity awareness training, whilst only 2 neither agreed nor disagreed (See figure E. 422). In addition, 4 participants received support from the organisation to protect personal information, and 3 did not (See figure E. 423). Given the nature of the industry, the organisations allocate sufficient funding, and security awareness training, and support to protect personal information.

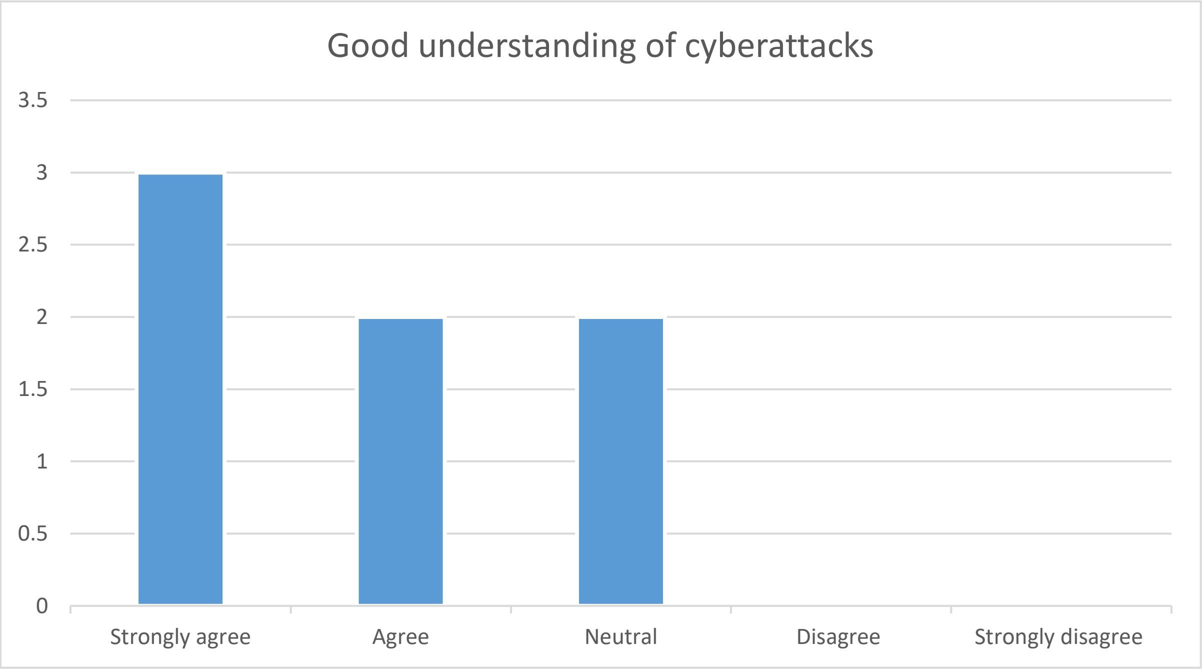


Figure E.424: Good understanding of cyberattacks (Business, consultancy and management- UK)

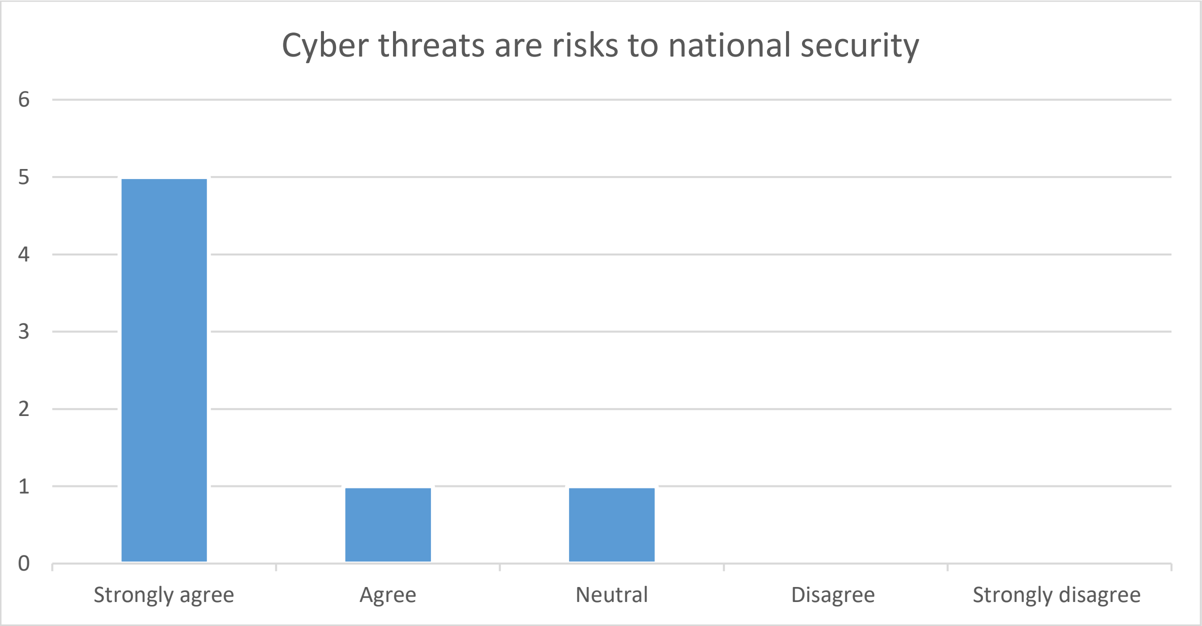


Figure E.425: Cyber threats are risks to national security (Business, consultancy and management- UK)

Despite the security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 5 participants do have, 2 have not expressed opinion either way (See figure E. 424). Furthermore, 86 percent of the participants realises the potential threats to national security from cyber-attacks (See figure E. 425). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

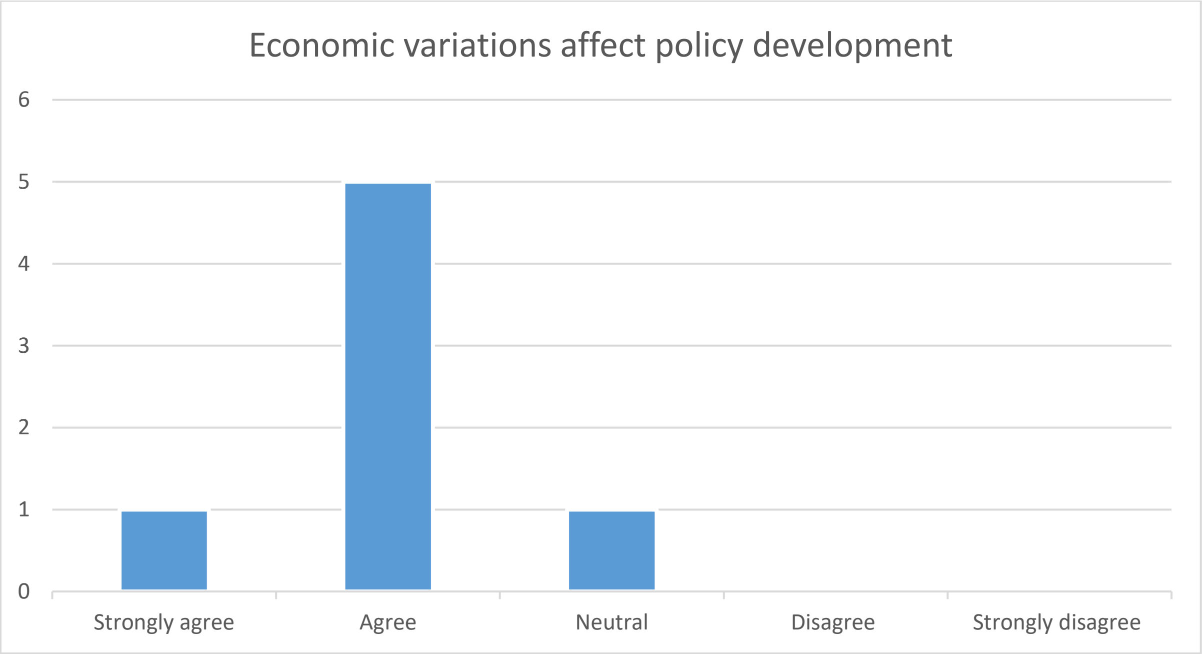


Figure E.426: Economic variations affect policy development (Business, consultancy and management- UK)

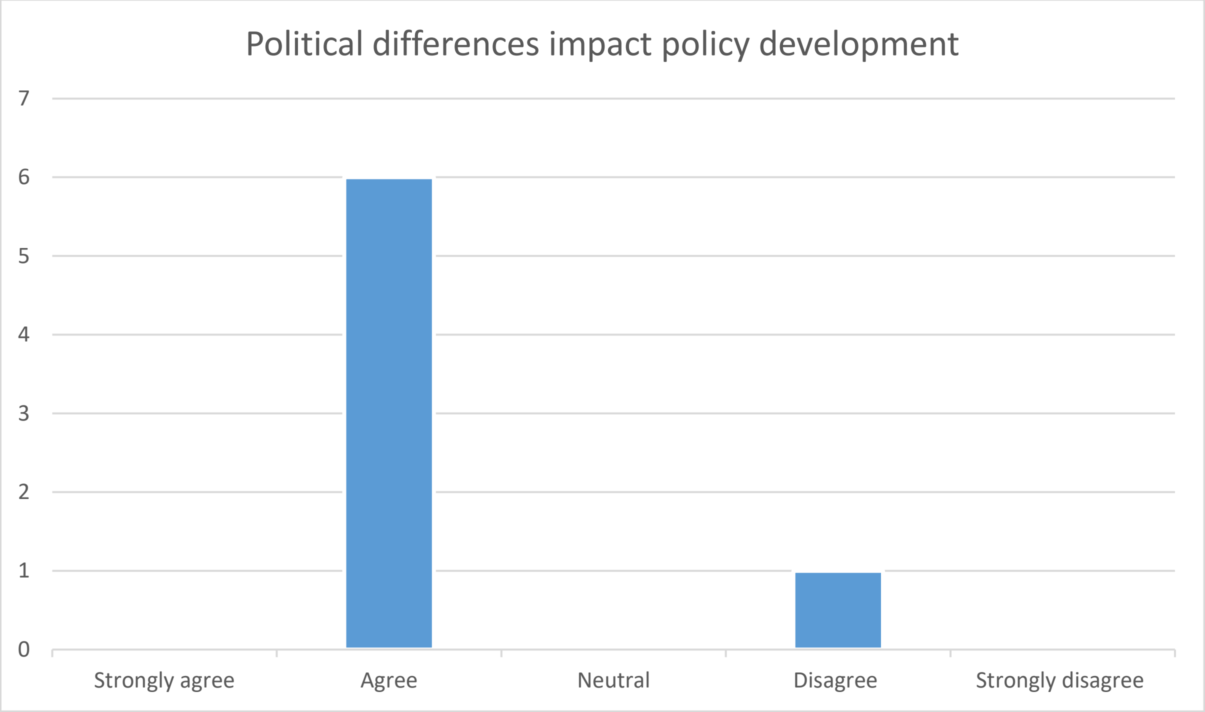


Figure E.427: Political differences impact policy development (Business, consultancy and management- UK)

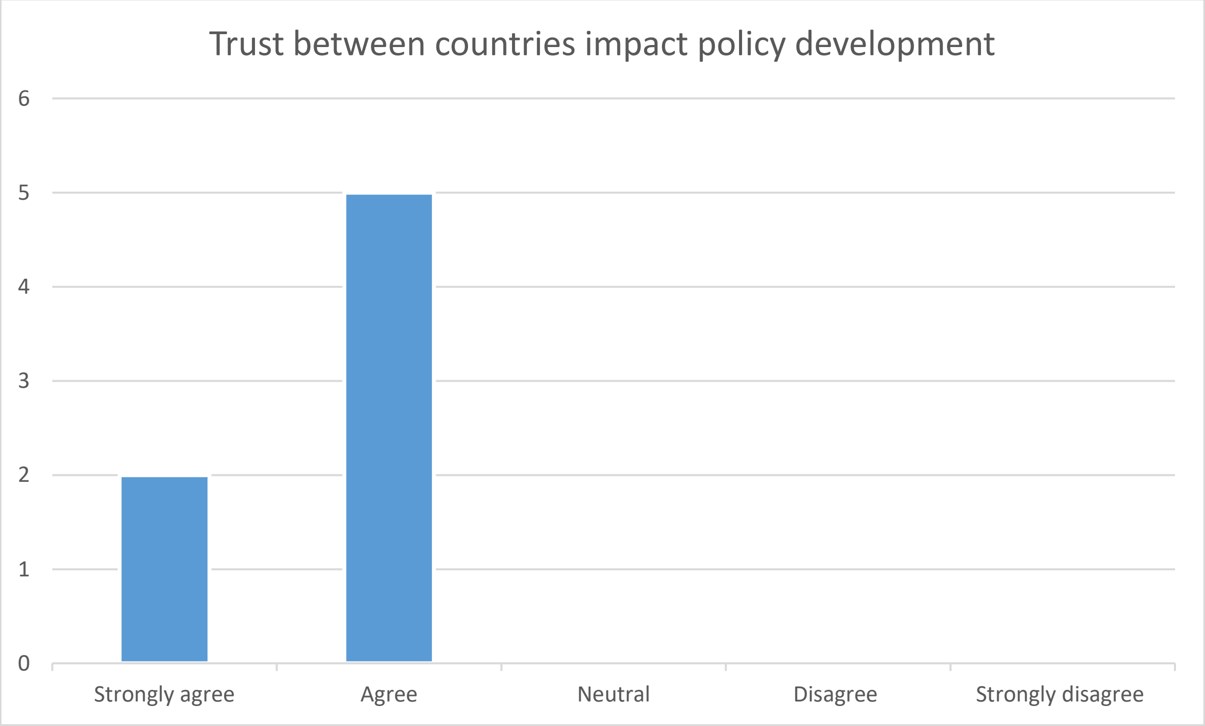


Figure E.428: Trust between countries impact policy development (Business, consultancy and management- UK)

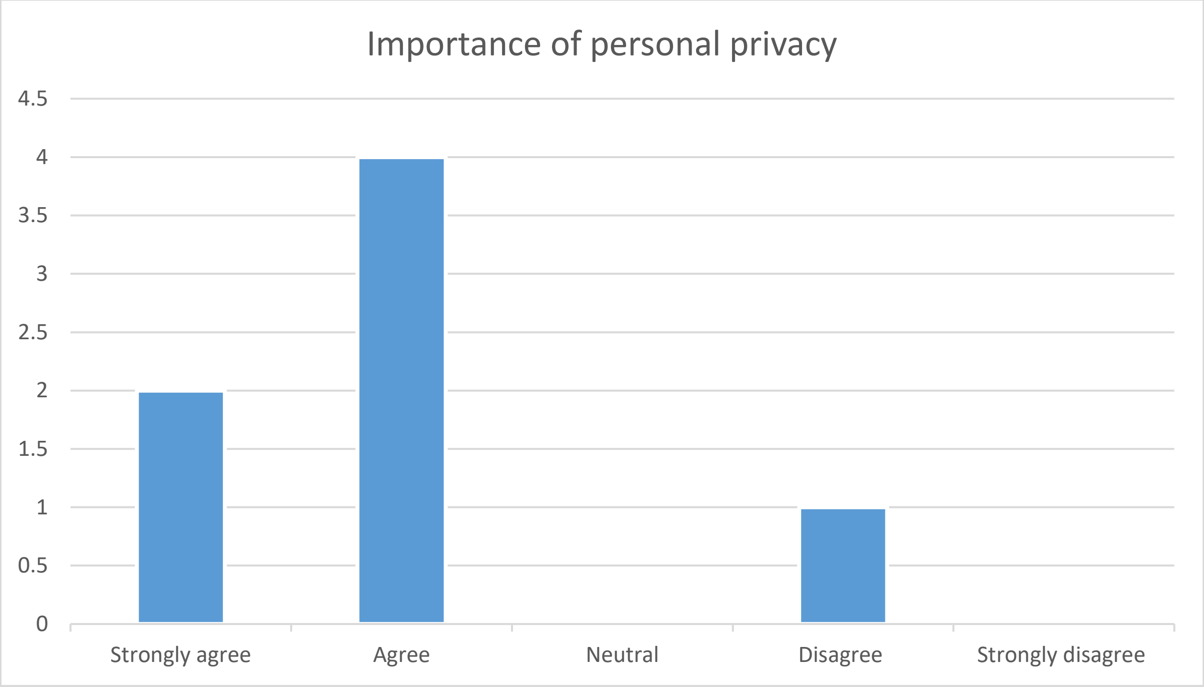


Figure E.429: Importance of personal privacy (Business, consultancy and management-UK)

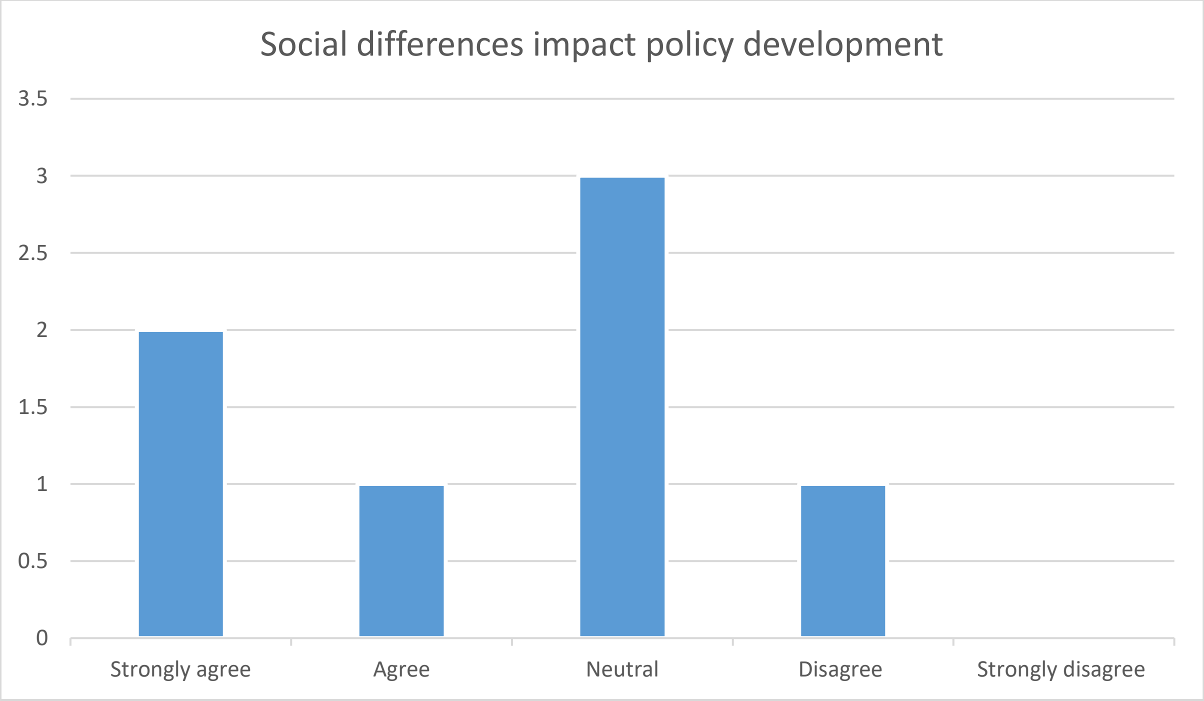


Figure E.430: Social differences impact policy development (Business, consultancy and management- UK)

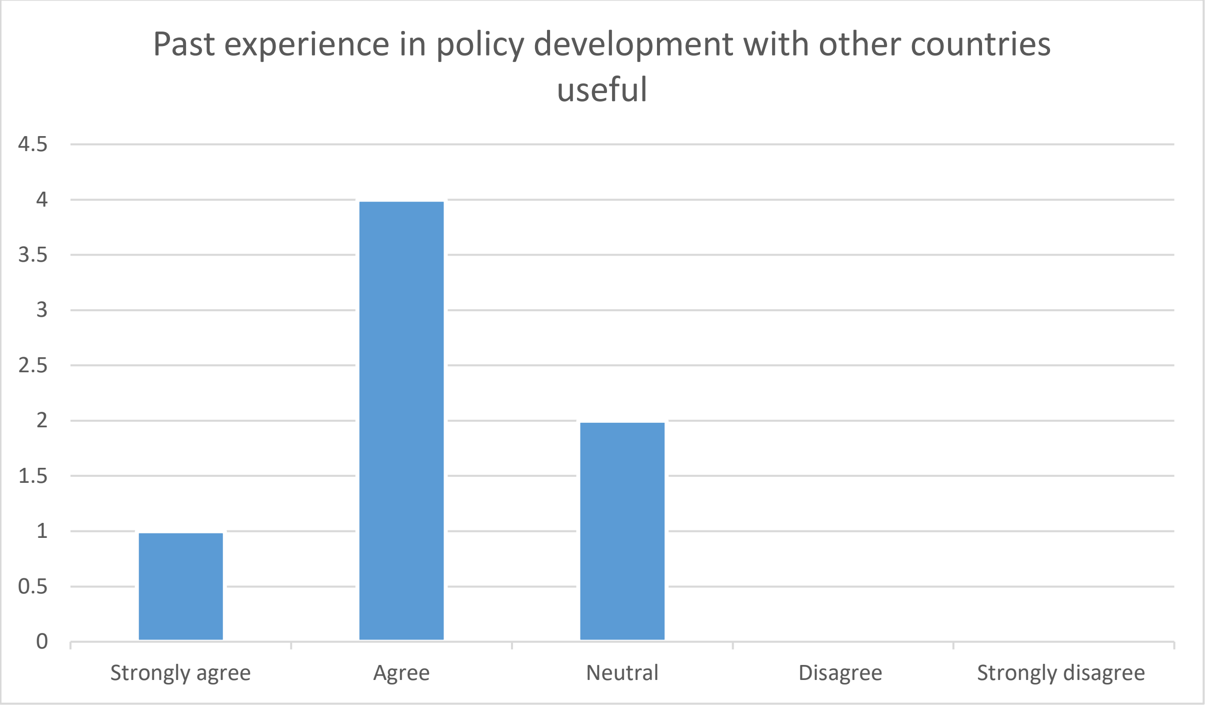


Figure E.431: Past experience in policy development with other countries useful (Business, consultancy and management- UK)

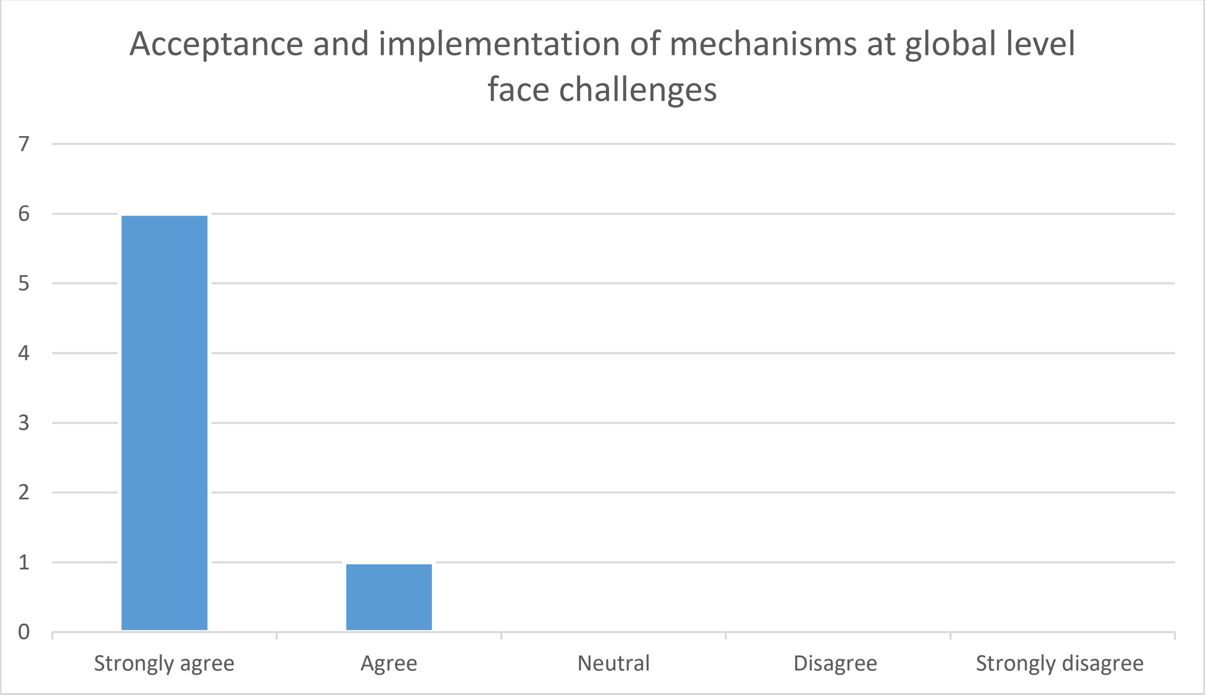


Figure E.432: Acceptance and implementation of mechanisms at global level face challenges (Business, consultancy and management- UK)

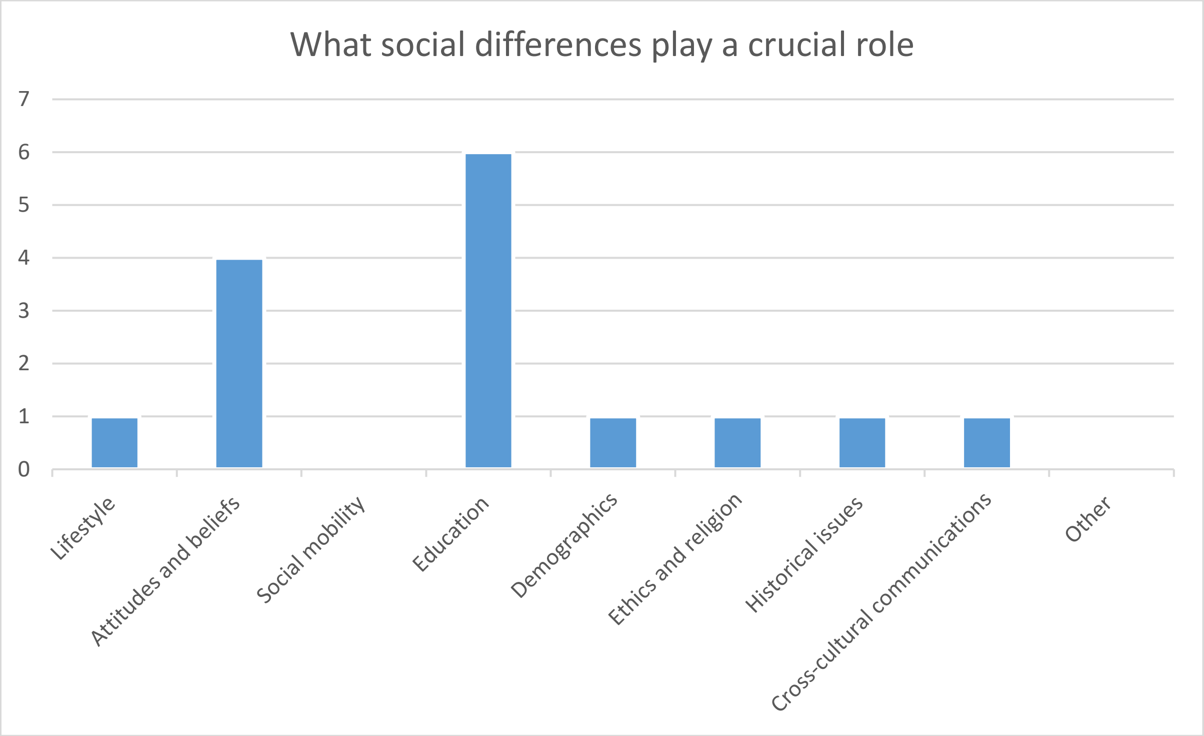


Figure E.433: What social differences play a crucial role (Business, consultancy and management- UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure E. 433). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

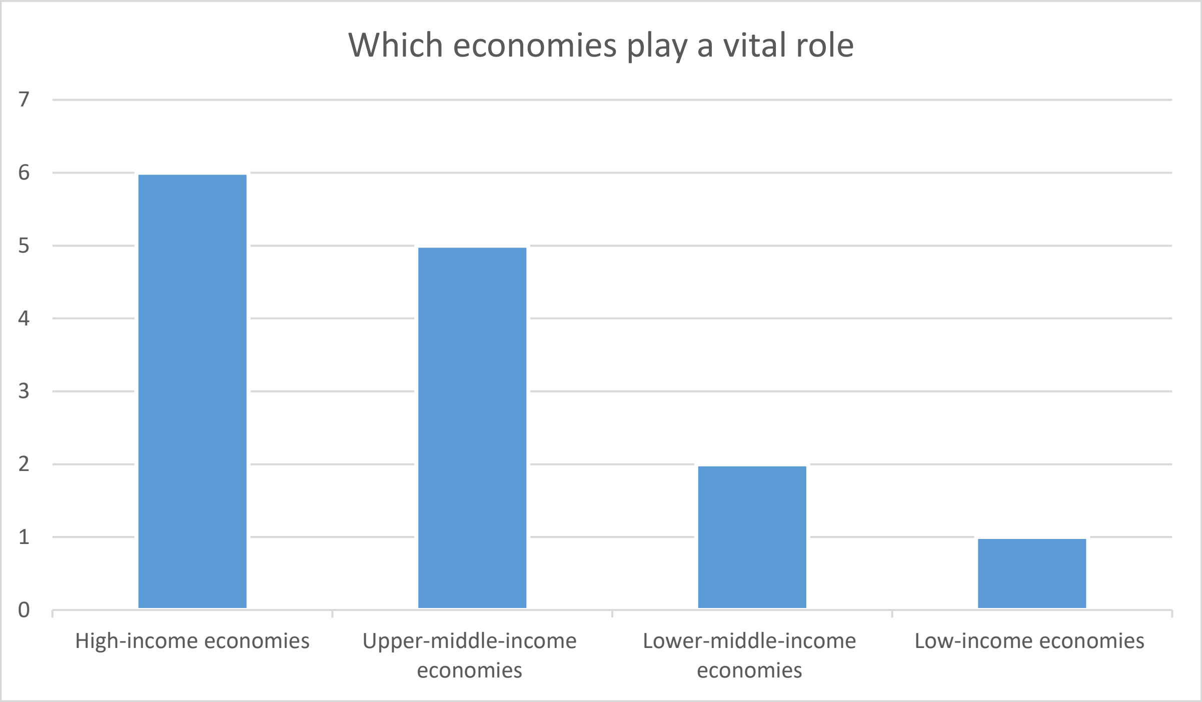


Figure E.434: Which economies play a vital role (Business, consultancy and management- UK)

In the questionnaire, the majority has stated that the high income and upper-middle-income countries play a vital role (See figure E. 434). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

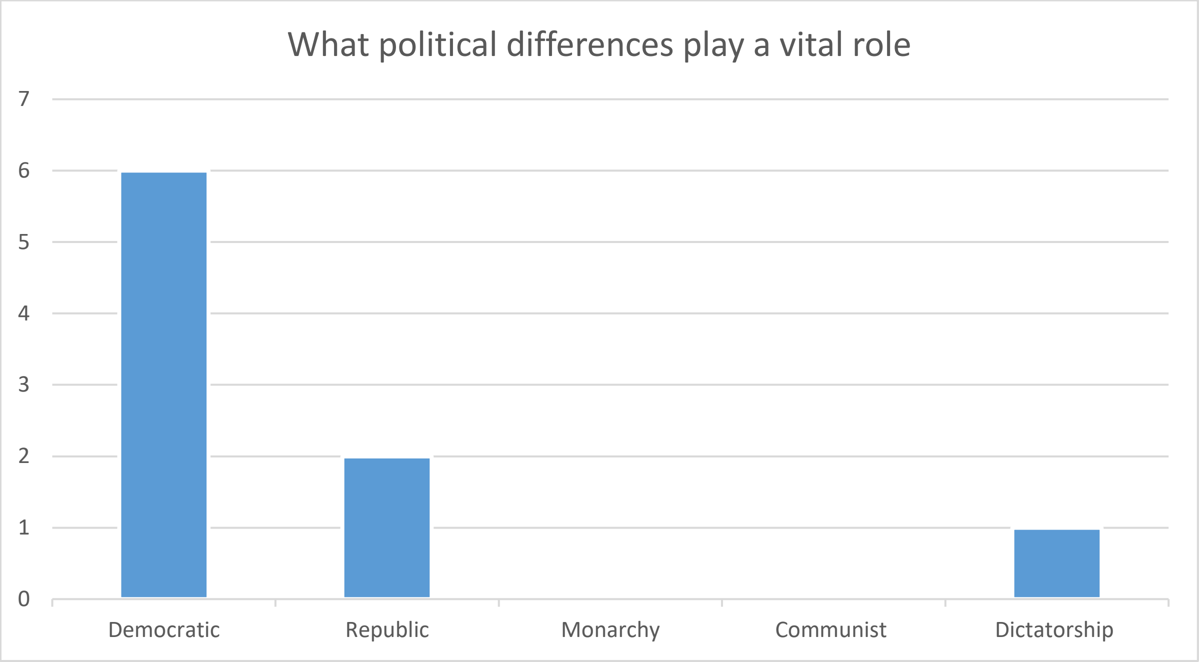


Figure E.435: What political differences play a vital role (Business, consultancy and management- UK)

The majority have chosen a democratic political system (See figure E. 435), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

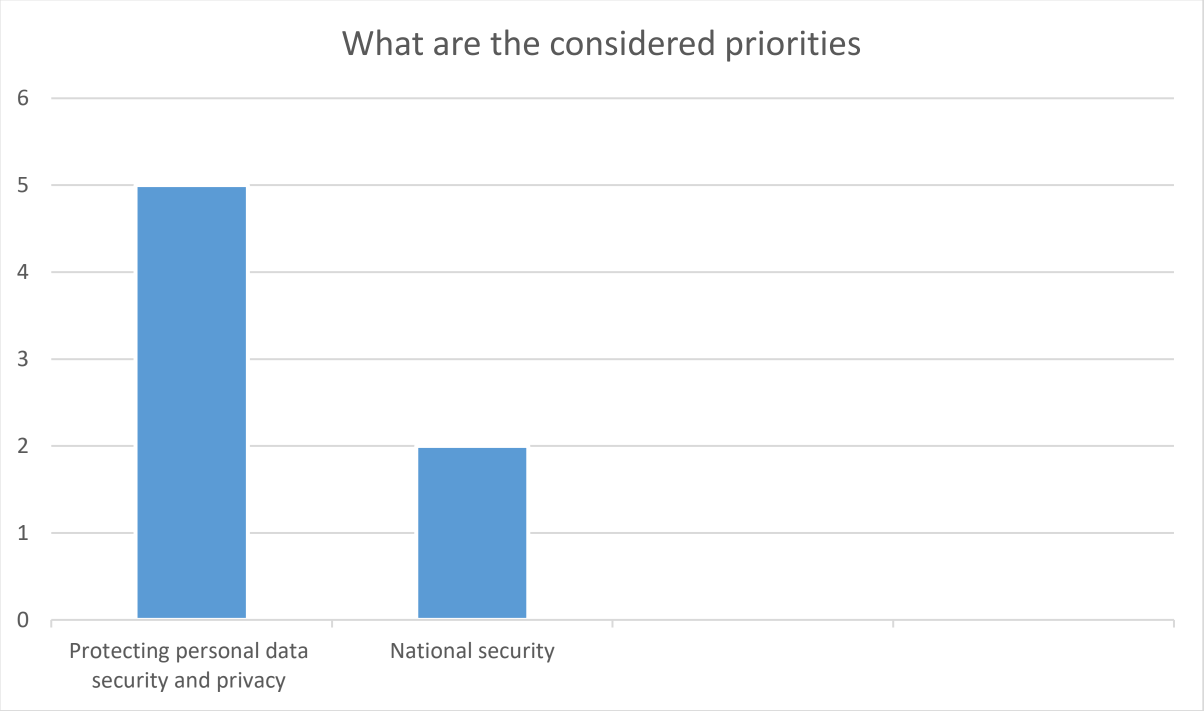


Figure E.436: What are the considered priorities (Business, consultancy and management- UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security, which is a significant factor (See figure E. 436). However, in an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

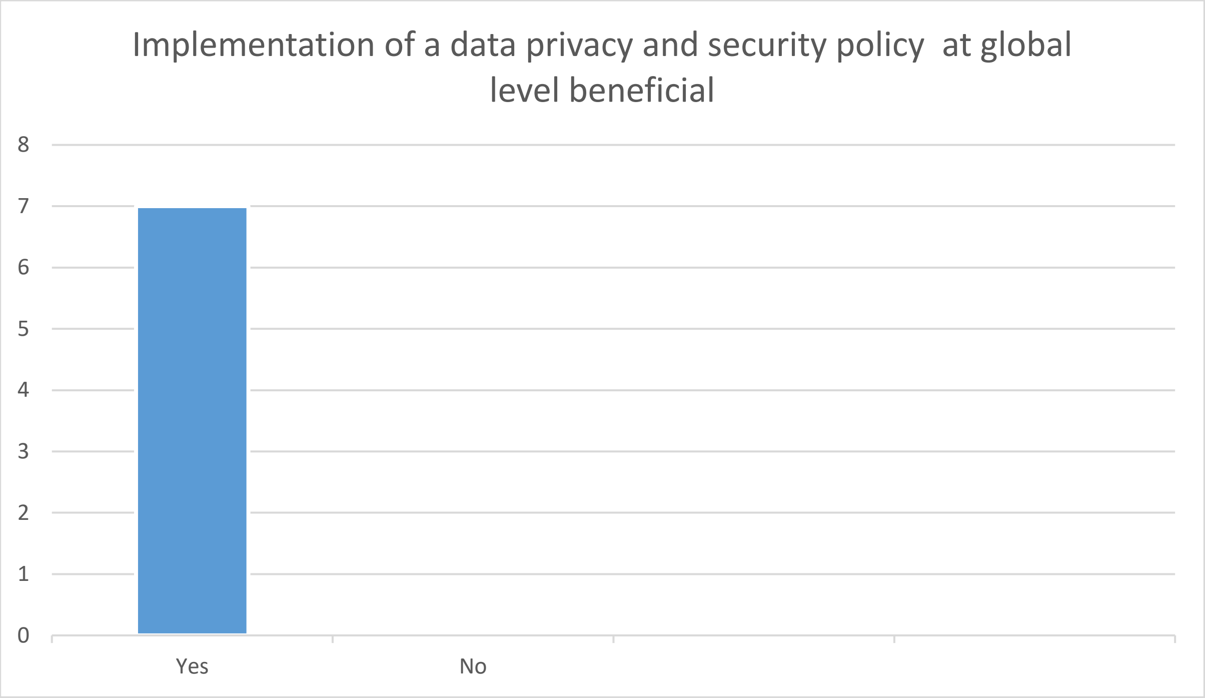


Figure E.437: Implementation of a data privacy and security policy at global level beneficial (Business, consultancy and management- UK)

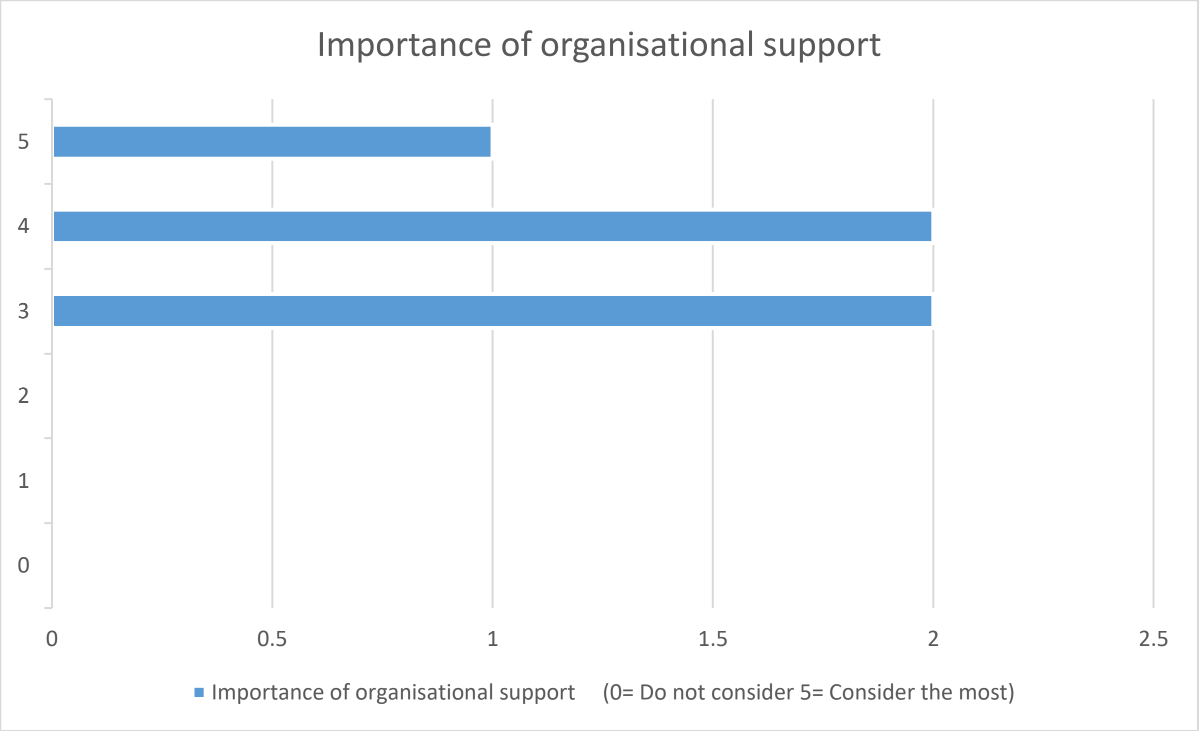


Figure E.438: Importance of organisational support (Business, consultancy and management- UK)

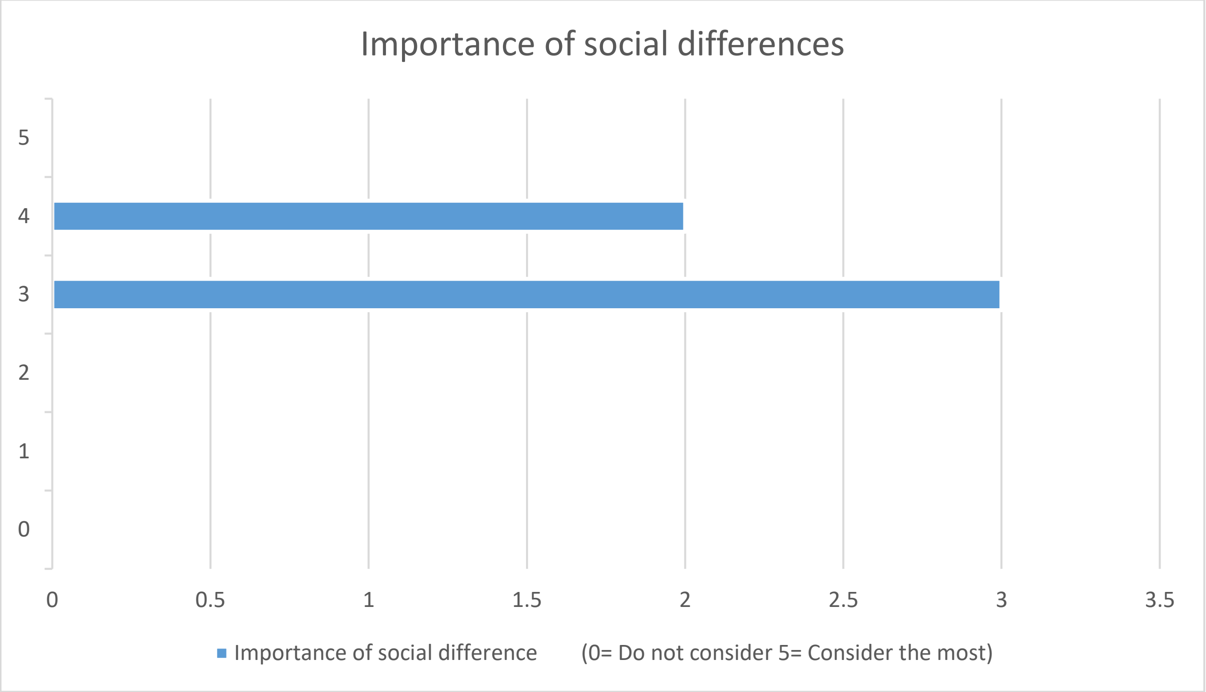


Figure E.439: Importance of social differences (Business, consultancy and management- UK)

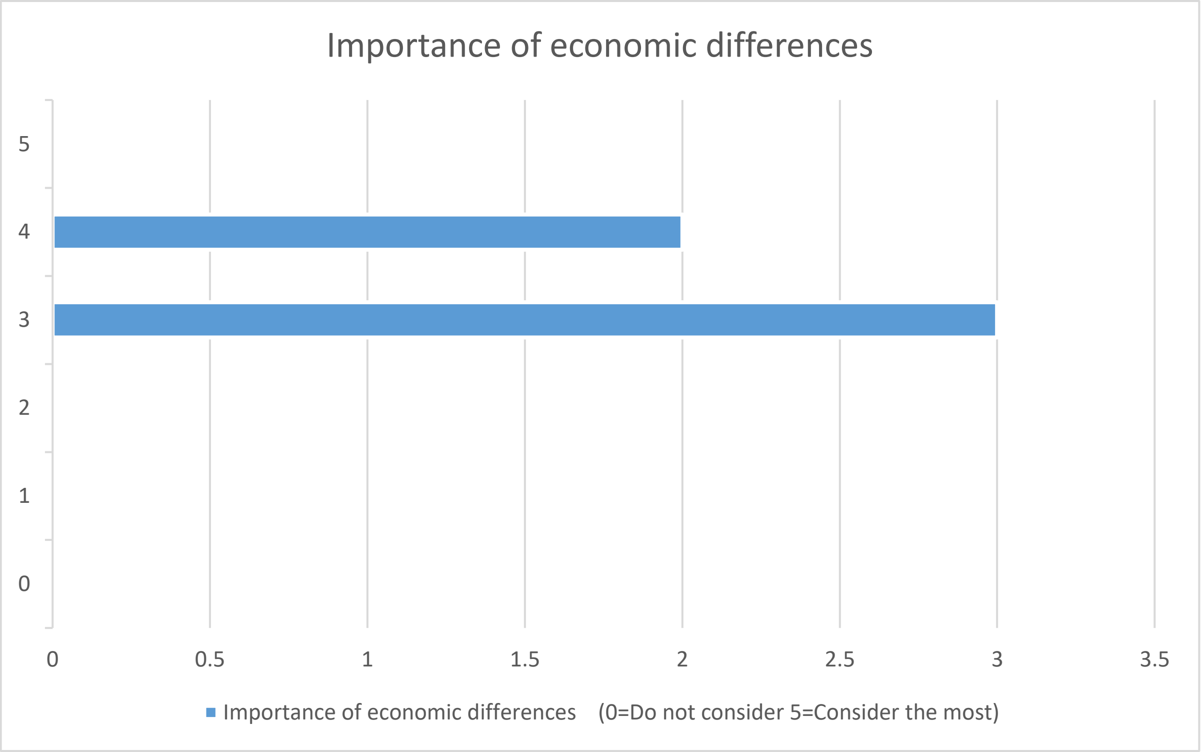


Figure E.440: Importance of economic differences (Business, consultancy and management- UK)

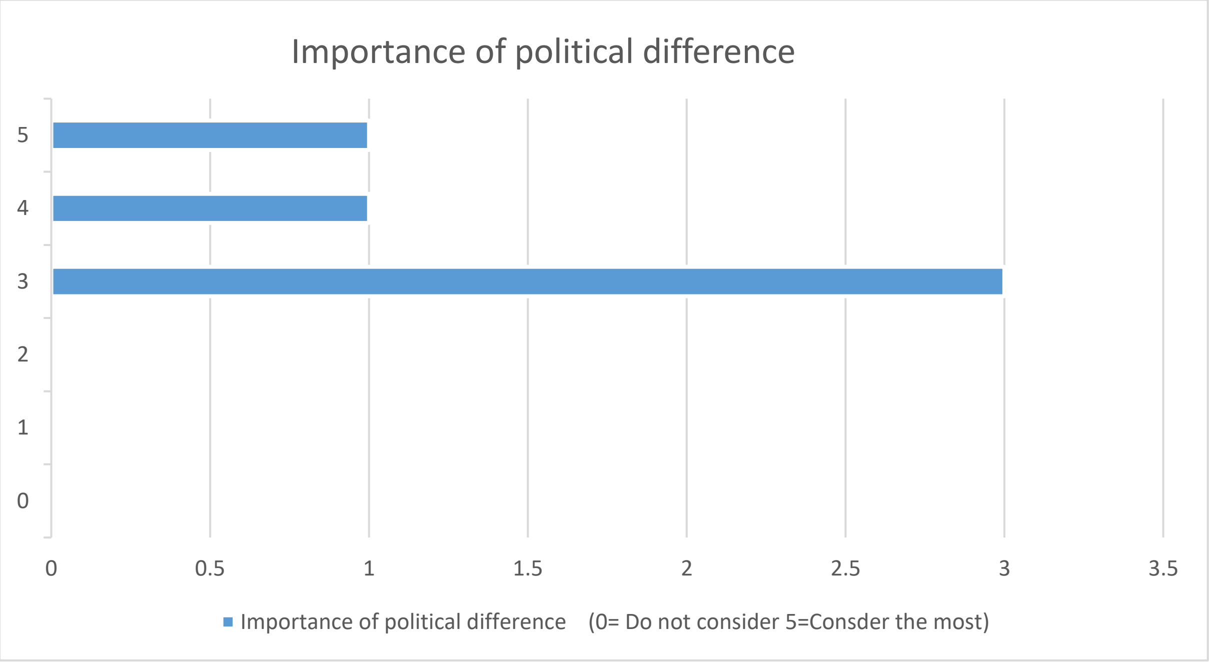


Figure E.441: Importance of political difference (Business, consultancy and management- UK)

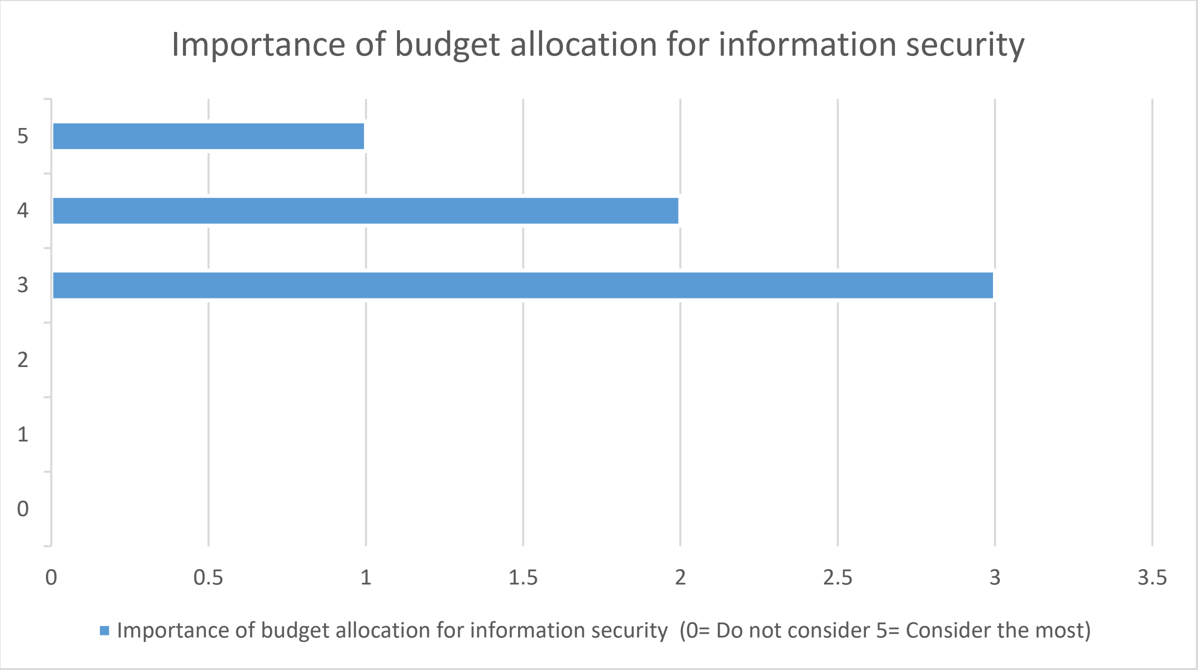


Figure E.442: Importance of budget allocation for information security (Business, consultancy and management- UK)

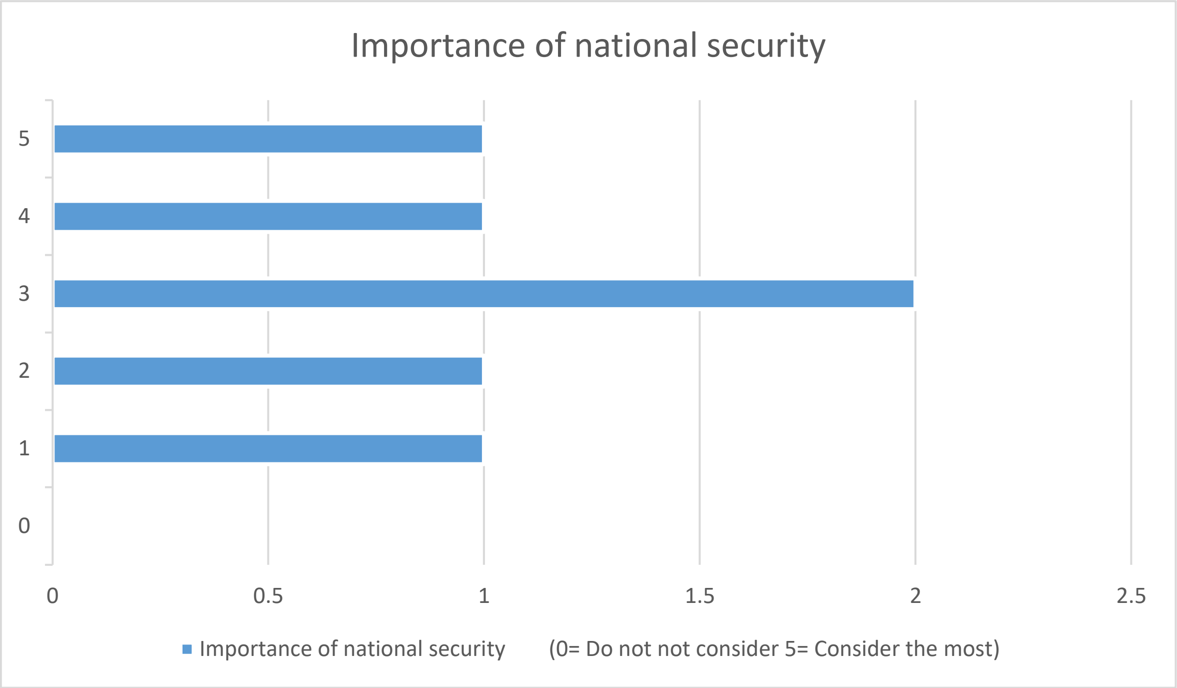


Figure E.443: Importance of national security (Business, consultancy and management- UK)

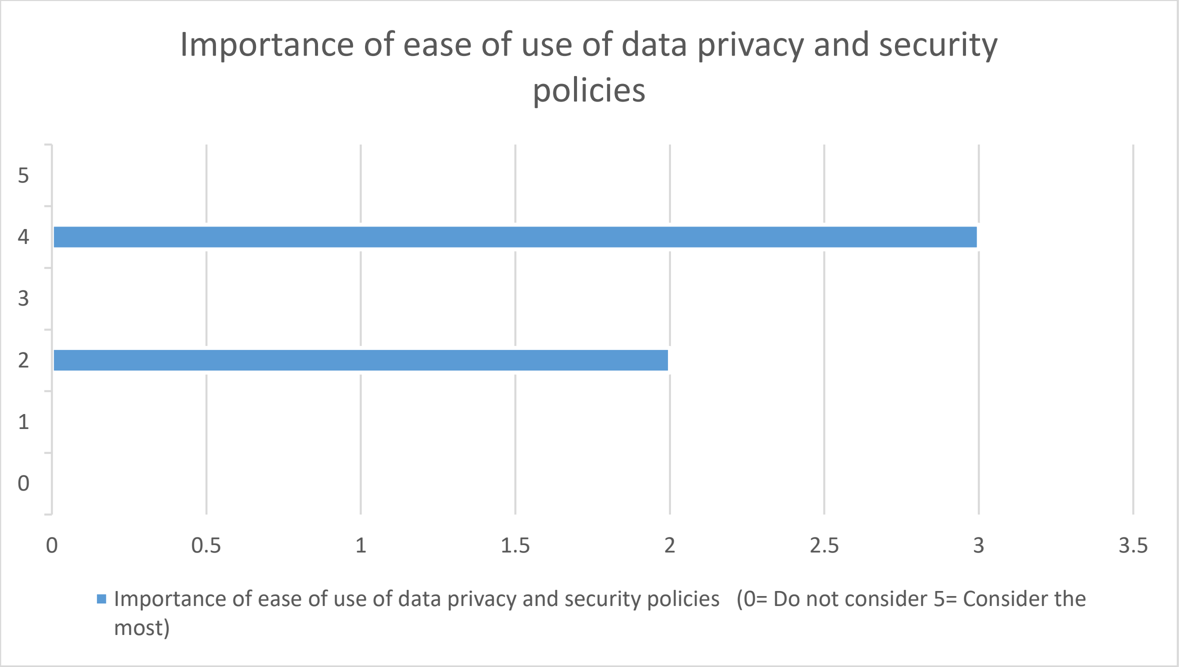


Figure E.444: Importance of ease of use of data privacy and security policies (Business, consultancy and management- UK)

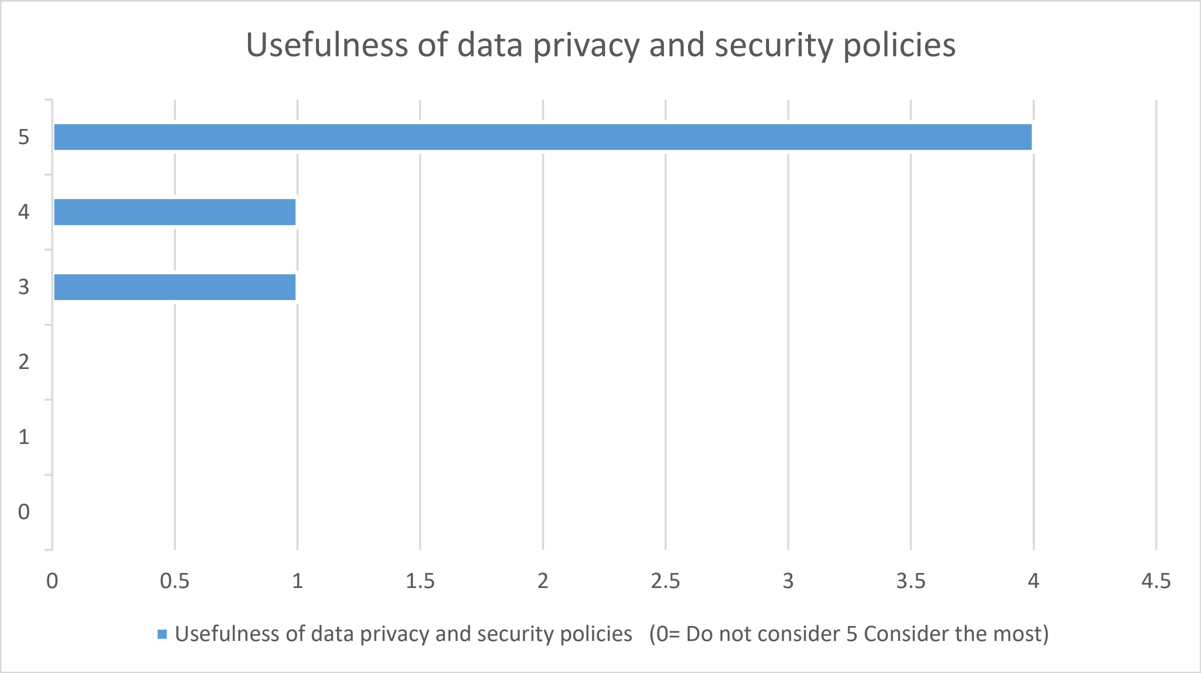


Figure E.445: Usefulness of data privacy and security policies (Business, consultancy and management- UK)

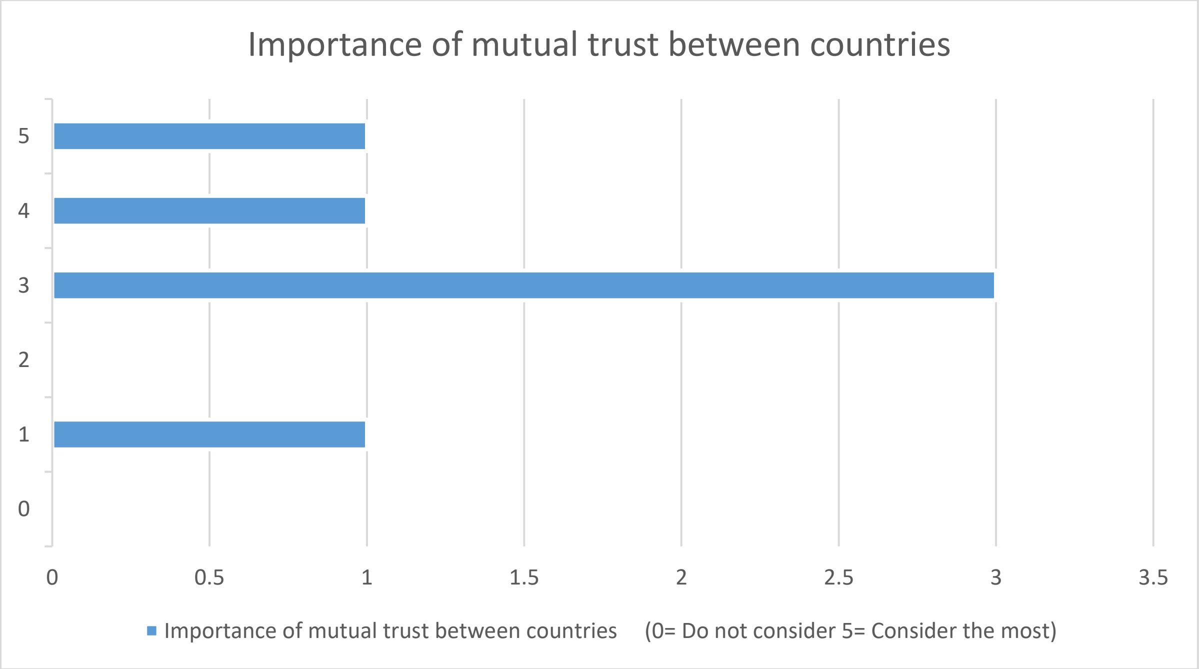


Figure E.446: Importance of mutual trust between countries (Business, consultancy and management- UK)

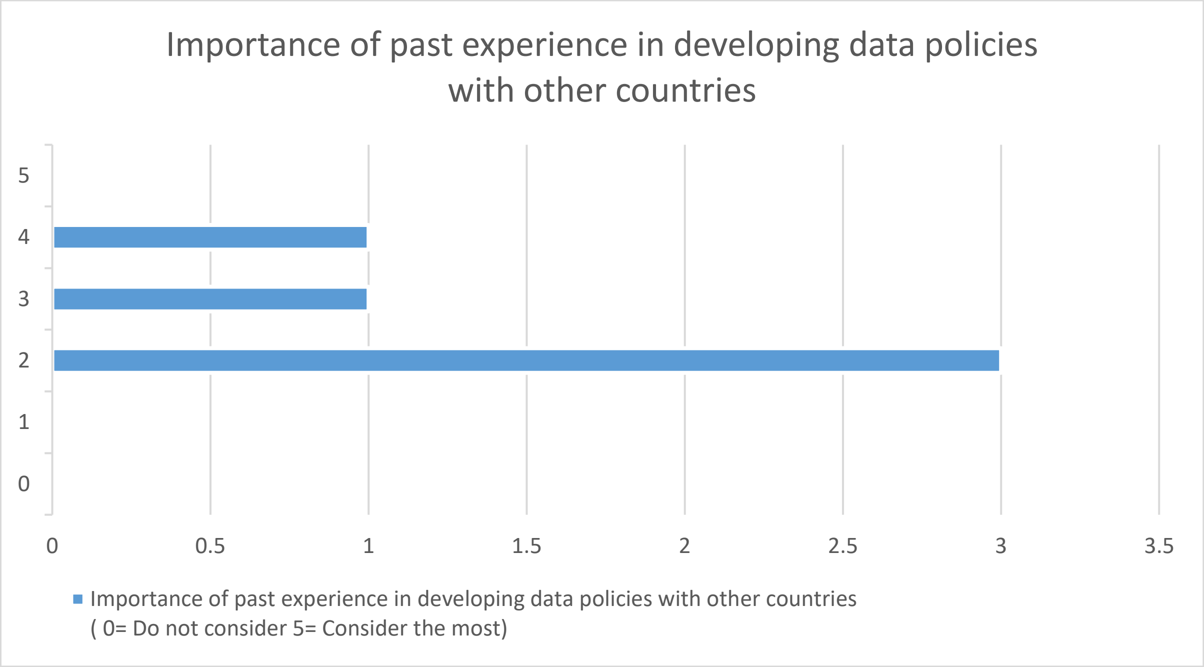


Figure E.447: Importance of past experience in developing data policies with other counties (Business, consultancy and management- UK)

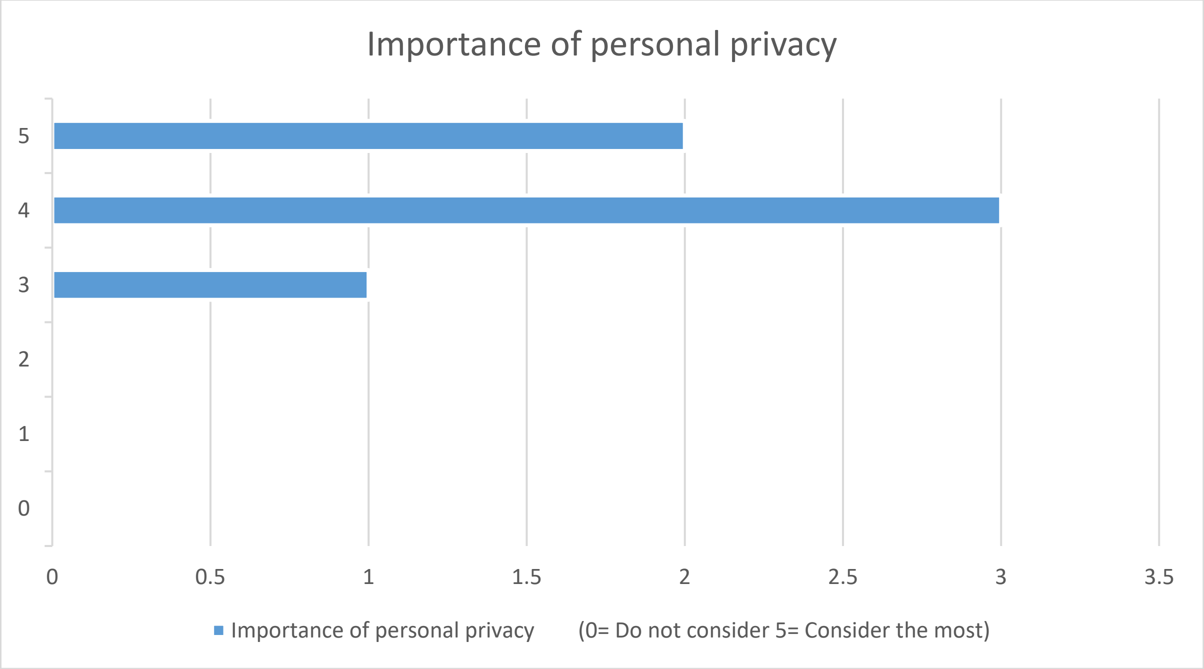


Figure E.448: Importance of personal privacy (Business, consultancy and management- UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 100 percent of the respondents have endorsed (See figure E. 437). The other notable factors that have come out of the survey are organisational support, budget allocation, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure E. 426-436) (See figure E. 438-448).

United Kingdom – Education

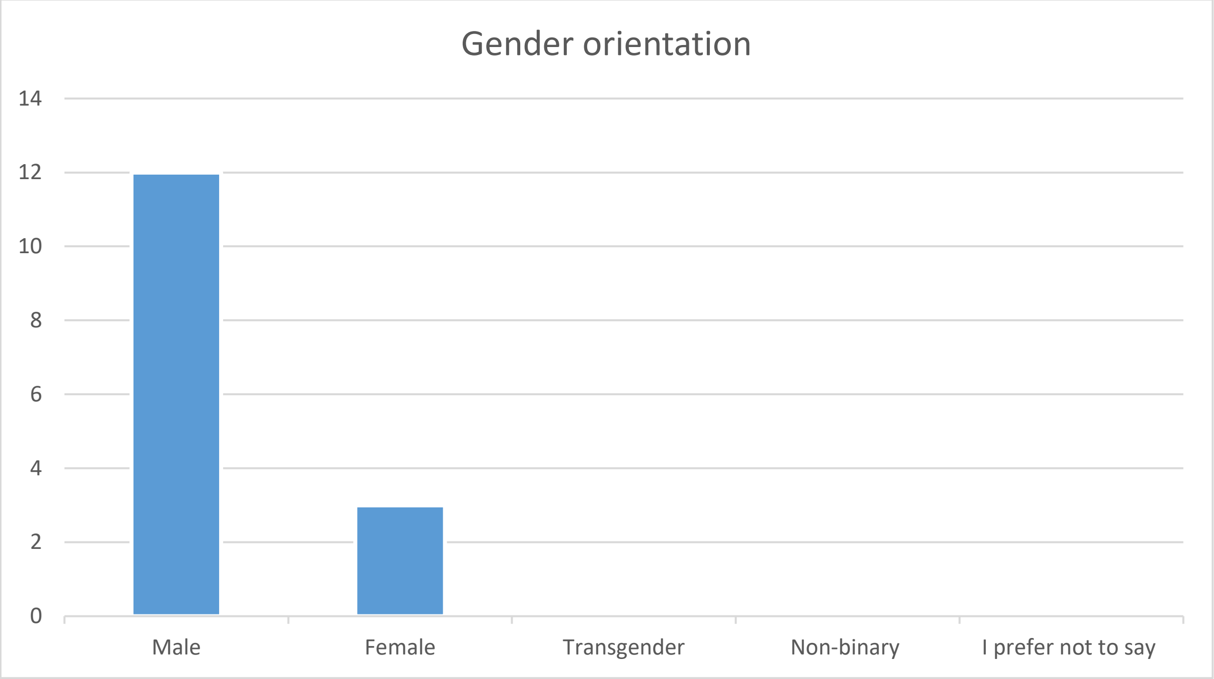


Figure E.449: Gender orientation (Education-UK)

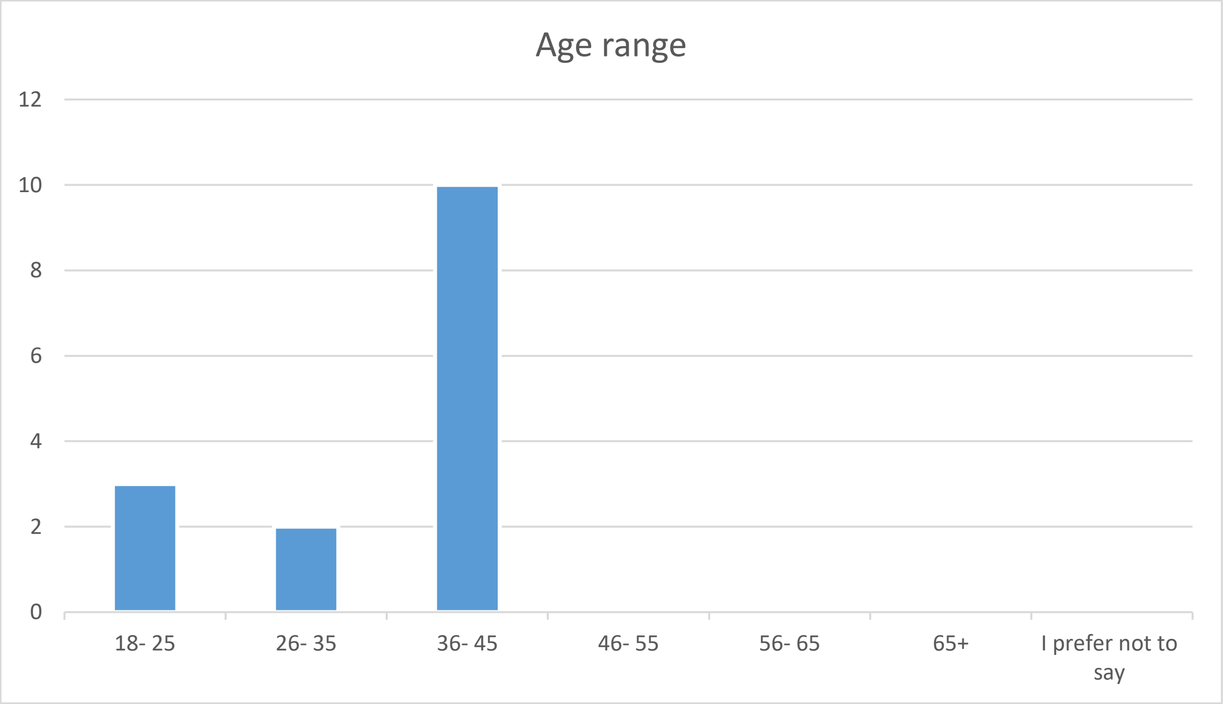


Figure E.450: Age range (Education-UK)

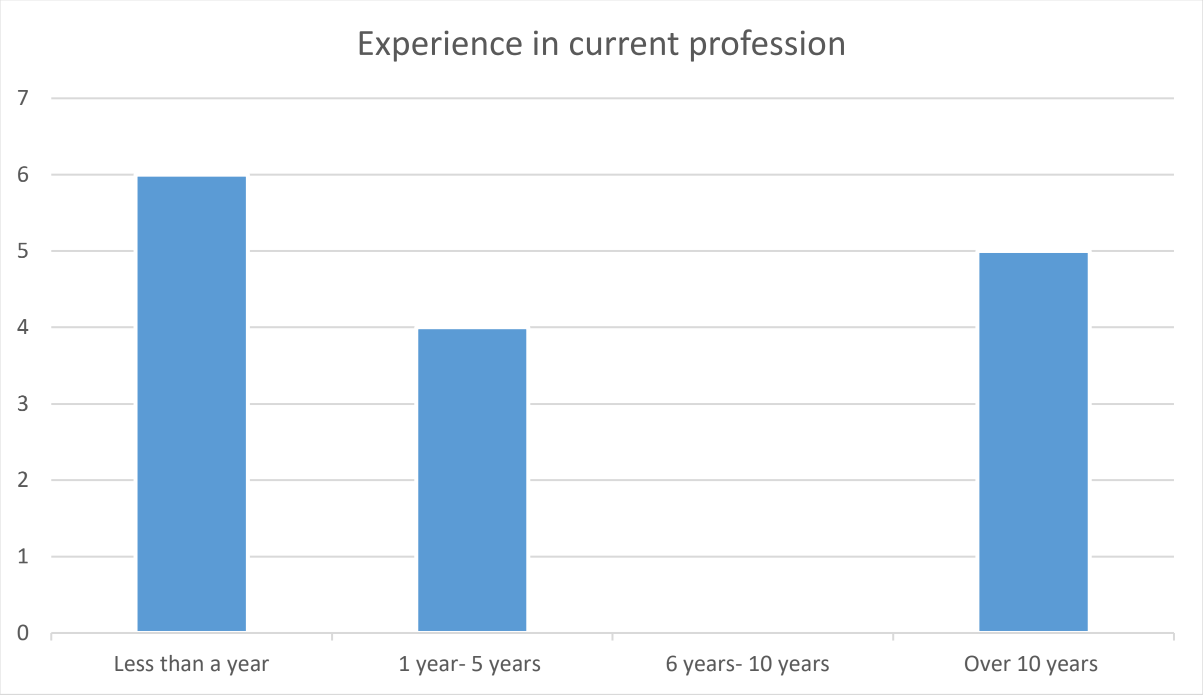


Figure E.451: Experience in current profession (Education-UK)

This analysis is based on the responses received from United Kingdom participants in the education sector. There were 15 participants and 12 out of them were males and 3 females (See figure E. 449). They were within the 18-45 age range out of which 3 in the 18-25, 2 in the 26-35, and 10 in the 36-45 range (See figure E. 450). The participants employed in industry between less than a year and over 10 years (See figure E. 451).

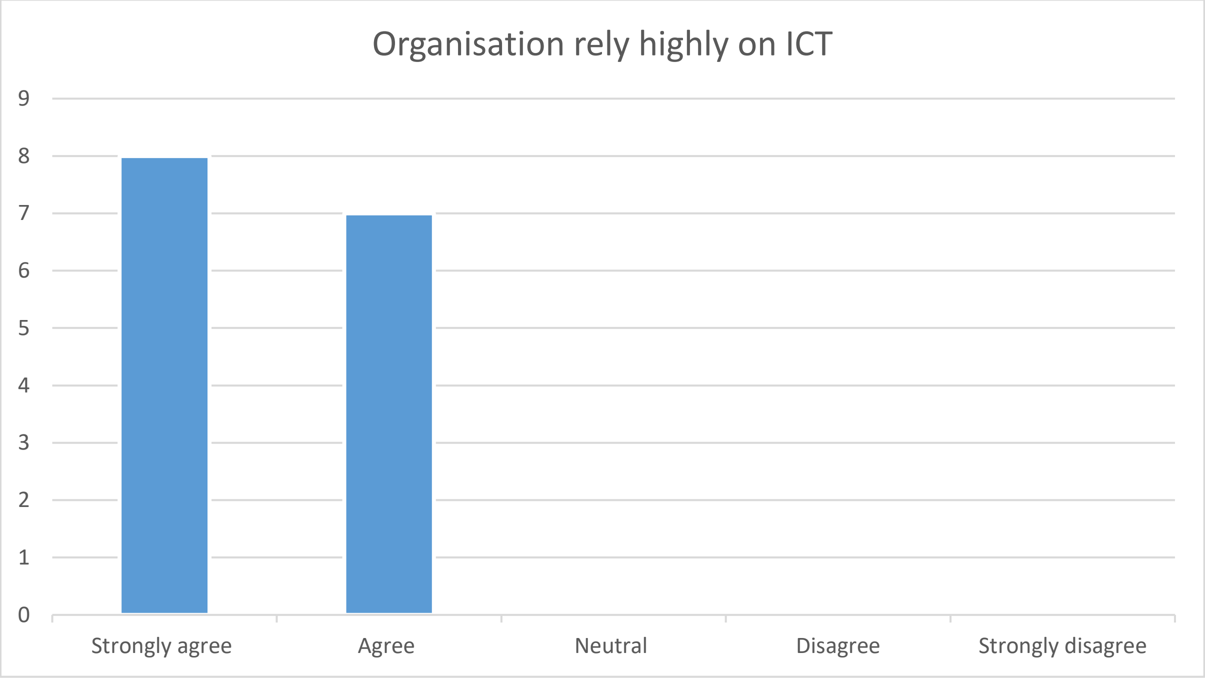


Figure E.452: Organisation rely highly on ICT (Education-UK)

Out of the 15 respondents, all of them have worked in a technology reliance working environment (See figure E. 452).

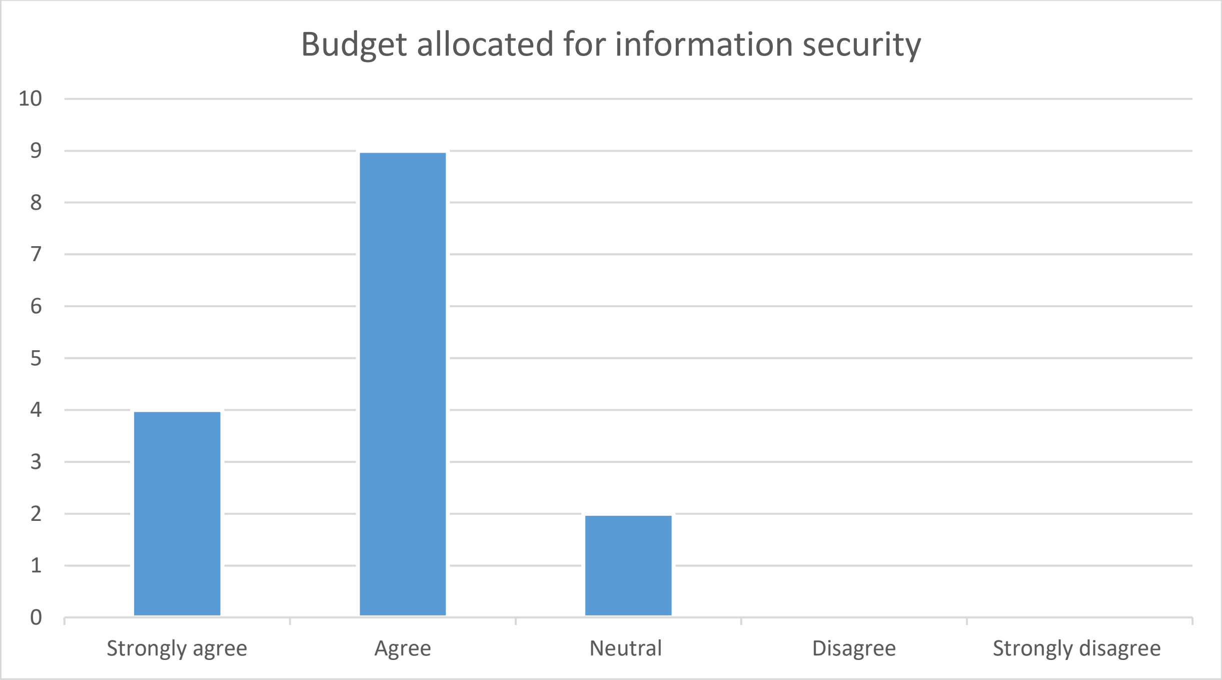


Figure E.453: Budget allocated for information security (Education-UK)

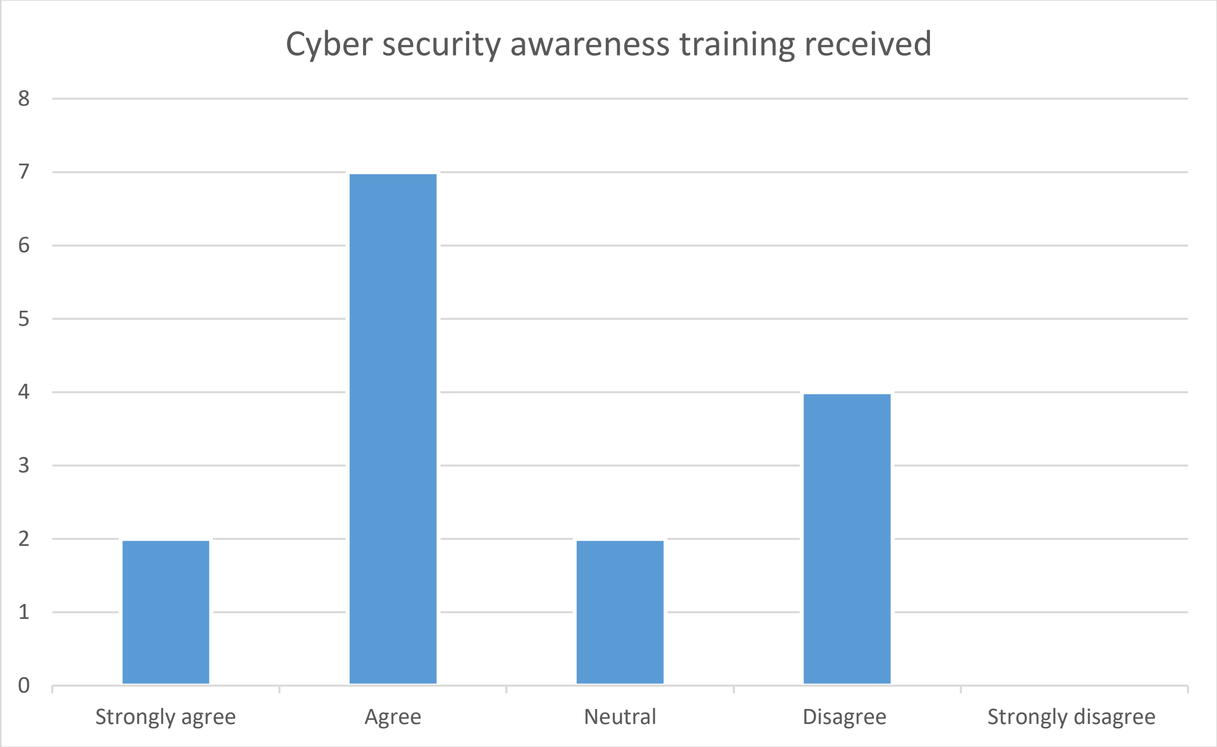


Figure E.454: Cyber security awareness training received (Education-UK)

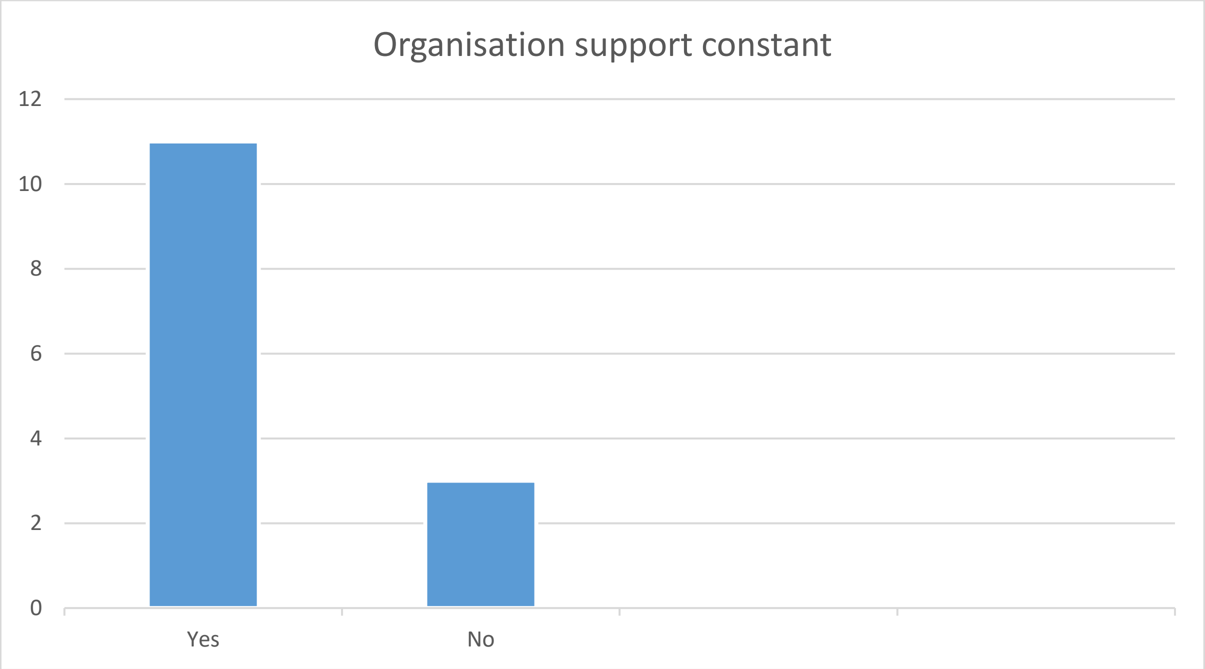


Figure E.455: Organisation support constant (Education-UK)

Funding has been sketchy. 13 out of the 15 have indicated that their organisations had an allocated budget for information security, whilst 2 had not expressed an opinion either way (See figure E. 453). According to some of the participants, regular security awareness training received was adequate despite the satisfactory level of resources allocated for information security. 9 participants have received regular cybersecurity awareness training, whilst 2 neither agreed nor disagreed, and 4 participants had not regularly received security awareness training (See figure E. 454). In addition, only 3 participants had not received support from the organisation to protect personal information, whilst 11 did (See figure E. 455). This clearly indicates that those in the education sector have a high reliance of technology. To support that, an adequate level of budget allocation, training and supporting systems provided towards protection of personal data of the staff, students, and their research work from unauthorised intruders. This strong commitment from the organisation will ensure their data bases are not compromised and preserve the good name of the institution.

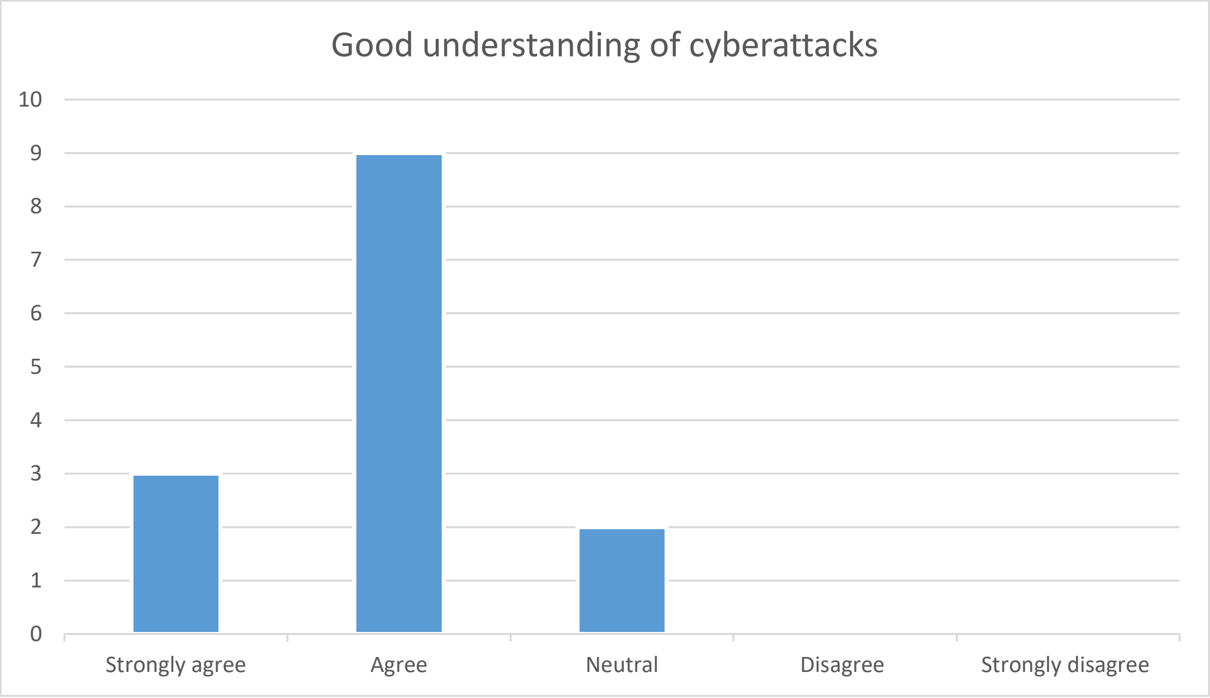


Figure E.456: Good understanding of cyberattacks (Education-UK)

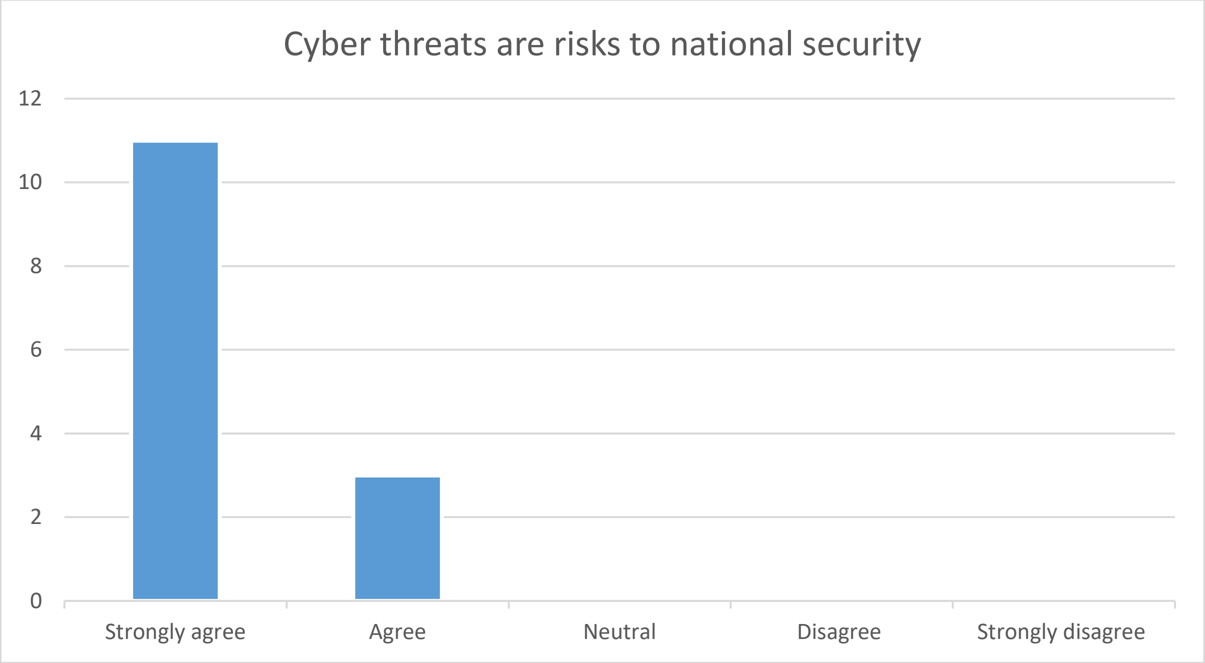


Figure E.457: Cyber threats are risks to national security (Education-UK)

Despite the security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 12 participants do have, 2 have not expressed opinion either way (See figure E. 456). Furthermore, 93 percent of the participants also realise the potential threats to national security from cyber-attacks (See figure E. 457). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

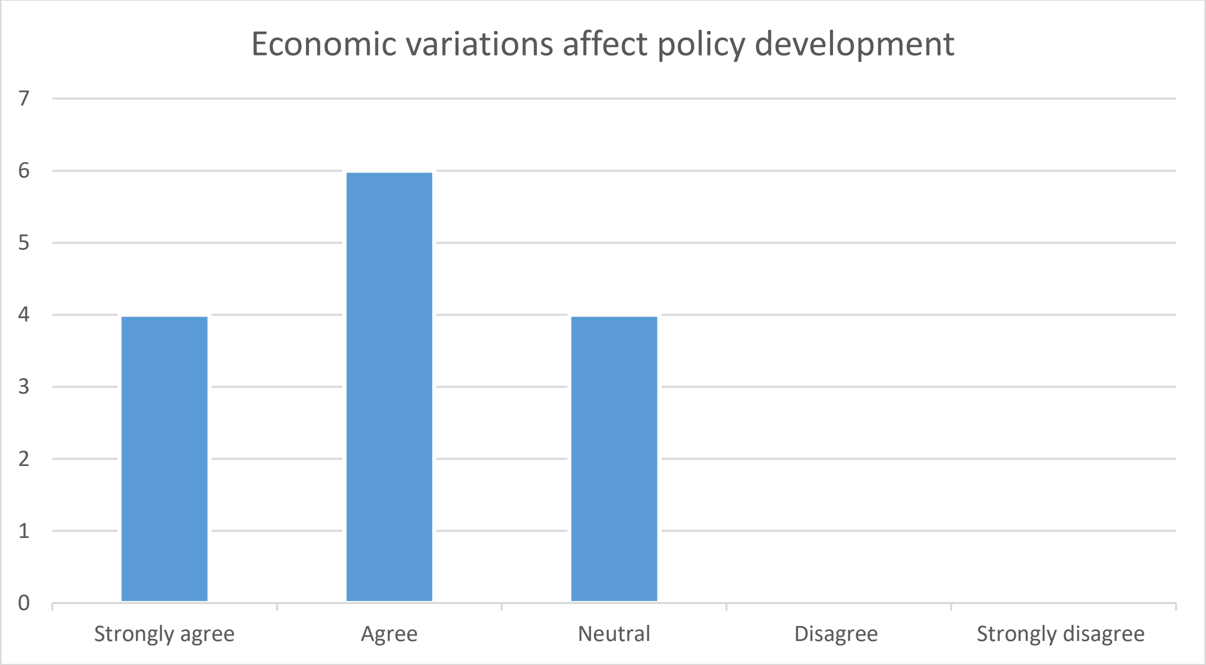


Figure E.458: Economic variations affect policy development (Education-UK)

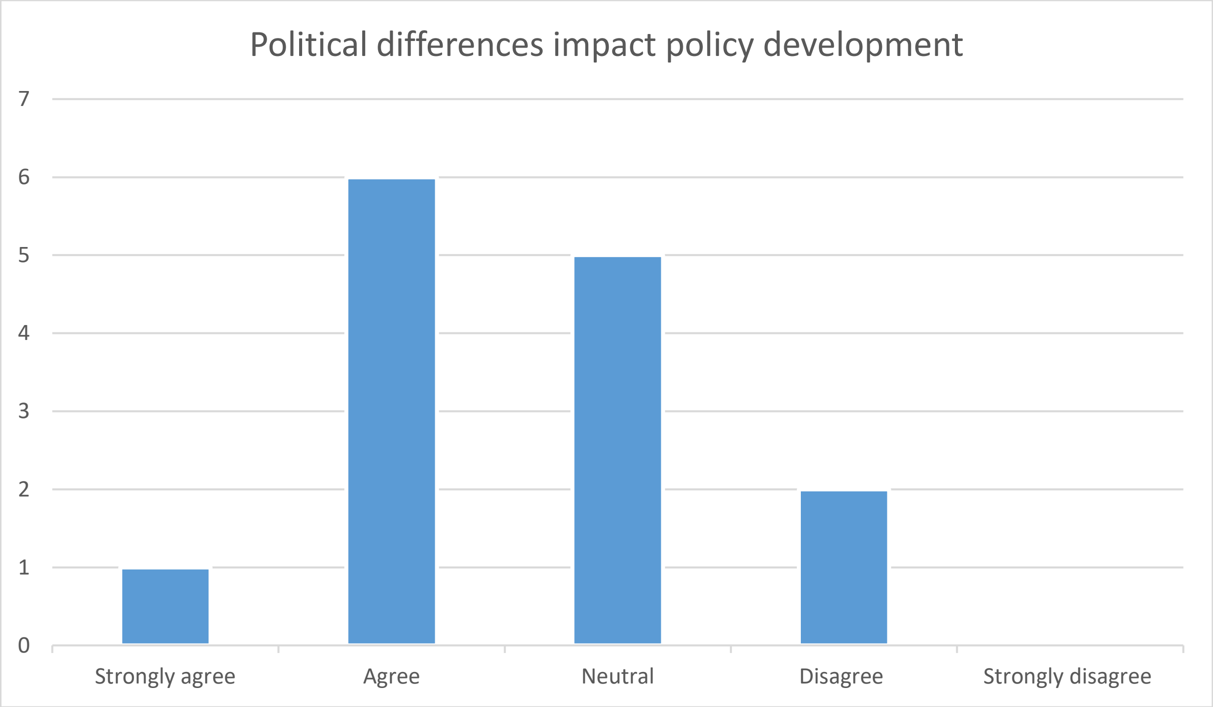


Figure E.459: Political differences impact policy development (Education-UK)

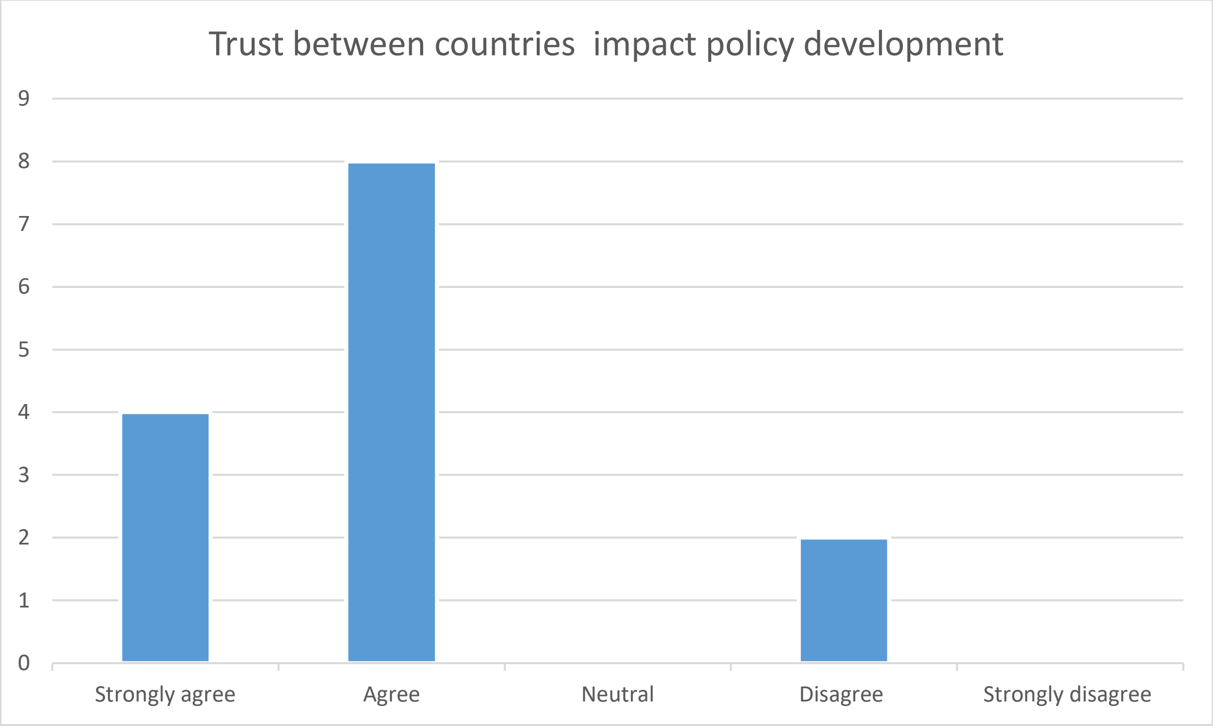


Figure E.460: Trust between countries impact policy development (Education-UK)

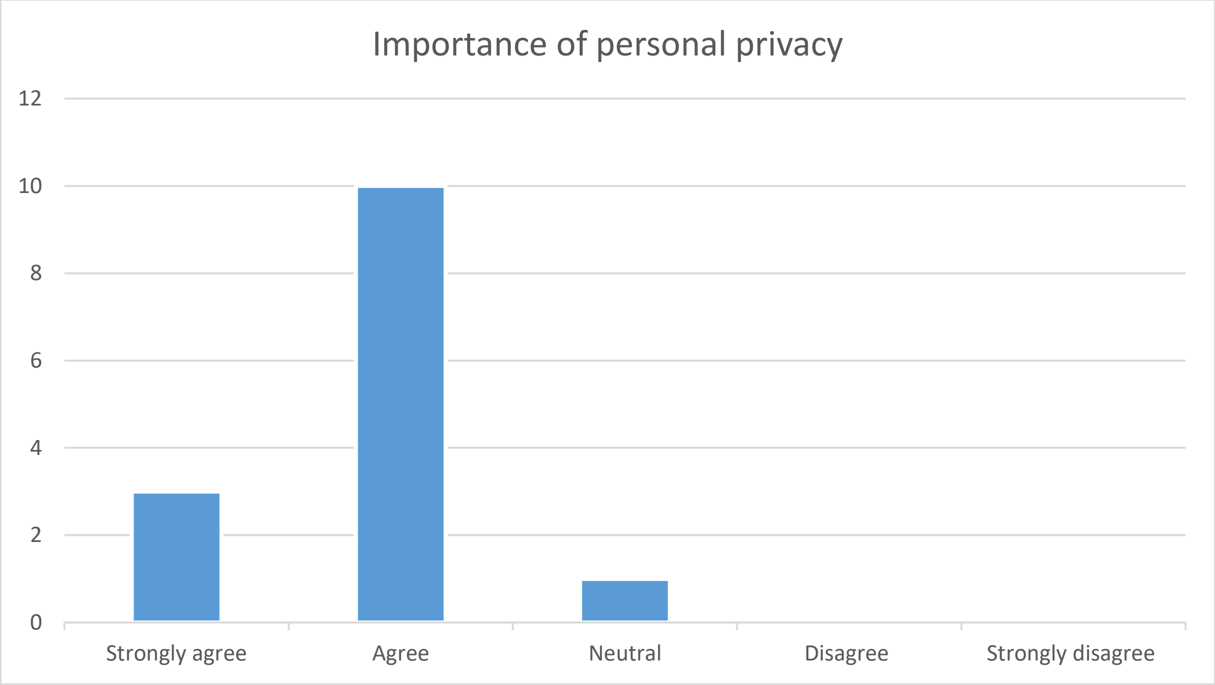


Figure E.461: Importance of personal privacy (Education-UK)

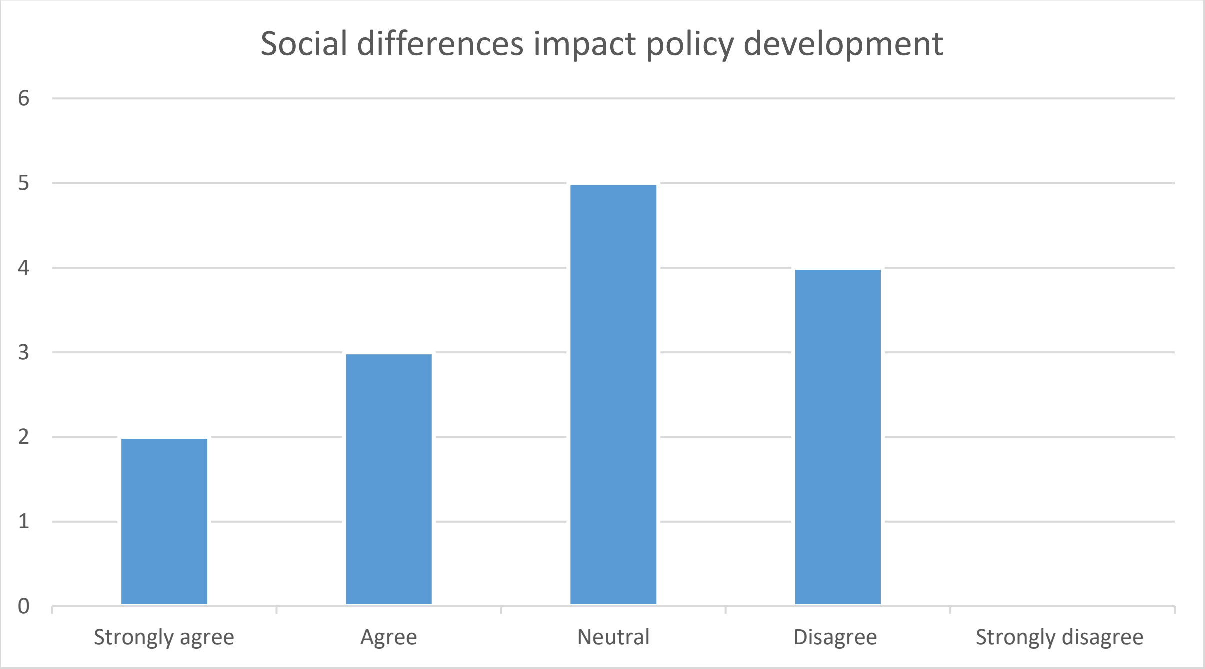


Figure E.462: Social differences impact policy development (Education-UK)

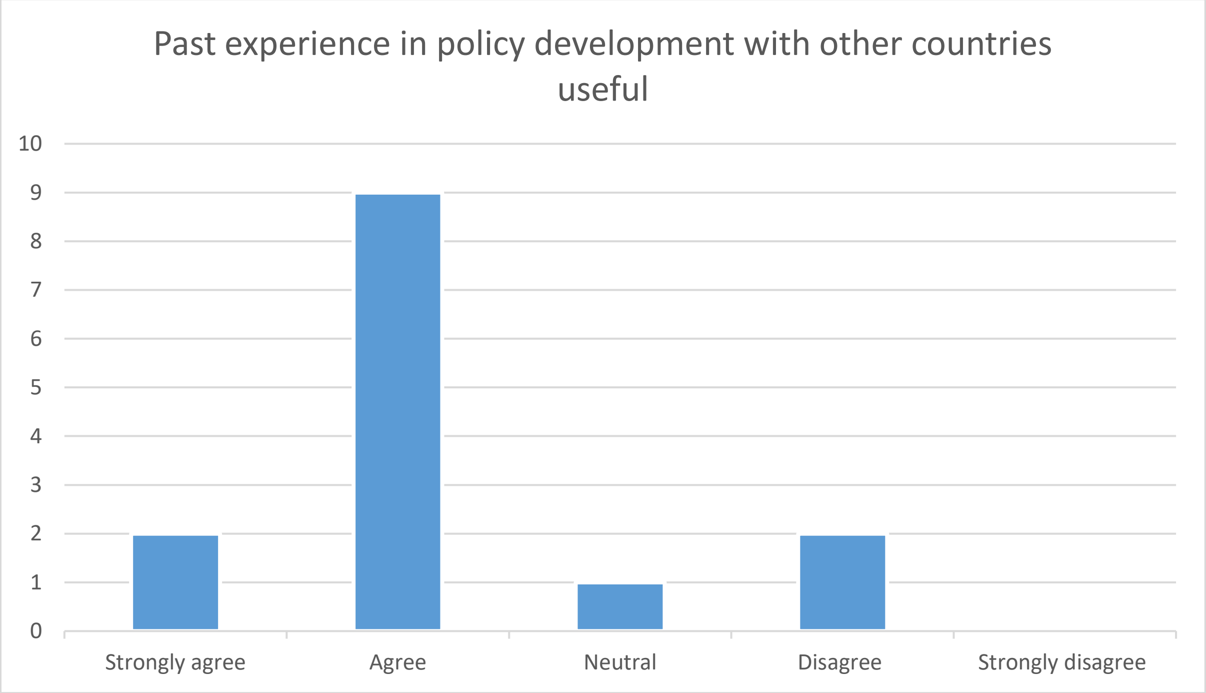


Figure E.463: Past experience in policy development with other countries useful (Education-UK)

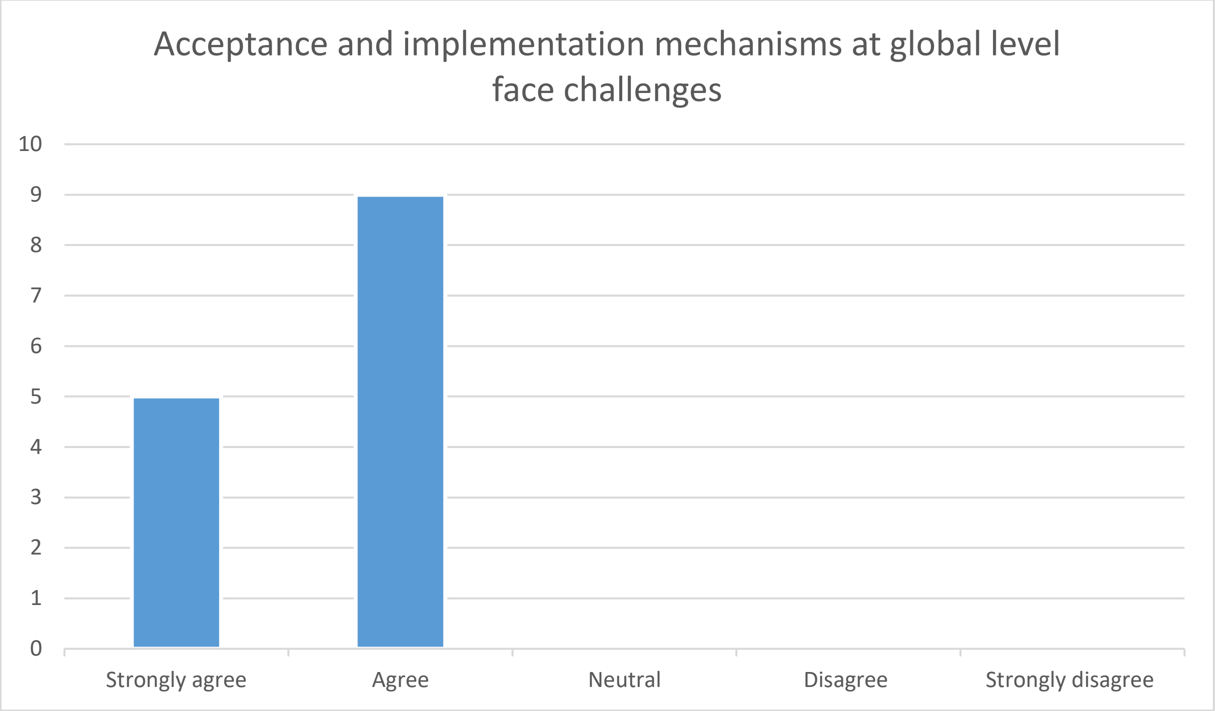


Figure E.464: Acceptance and implementation of mechanisms at global level face challenges (Education-UK)

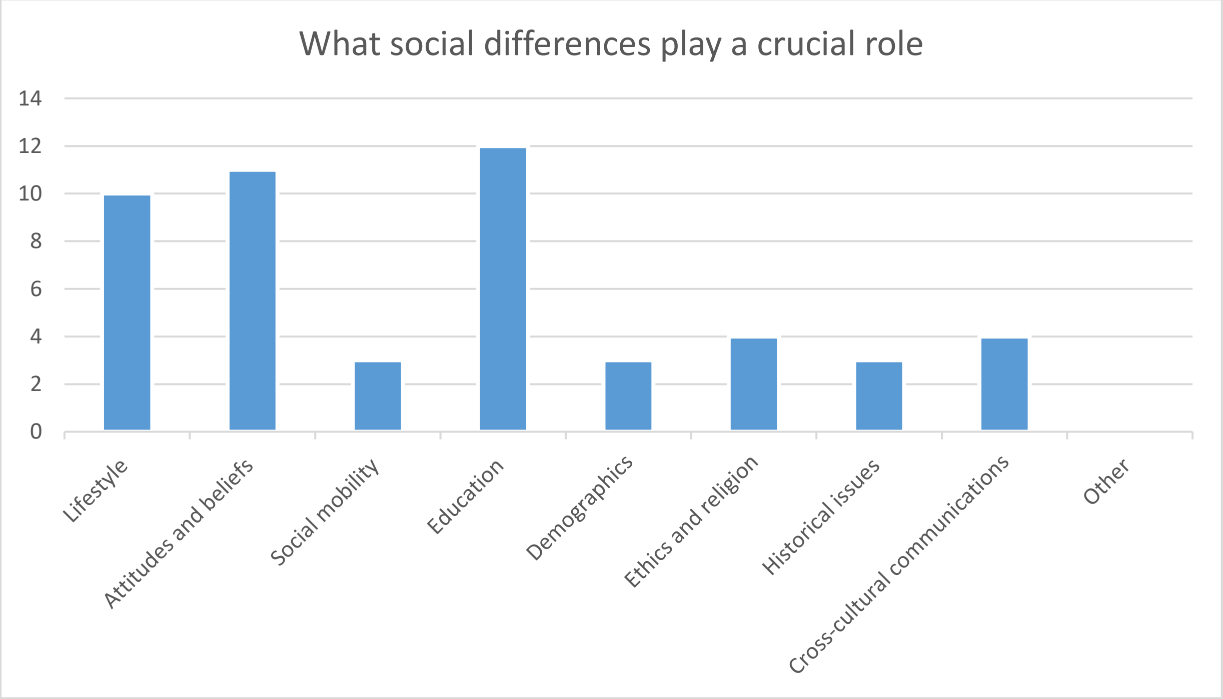


Figure E.465: What social differences play a crucial role (Education-UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education, lifestyle and attitude and beliefs (See figure E.465). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. It becomes clear that educational training can be an effective way to make people understand the importance of privacy and the implications associated with privacy violations. People will have to make a crucial choice in their lifestyles when considering reliance on technology at the workplace. If there is a high reliance on technology in sharing or handling personal information, the demand for accepting and implementing policies associated with data privacy and security also should be high. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

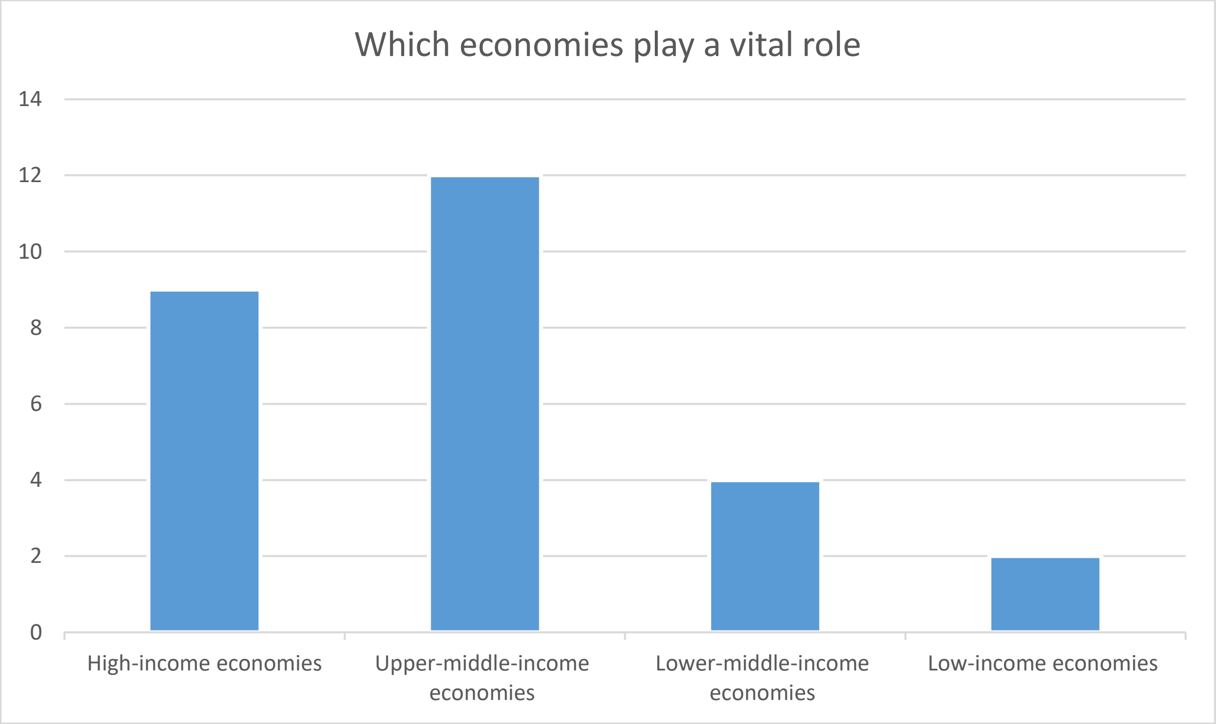


Figure E.466: Which economies play a vital role (Education-UK)

In the questionnaire majority has stated that the high income and upper middle-income countries play a vital role (See figure E. 466). There are key stages in policymaking. This includes, identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, financial stability of a country counts as a crucial factor in policymaking.

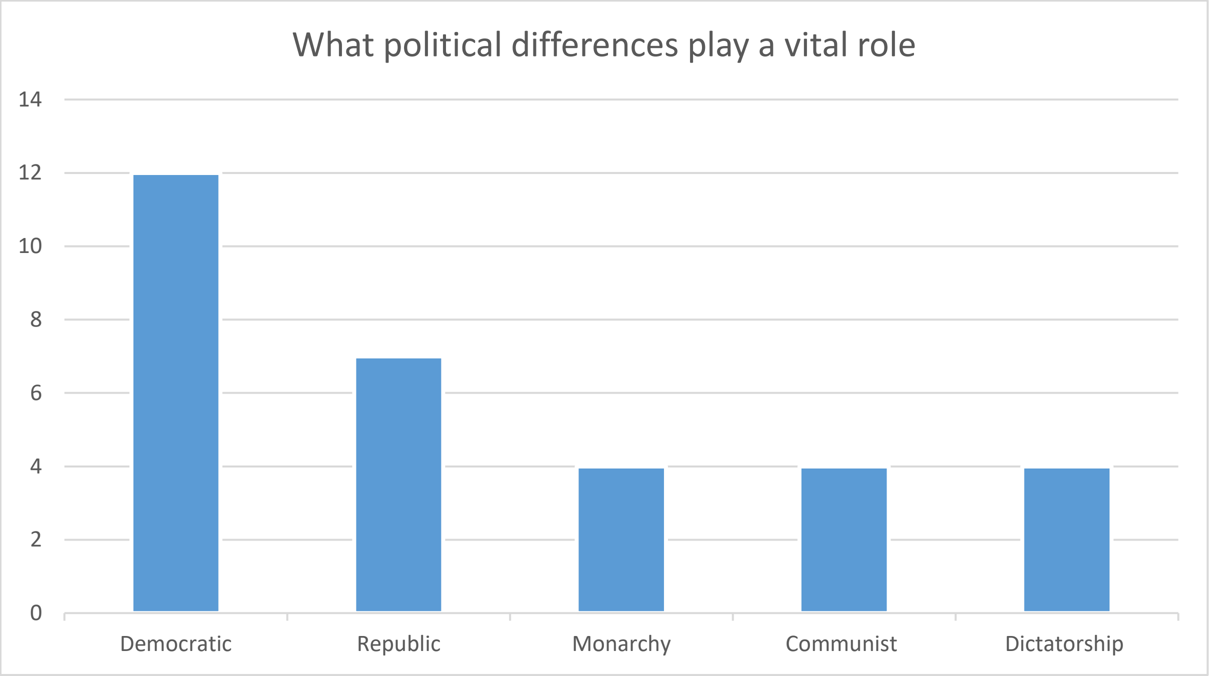


Figure E.467: What political differences play a vital role (Education-UK)

The majority have chosen a democratic political system (See figure E. 467), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

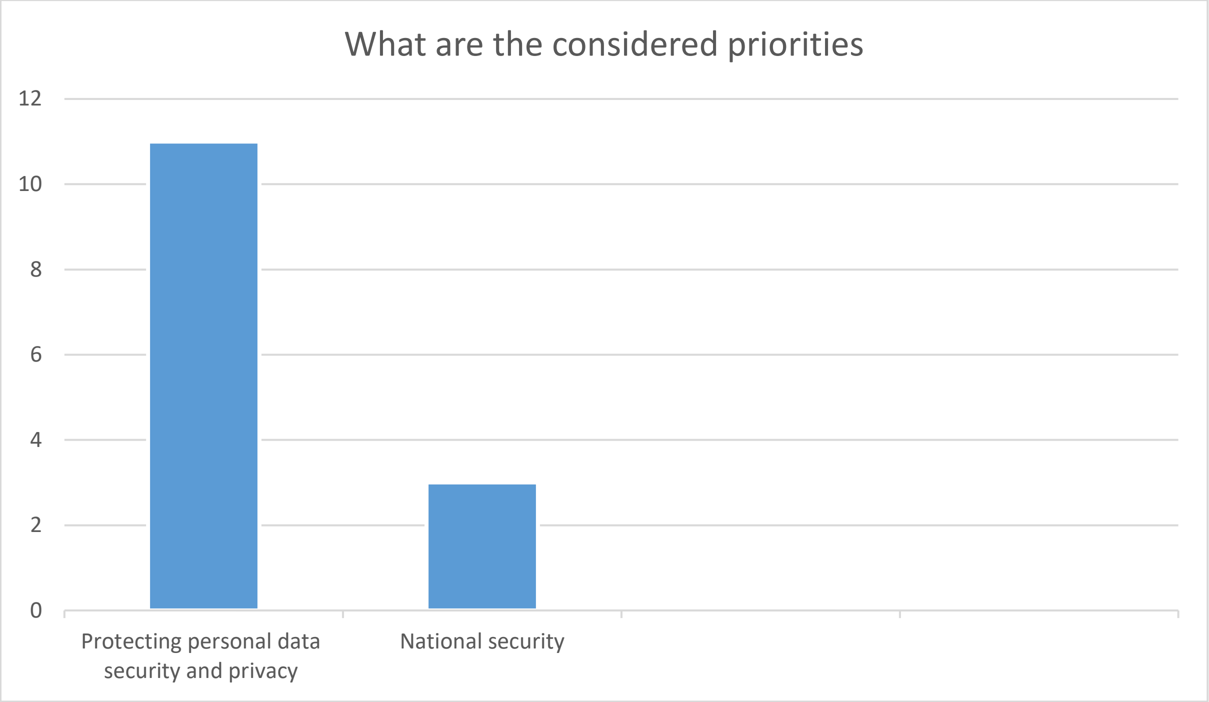


Figure E.468: What are the considered priorities (Education-UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security, which is a significant factor (See figure E. 468). However, in an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

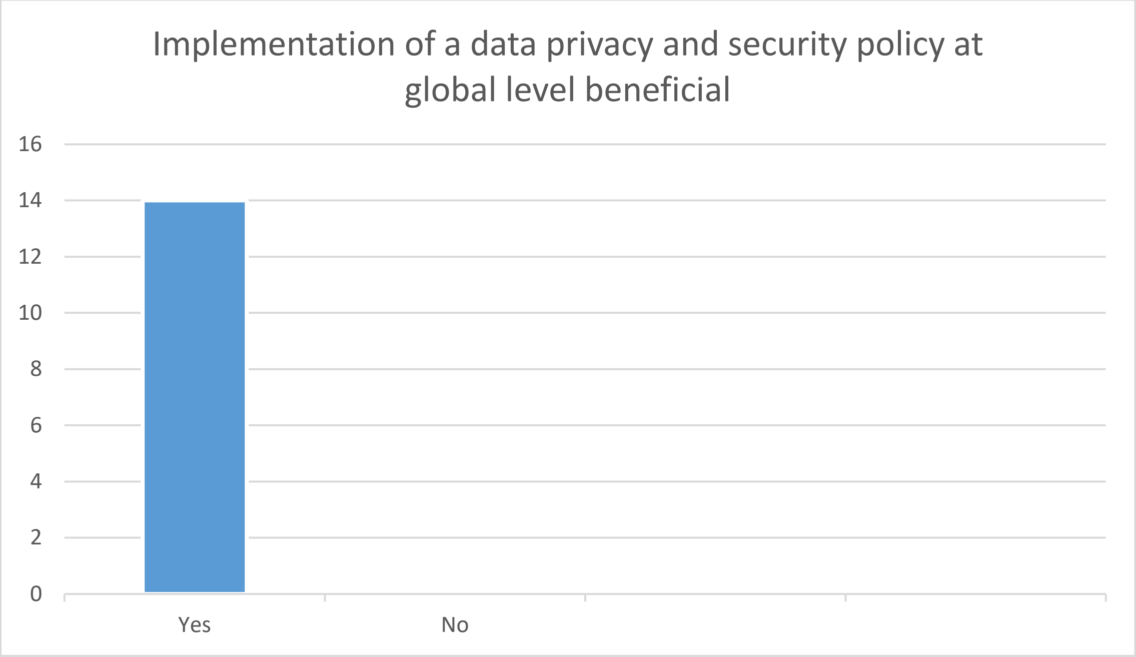


Figure E.469: Implementation of a data privacy and security policy at global level beneficial (Education-UK)

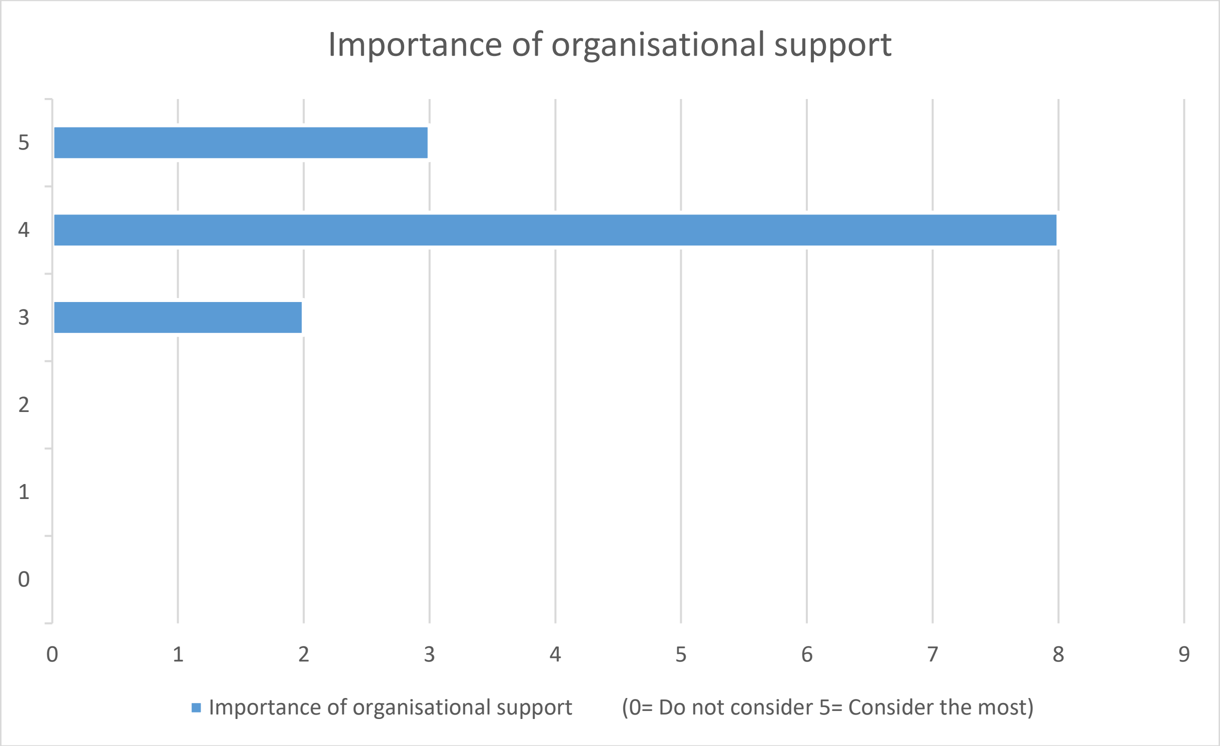


Figure E.470: Importance of organisational support (Education-UK)

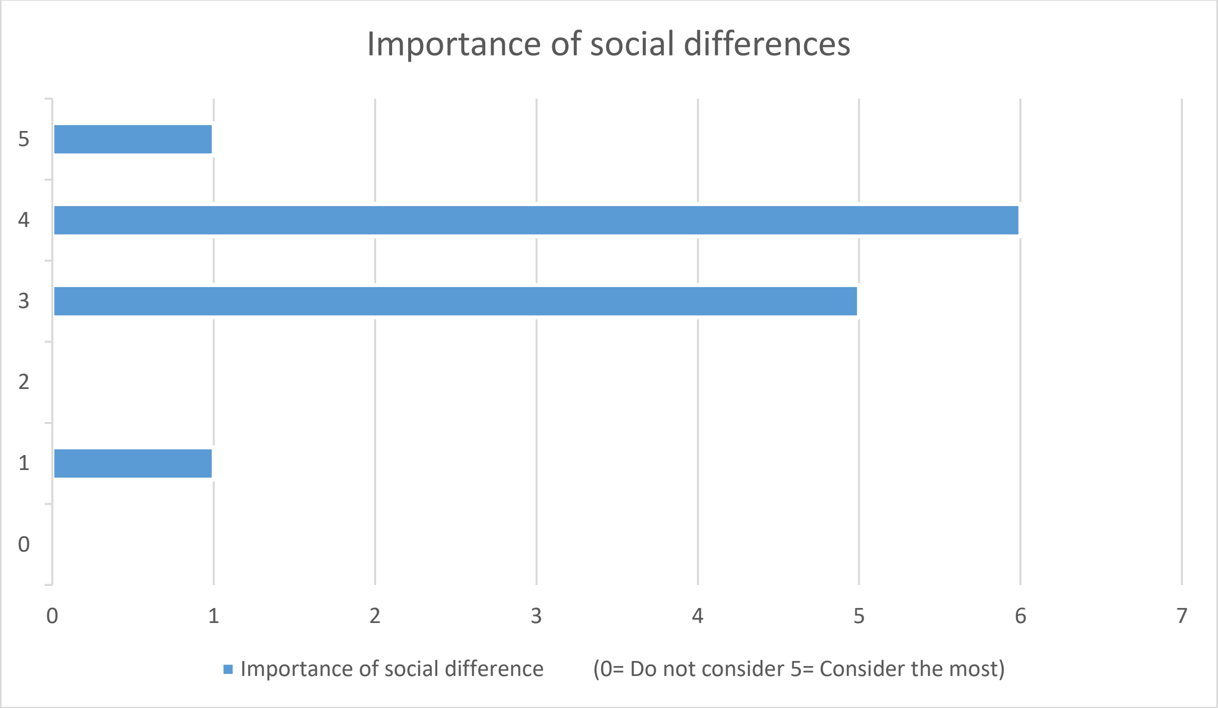


Figure E.471: Importance of social differences (Education-UK)

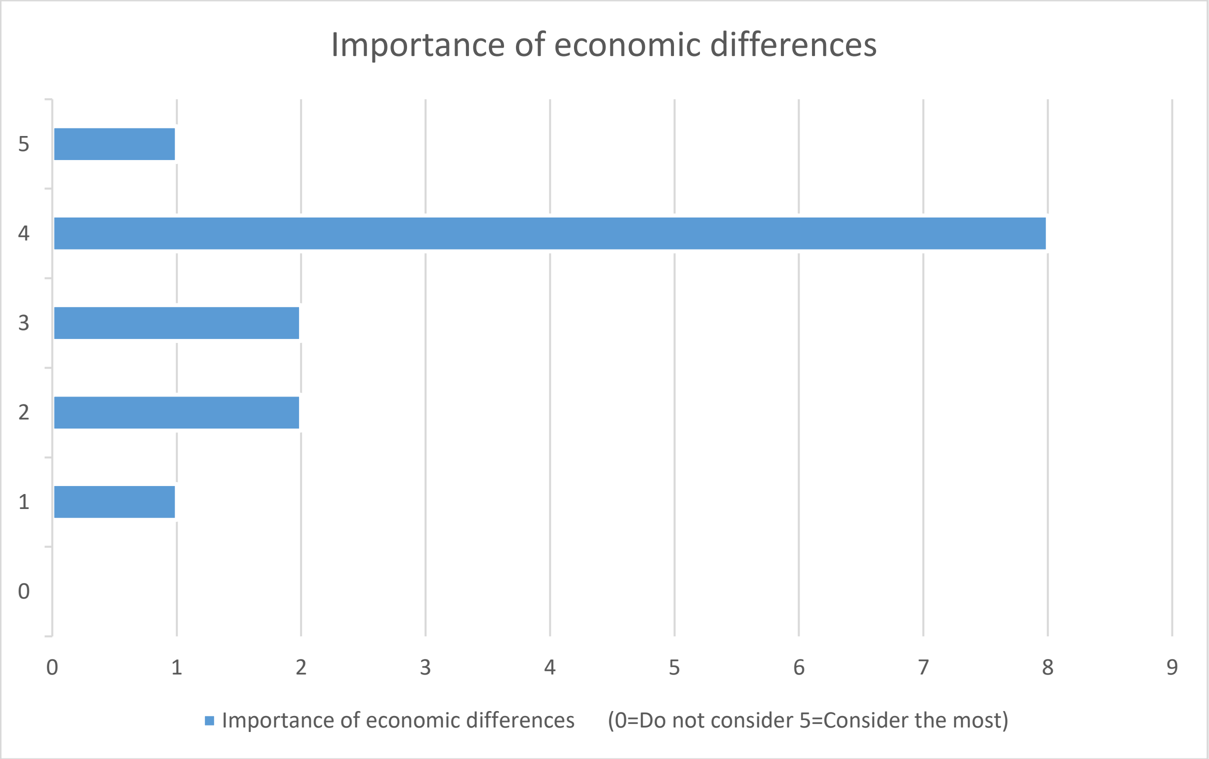


Figure E.472: Importance of economic differences (Education-UK)

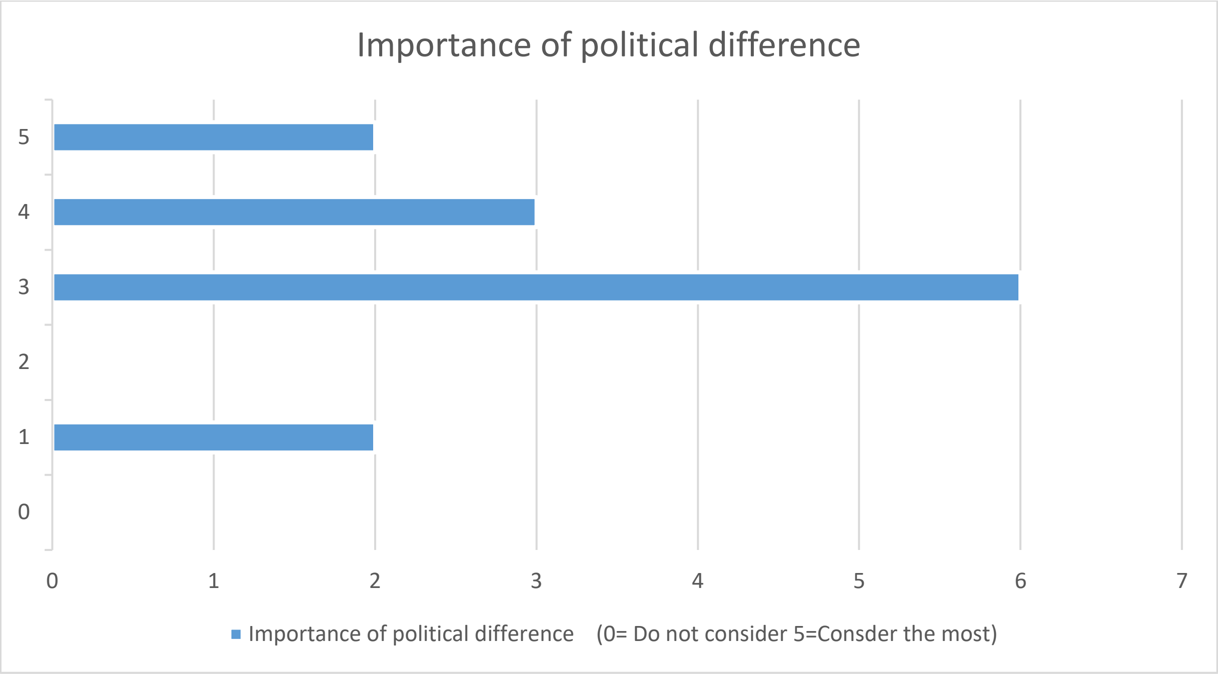


Figure E.473: Importance of political difference (Education-UK)

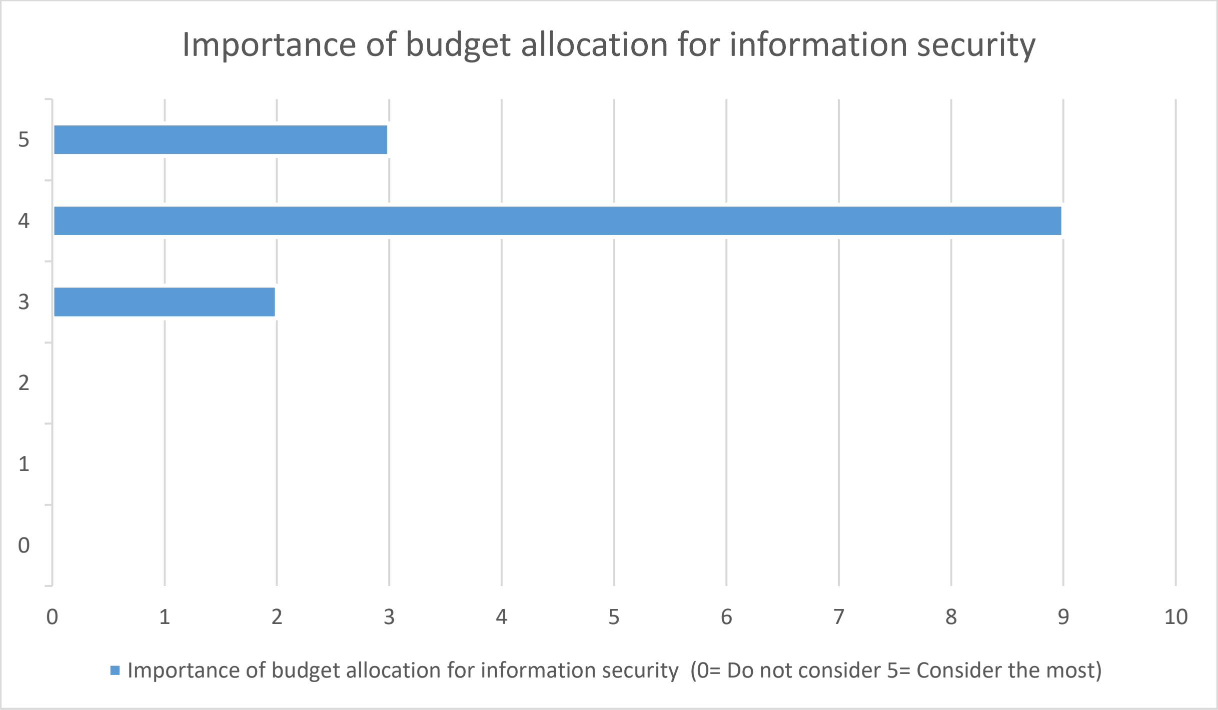


Figure E.474: Importance of budget allocation for information security (Education-UK)

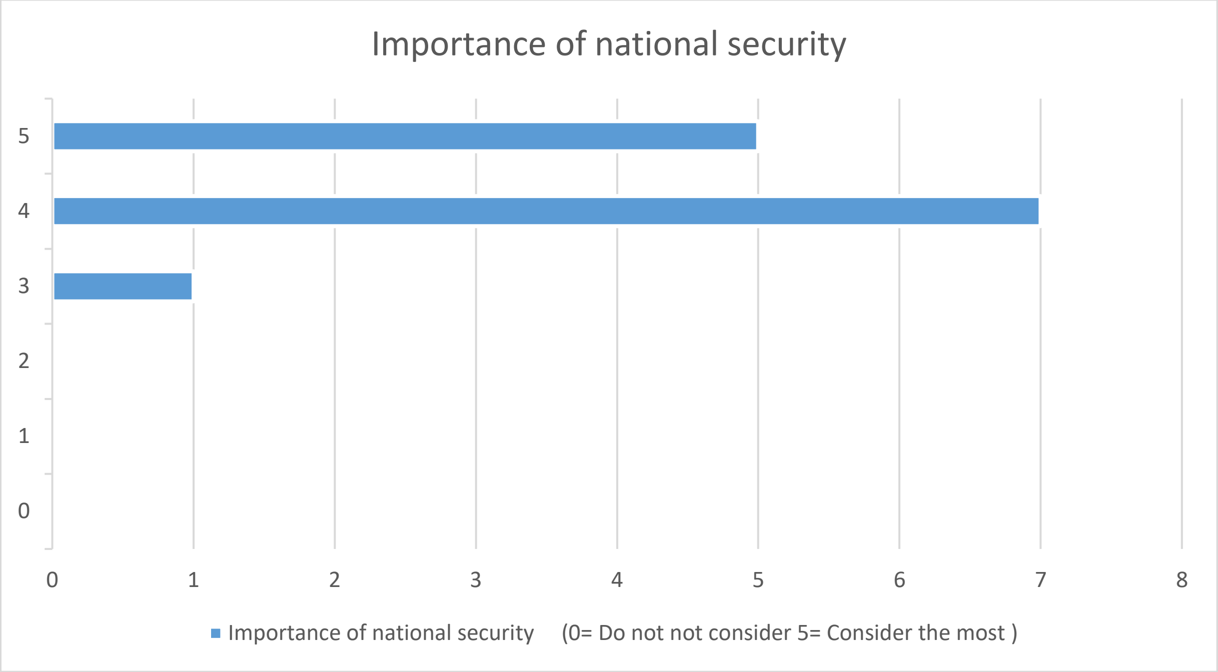


Figure E.475: Importance of national security (Education-UK)

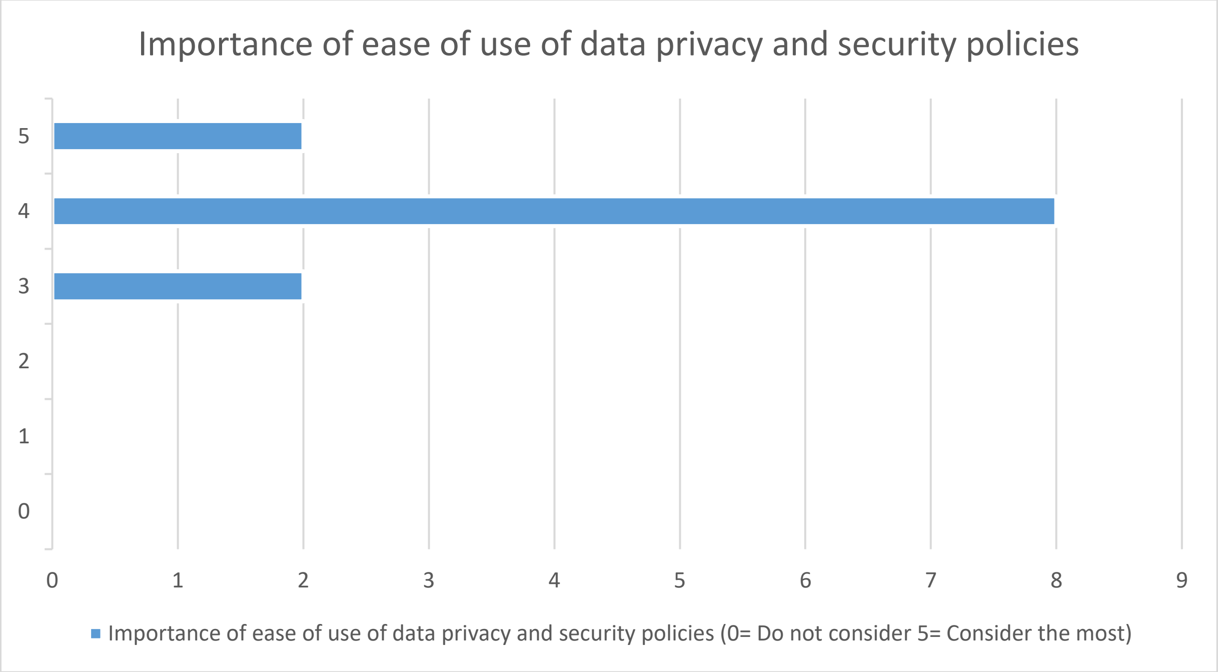


Figure E.476: Importance of ease of use of data privacy and security policies (Education-UK)

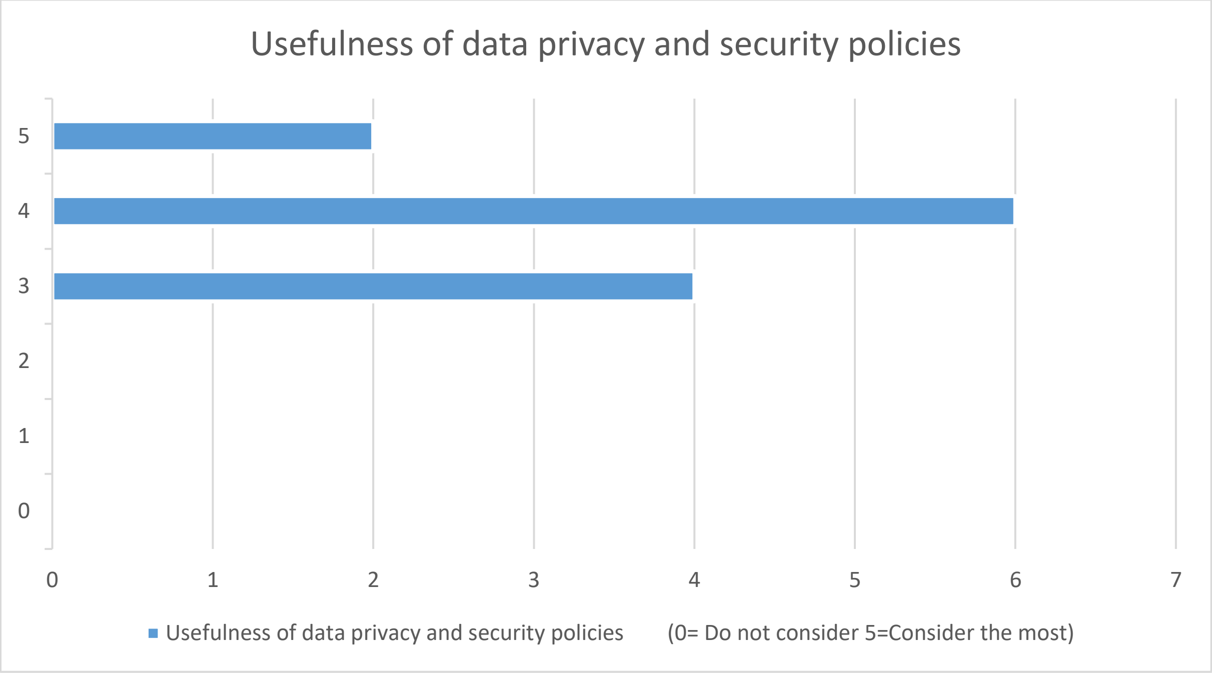


Figure E.477: Usefulness of data privacy and security policies (Education-UK)

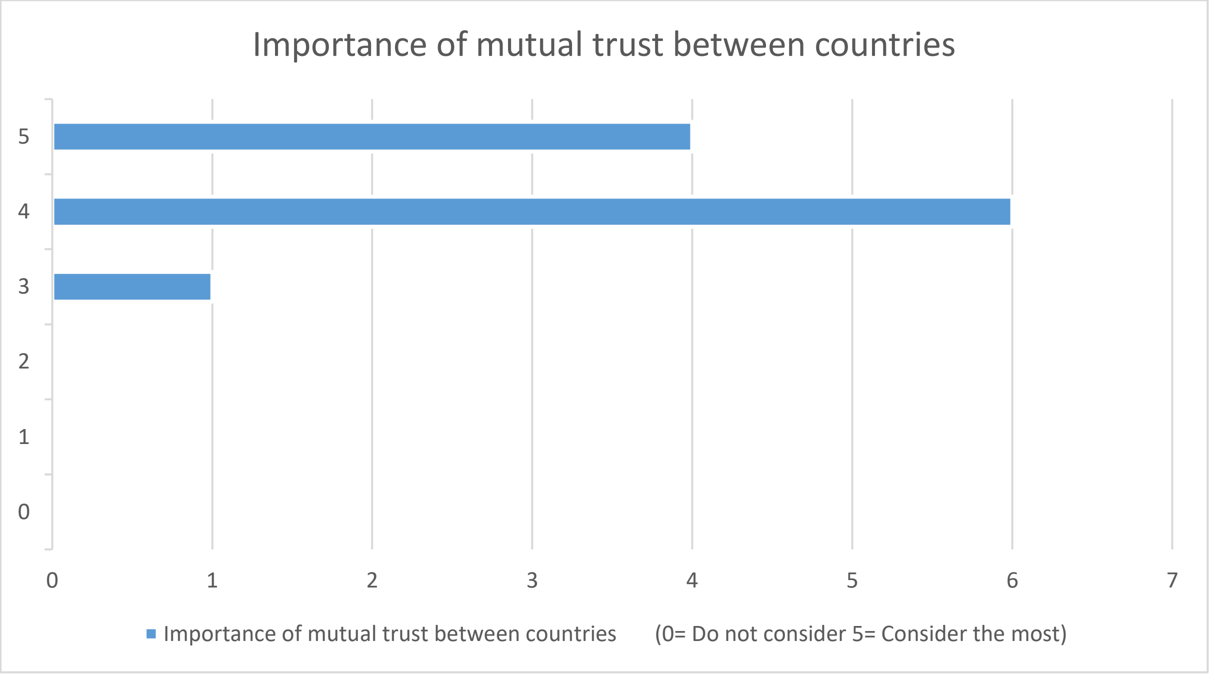


Figure E.478: Importance of mutual trust between countries (Education-UK)

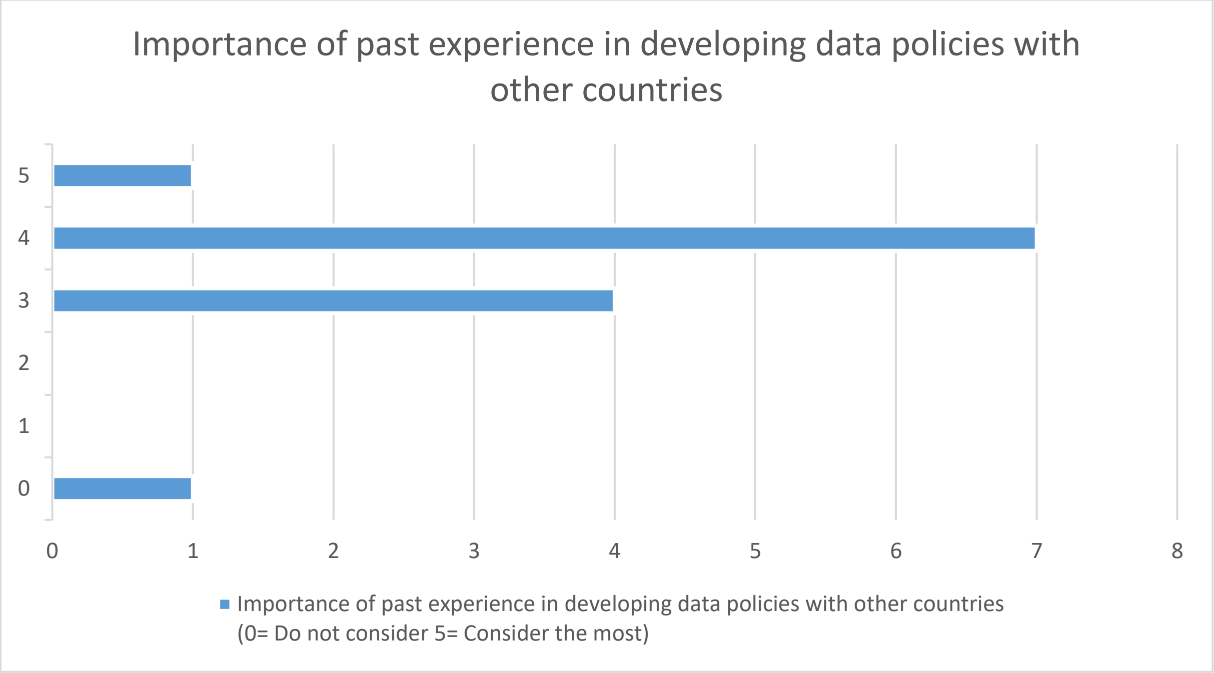


Figure E.479: Importance of past experience in developing data policies with other counties (Education-UK)

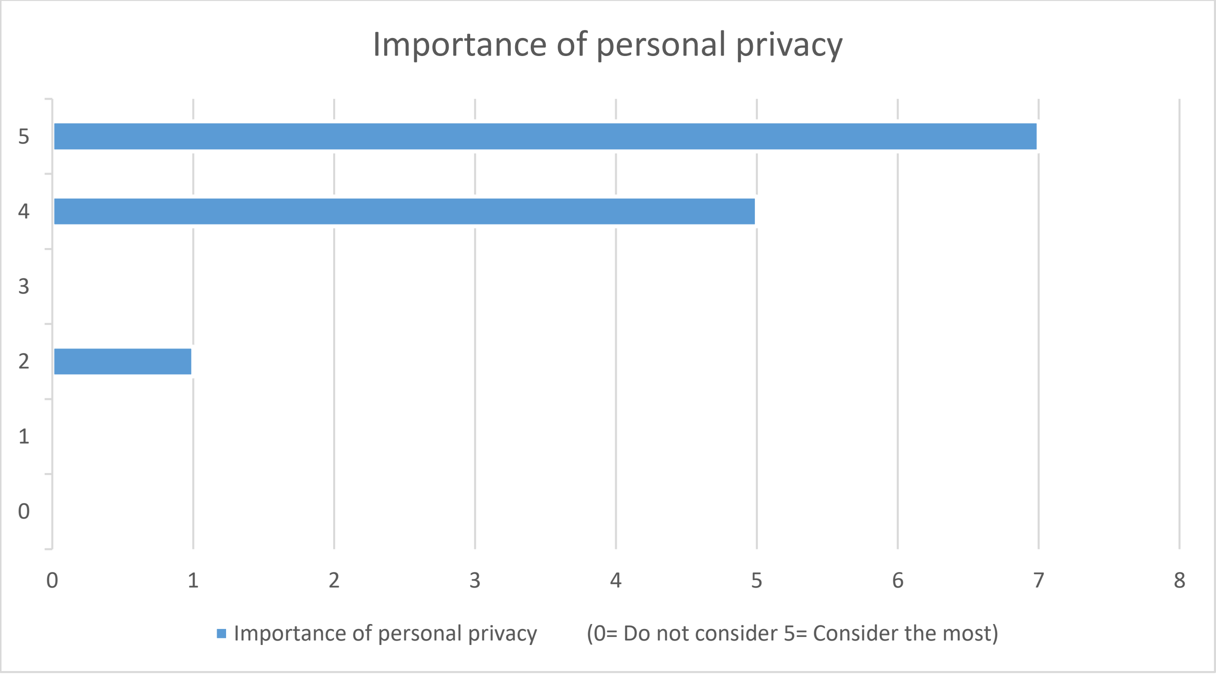


Figure E.480: Importance of personal privacy (Education-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 93 percent of the respondents have endorsed (See figure E. 469). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, political differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure E. 458-468) (See figure E. 470-480).

United Kingdom – Healthcare

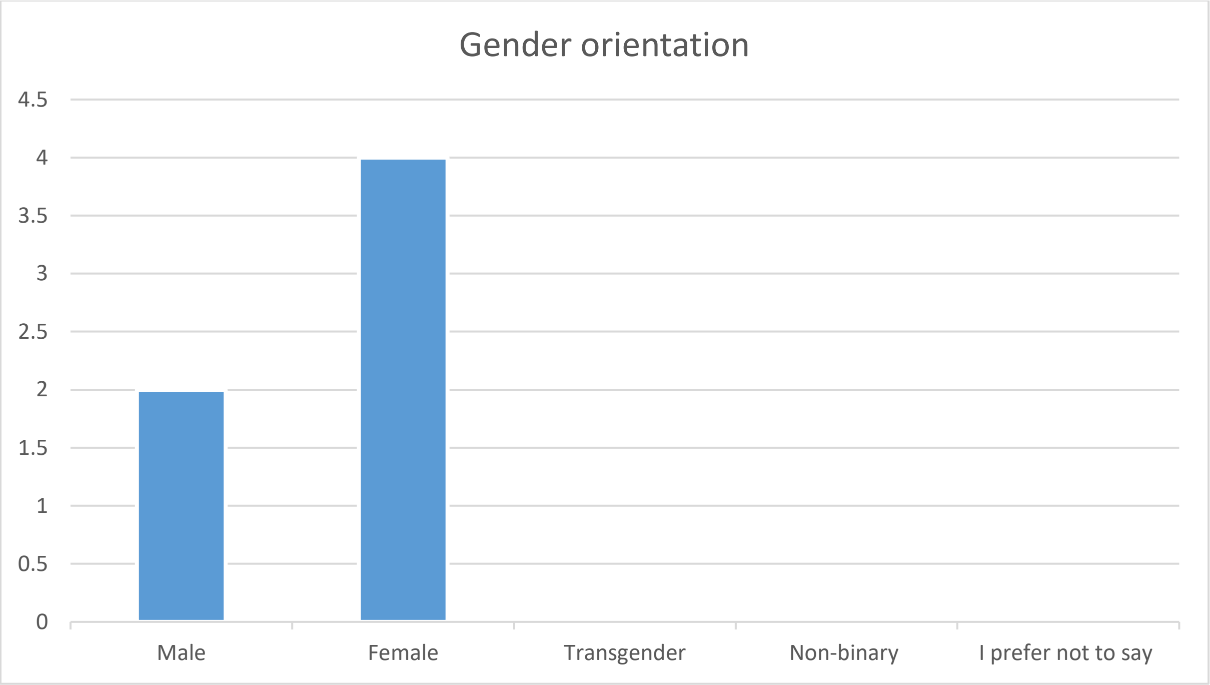


Figure E.481: Gender orientation (Healthcare-UK)

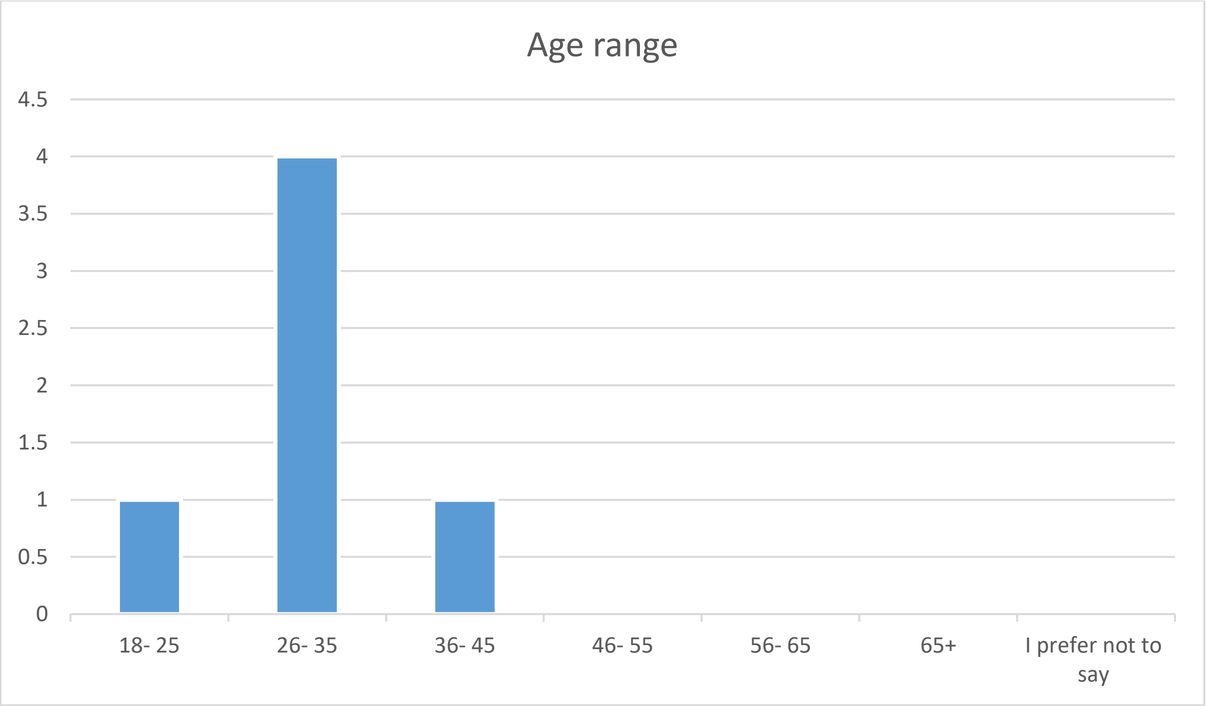


Figure E.482: Age range (Healthcare-UK)

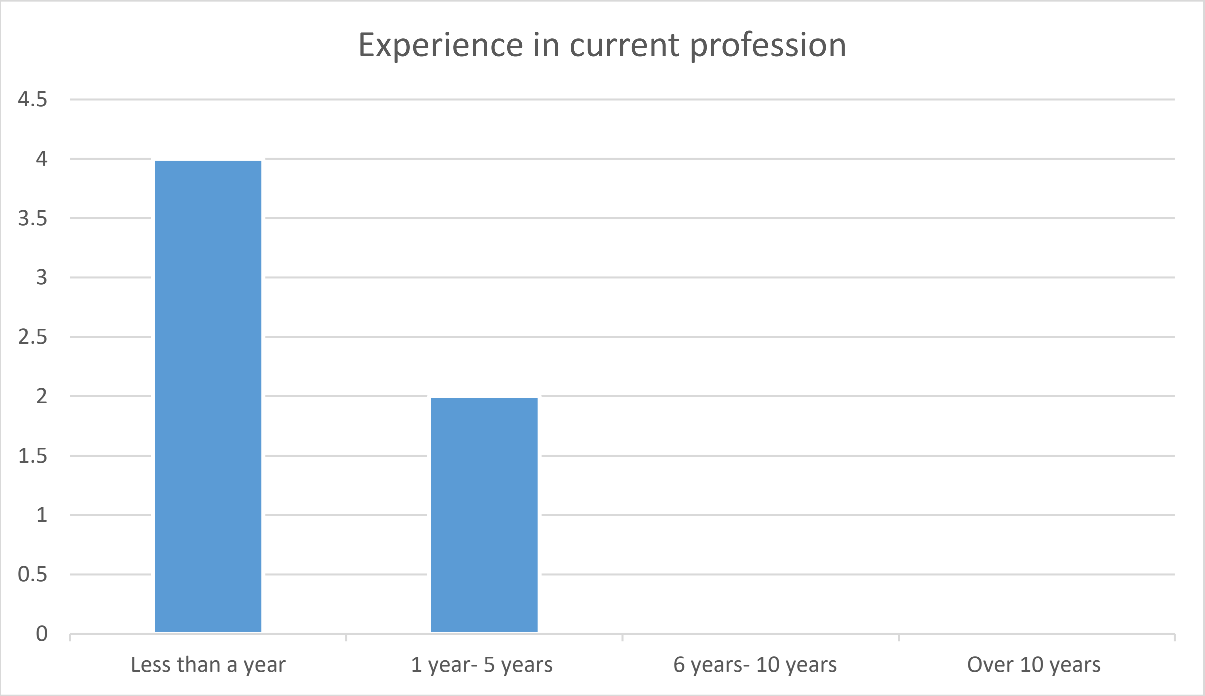


Figure E.483: Experience in current profession (Healthcare-UK)

This analysis is based on the responses received from United Kingdom participants employed in the healthcare sector. There were 6 participants and 2 out of them were males and 4 females (See figure E. 481). They were within the 18-45 age range out of which 1 in the 18-25, 4 in the 26-35, and 1 in the 36-45 range (See figure E. 482). The participants employed in industry between less than a year and 5 years (See figure E. 483).

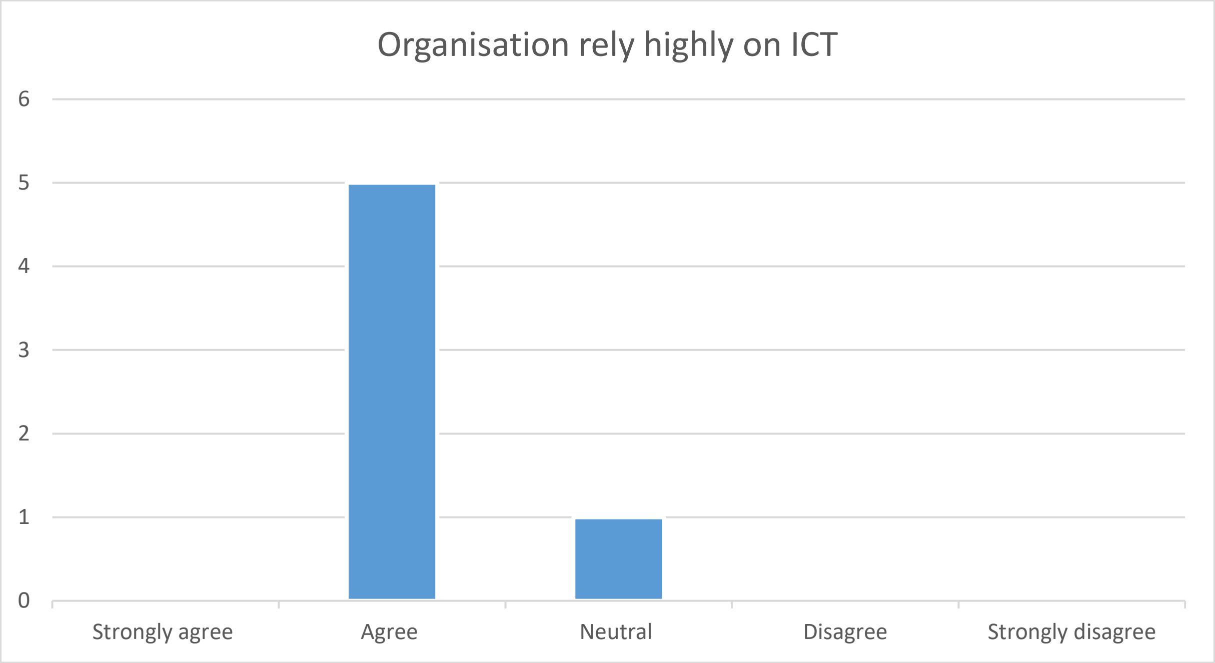


Figure E.484: Organisation rely highly on ICT (Healthcare-UK)

Out of the 6 respondents, 5 have worked in a technology reliance working environment, and 1 unaware of reliance on technology because of the nature of the work assigned to them (See figure E. 484). This indicates a majority of those who have been working in healthcare sector have had high reliance on ICT.

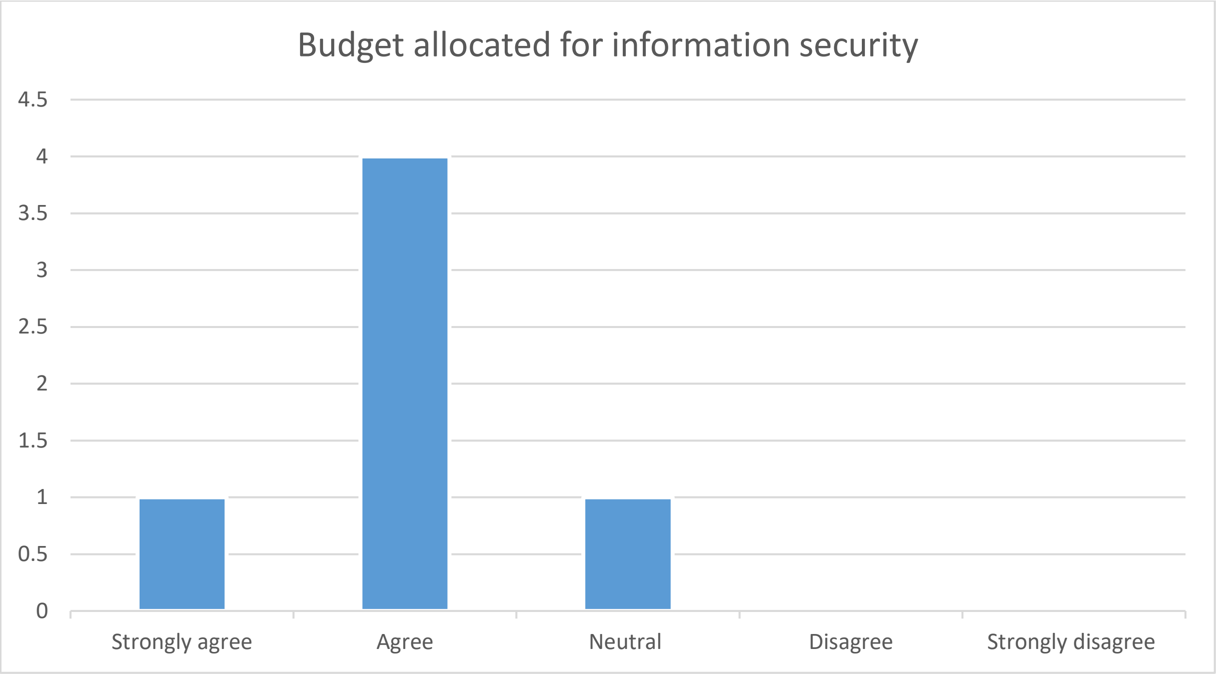


Figure E.485: Budget allocated for information security (Healthcare-UK)

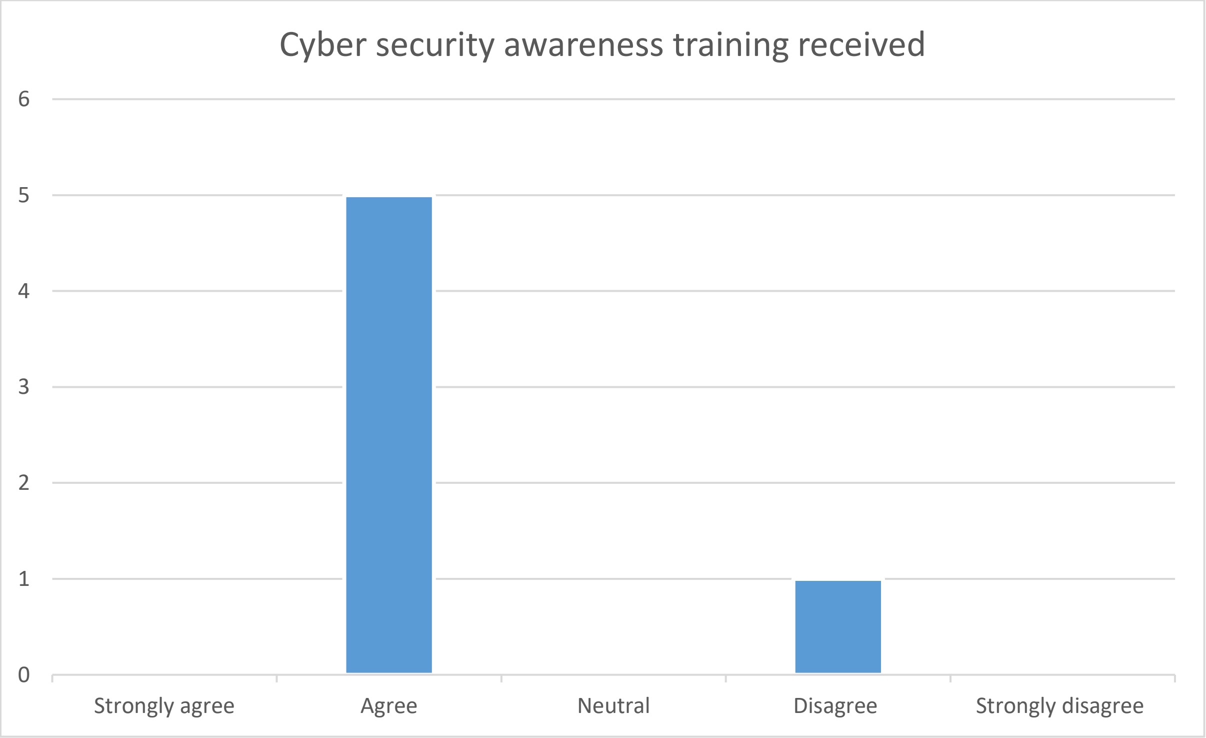


Figure E.486: Cyber security awareness training received (Healthcare-UK)

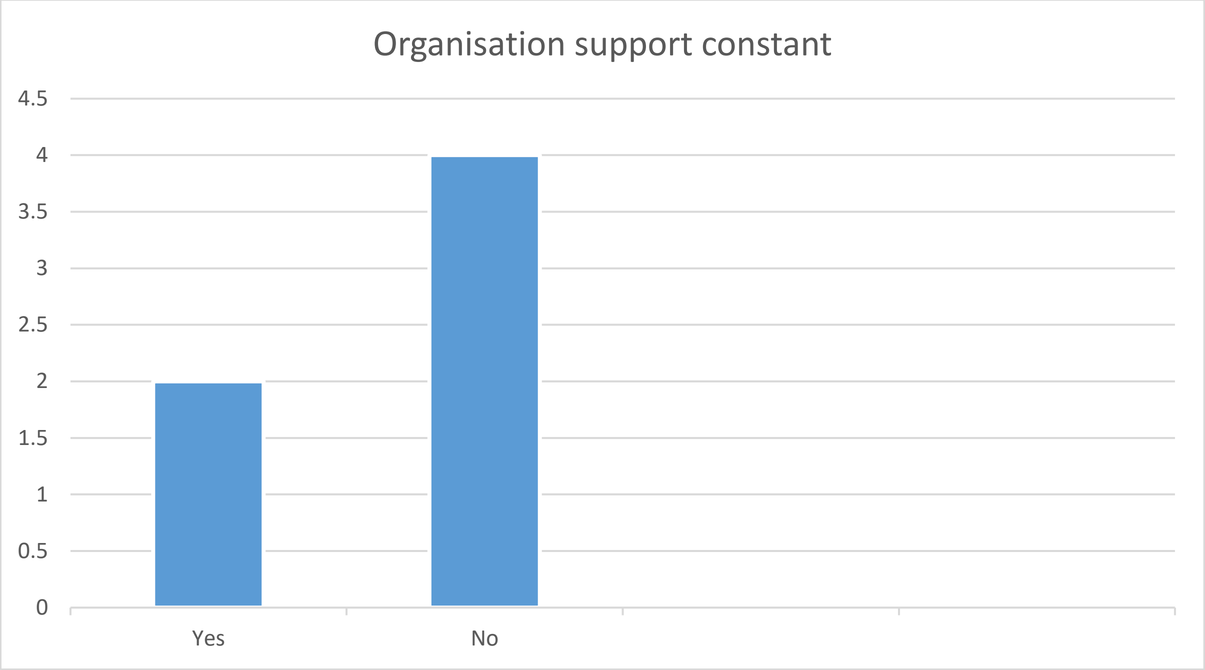


Figure E.487: Organisation support constant (Healthcare-UK)

Funding has been sketchy. 5 out of the 6 have indicated that their organisations had an allocated budget for information security, whilst 1 had not expressed an opinion either way (See figure E. 485). According to some of the participants, regular security awareness training received was adequate despite the satisfactory level of resources allocated for information security. 5 participants have received regular cybersecurity awareness training, whilst 1 participant had not regularly received security awareness training (See figure E. 486). However, 4 participants had not received support from the organisation to protect personal information, whilst only 2 did (See figure E. 487). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

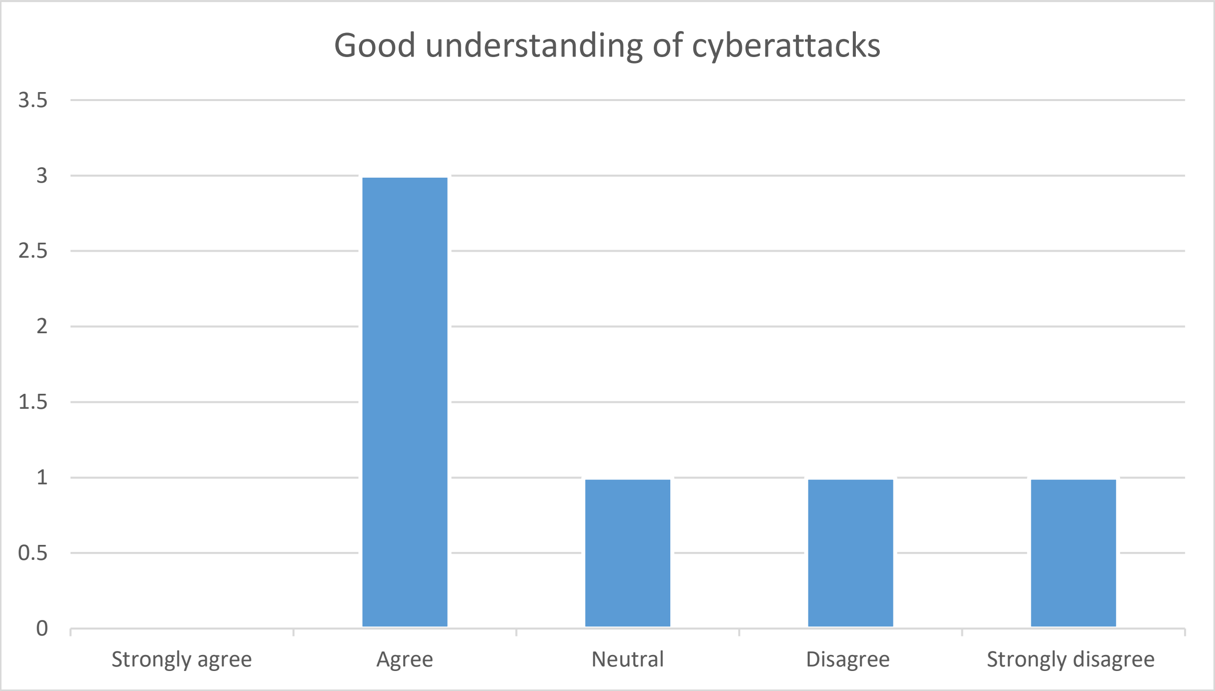


Figure E.488: Good understanding of cyberattacks (Healthcare-UK)

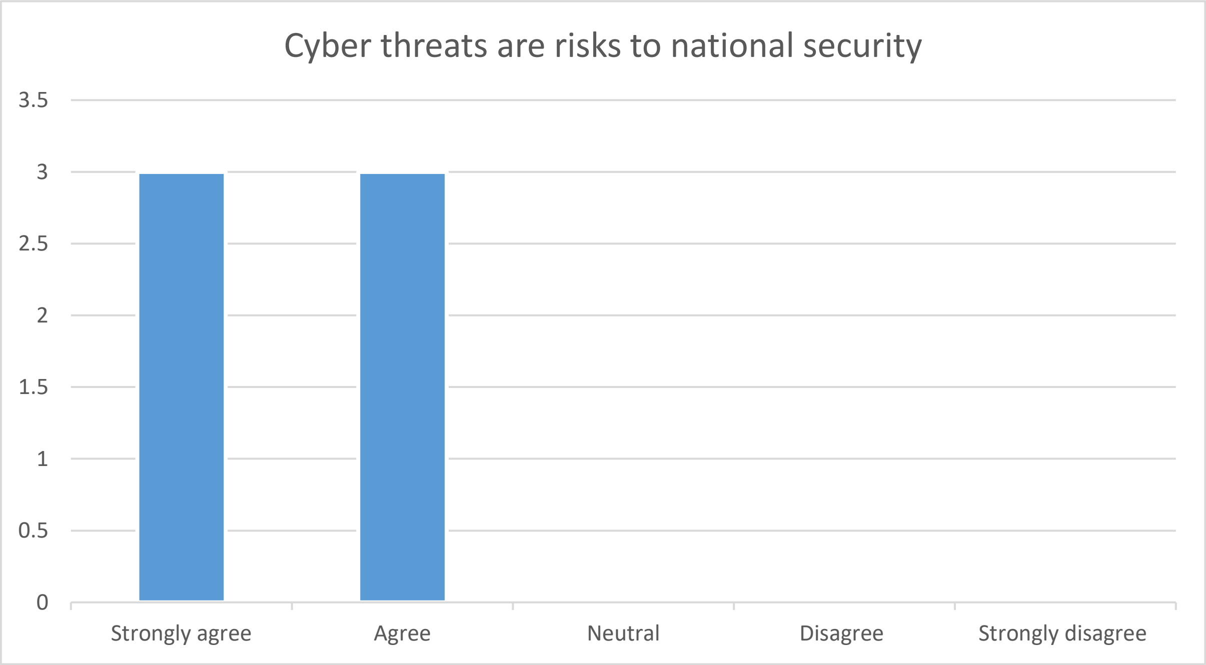


Figure E.489: Cyber threats are risks to national security (Healthcare-UK)

Despite the security awareness training, the participants appear to have a satisfactory level of understanding of the impact of cyber-attacks on the public and the organisation. 3 participants do have, 1 have not expressed opinion either way, and 2 participants had no understanding (See figure E. 488). Furthermore, 100 percent of the participants realise the potential threats to national security from cyber-attacks (See figure E. 489). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

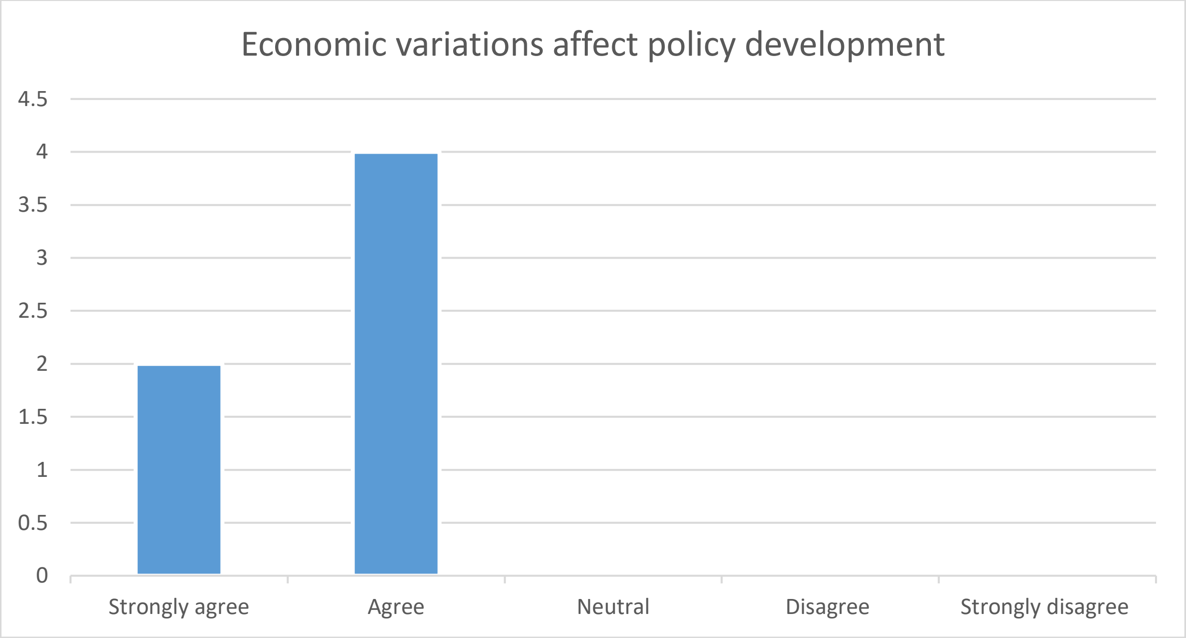


Figure E.490: Economic variations affect policy development (Healthcare-UK)

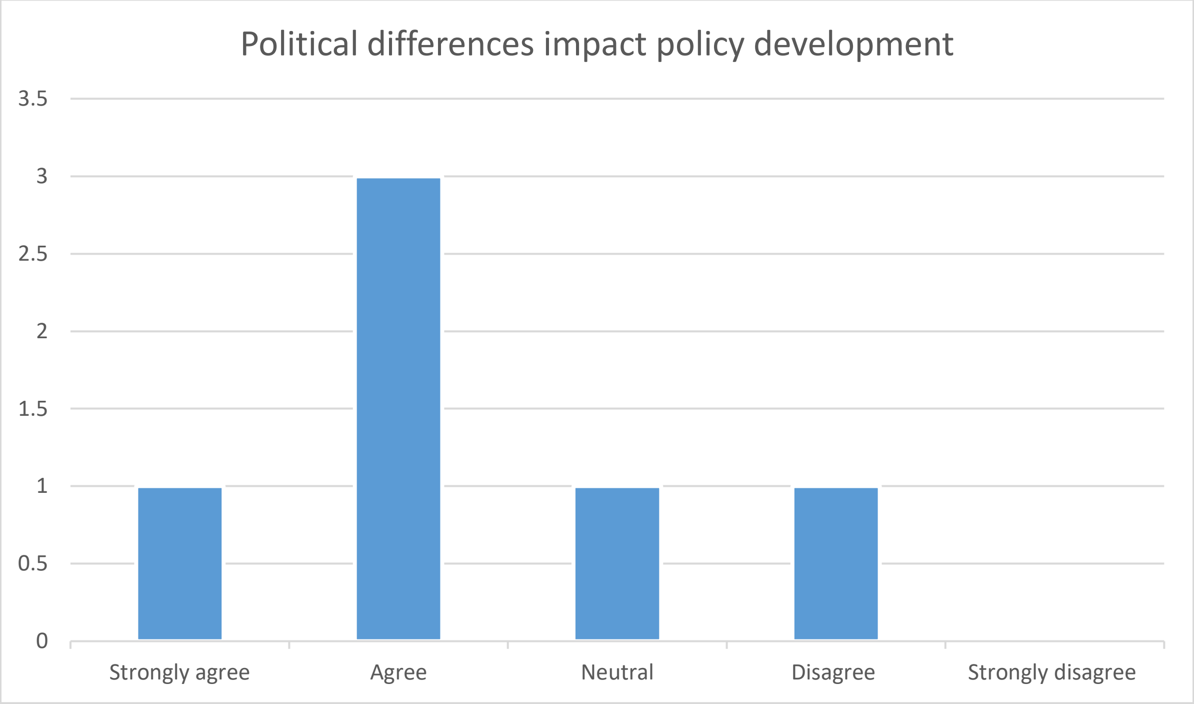


Figure E.491: Political differences impact policy development (Healthcare-UK)

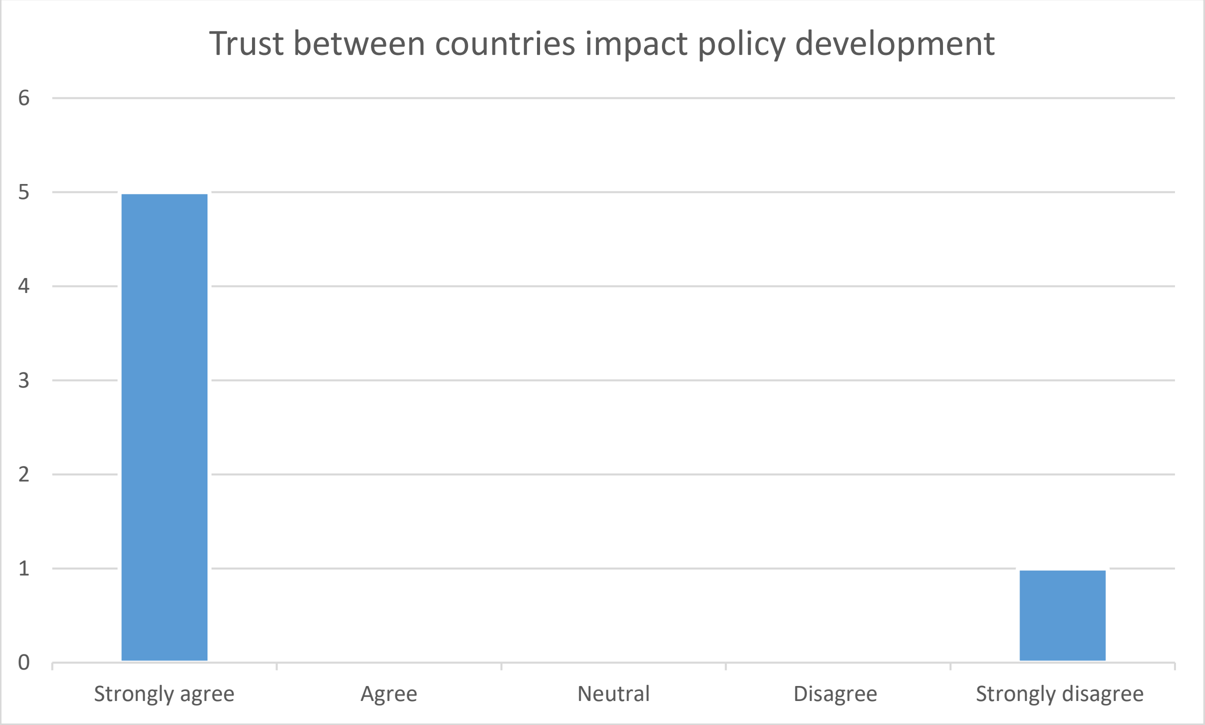


Figure E.492: Trust between countries impact policy development (Healthcare-UK)

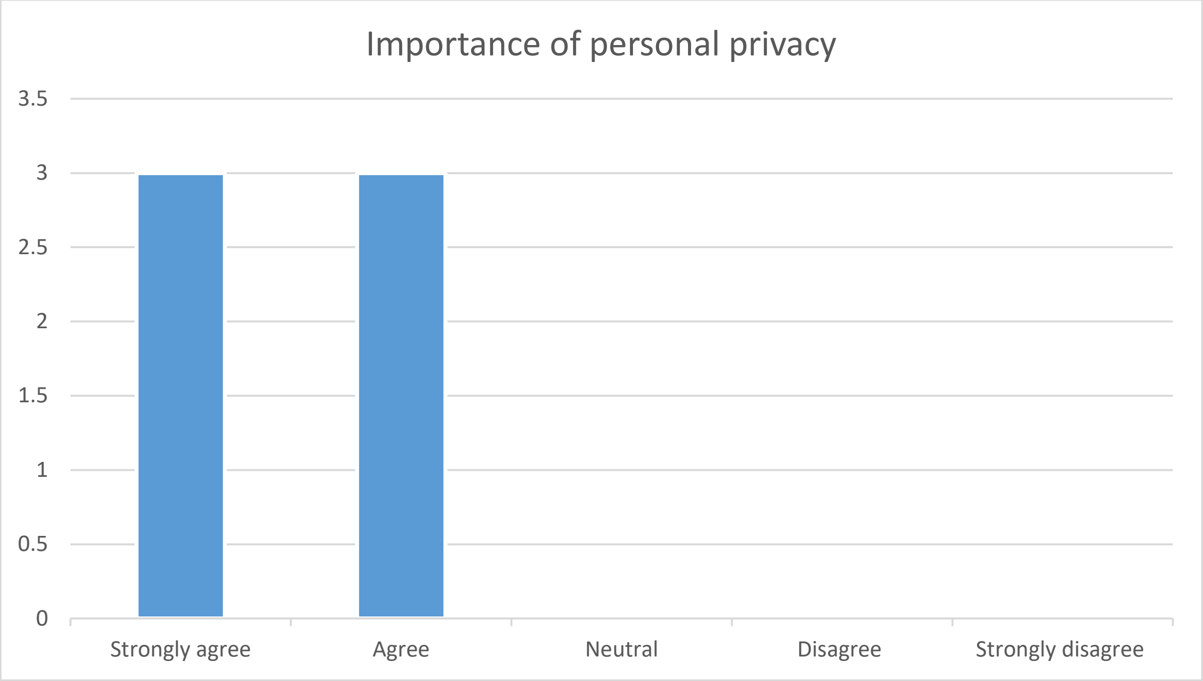


Figure E.493: Importance of personal privacy (Healthcare-UK)

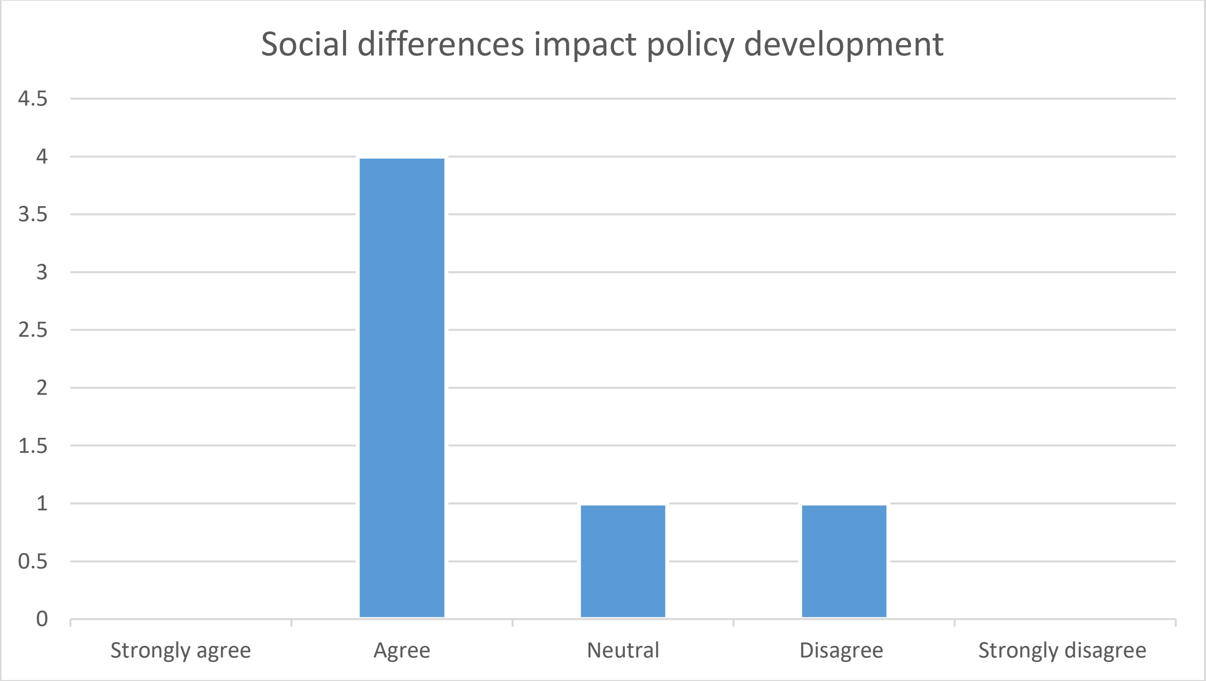


Figure E.494: Social differences impact policy development (Healthcare-UK)

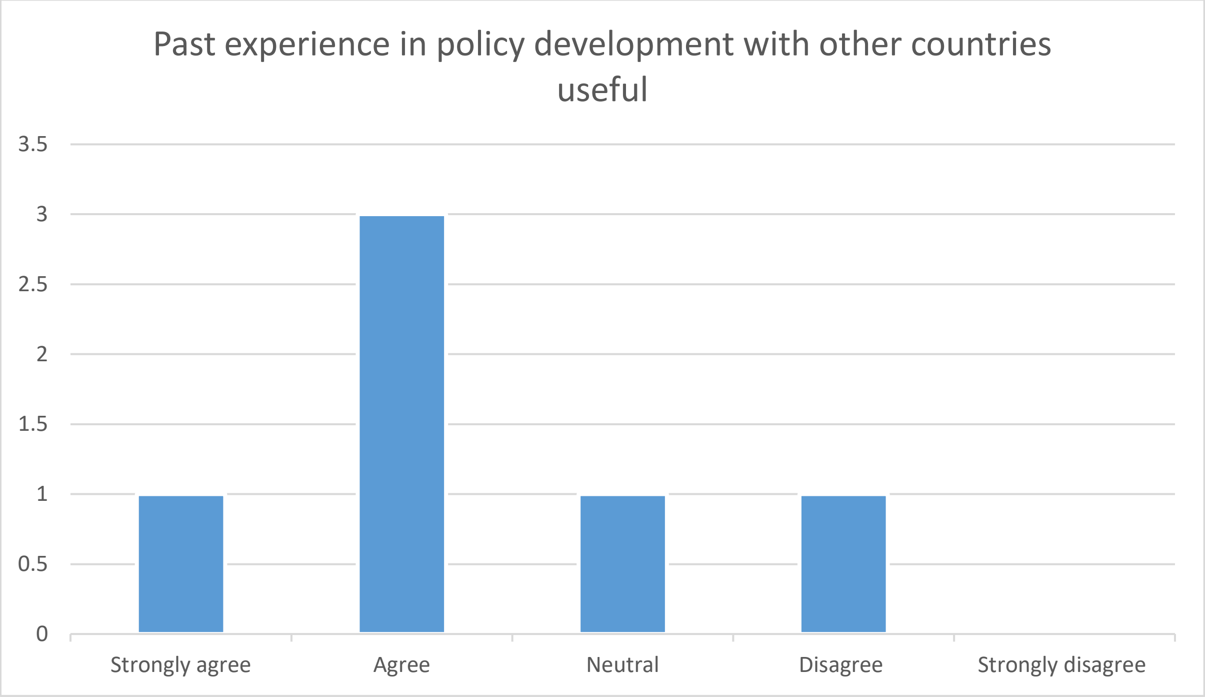


Figure E.495: Past experience in policy development with other countries useful (Healthcare-UK)

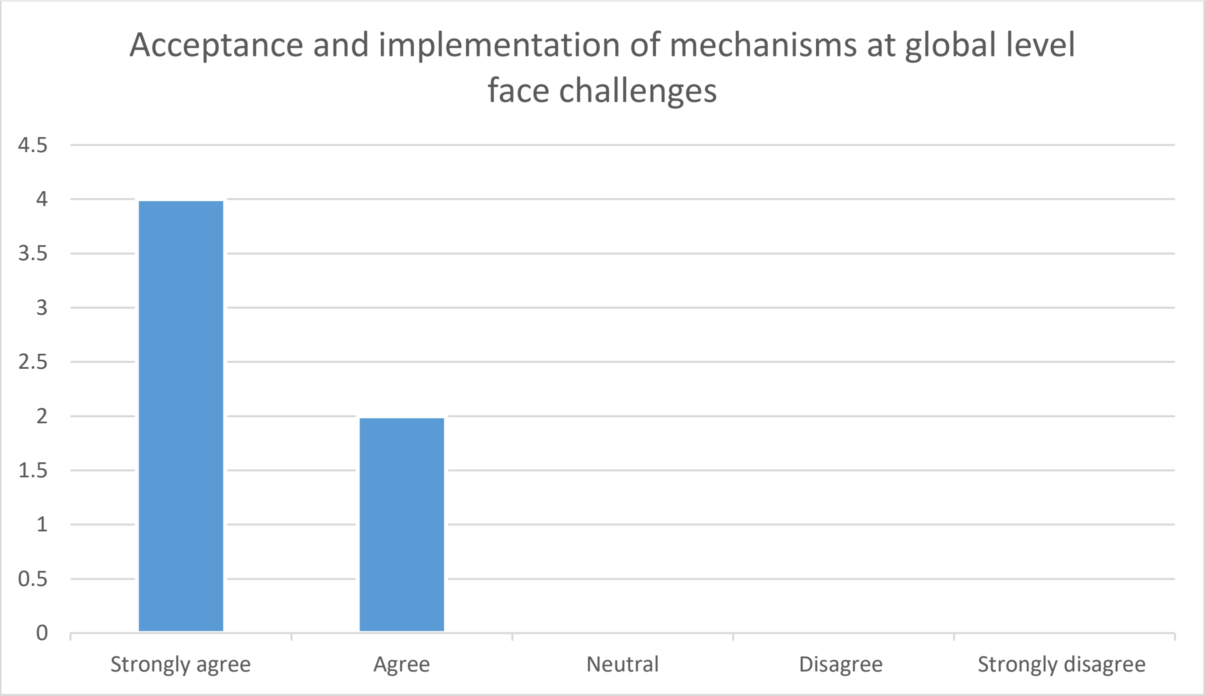


Figure E.496: Acceptance and implementation of mechanisms at global level face challenges (Healthcare-UK)

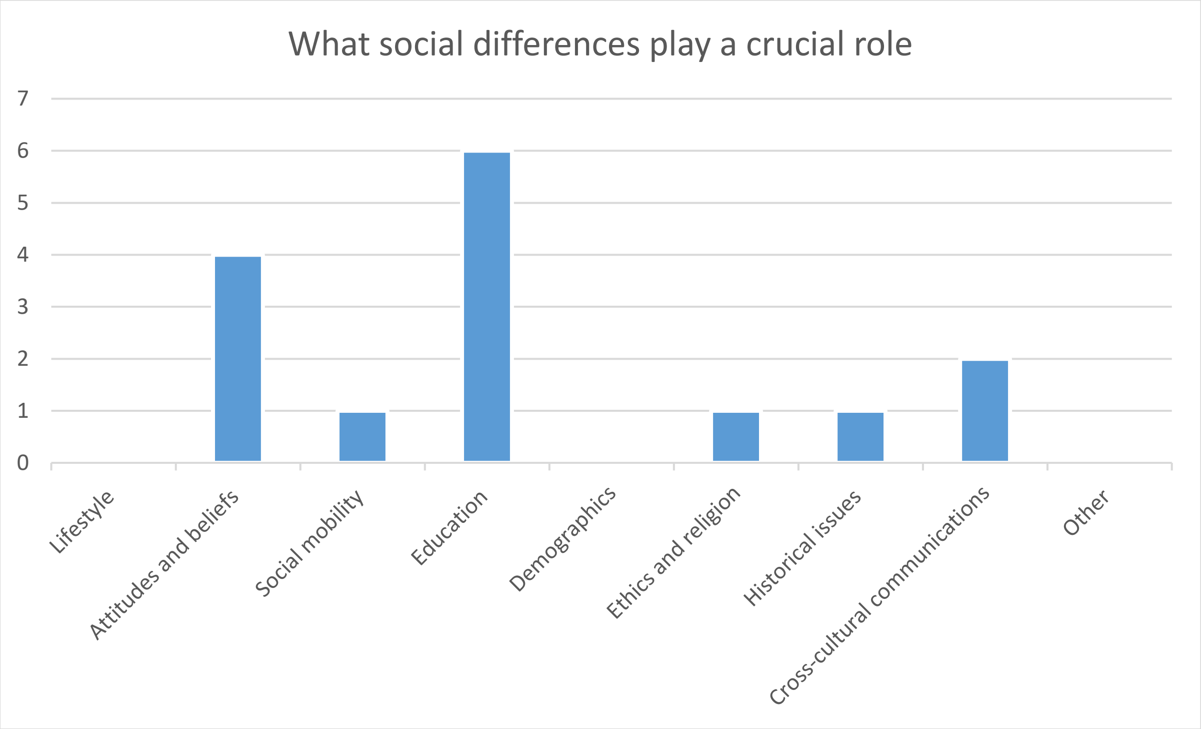


Figure E.497: What social differences play a crucial role (Healthcare-UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education and attitude and beliefs (See figure E. 497). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

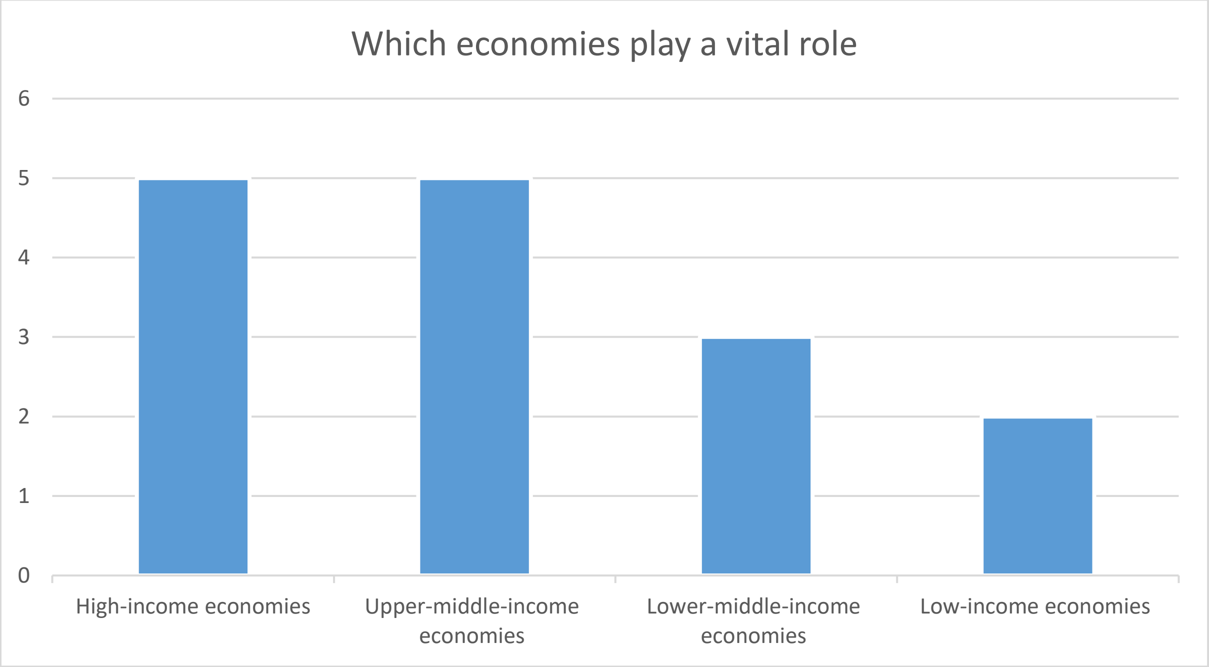


Figure E.498: Which economies play a vital role (Healthcare-UK)

In the questionnaire, majority has stated that the high income, upper-middle-income countries and lower middle income play a vital role (See figure E. 498). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

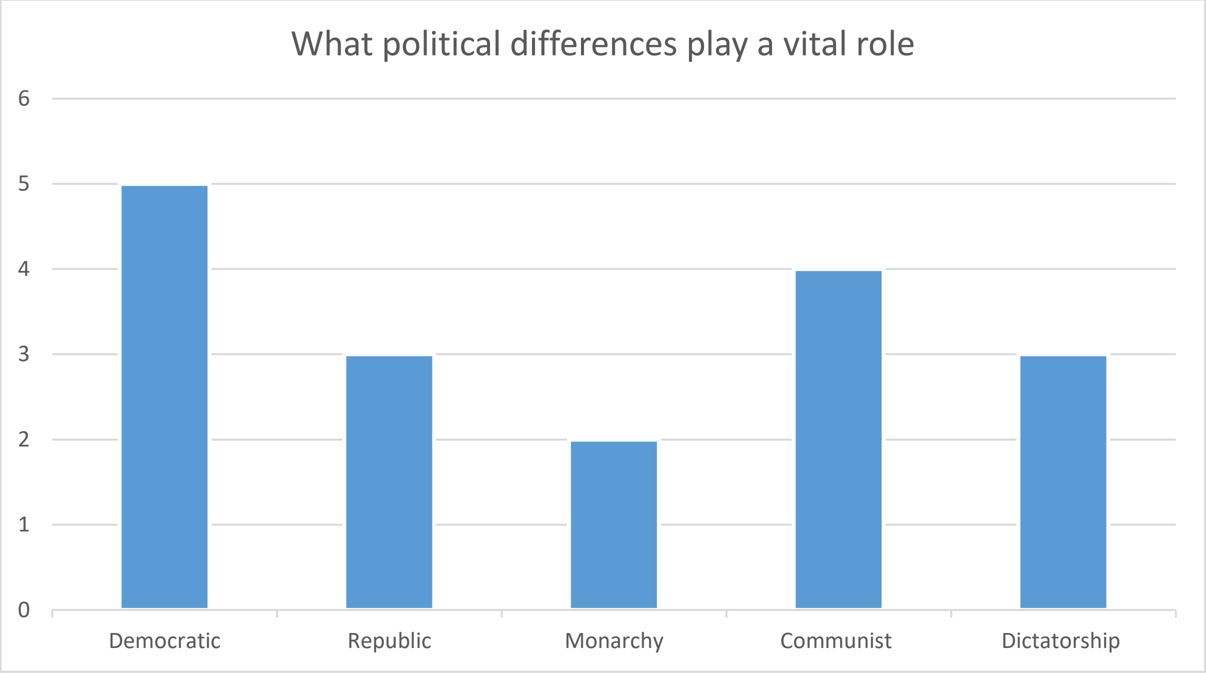


Figure E.499: What political differences play a vital role (Healthcare-UK)

Unlike the participants in other industries, majority in the healthcare sector have chosen democratic, republic, communist and dictatorship governance systems (See figure E. 499). The democratic system allows the public to participate in the process of policy development and, encourage consensus based collective responsibility for their actions. It provides an environment conducive to developing trust between public and the organisations and induces coherence and transparency to the policy development process. In a Republican system, the people and their elected representatives hold the power and the decision they take are governed by the constitution. In constitutional governance, the people look to the administration for legal safeguards to prevent the governments and the organisations collect, share, and store personal information for anything other than valid reasons without compromising their privacy for any reason. In a Communist system, there is no class systems, or a statehood and community has the power to make decisions. The dictatorship is a form of government characterized by a single leader or group of leaders. The participants might have a expressed their preferences regardless of the political system, because the protection of privacy and individual information cannot be ignored and, for that reason it is important for every country to work collectively to accept and implement data protection mechanisms.

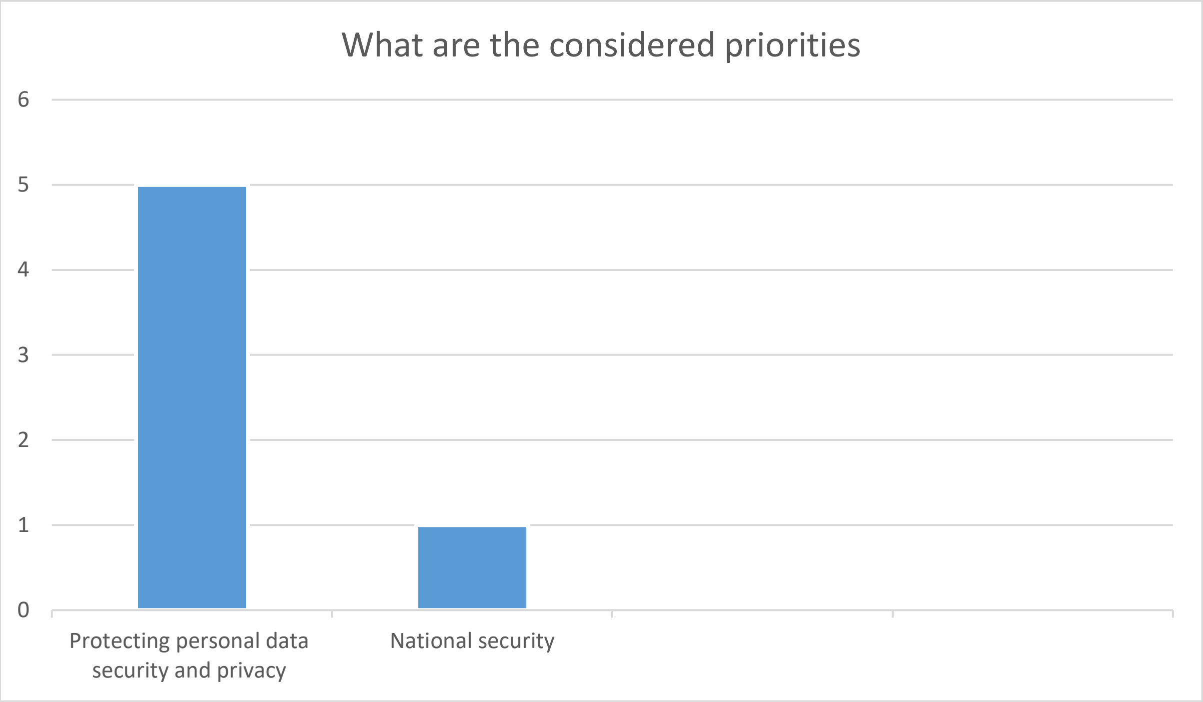


Figure E.500: What are the considered priorities (Healthcare-UK)

In accepting and implementing a global data privacy and security policies, the importance of protection of personal data security and privacy counts above the protection of national security, which is a significant factor (See figure E. 500). However, in an incident of a personal data breach, there will potentially be a knock-on effect on national security as well, and it will also be felt right across the groups as well as the community alike.

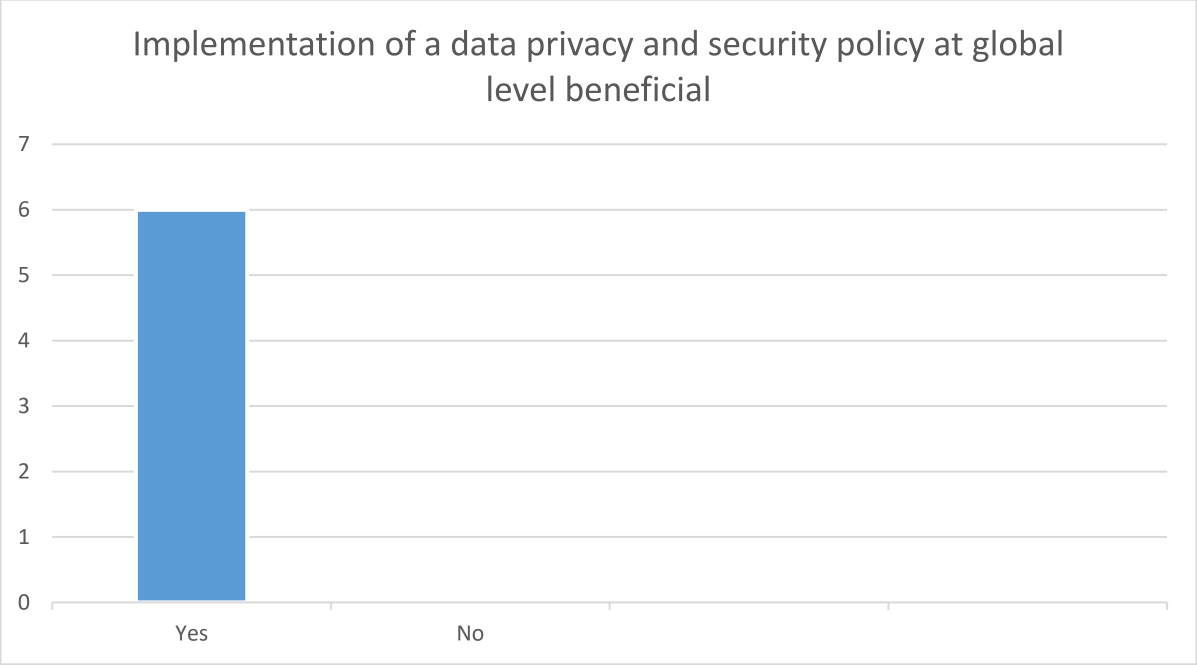


Figure E.501: Implementation of a data privacy and security policy at global level beneficial (Healthcare-UK)

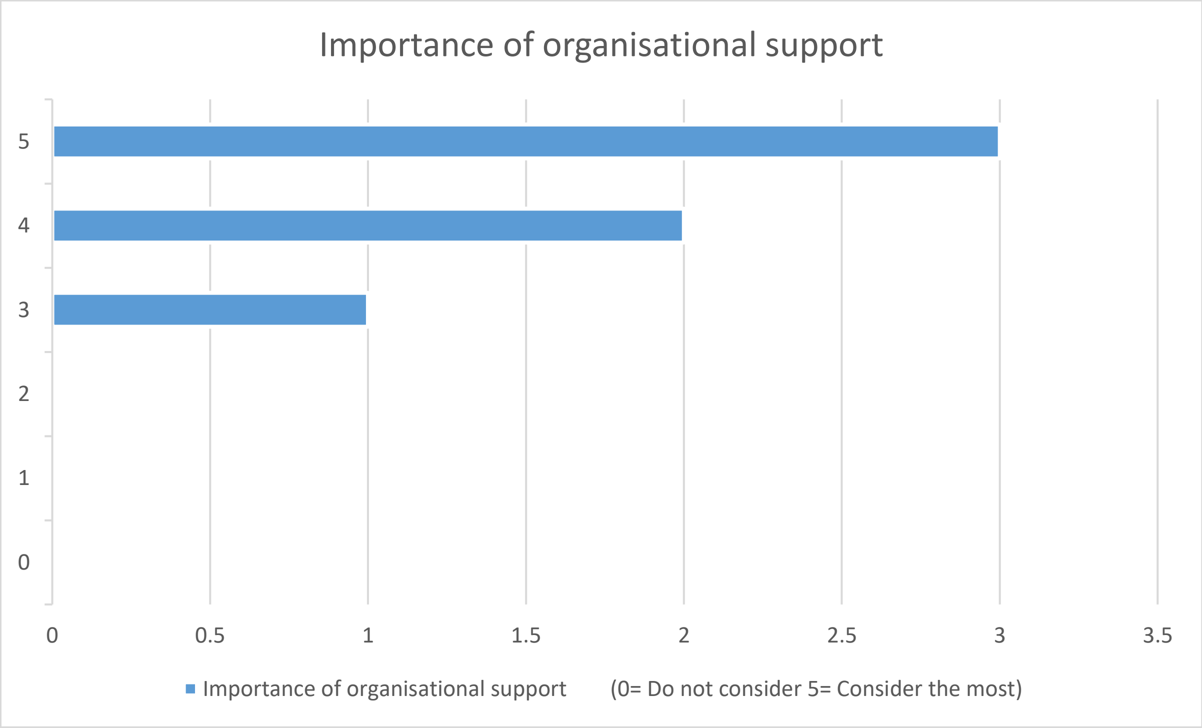


Figure E.502: Importance of organisational support (Healthcare-UK)

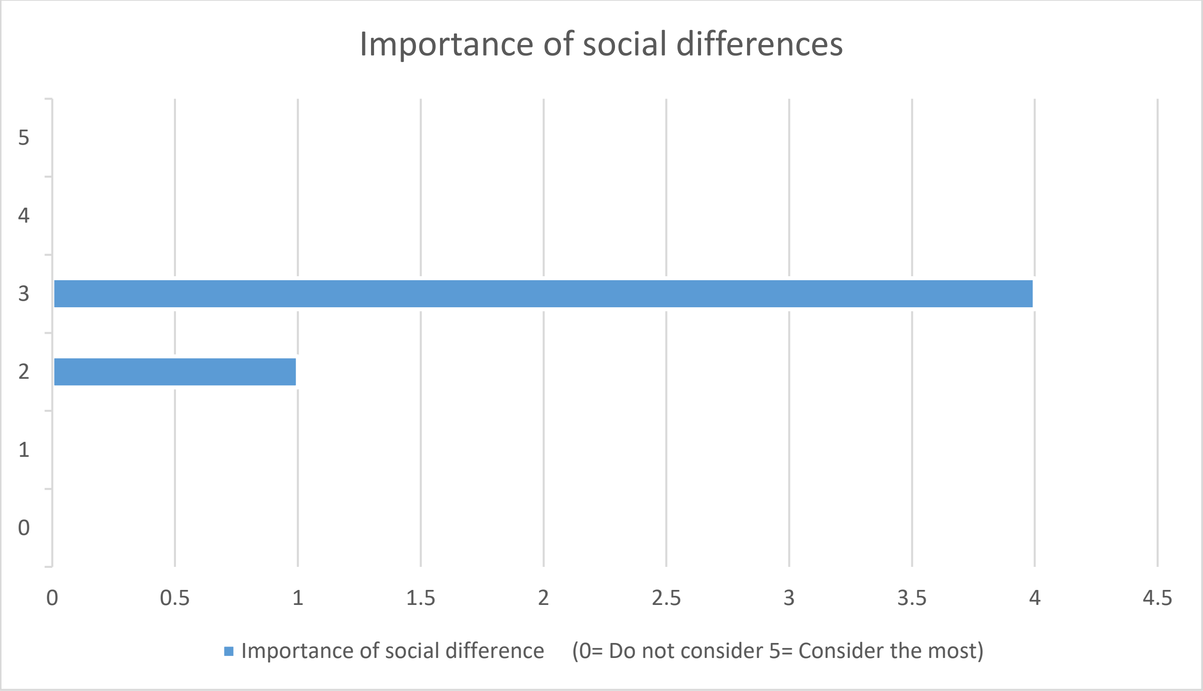


Figure E.503: Importance of social differences (Healthcare-UK)

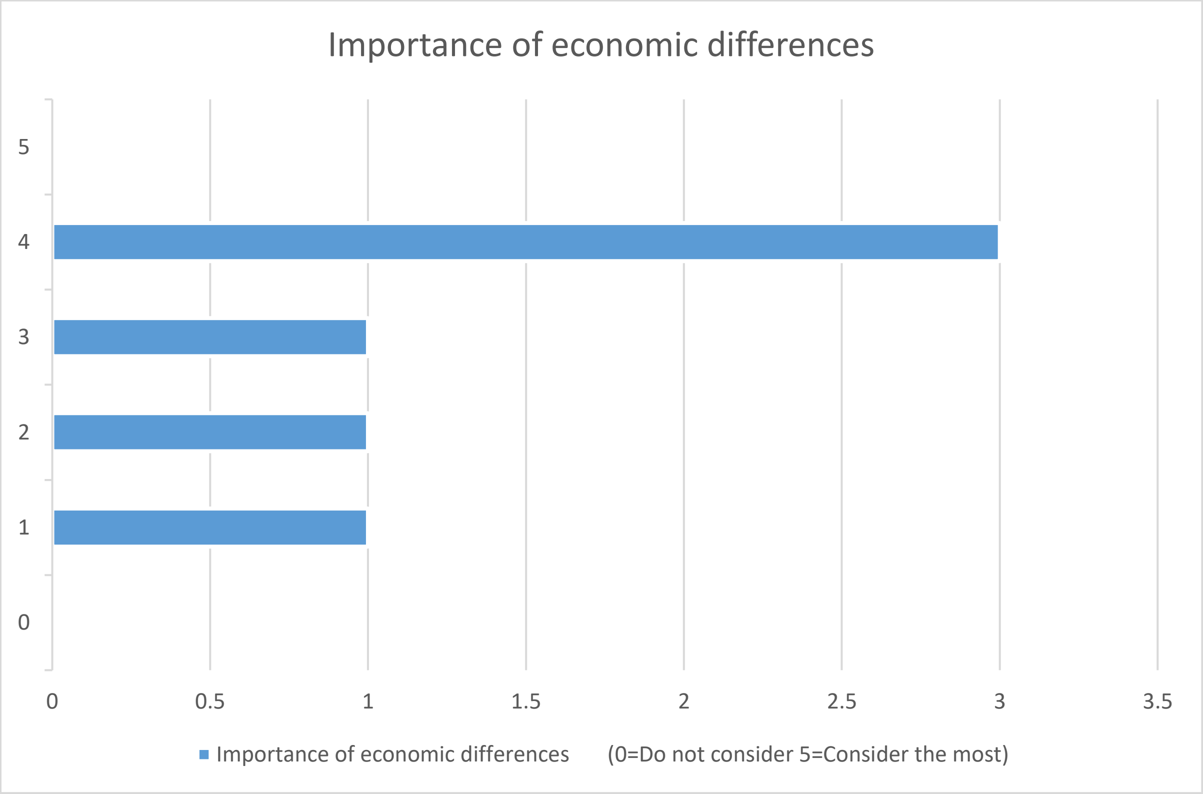


Figure E.504: Importance of economic differences (Healthcare-UK)

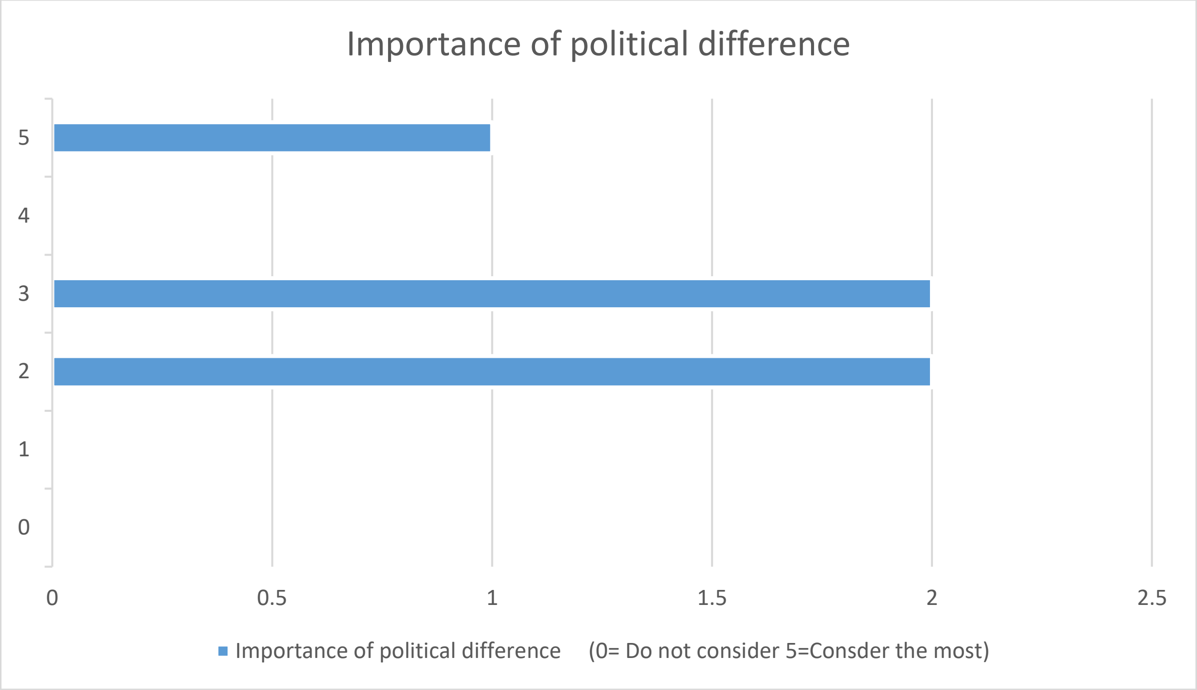


Figure E.505: Importance of political difference (Healthcare-UK)

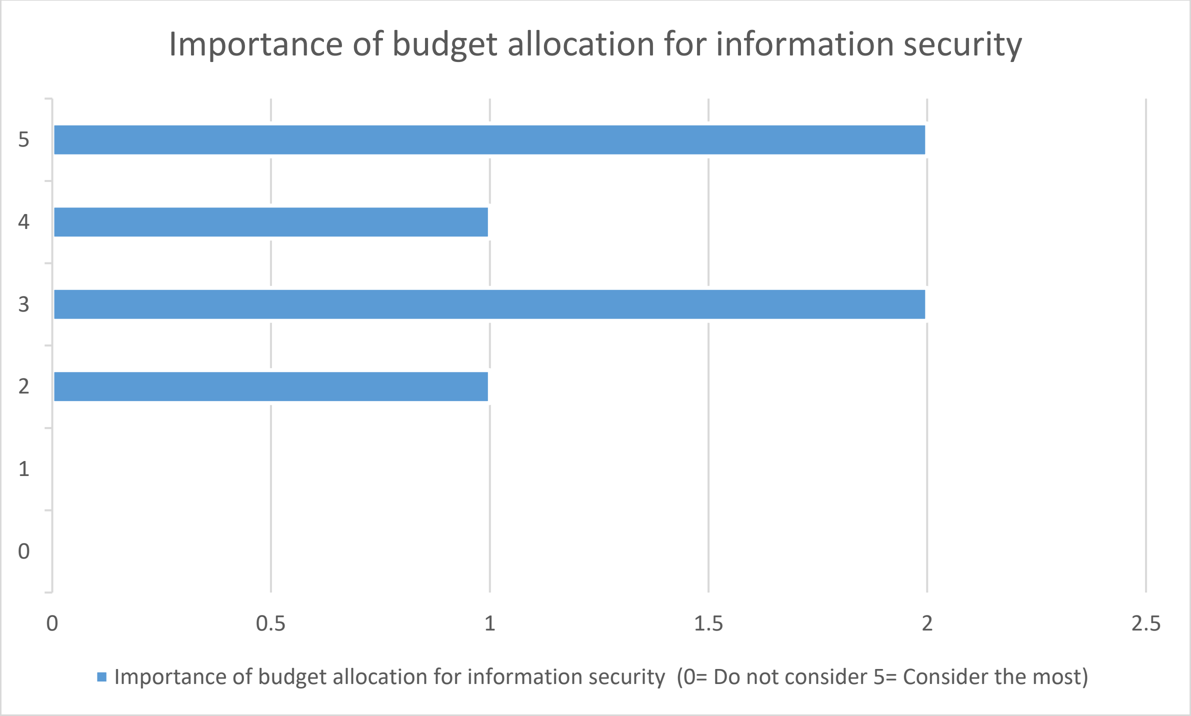


Figure E.506: Importance of budget allocation for information security (Healthcare-UK)

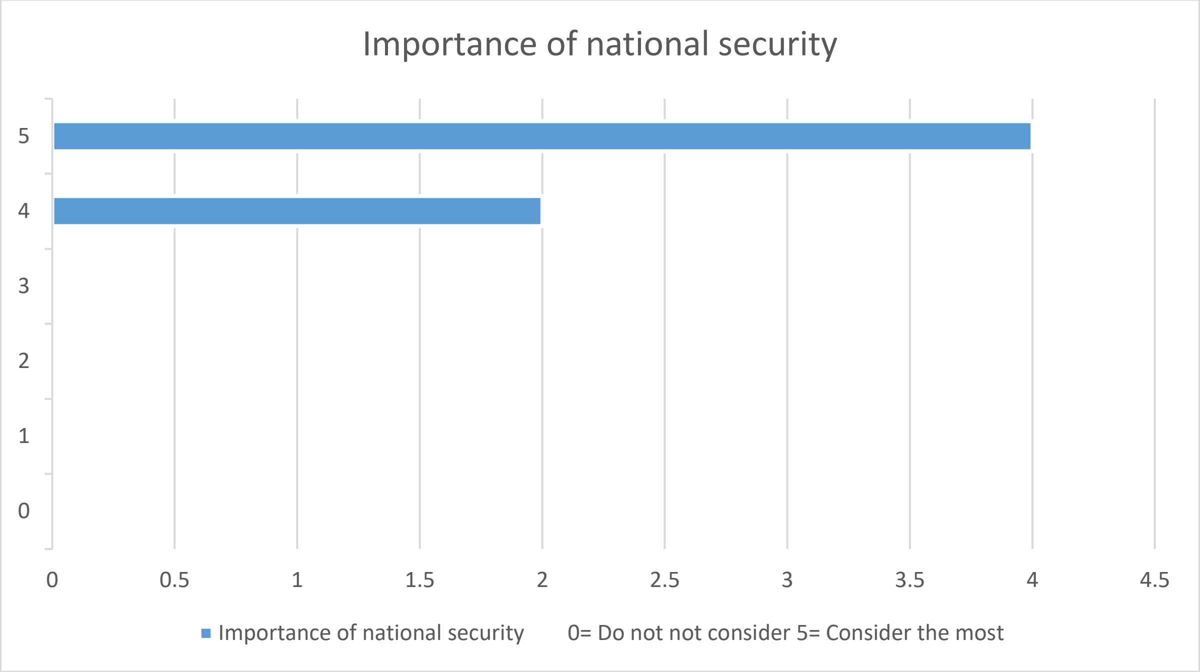


Figure E.507: Importance of national security (Healthcare-UK)

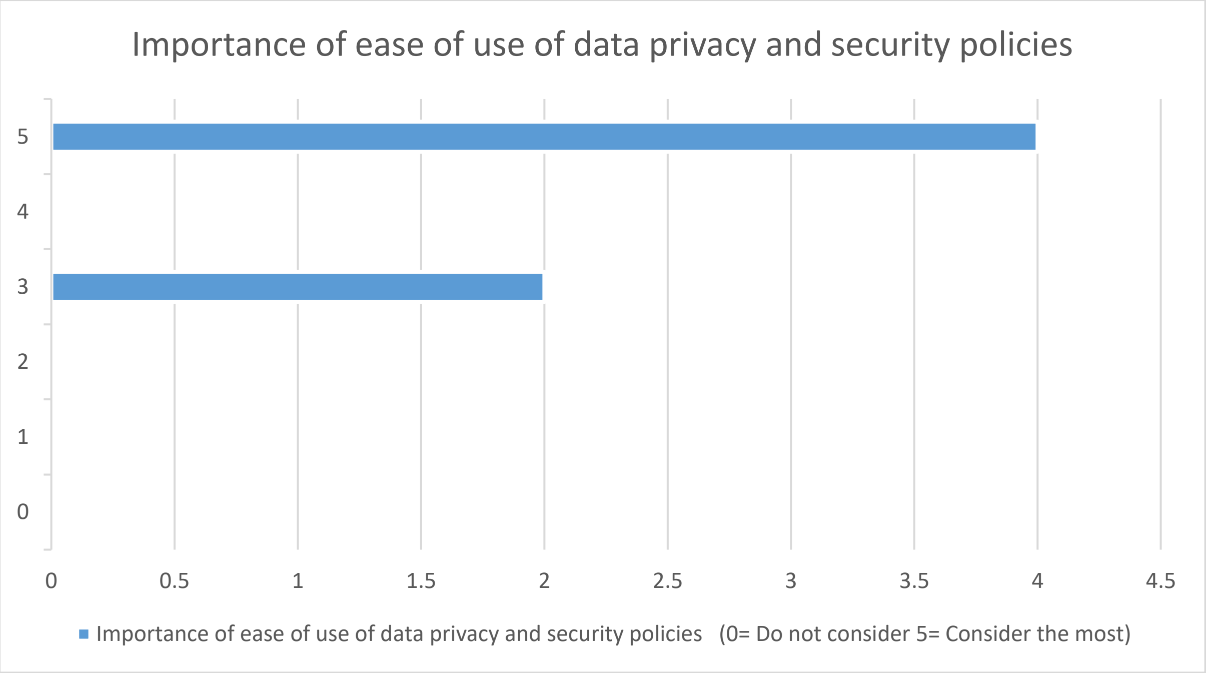


Figure E.508: Importance of ease of use of data privacy and security policies (Healthcare-UK)

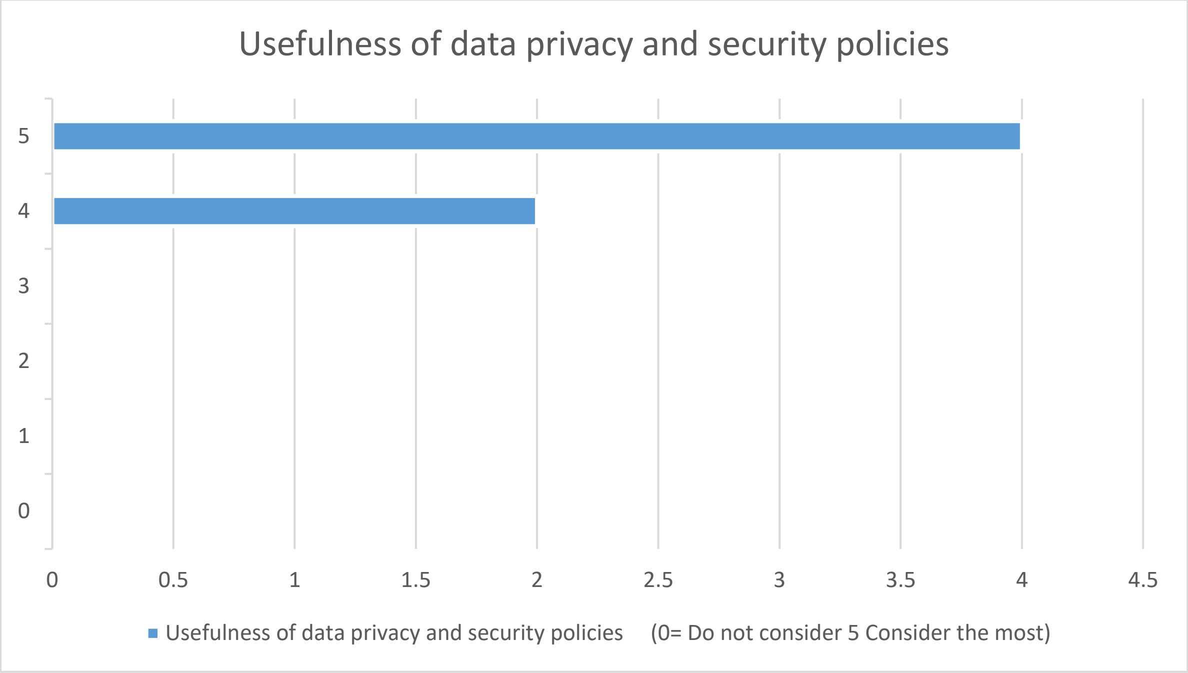


Figure E.509: Usefulness of data privacy and security policies (Healthcare-UK)

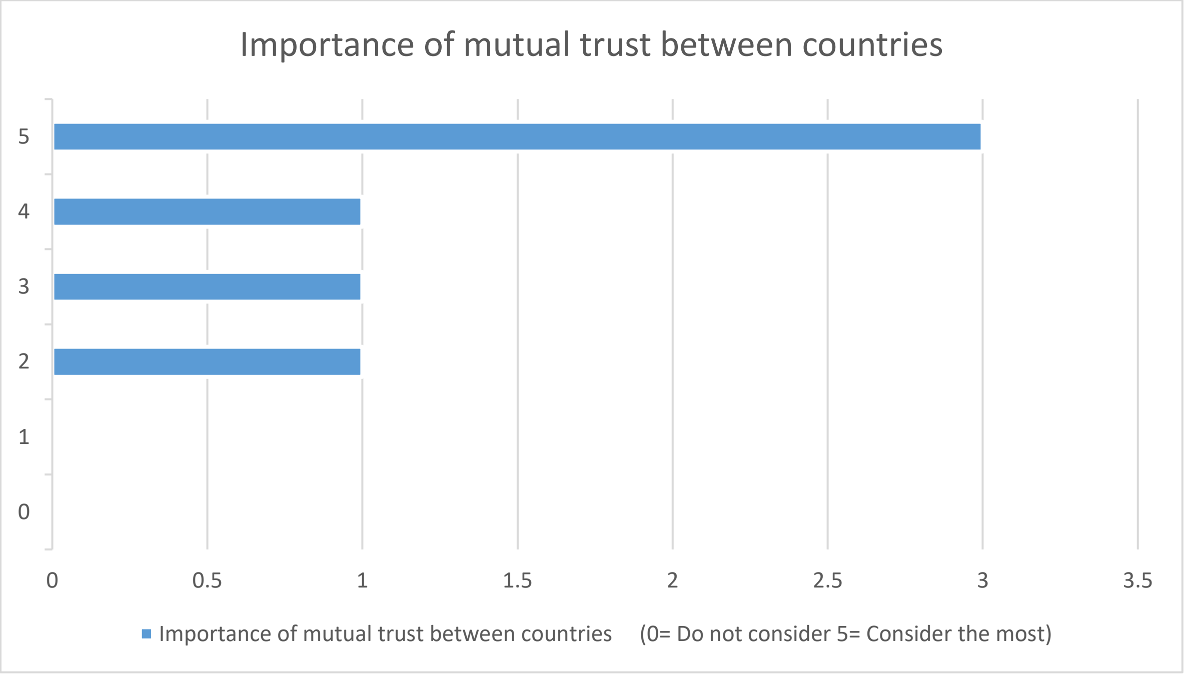


Figure E.510: Importance of mutual trust between countries (Healthcare-UK)

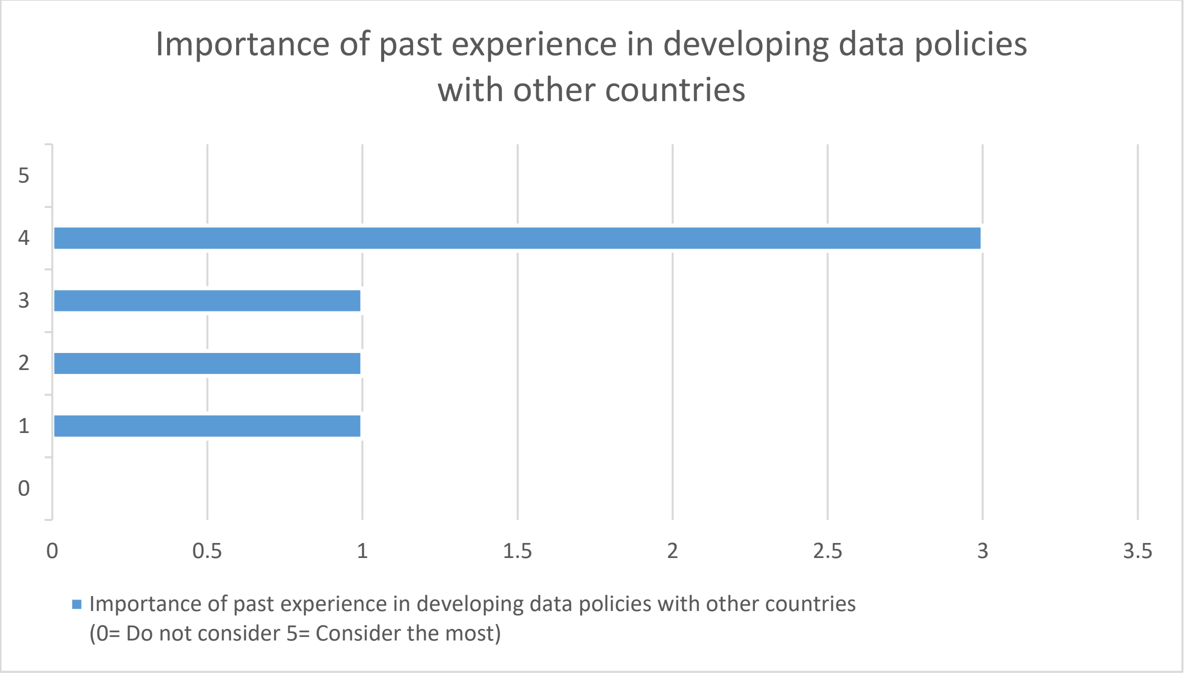


Figure E.511: Importance of past experience in developing data policies with other counties (Healthcare-UK)

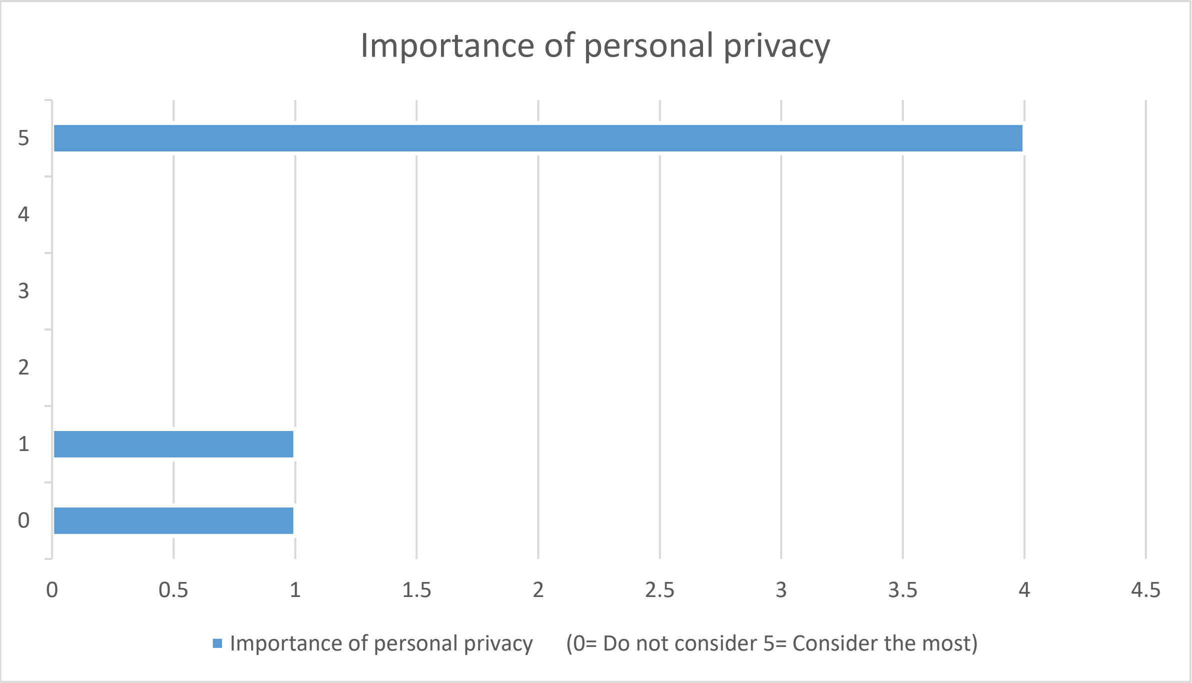


Figure E.512: Importance of personal privacy (Healthcare-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 100 percent of the respondents have endorsed (See figure E. 501). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, political differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure E. 490-500) (See figure E. 502-512)

United Kingdom – Information Security

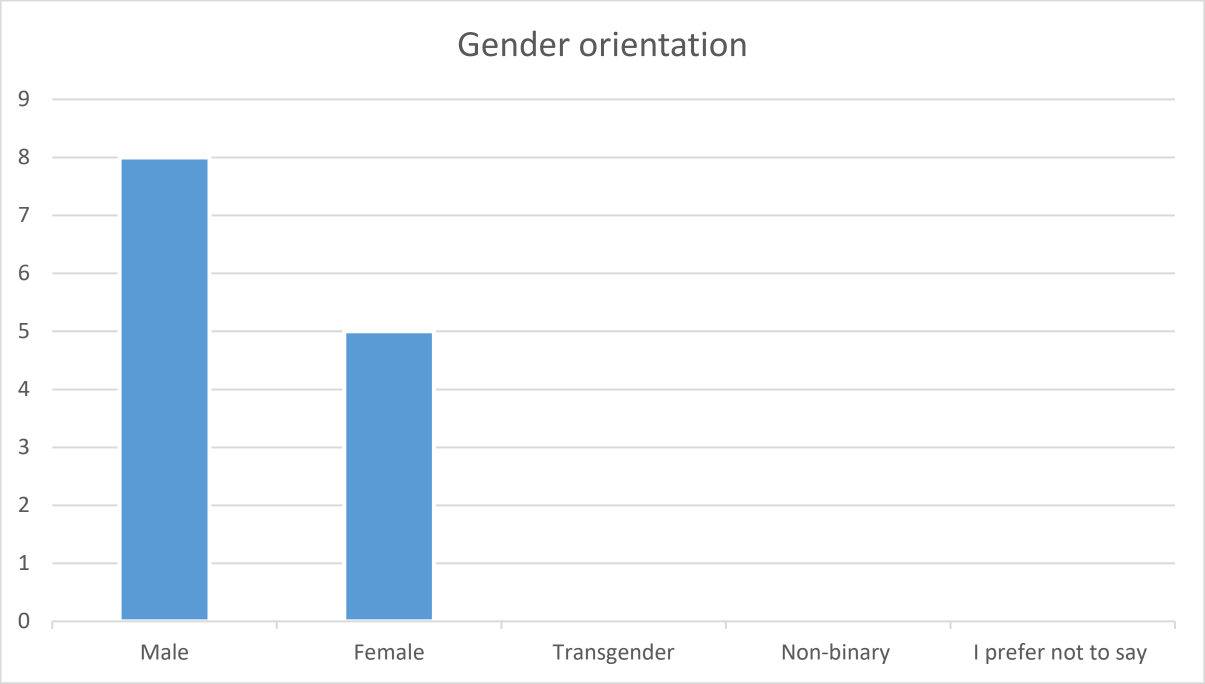


Figure E.513: Gender orientation (Information Security-UK)

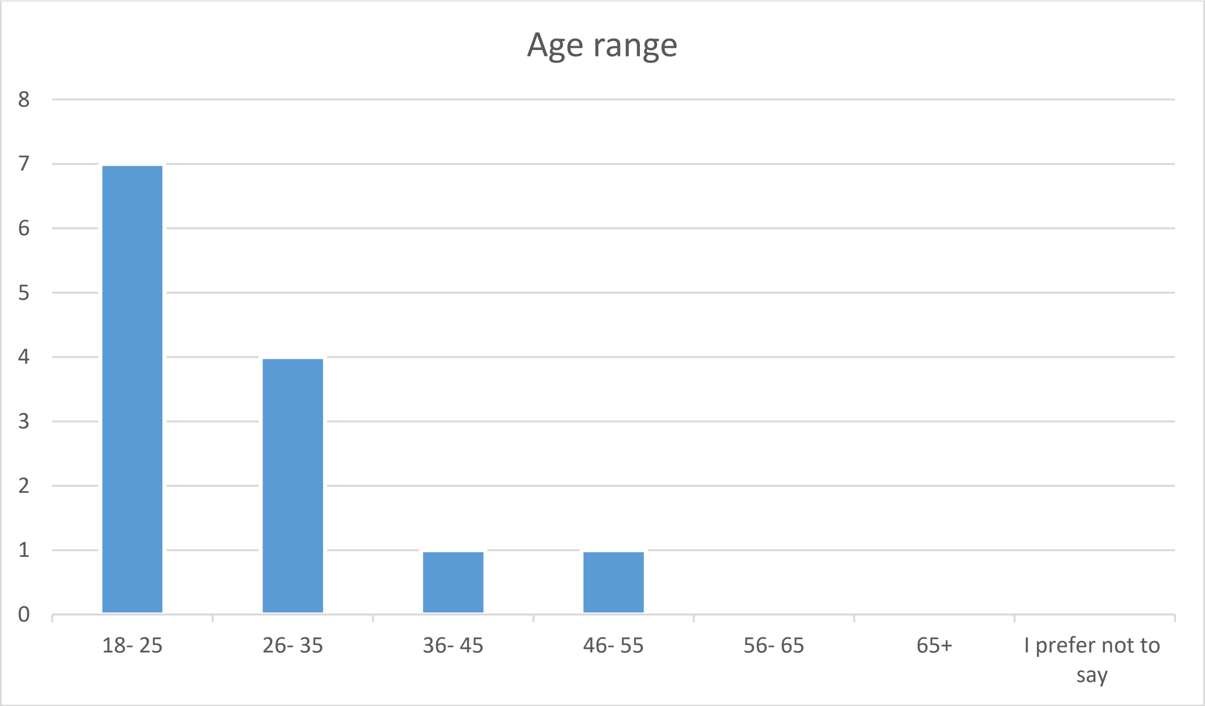


Figure E.514: Age range (Information Security-UK)

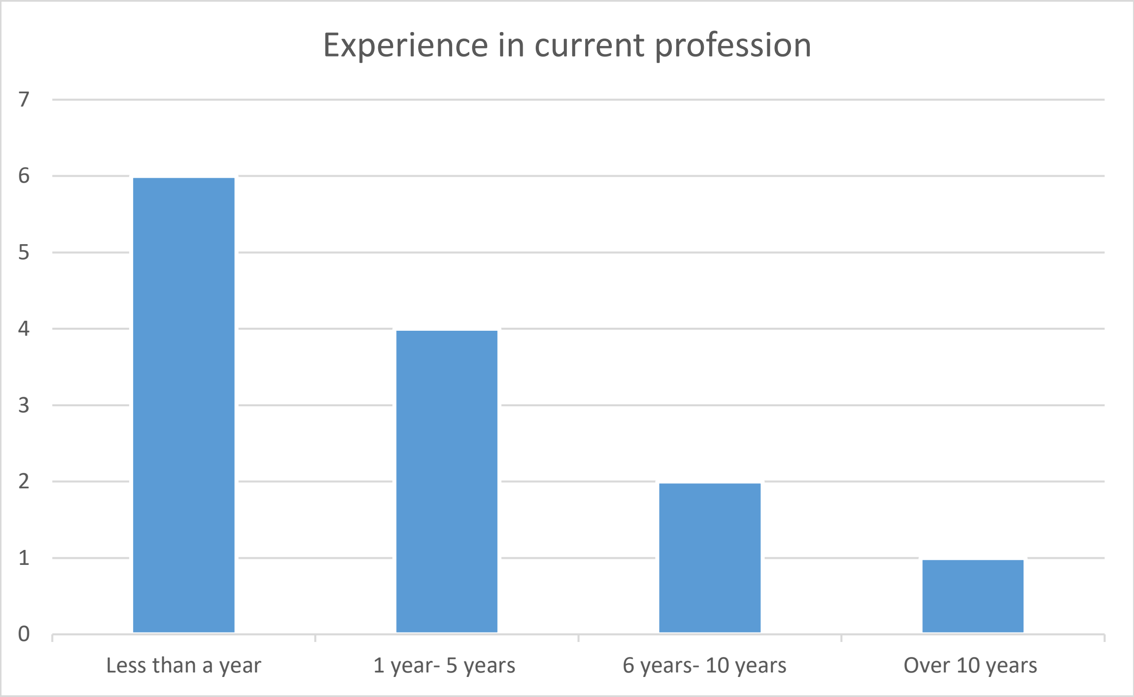


Figure E.515: Experience in current profession (Information Security-UK)

This analysis is based on the responses received from United Kingdom participants employed in Information Technology sector. There were 13 participants and 8 out of them were males and 5 females (See figure E.513). They were within 18-55 age range out of which 7 in the 18-25, 4 in the 26-35, 1 in the 36-45, and 1 in the 46-55 range (See figure E.514). The participants employed in industry between less than a year and over 10 years (See figure E.515).

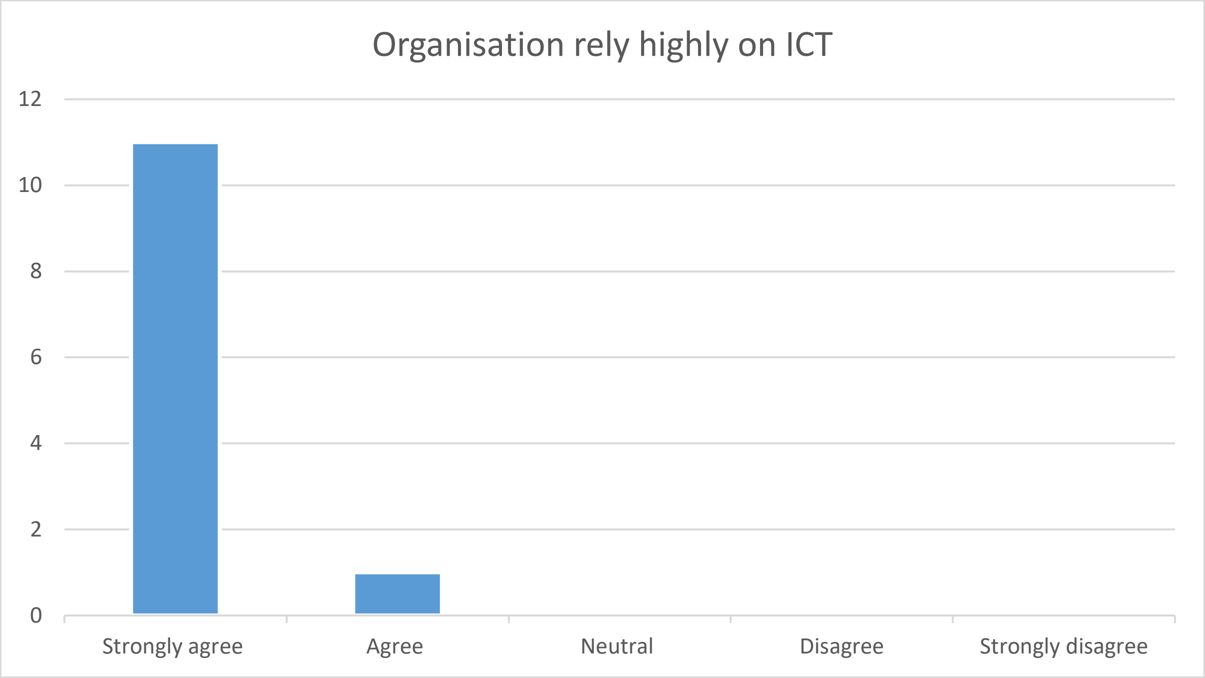


Figure E.516: Organisation rely highly on ICT (Information Security-UK)

Out of the 13 respondents, 92 percent work in a technology reliance environment. The majority of those employed in Information Technology sector have a high reliance on ICT.

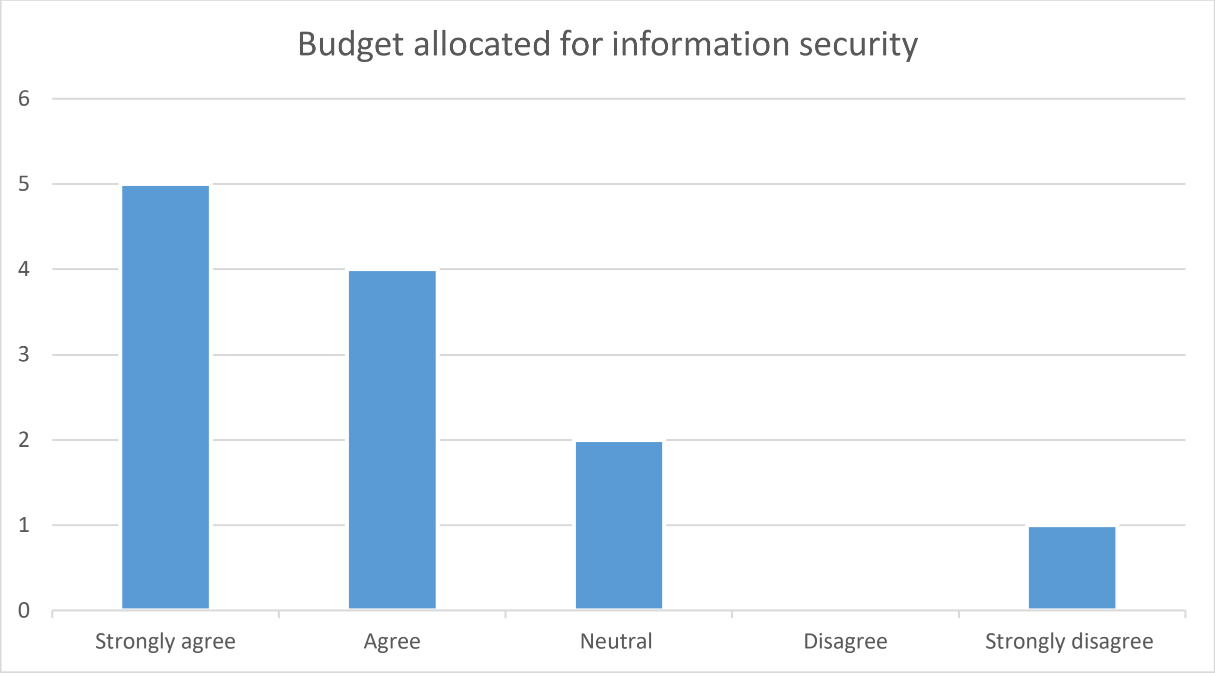


Figure E.517: Budget allocated for information security (Information Security-UK)

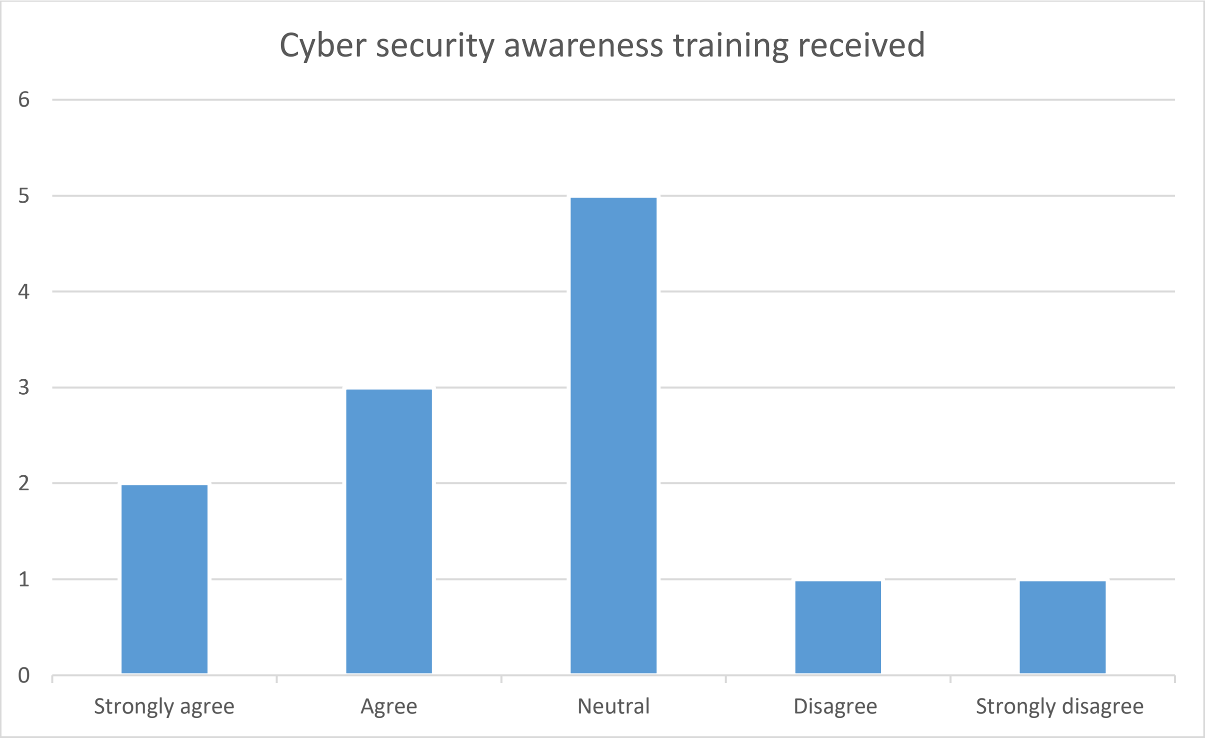


Figure E.518: Cyber security awareness training received (Information Security-UK)

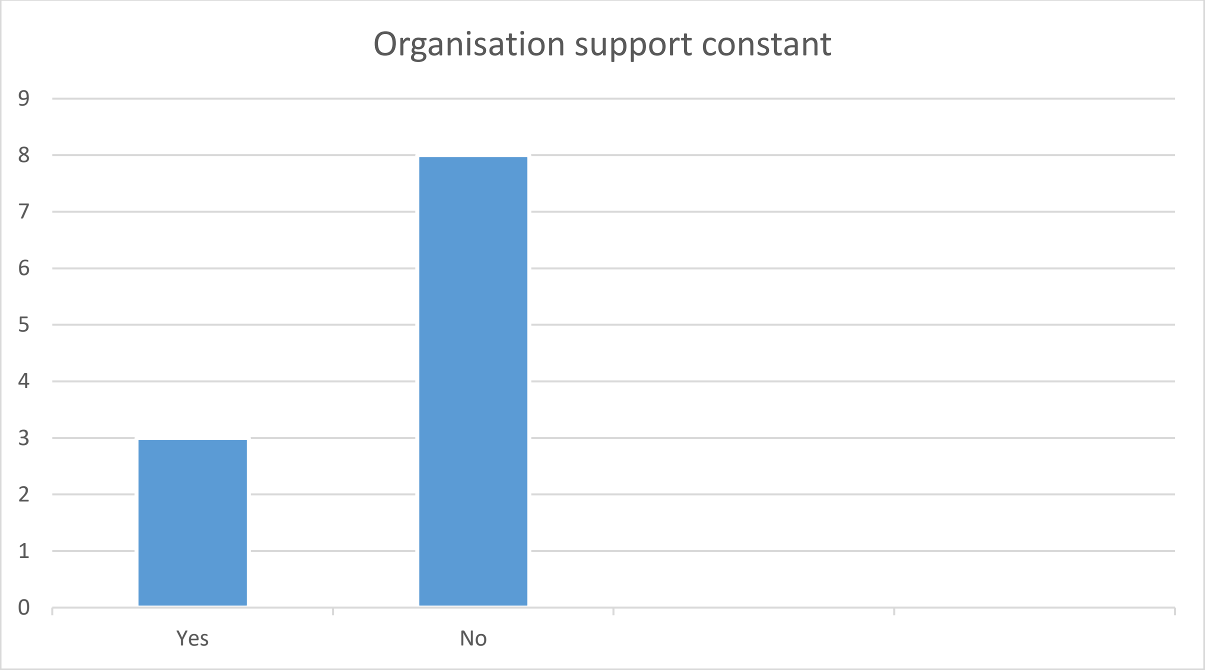


Figure E.519: Organisation support constant (Information Security-UK)

Funding has been sketchy. 9 out of the 13 have indicated that their organisations had an allocated budget for information security, whilst 2 had not expressed an opinion either way, and notably according to the 1 disagreed, their organisations had no budget allocation for information security (See figure E.517). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 5 participants have received regular cyber security awareness training, whilst 5 neither agreed nor disagreed, and 2 participants who had not regularly received security awareness training (See figure E.518). In addition, 8 participants had not received support from the organisation to protect personal information, whilst only 3 did (See figure E.519). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

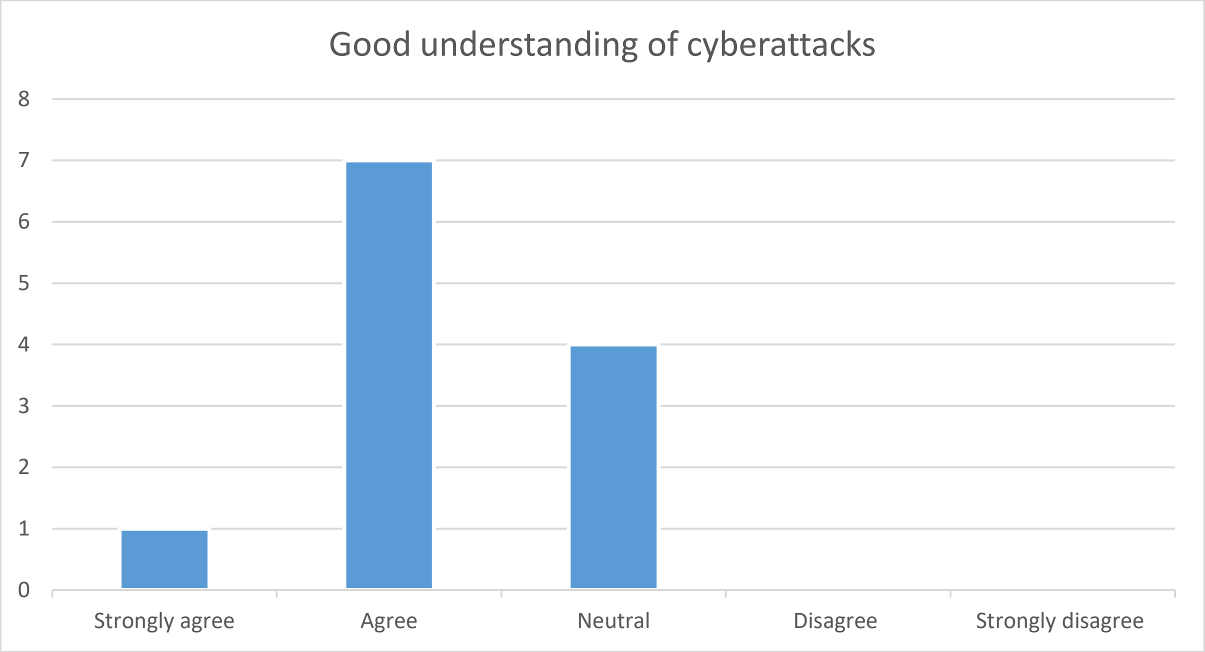


Figure E.520: Good understanding of cyberattacks (Information Security-UK)

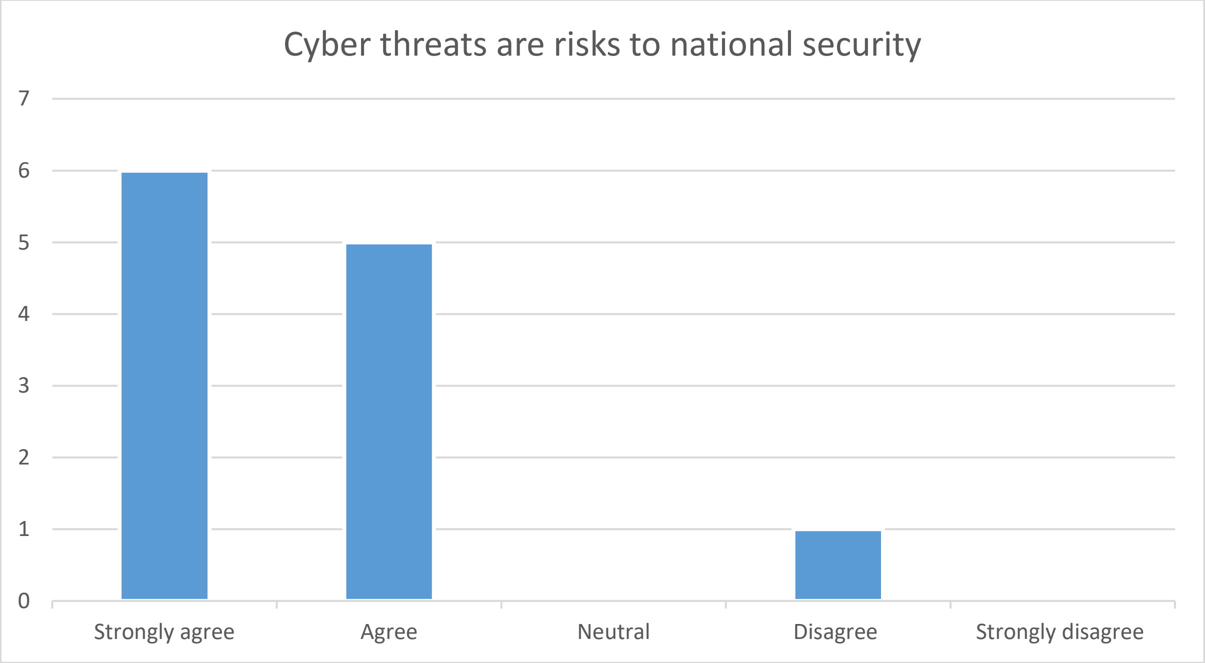


Figure E.521: Cyber threats are risks to national security (Information Security-UK)

Despite the lack of security awareness training, the participants appears to have a high understanding of the impact of cyber-attacks on the public and the organisation. 8 participants do have, 4 have not expressed opinion either way (See figure E.520). Furthermore, 85 percent of the participants also realises the potential threats to national security from cyber-attacks (See figure E.521). In general, understanding of cyber threats and their impact to national security will make people act responsibly to minimise end user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

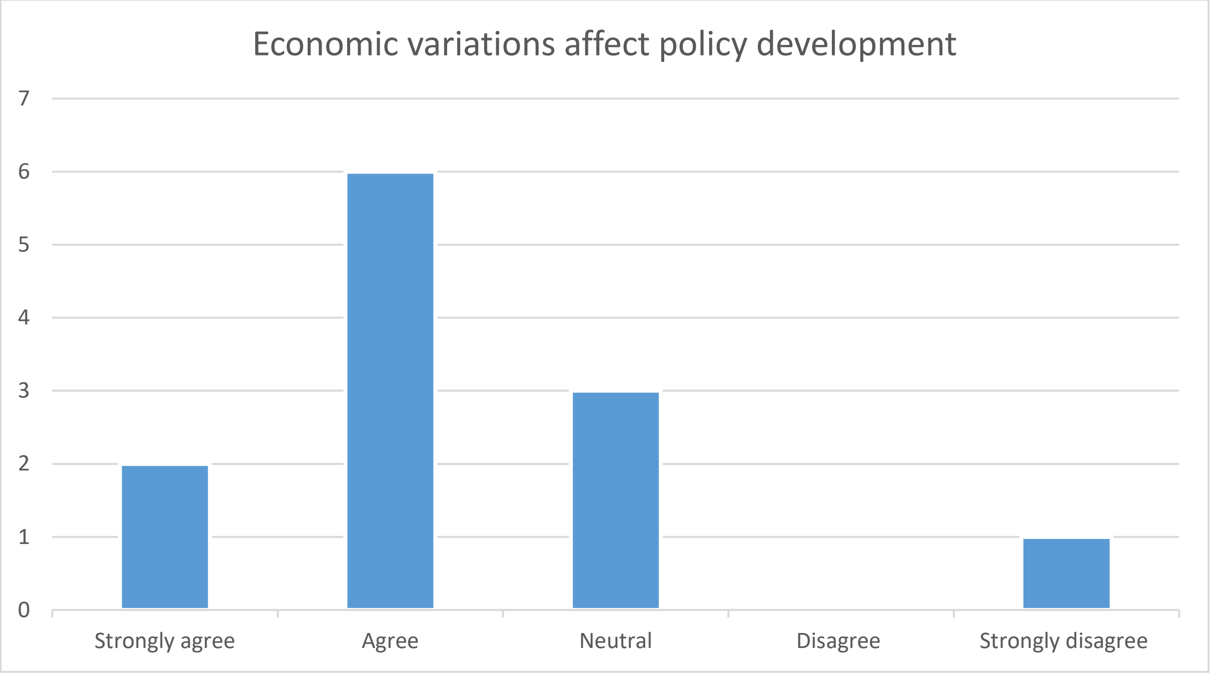


Figure E.522: Economic variations affect policy development (Information Security-UK)

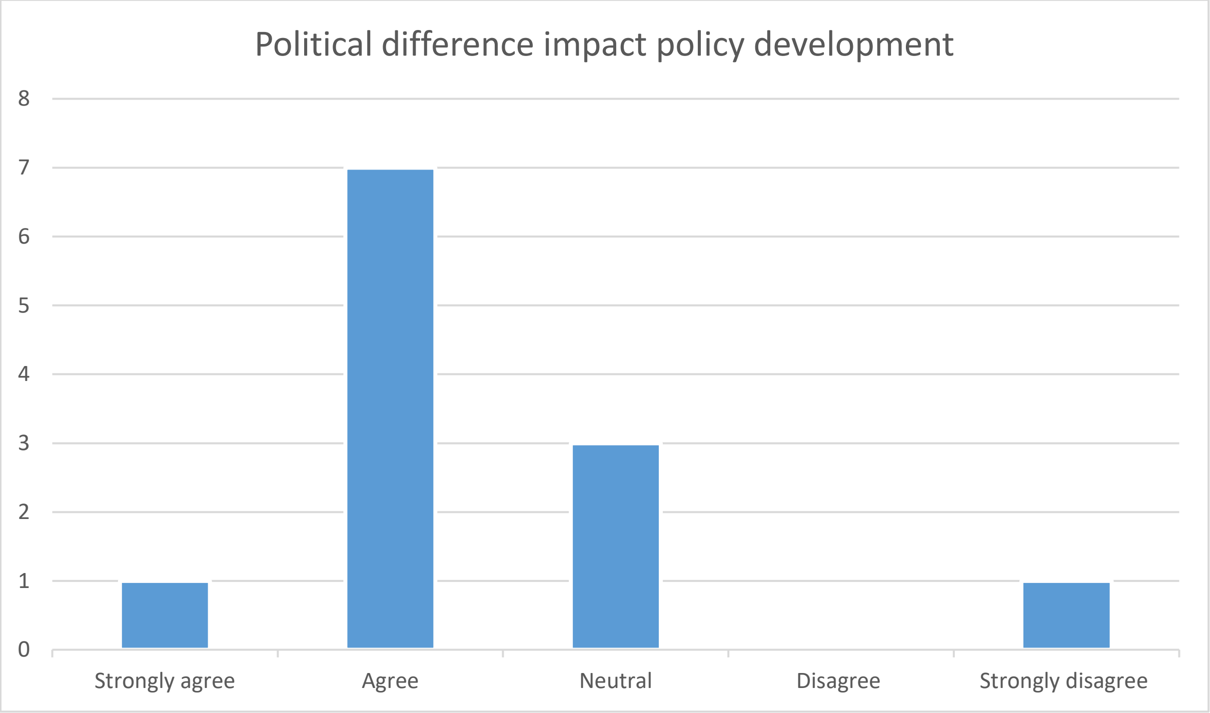


Figure E.523: Political differences impact policy development (Information Security-UK)

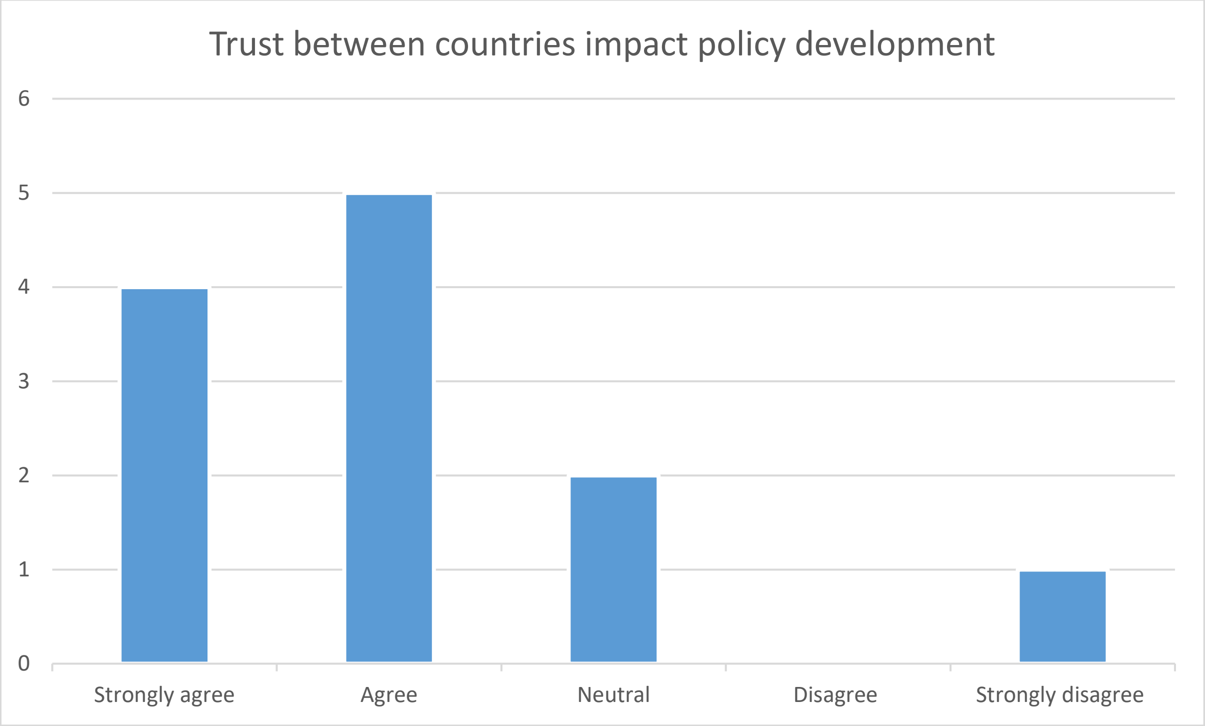


Figure E.524: Trust between countries impact policy development (Information Security-UK)

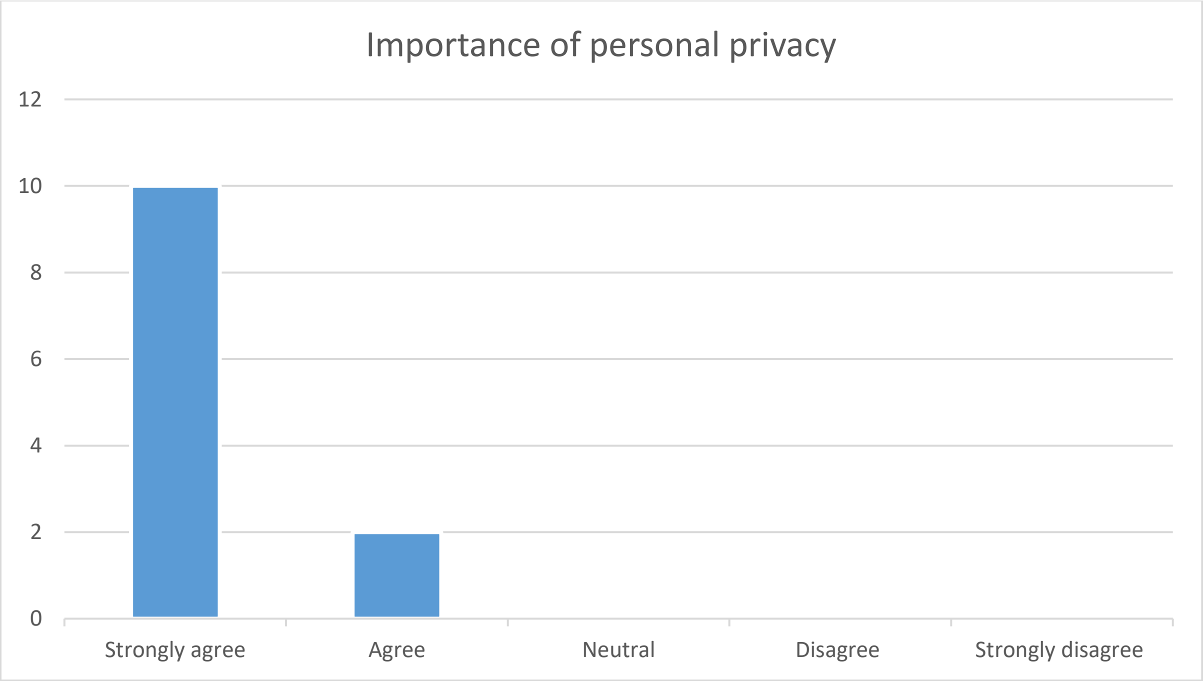


Figure E.525: Importance of personal privacy (Information Security-UK)

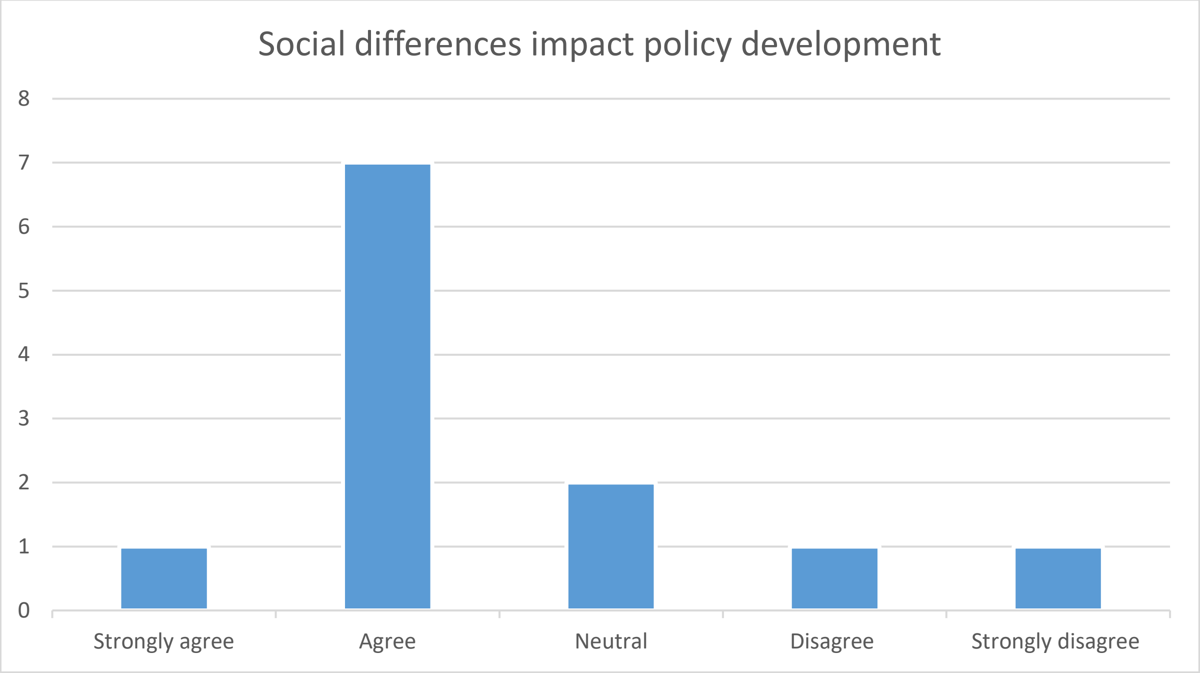


Figure E.526: Social differences impact policy development (Information Security-UK)

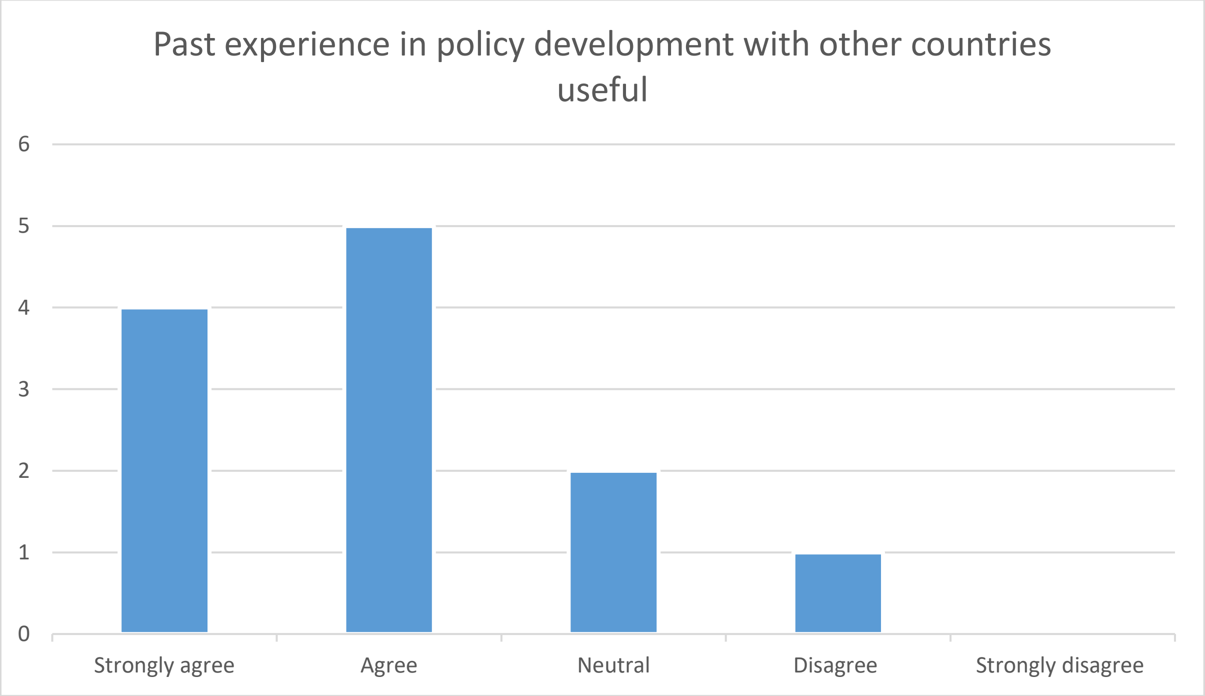


Figure E.527: Past experience in policy development with other countries useful (Information Security-UK)

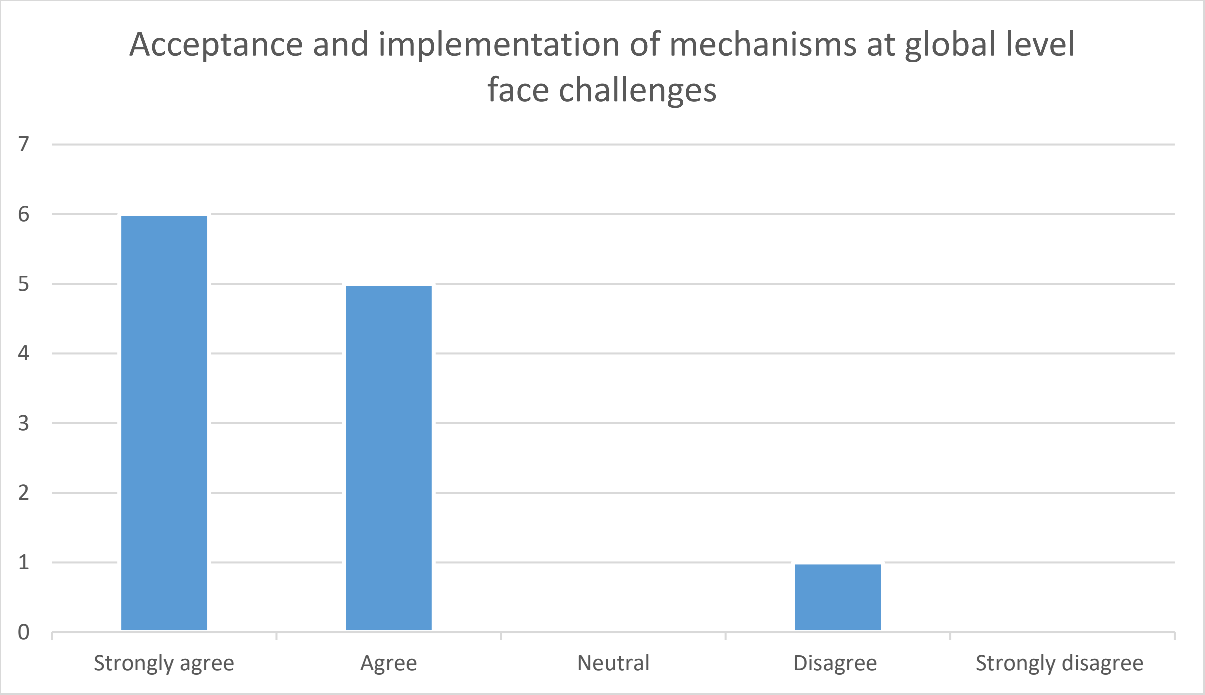


Figure E.528 Acceptance and implementation of mechanisms at global level face challenges (Information Security-UK)

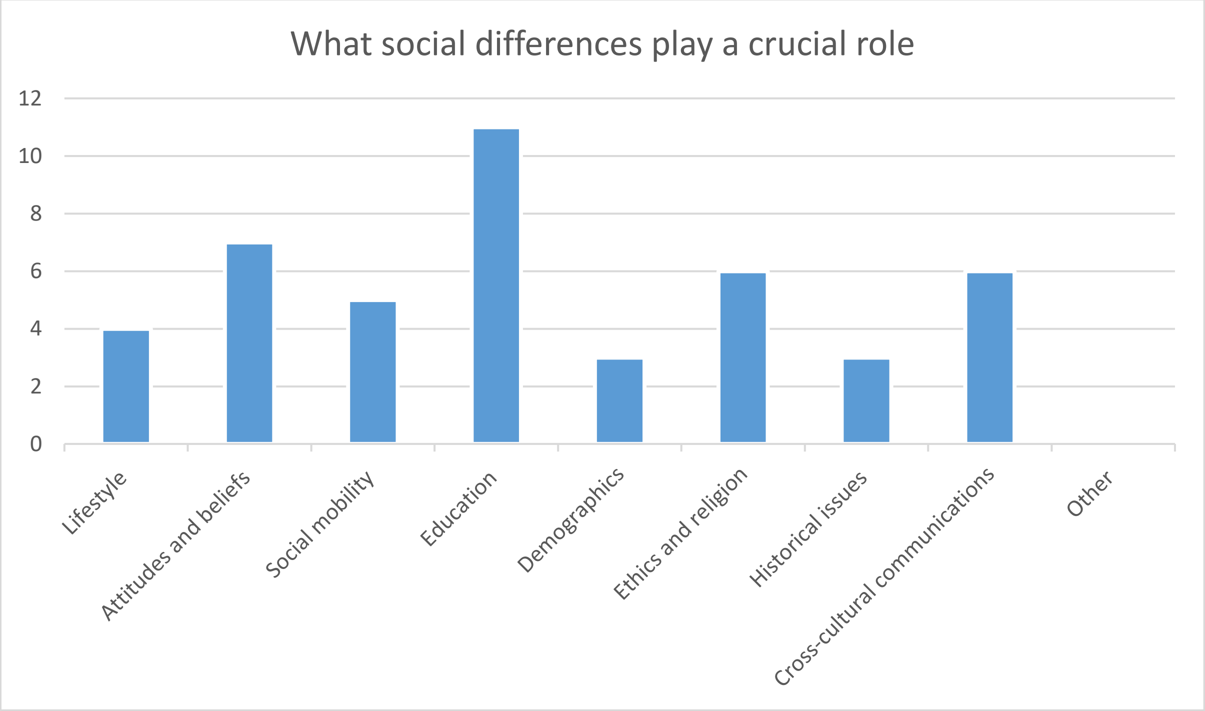


Figure E.529: What social differences play a crucial role (Information Security-UK)

The response to the social differences listed in the questionnaire, majority has highlighted the importance of education and attitude and beliefs (See figure E.529). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cyber security awareness training at schools and at organisational level. Believing in privacy and respecting privacy of self and others are contributory factors that have been discuss under attitude and believes.

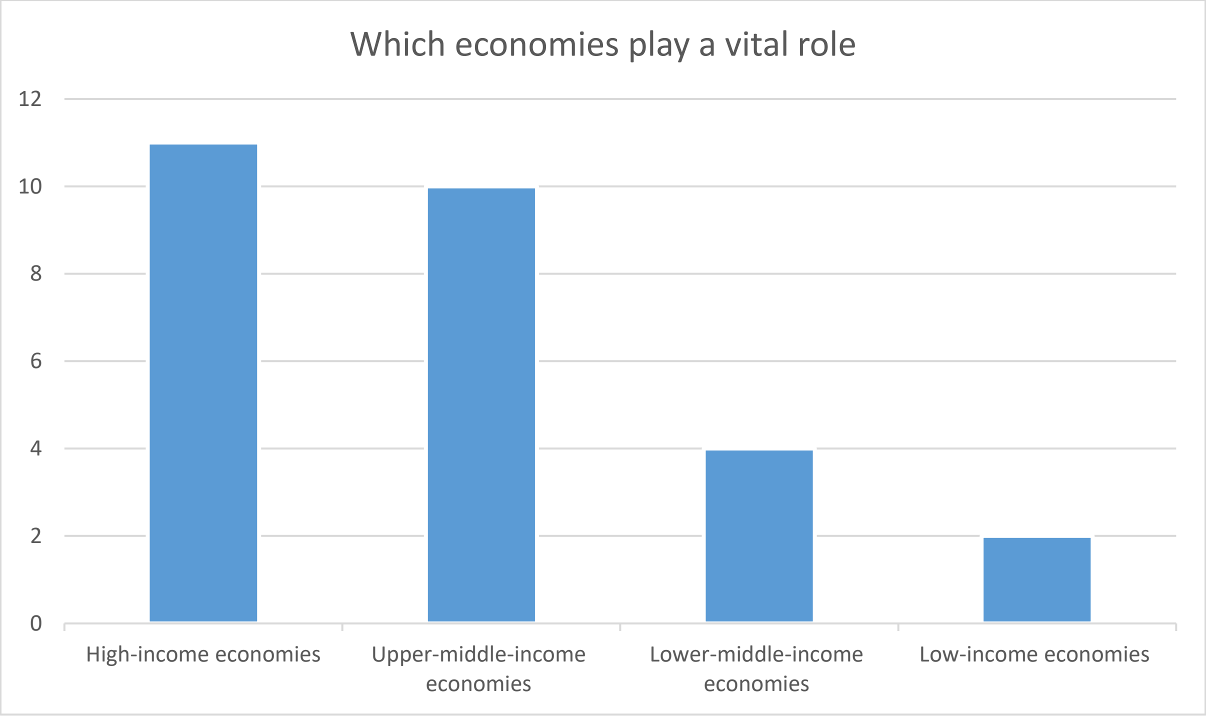


Figure E.530: Which economies play a vital role (Information Security-UK)

In the questionnaire majority has stated that the high income and upper middle-income countries play a vital role (See figure E.530). There are key stages in policymaking. This includes, identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, financial stability of a country counts as a crucial factor in policymaking.

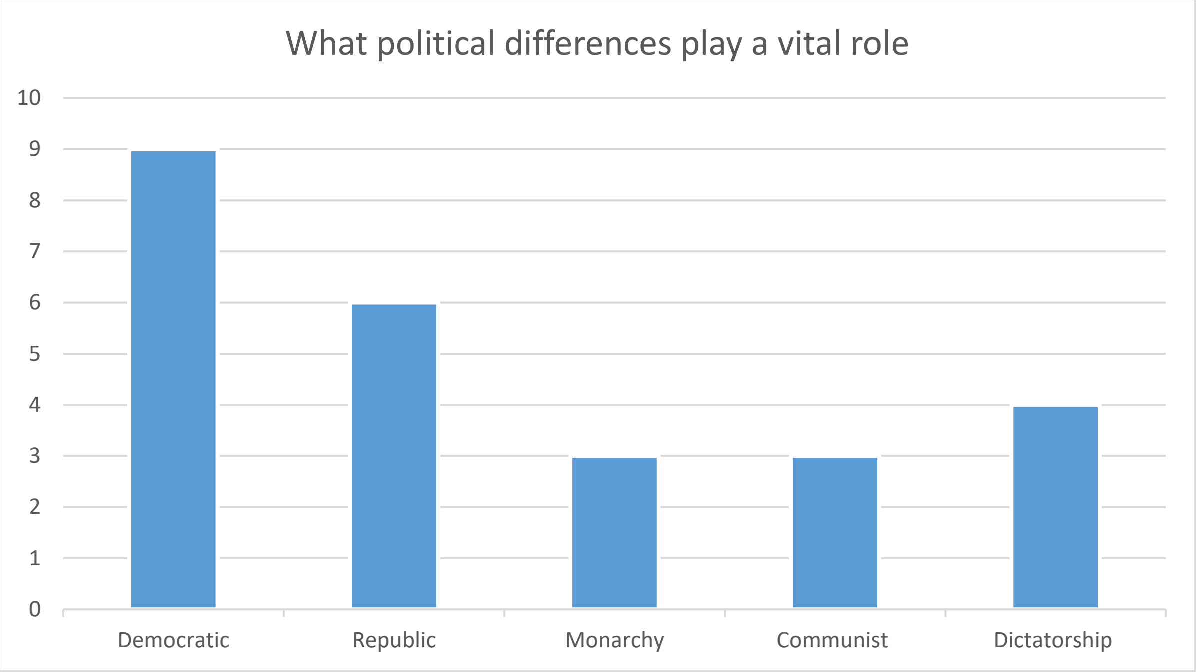


Figure E.531: What political differences play a vital role (Information Security-UK)

Majority have chosen democratic political system (See figure E.531), in preference to others as because it allows a public voice to influence in the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

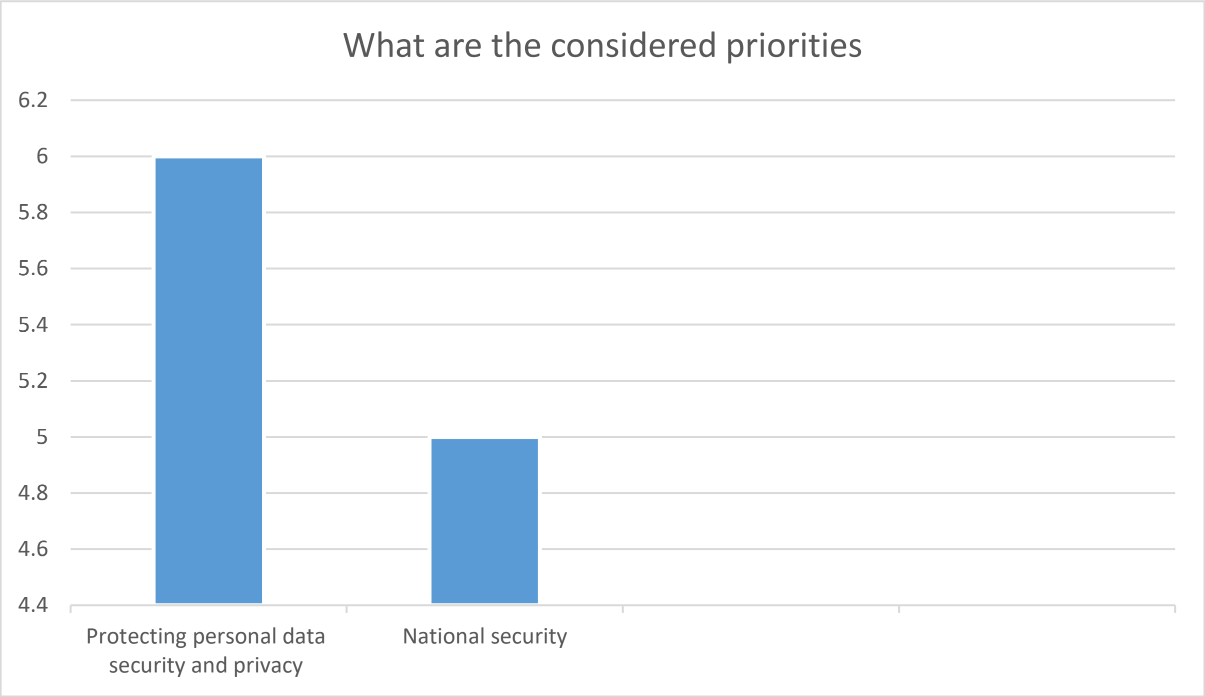


Figure E.532: What are the considered priorities (Information Security-UK)

The majority not considered either the importance of protection of personal data security and privacy or protection of national security, in accepting and implementing a global data privacy and security policies (See figure E.532).

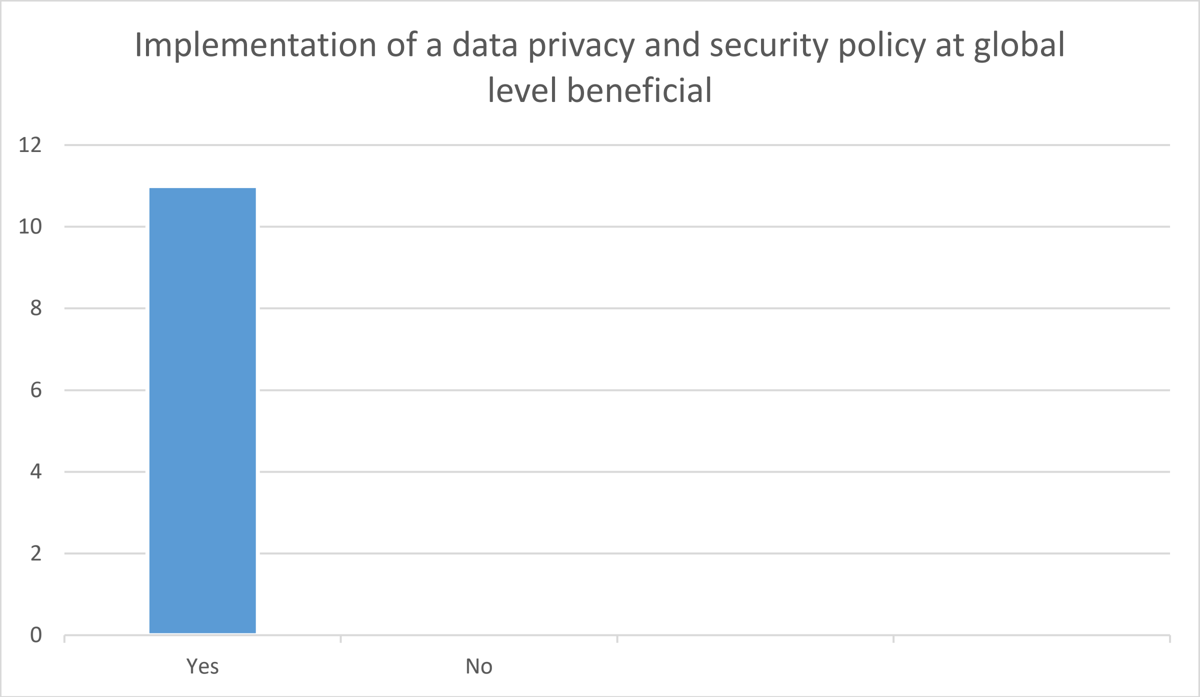


Figure E.533: Implementation of a data privacy and security policy at global level beneficial (Information Security-UK)

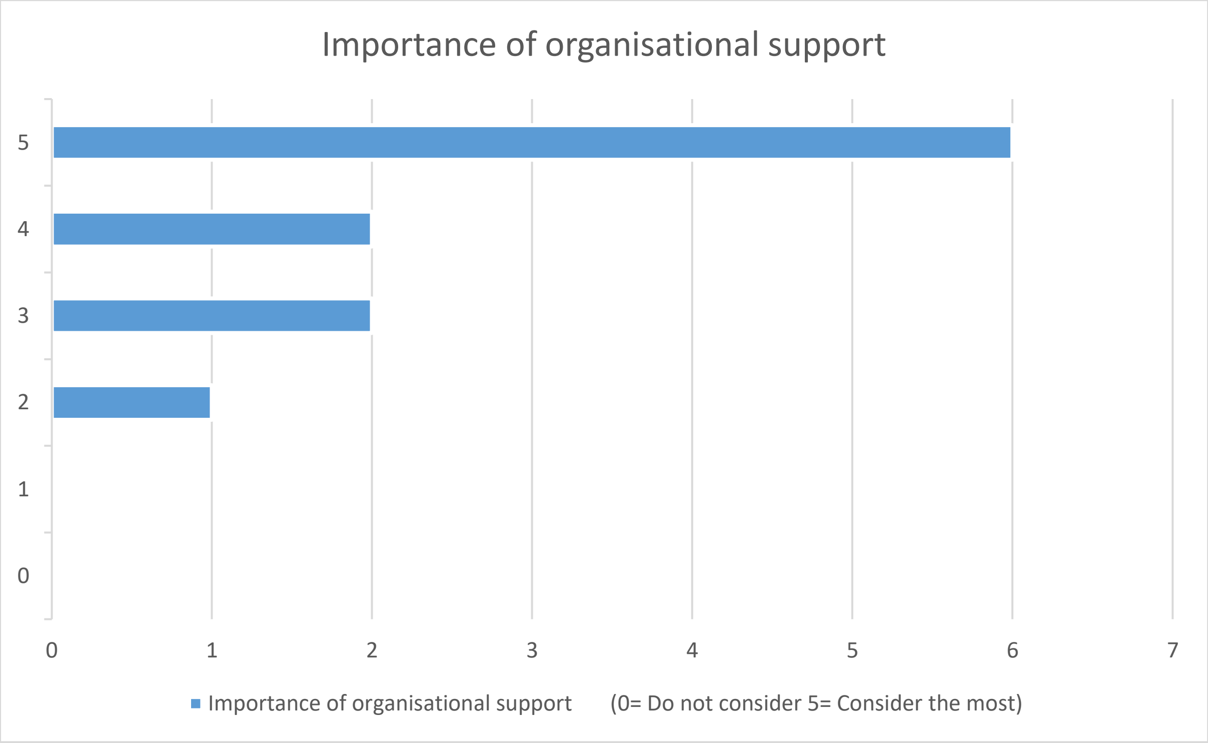


Figure E.534: Importance of organisational support (Information Security-UK)

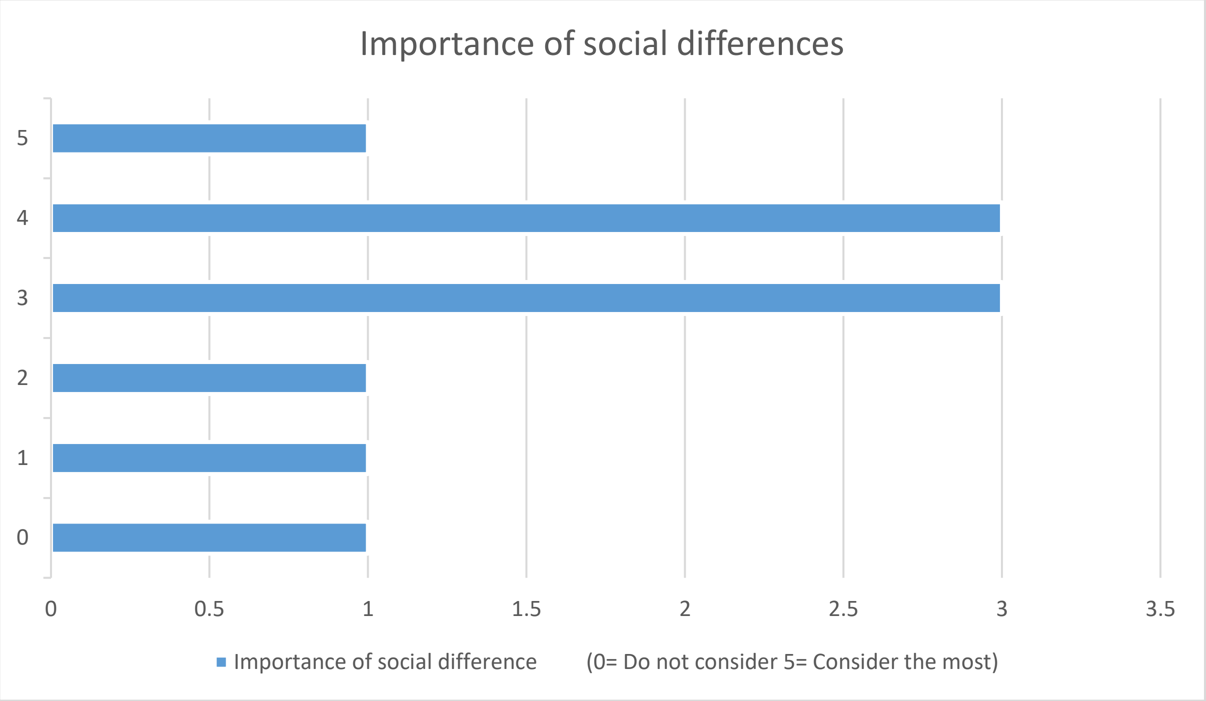


Figure E.535: Importance of social differences (Information Security-UK)

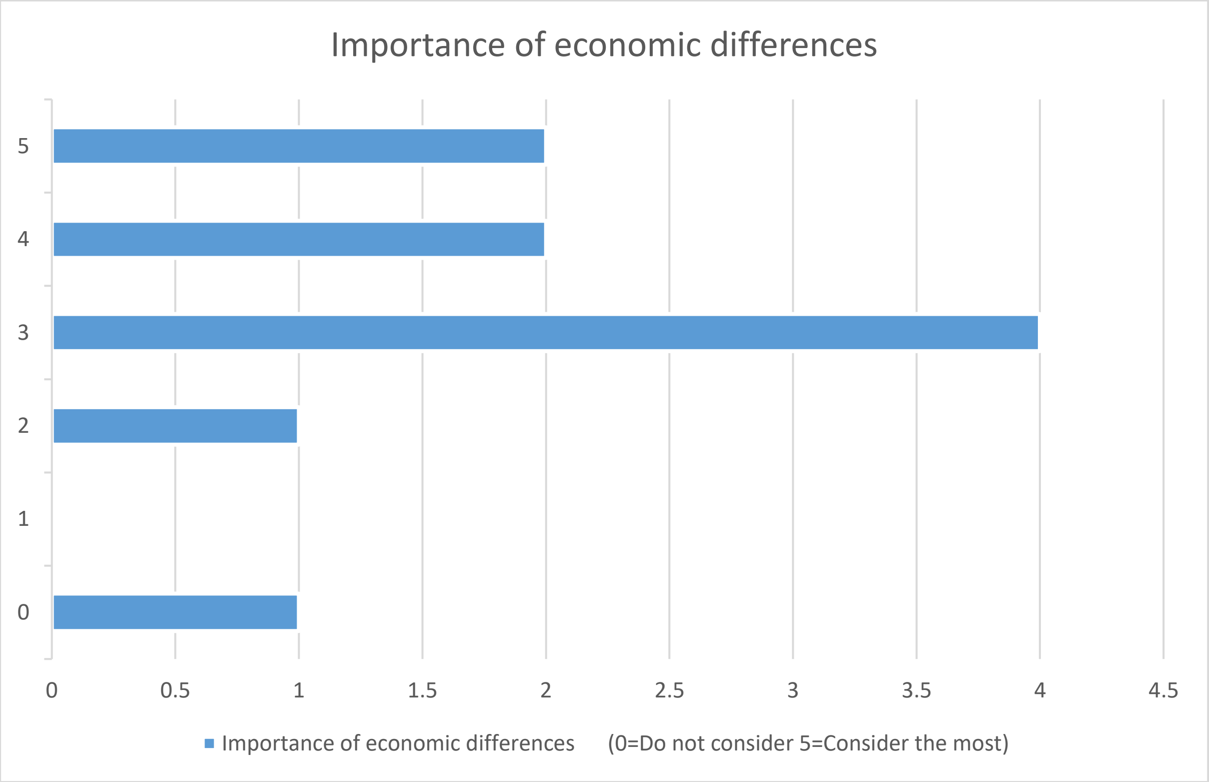


Figure E.536: Importance of economic differences (Information Security-UK)

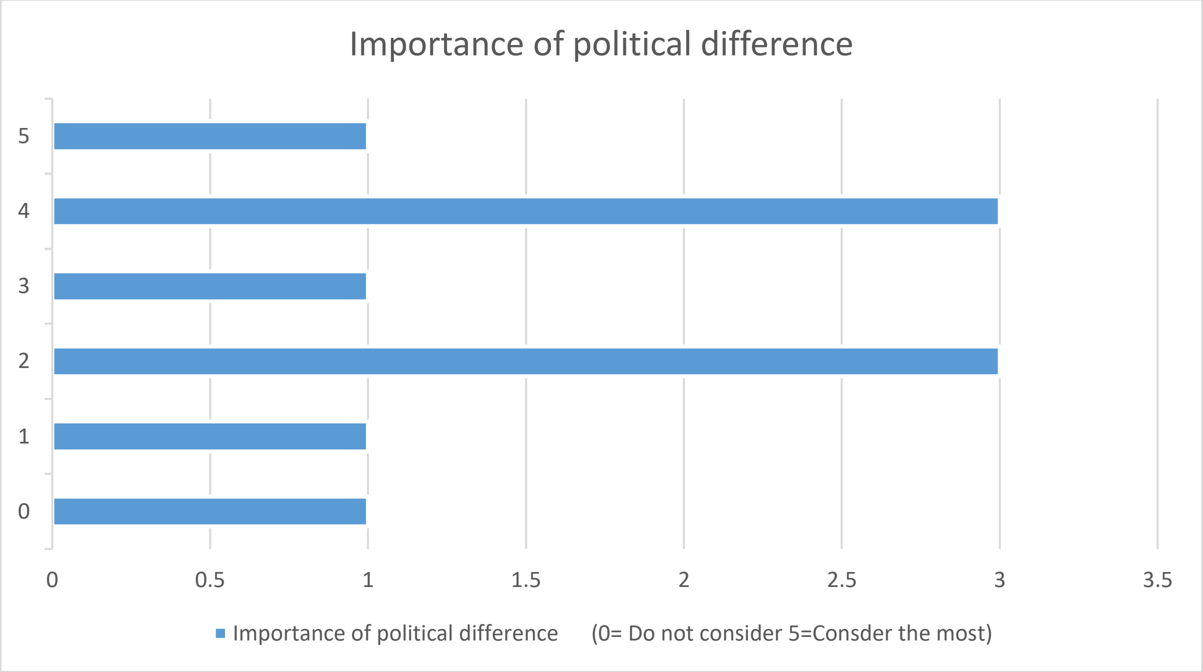


Figure E.537: Importance of political difference (Information Security-UK)

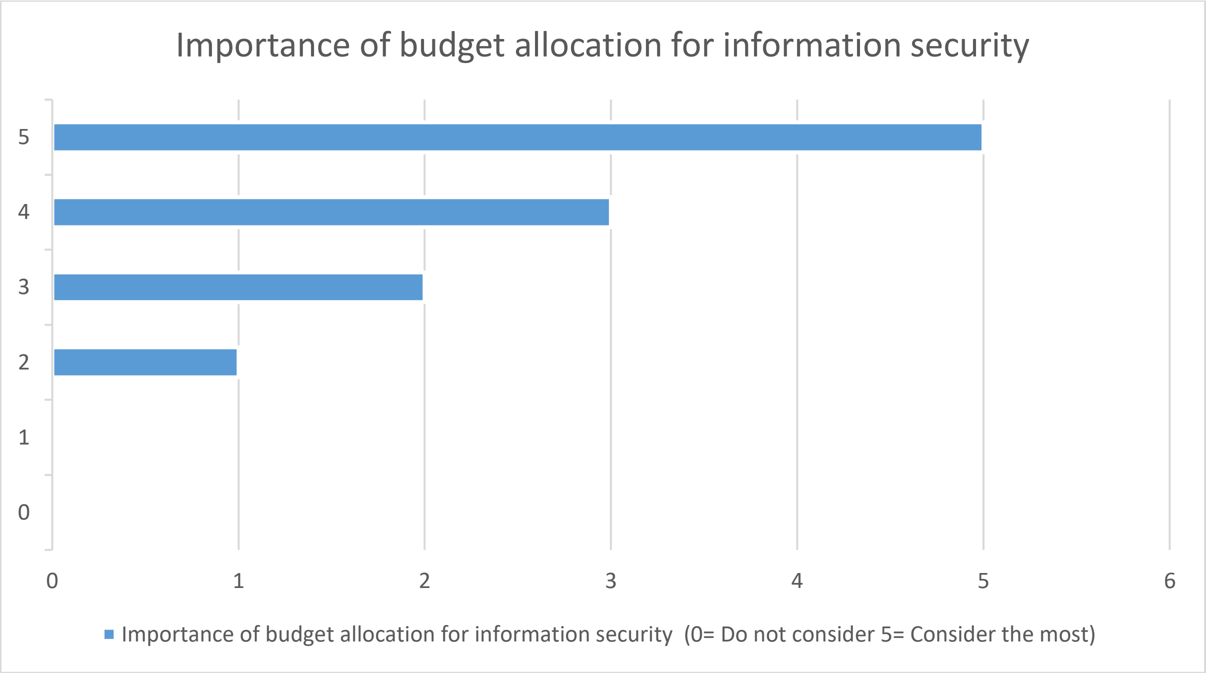


Figure E.538: Importance of budget allocation for information security (Information Security-UK)

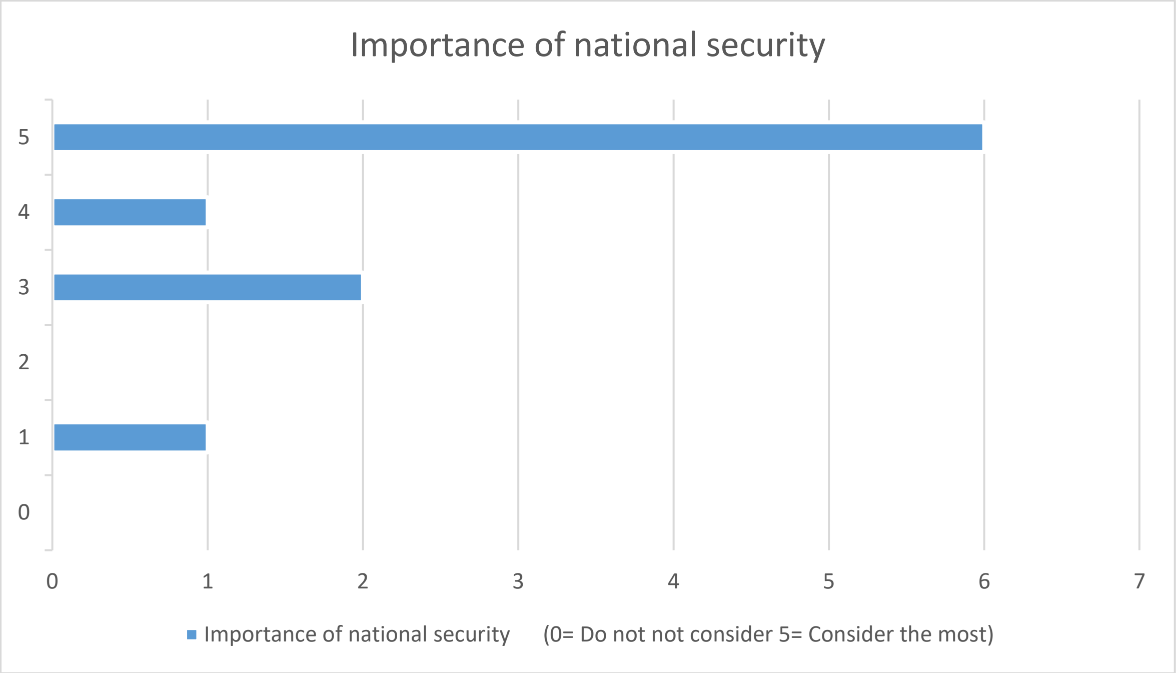


Figure E.539: Importance of national security (Information Security-UK)

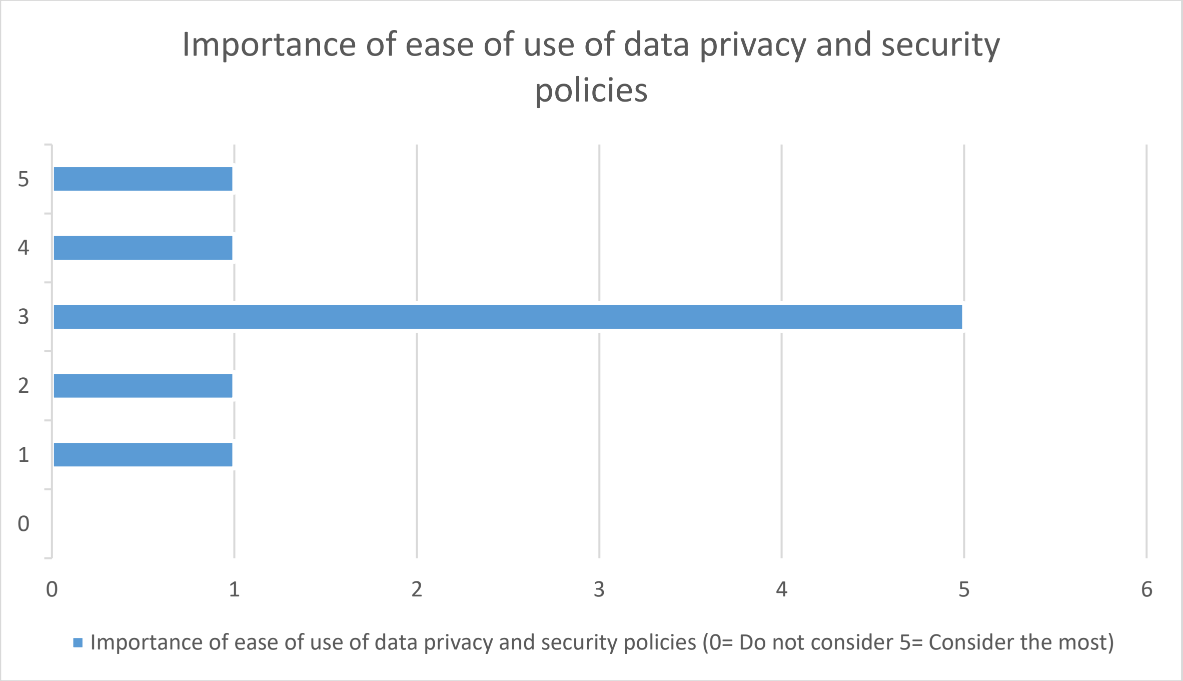


Figure E.540: Importance of ease of use of data privacy and security policies (Information Security-UK)

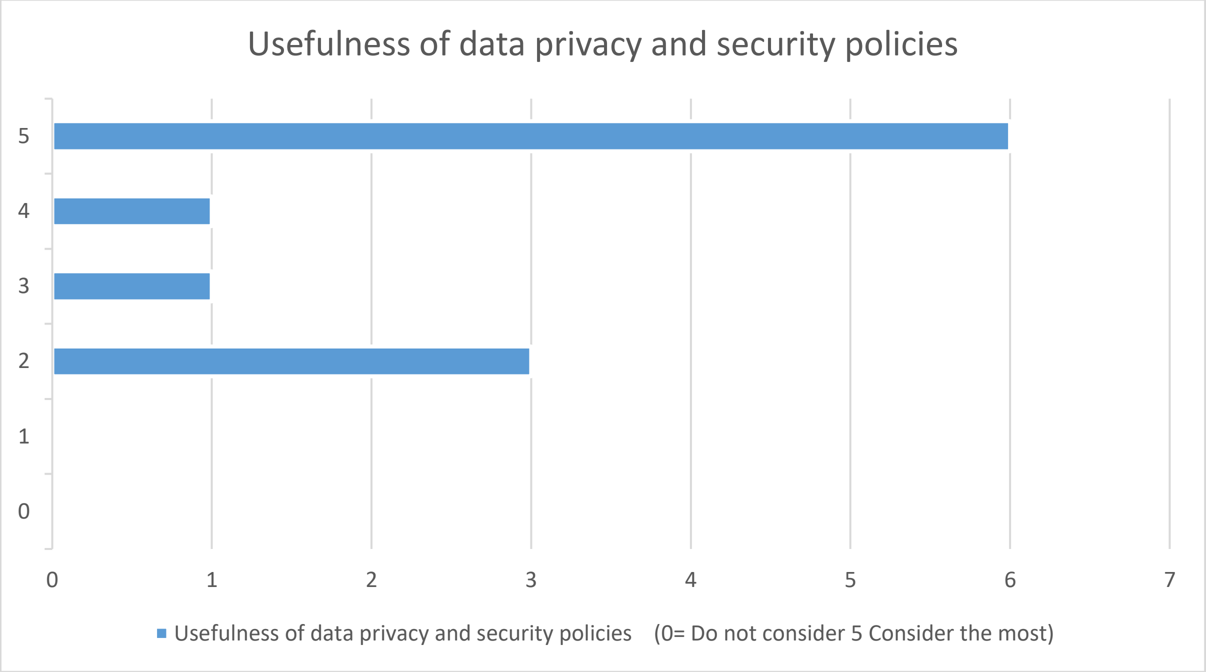


Figure E.541: Usefulness of data privacy and security policies (Information Security-UK)

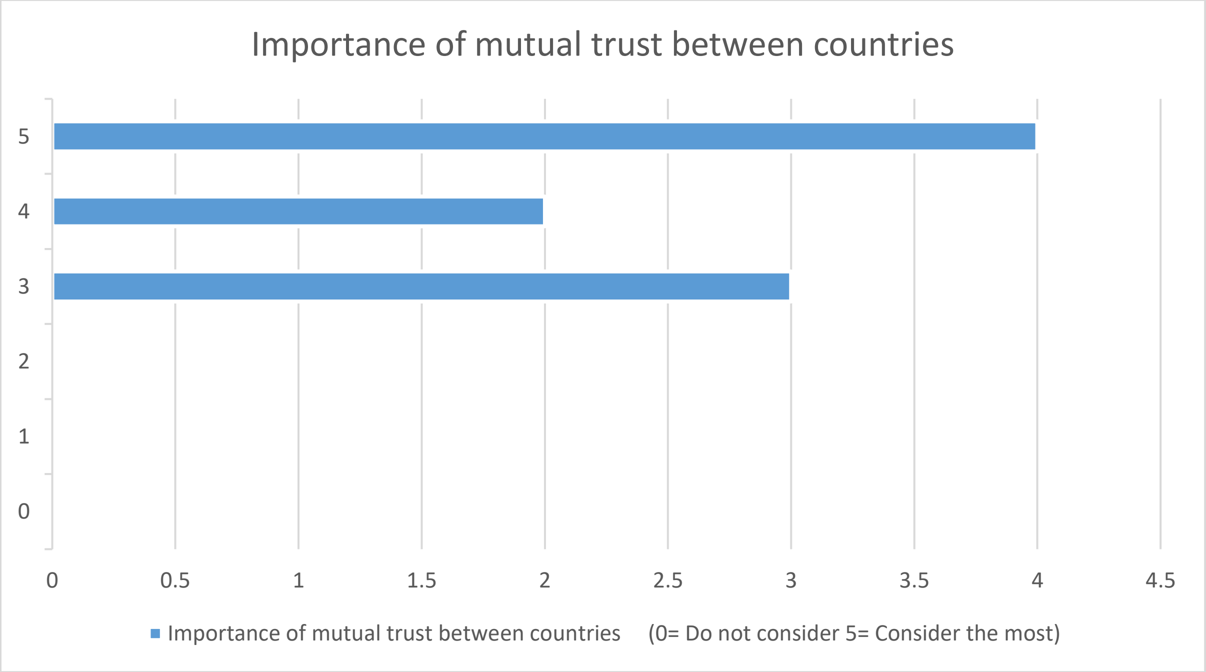


Figure E.542: Importance of mutual trust between countries (Information Security-UK)

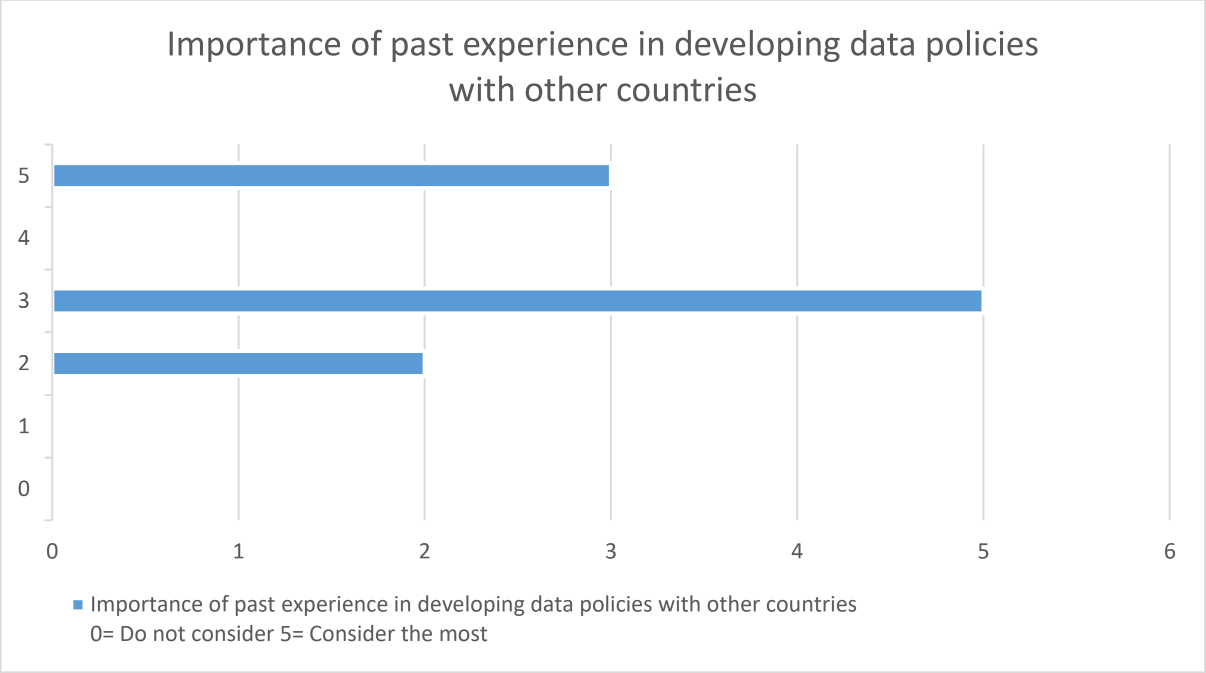


Figure E.543: Importance of past experience in developing data policies with other counties (Information Security-SL)

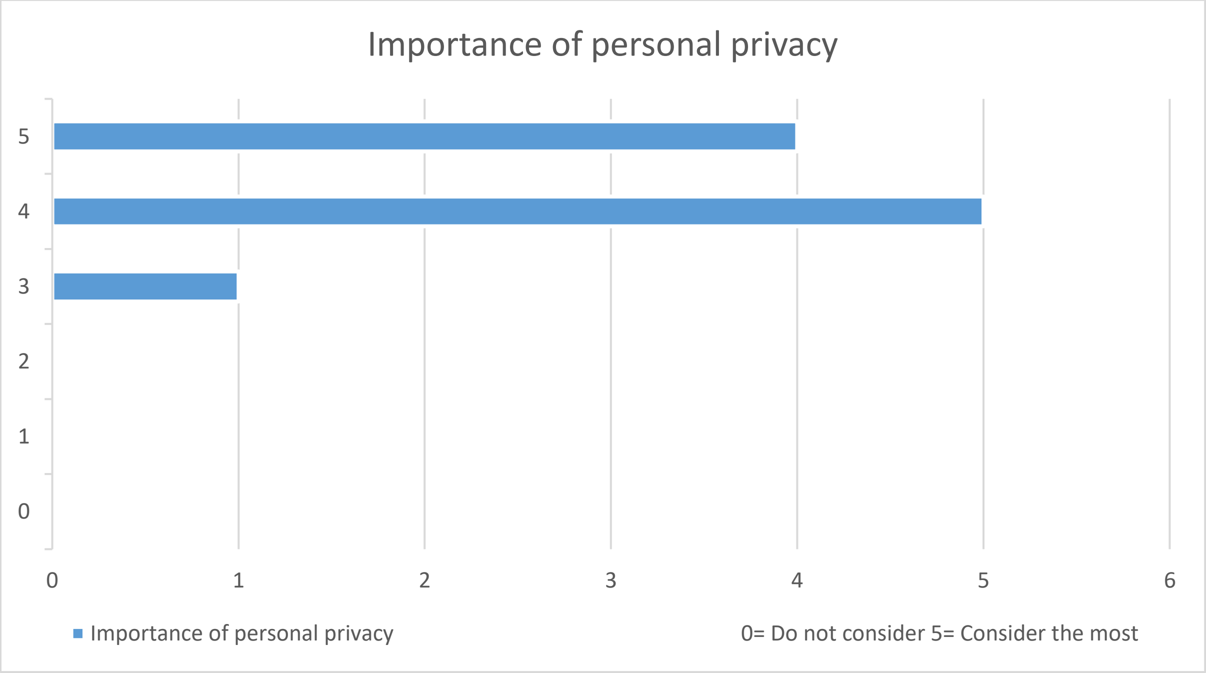


Figure E.544: Importance of personal privacy (Information Security-SL)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 85 percent of the respondents have endorsed (See figure E.533). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, economical differences, personal privacy, national security, ease of use of data privacy and security policies, usefulness of data privacy and security policies, mutual trust between countries previous experience with other countries in developing policies (See figure E.522-532) (See figure E.534-544).

United Kingdom – Media

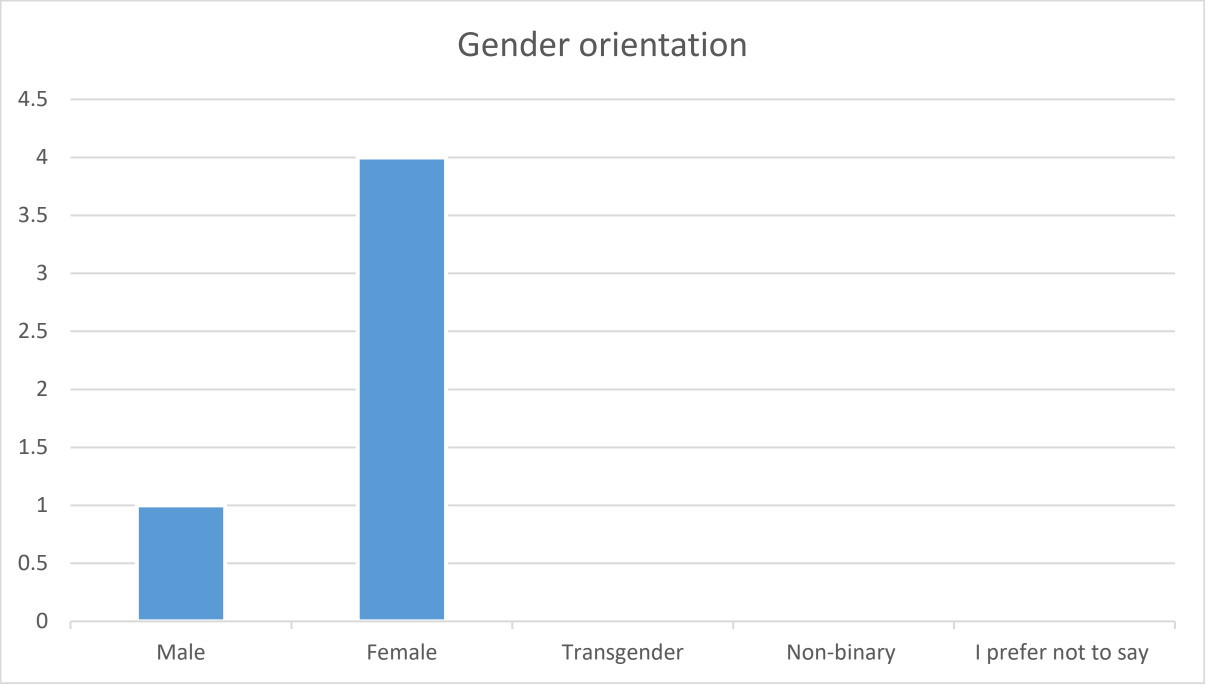


Figure E.545: Gender orientation (Media-UK)

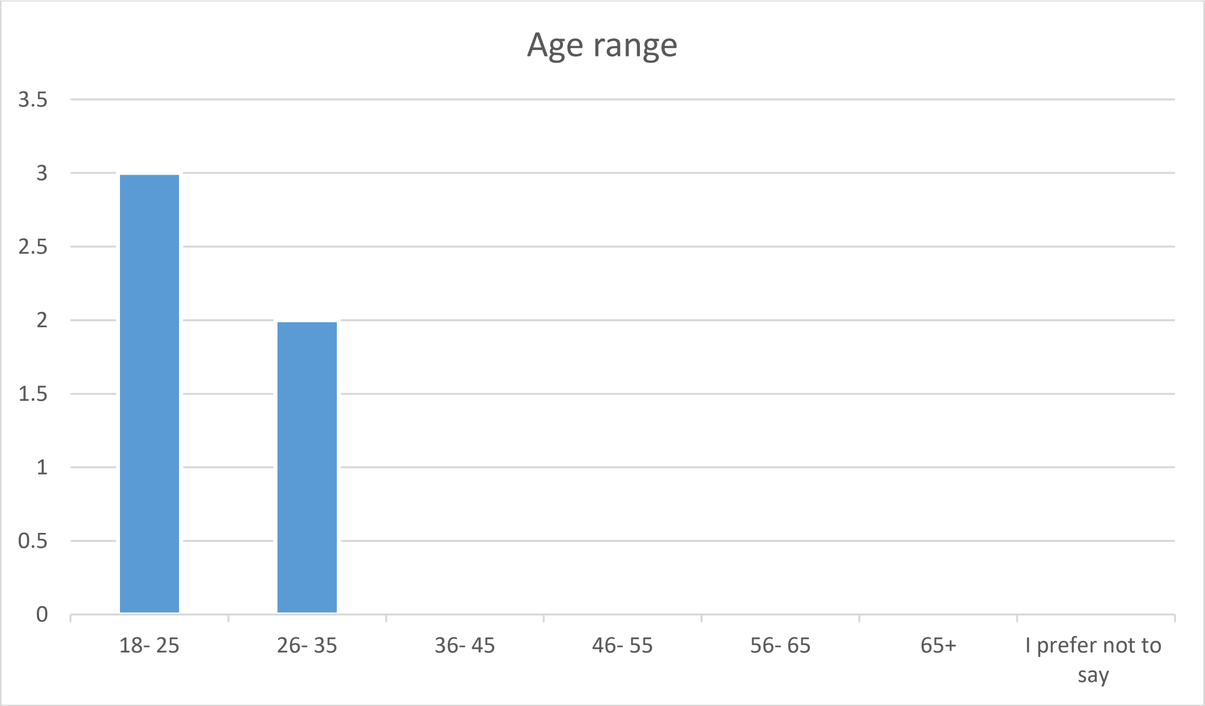


Figure E.546: Age range (Media-UK)

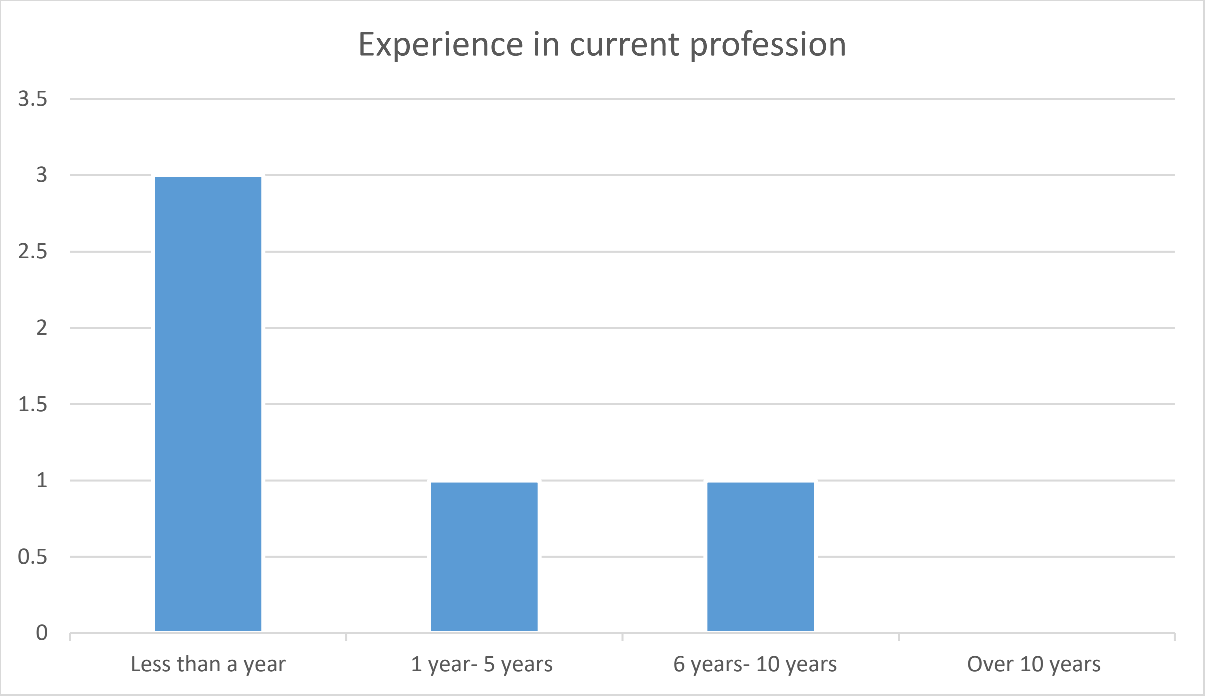


Figure E.547: Experience in current profession (Media-UK)

This analysis is based on the responses received from United Kingdom participants employed in the media sector. There were 5 participants and 1 out of them were males and 4 females (See figure E.545). They were within the 18-35 age range out of which 3 in the 18-25 and 2 in the 26-35 range (See figure E.546). The participants employed in the industry between less than a year and 6 to 10 years (See figure E.547).

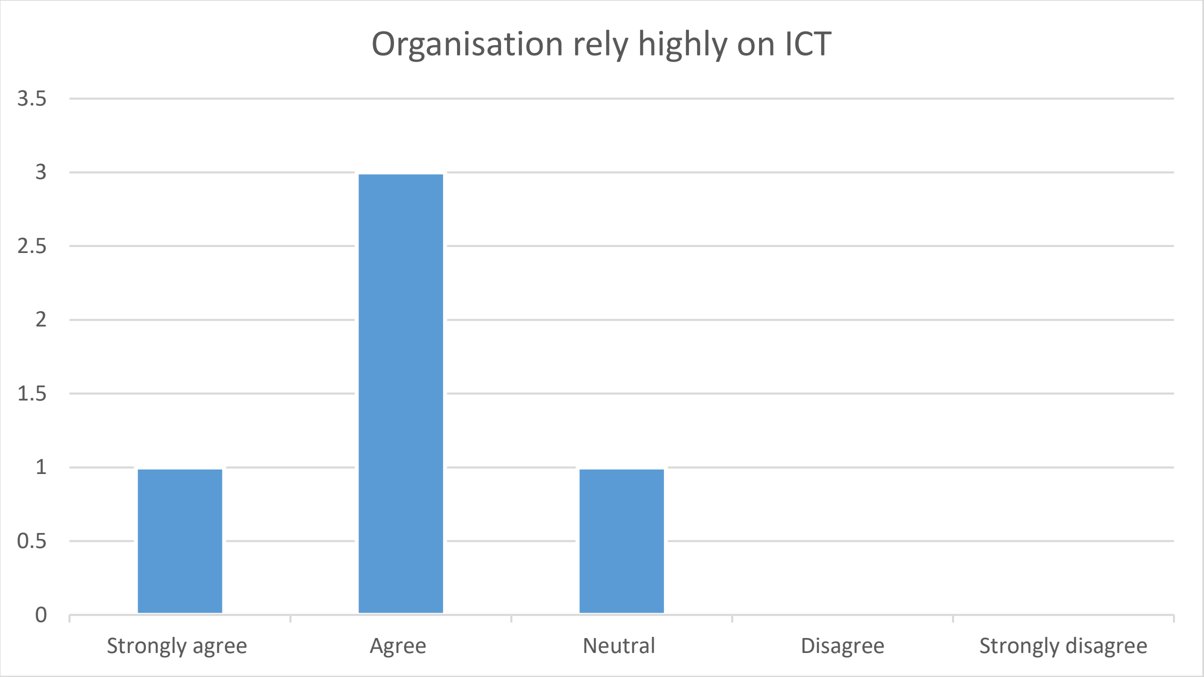


Figure E.548: Organisation rely highly on ICT (Media-UK)

Out of the 5 respondents, 4 have worked in a technology reliance working environment, and 1 unaware of reliance on technology because of the nature of the work assigned to them (See figure E.548). This indicates a majority of those who have been working in the media sector have had a high reliance on ICT.

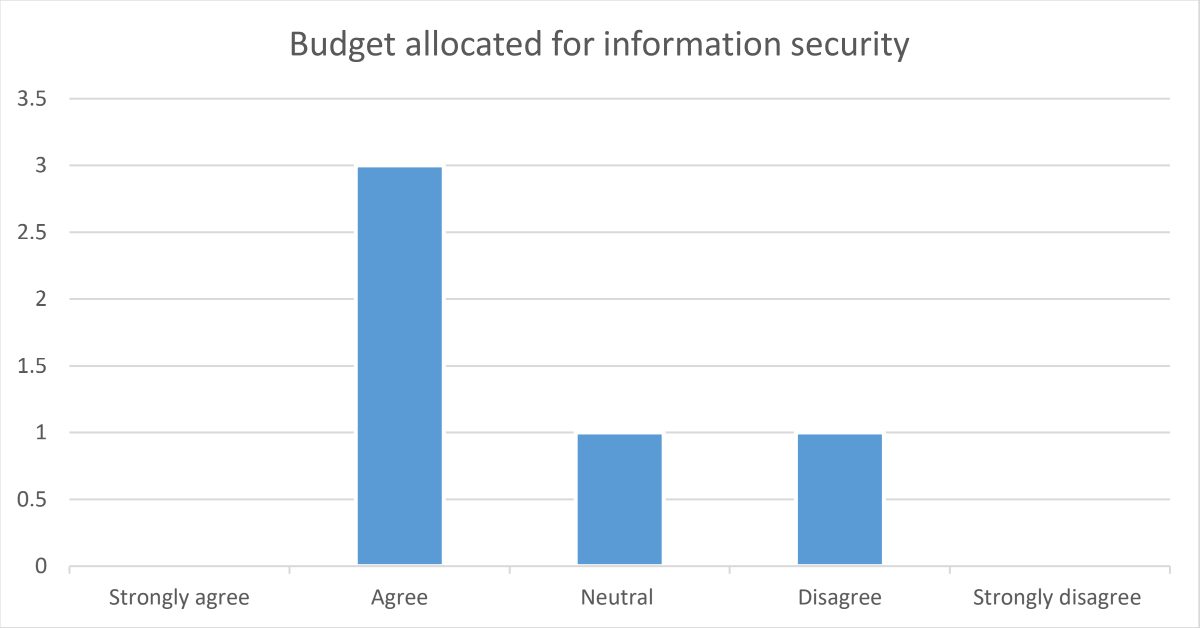


Figure E.549: Budget allocated for information security (Media-UK)

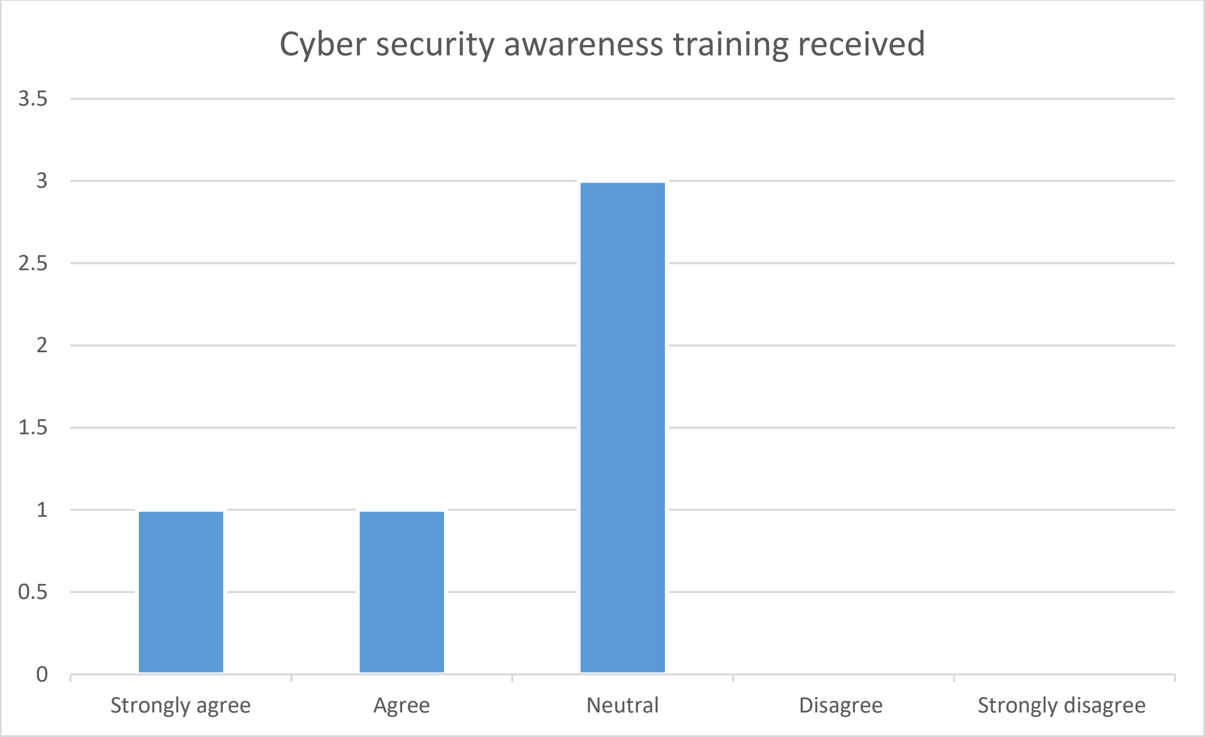


Figure E. 550: Cyber security awareness training received (Media-UK)

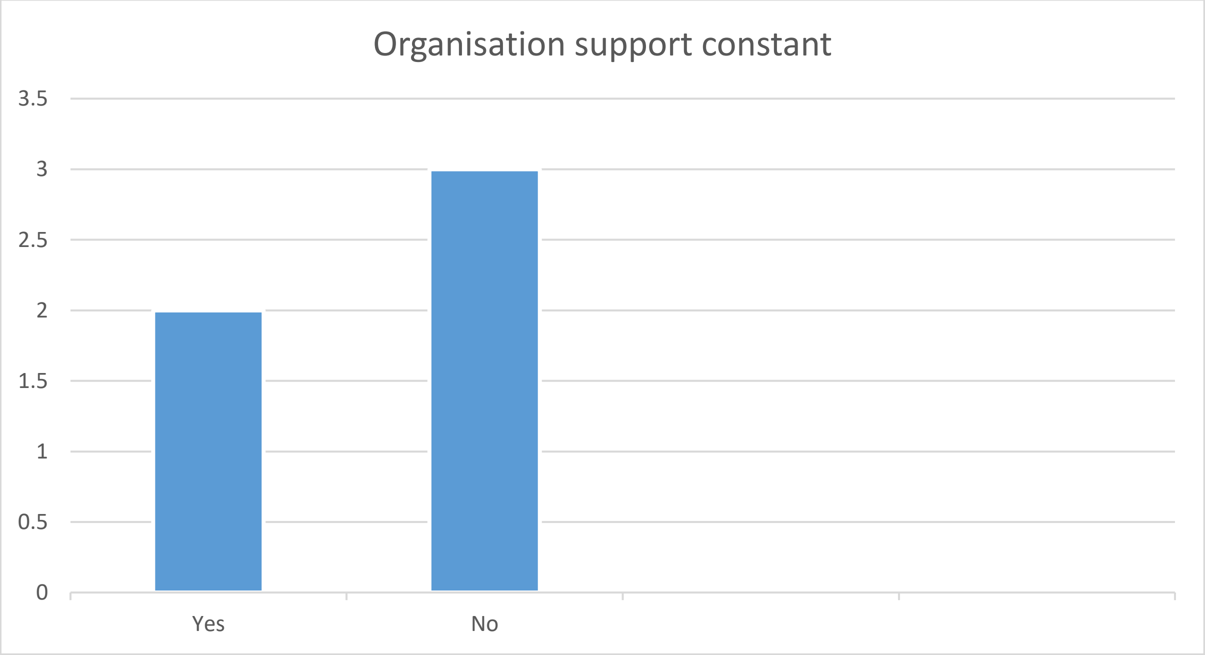


Figure E.551: Organisation support constant (Media-UK)

Funding has been sketchy. 3 out of the 5 have indicated that their organisations had an allocated budget for information security, whilst 1 had not expressed an opinion either way and notably according to the 1 disagreed, their organisations had no budget allocation for information security (See figure E.549). Some of the participants made the point that despite the satisfactory level of resources allocated for information security, regular security awareness training that they received was inadequate. Only 2 participants have received regular cybersecurity awareness training, whilst 3 neither agreed nor disagreed (See figure E.550). In addition, 3 participants had not received support from the organisation to protect personal information, whilst only 2 did (See figure E.551). This is a clear indication of lack of organisational support to protect personal information despite the standalone budget allocation for information security and high reliance on technology.

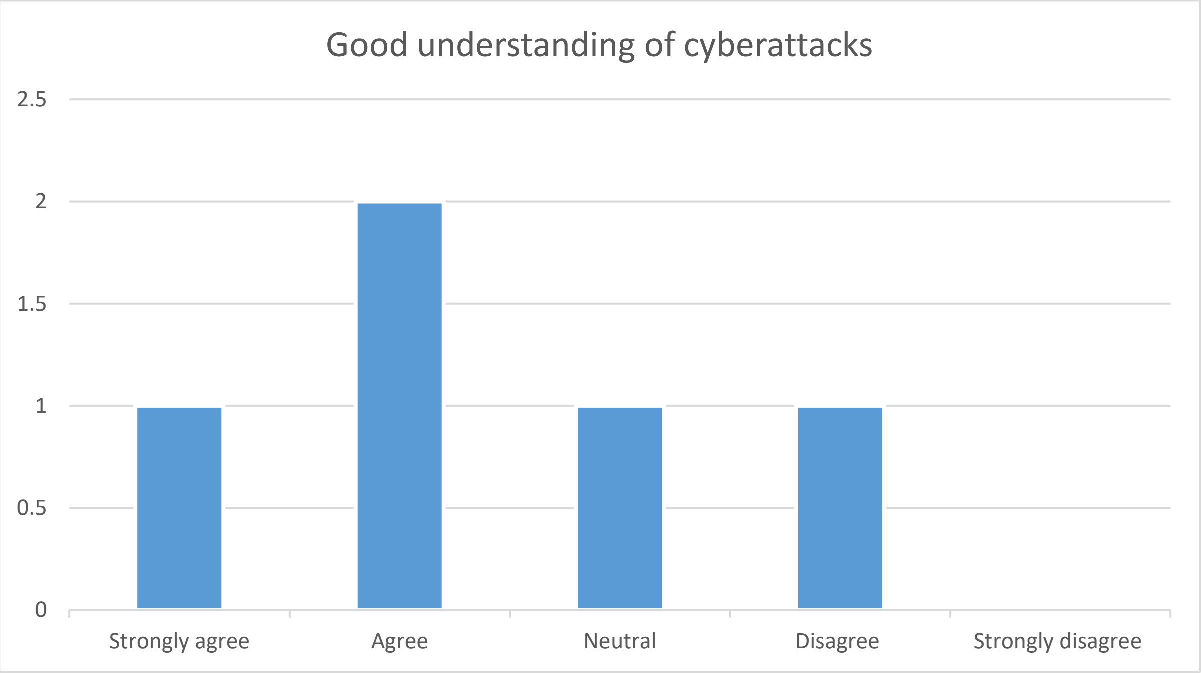


Figure E.552: Good understanding of cyberattacks (Media-UK)

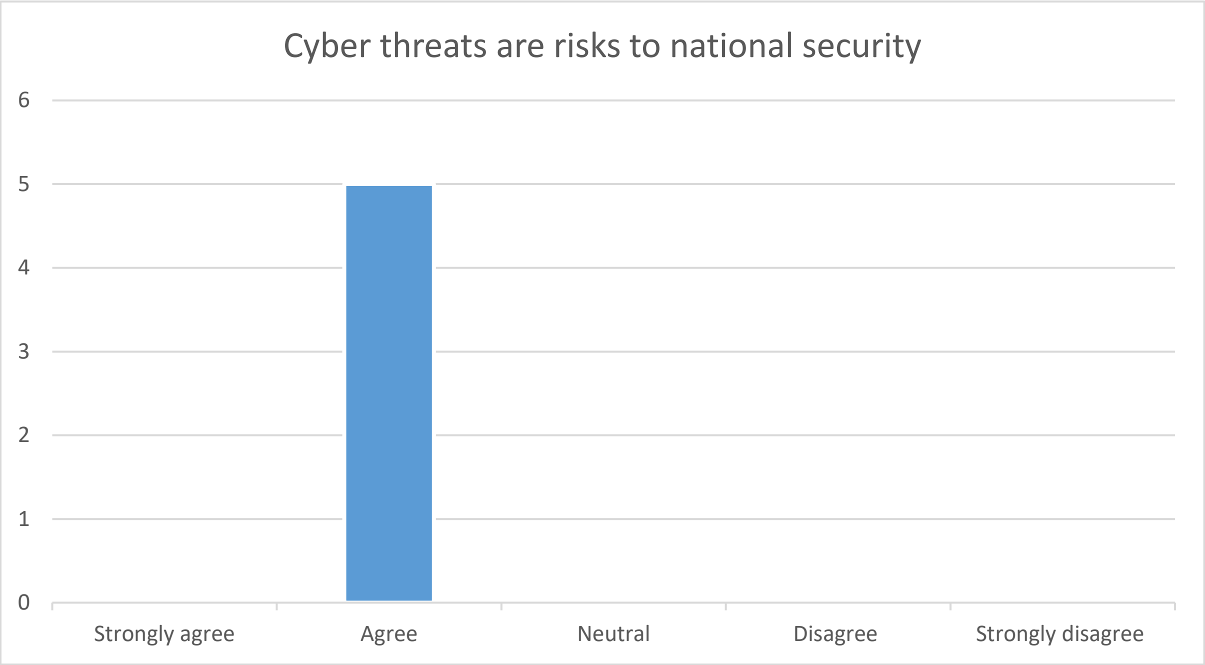


Figure E.553: Cyber threats are risks to national security (Media-UK)

Despite the lack of security awareness training, the participants appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. 3 participants do have, 1 have not expressed opinion either way, and only 1 participant had no understanding(See figure E.552). Furthermore, 100 percent of the participants realise the potential threats to national security from cyber-attacks (See figure E.553). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

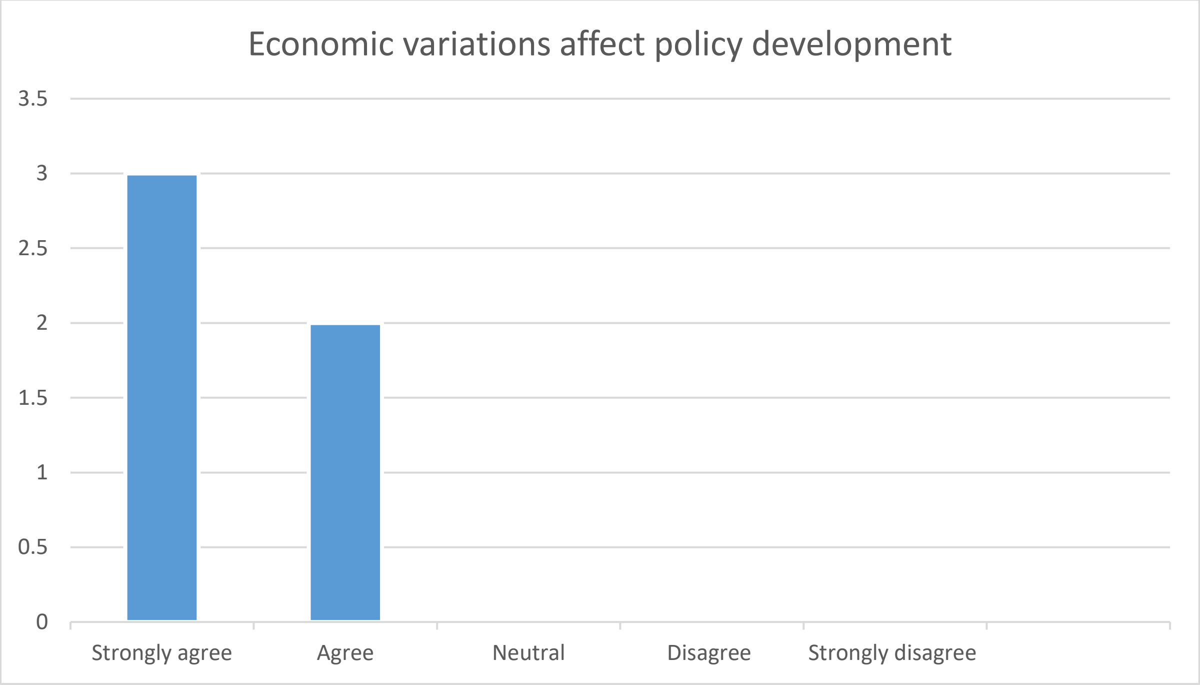


Figure E.554 Economic variations affect policy development (Media-UK)

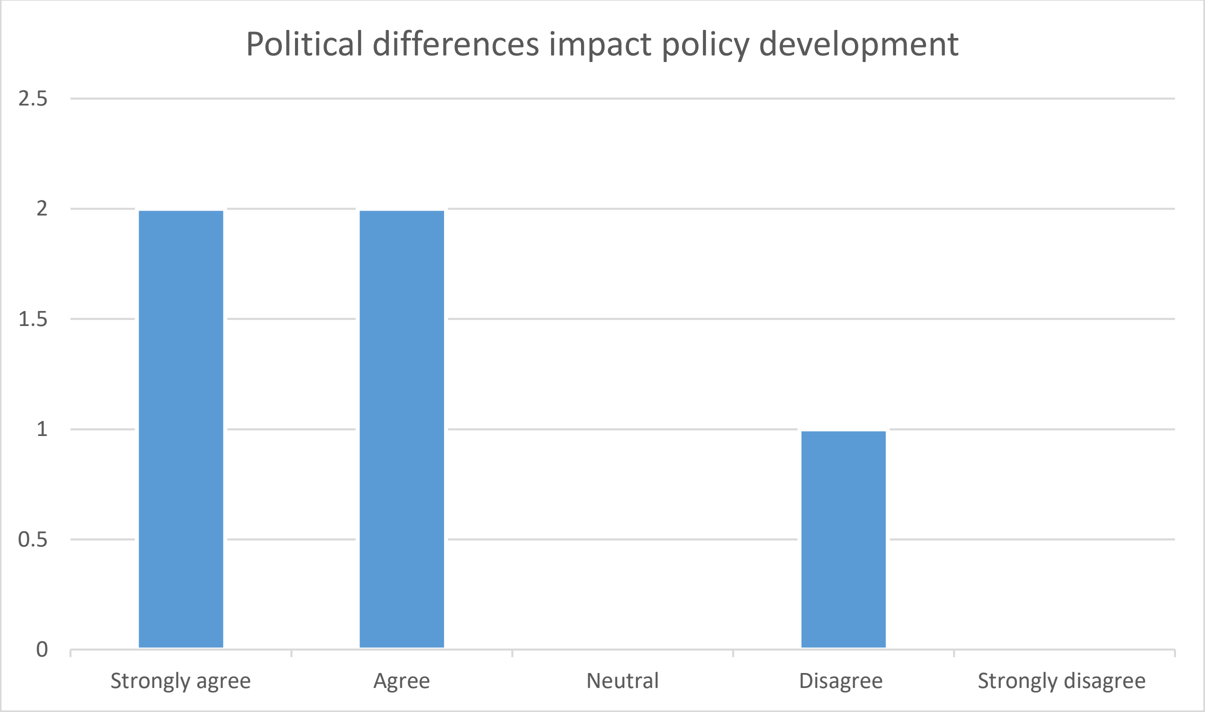


Figure E.555: Political differences impact policy development (Media-UK)

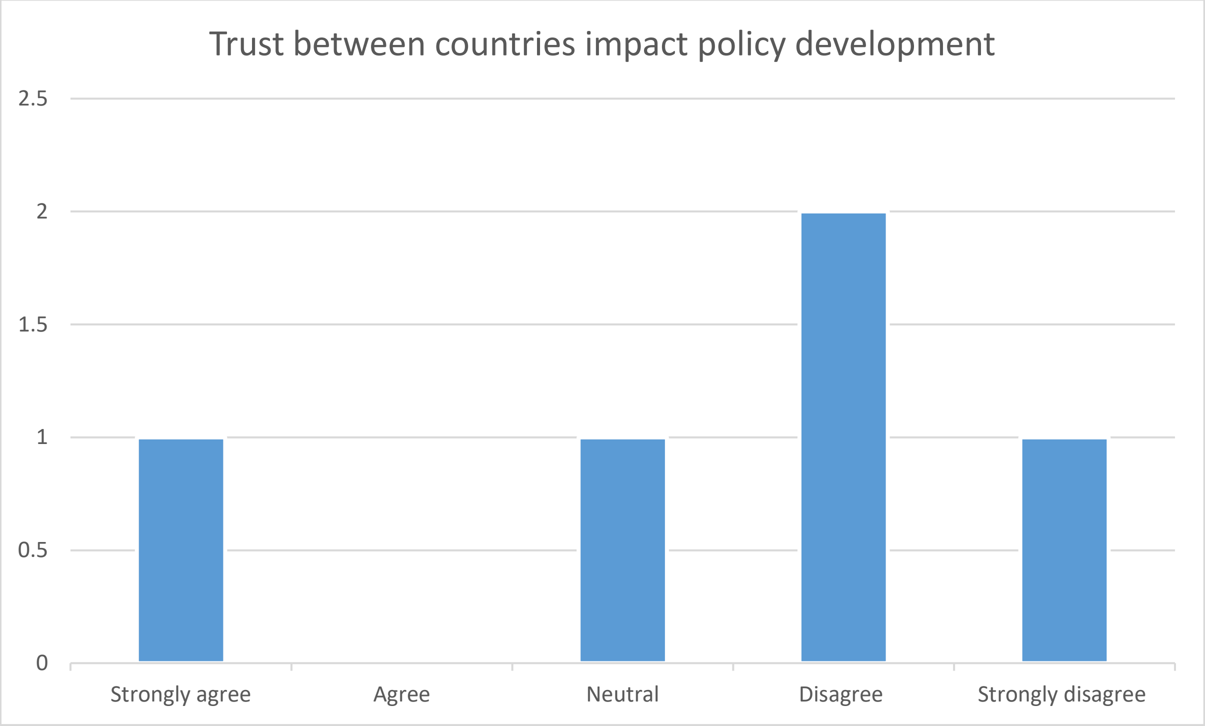


Figure E.556: Trust between countries impact policy development (Media-UK)

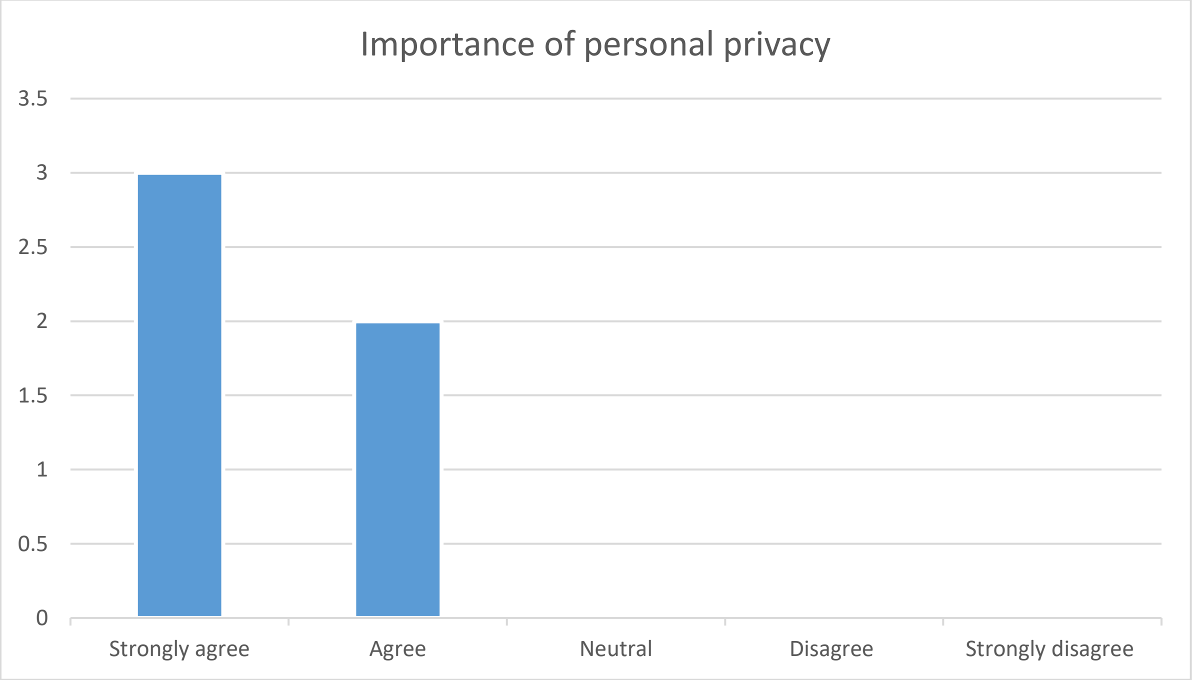


Figure E.557: Importance of personal privacy (Media-UK)

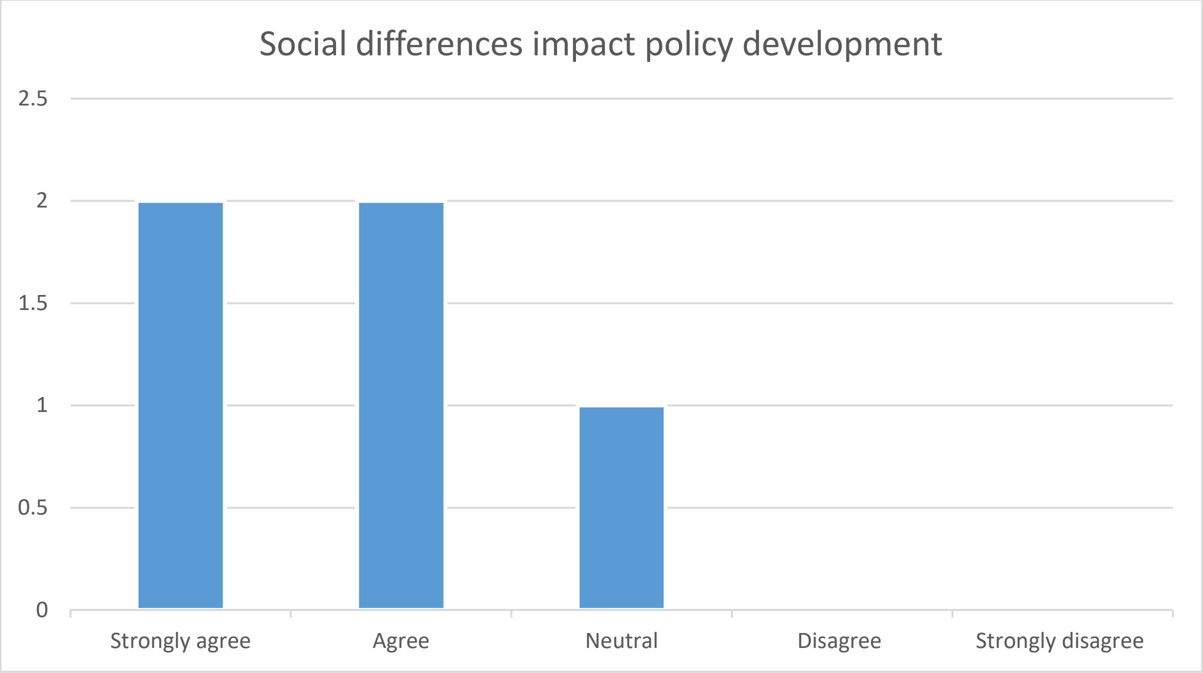


Figure E.558: Social differences impact policy development (Media-UK)

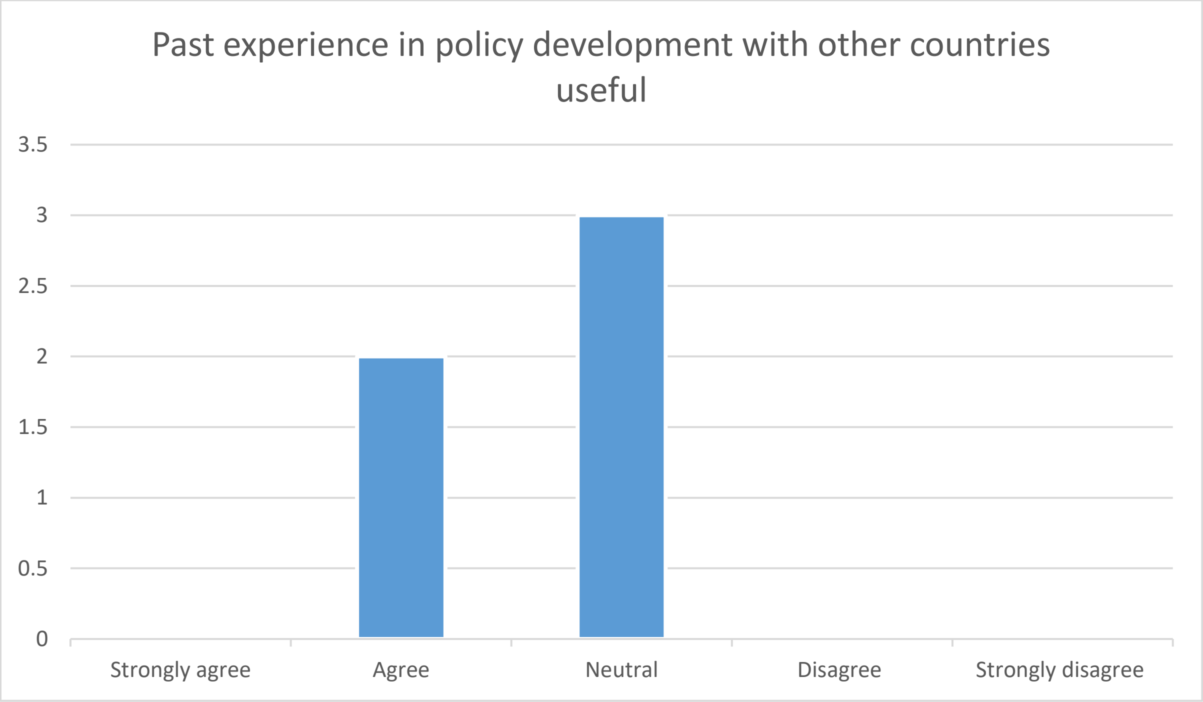


Figure E.559: Past experience in policy development with other countries useful (Media-UK)

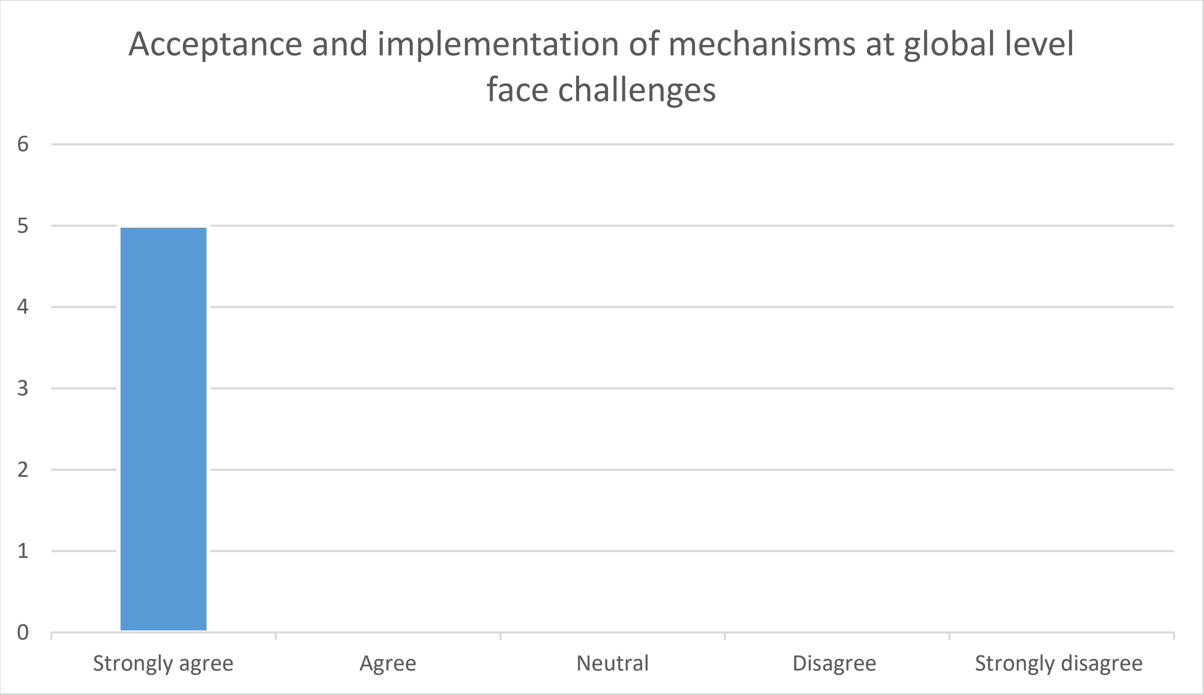


Figure E.560: Acceptance and implementation of mechanisms at global level face challenges (Media-UK)

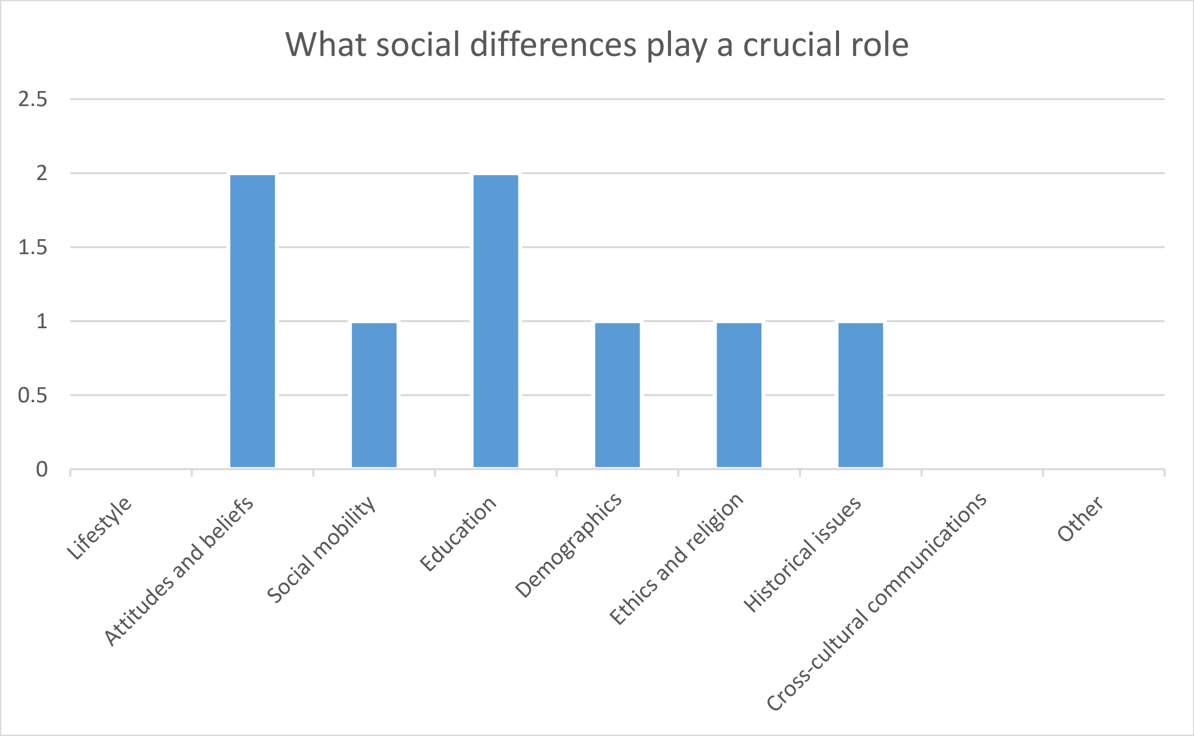


Figure E.561: What social differences play a crucial role (Media-UK)

Interestingly, the majority of the participants in the Media sector do not specify a particular social difference category (See figure E.561). There are two possible explanations for this, either the participants do not have an understanding of the social differences, and their impact on policy acceptance and implementation, or they do not believe social differences matter.

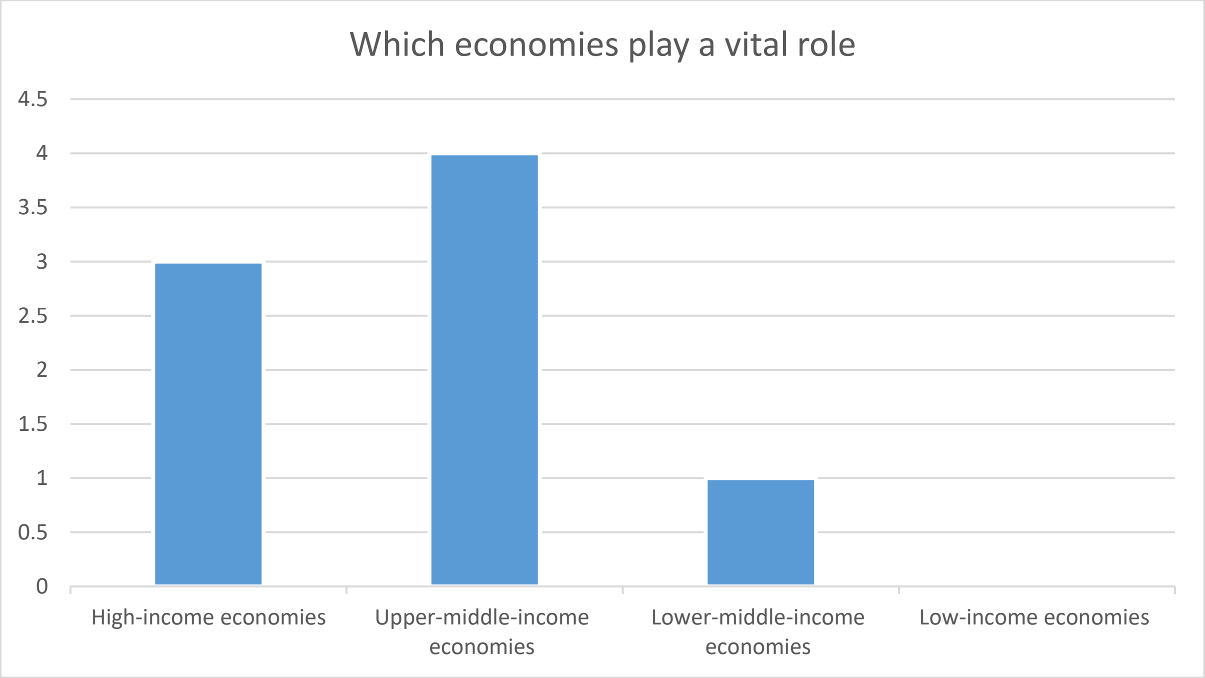


Figure E.562: Which economies play a vital role (Media-UK)

In the questionnaire majority has stated that the high income and upper-middle-income countries play a vital role (See figure E.562). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

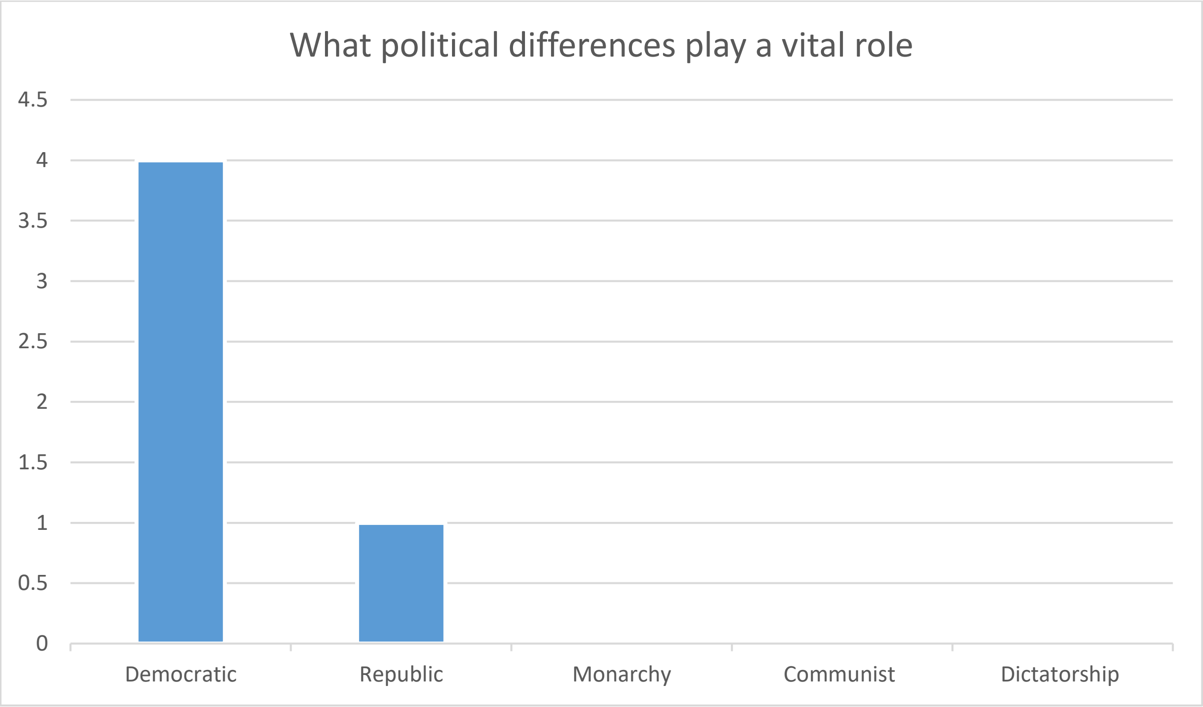


Figure E.563: What political differences play a vital role (Media-UK)

The majority have chosen a democratic political system (See figure E.563), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions. This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

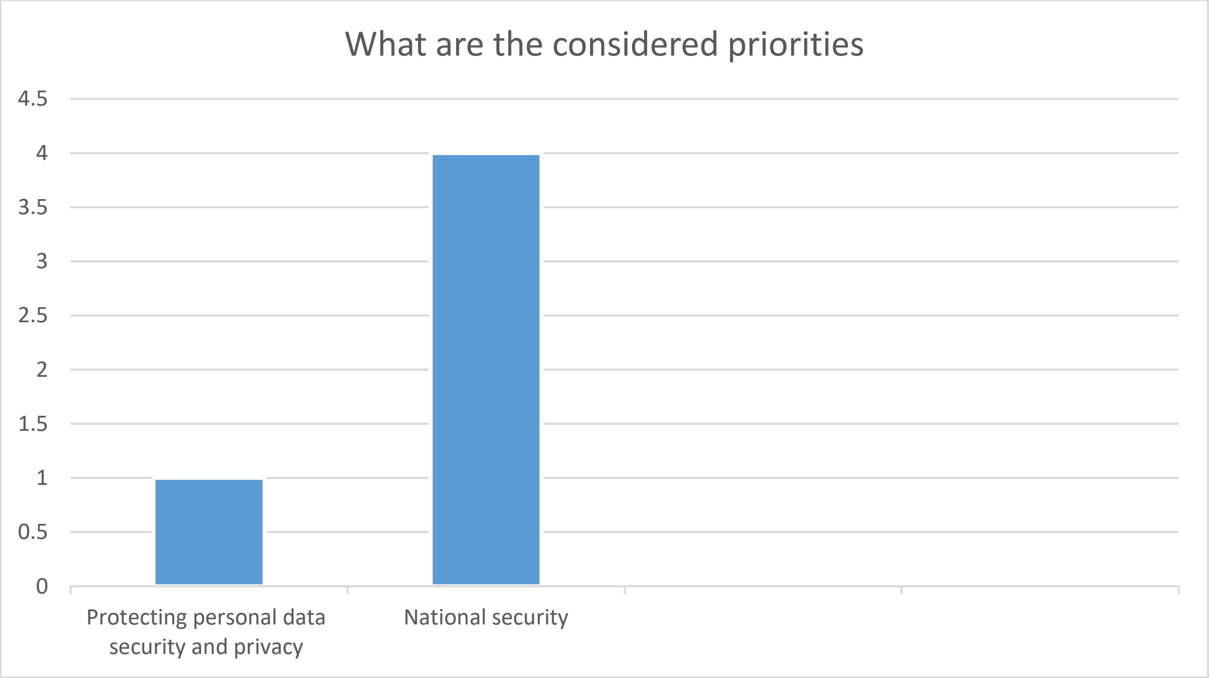


Figure E.564: What are the considered priorities (Media-UK)

In accepting and implementing global data privacy and security policies, the importance of protection of national security overrides the importance of personal data security and privacy (See figure E.564). One reason for their choice could be they concentrate on national security, which is a part of their job.

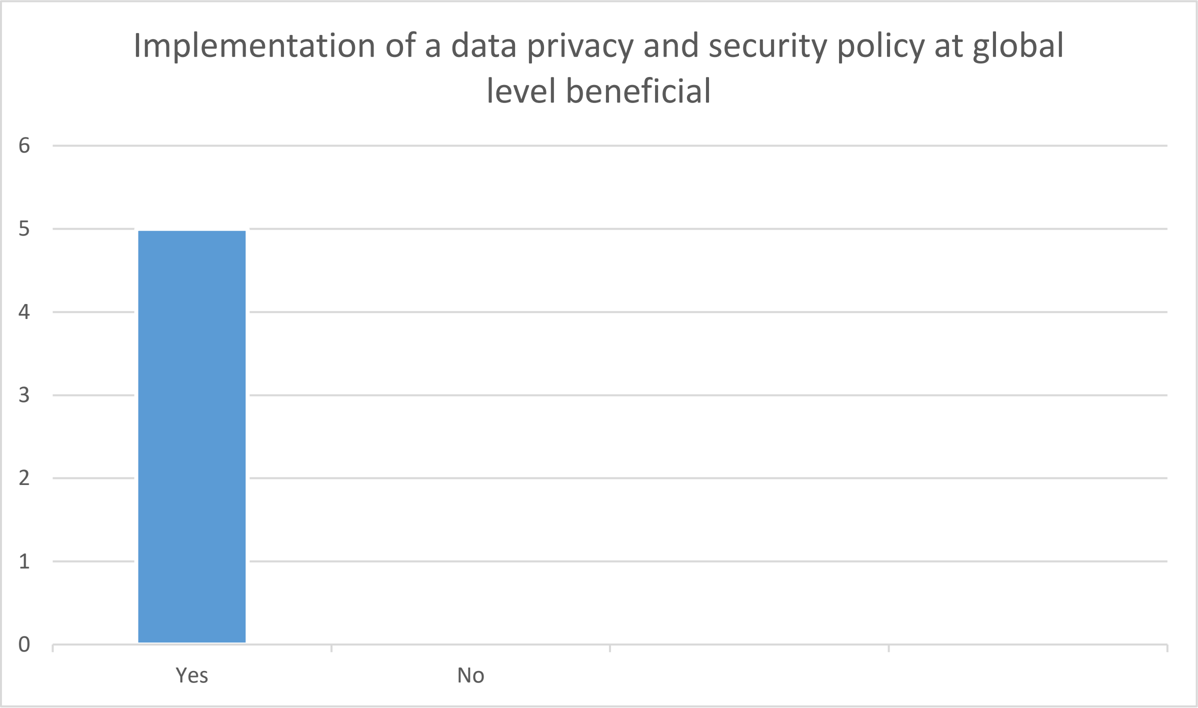


Figure E.565: Implementation of a data privacy and security policy at global level beneficial (Media-UK)

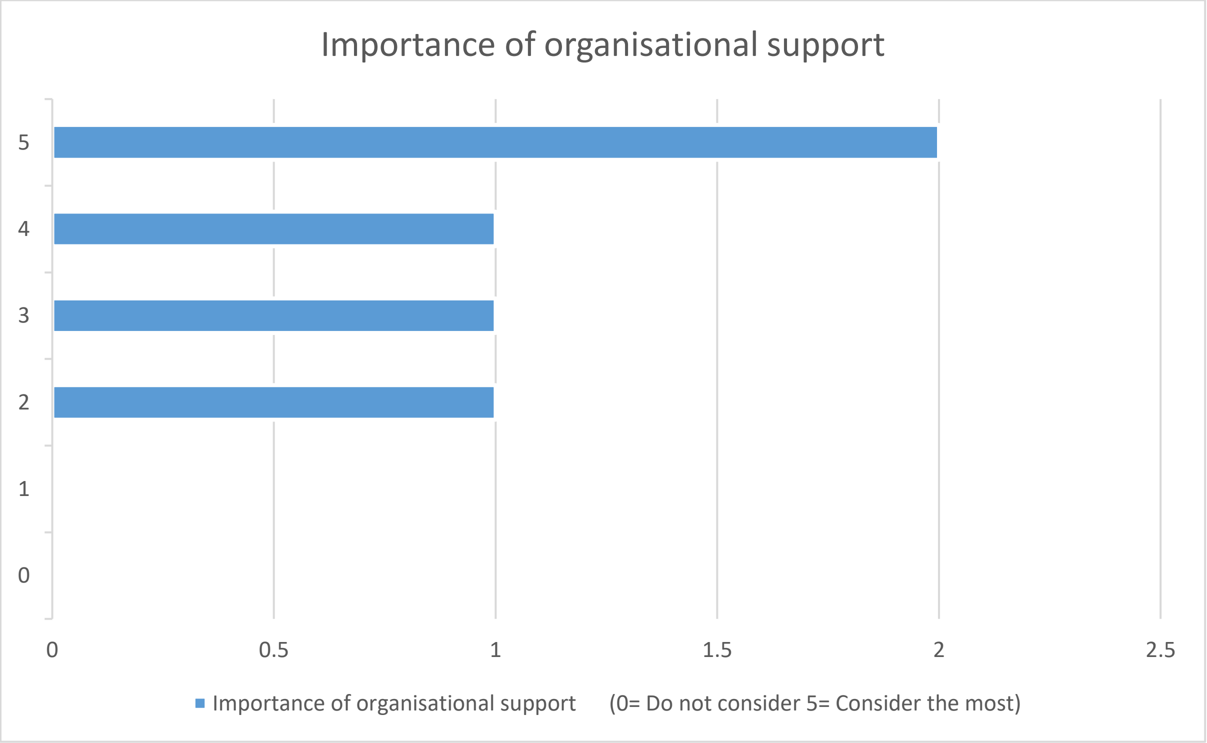


Figure E.566: Importance of organisational support (Media-UK)

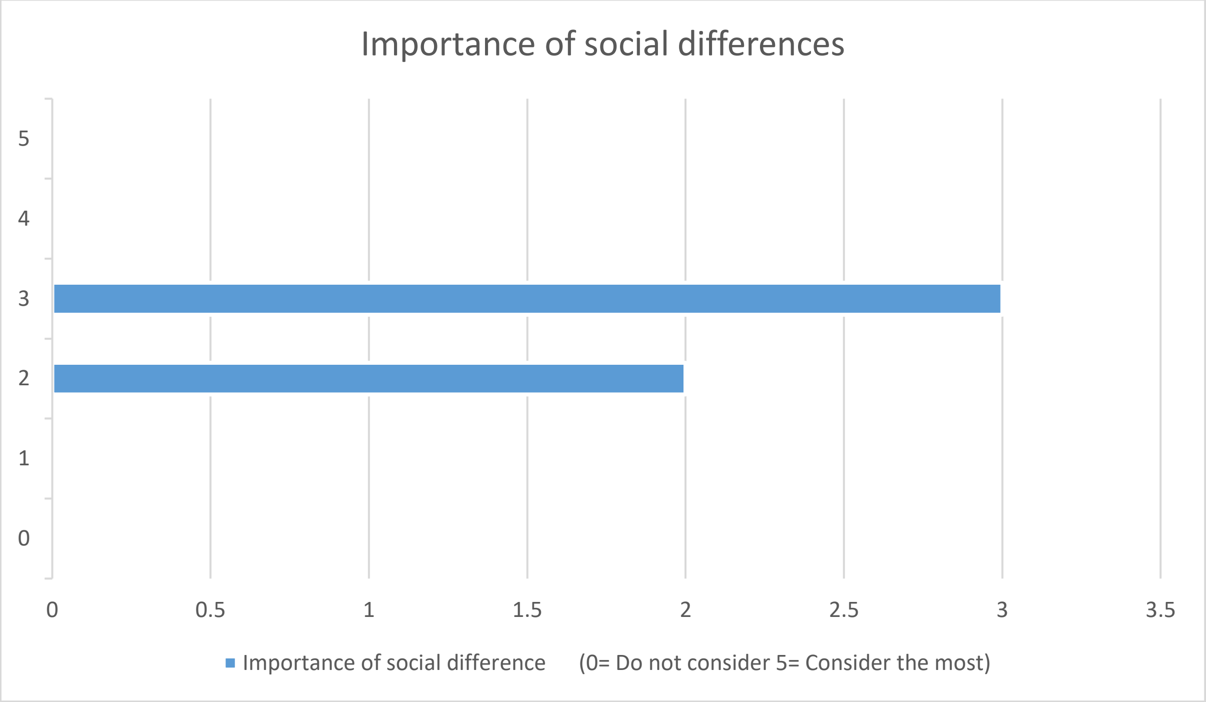


Figure E.567: Importance of social differences (Media-UK)

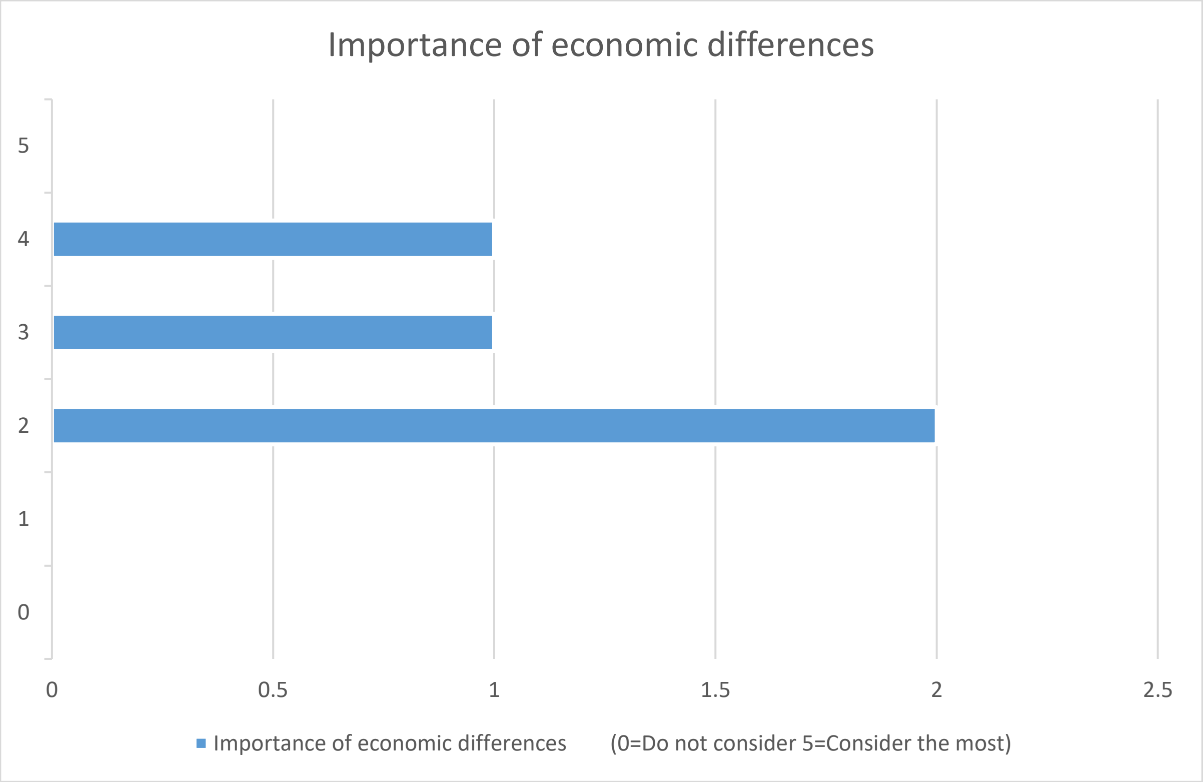


Figure E.568: Importance of economic differences (Media-UK)

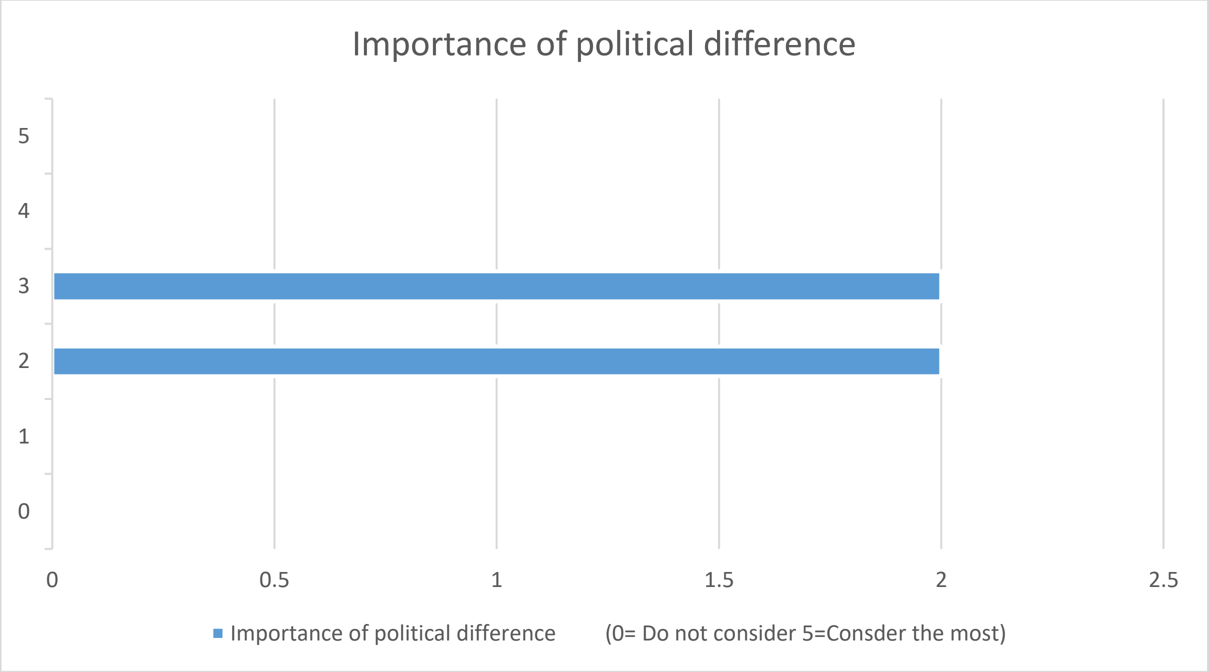


Figure E.569: Importance of political difference (Media-UK)

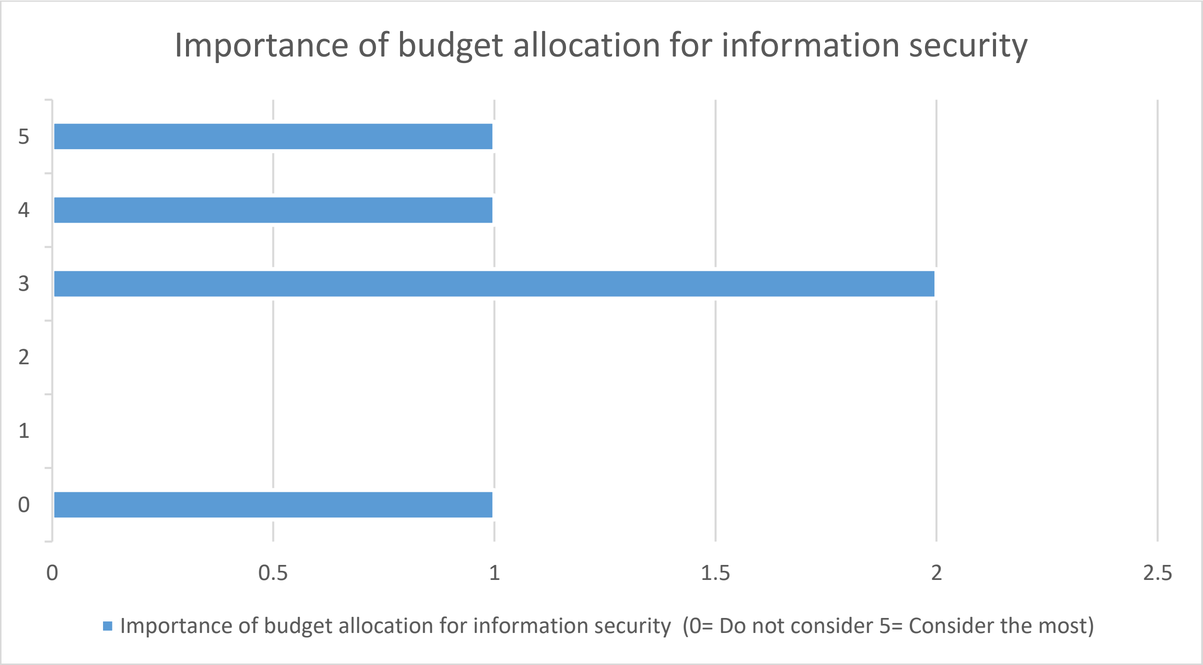


Figure E.570: Importance of budget allocation for information security (Media-UK)

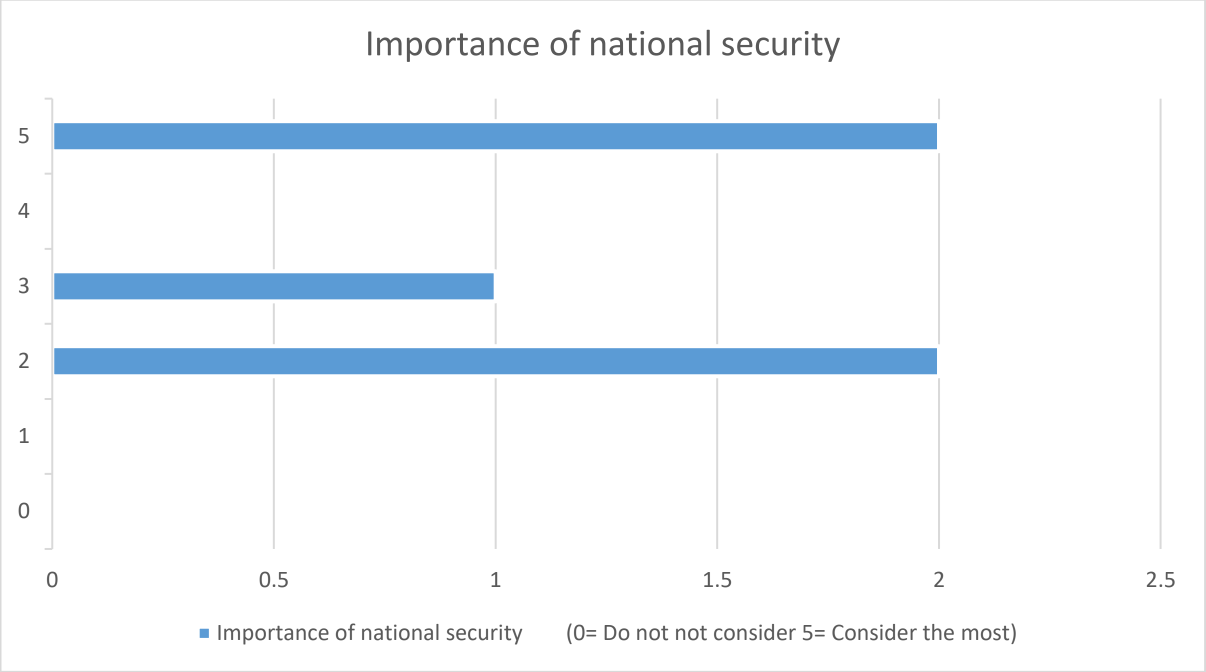


Figure E.571: Importance of national security (Media-UK)

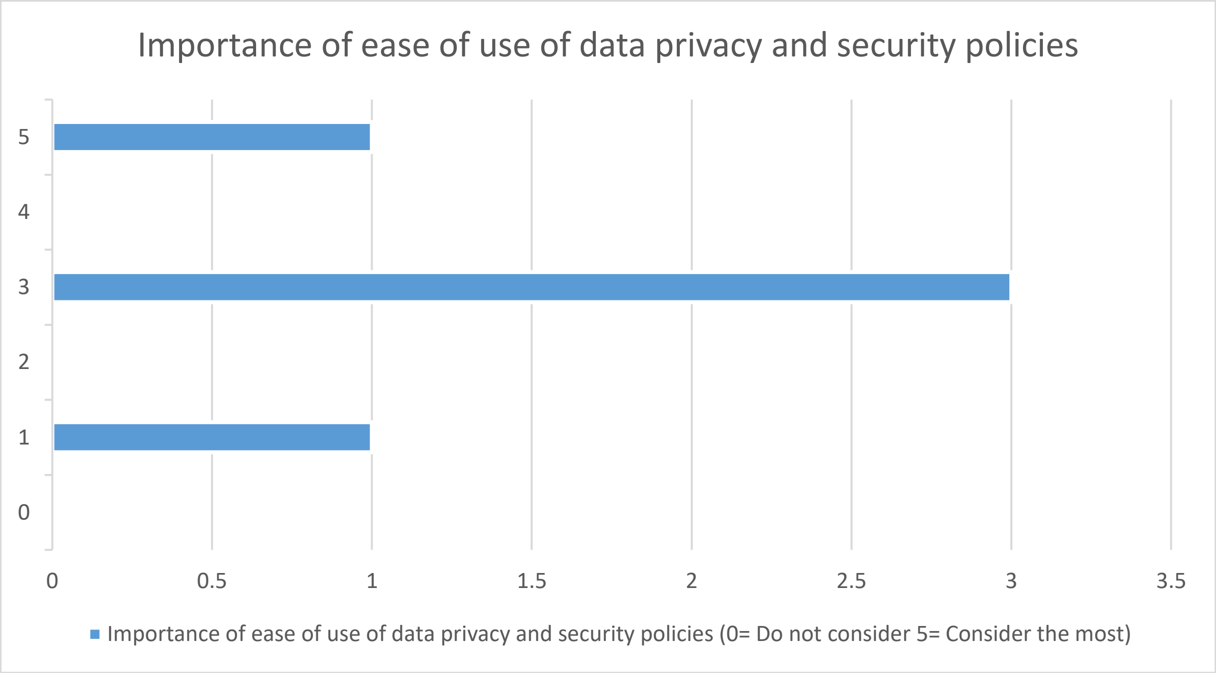


Figure E.572: Importance of ease of use of data privacy and security policies (Media-UK)

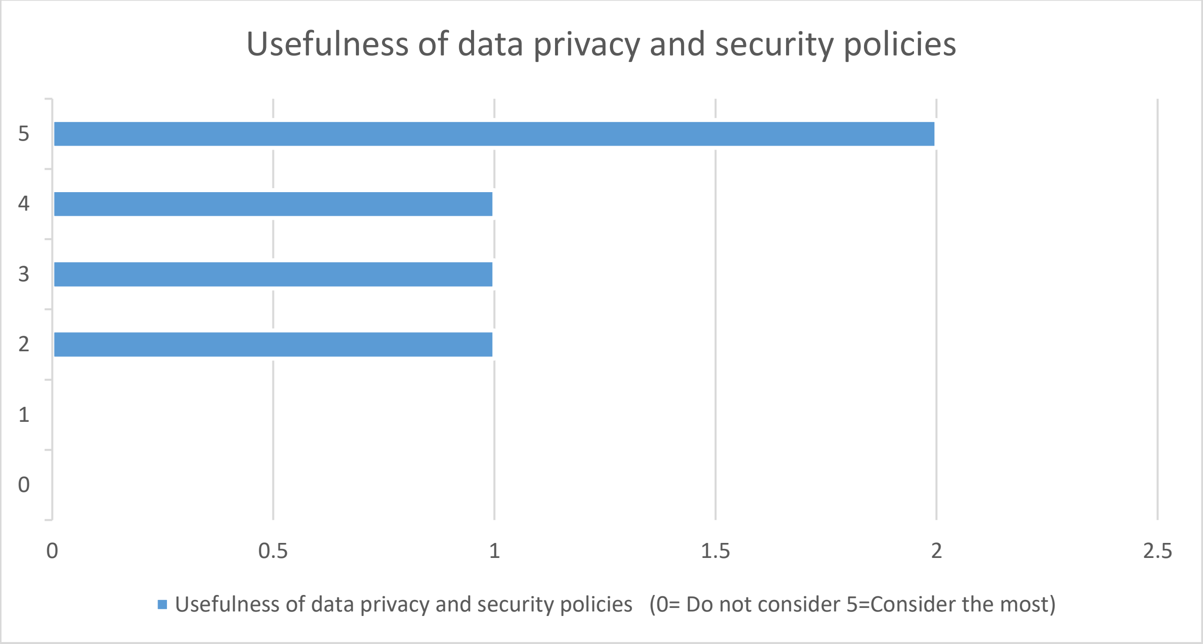


Figure E.573: Usefulness of data privacy and security policies (Media-UK)

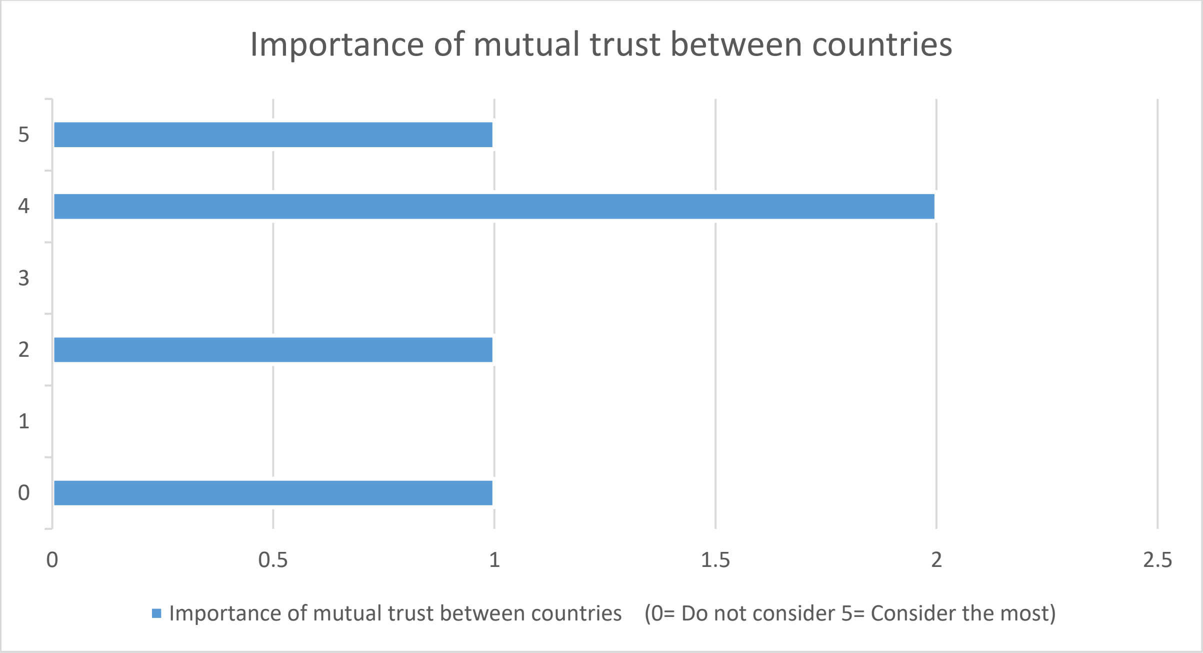


Figure E.574: Importance of mutual trust between countries (Media-UK)

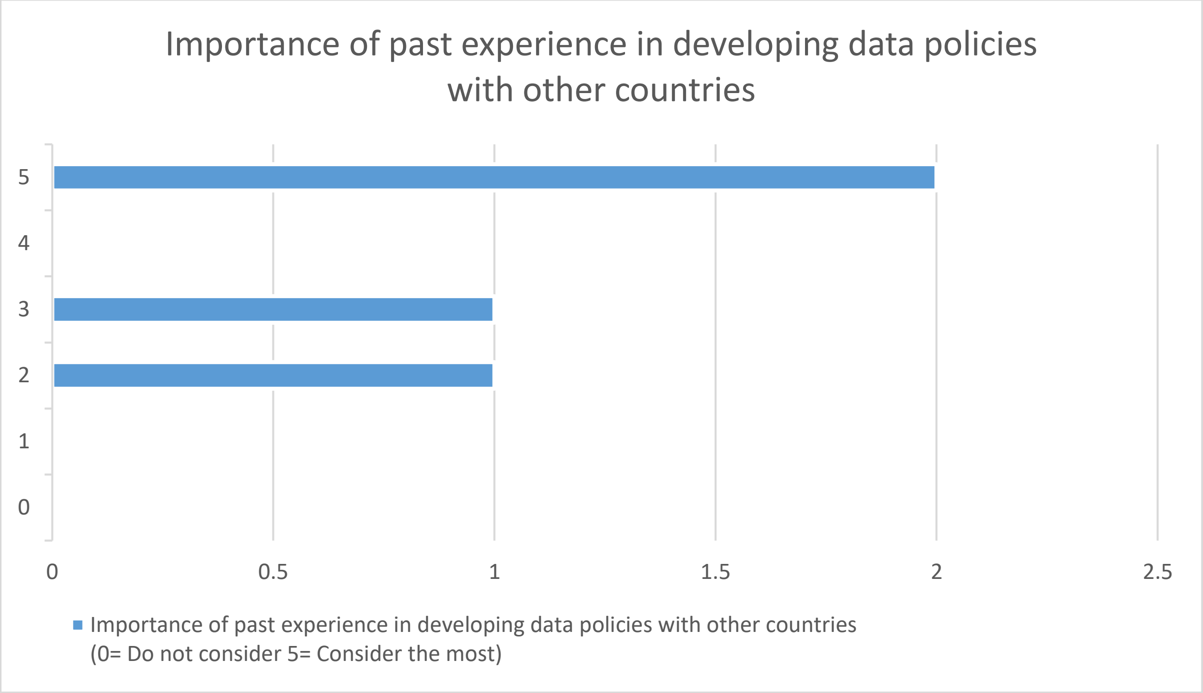


Figure E.575: Importance of past experience in developing data policies with other counties (Media-UK)

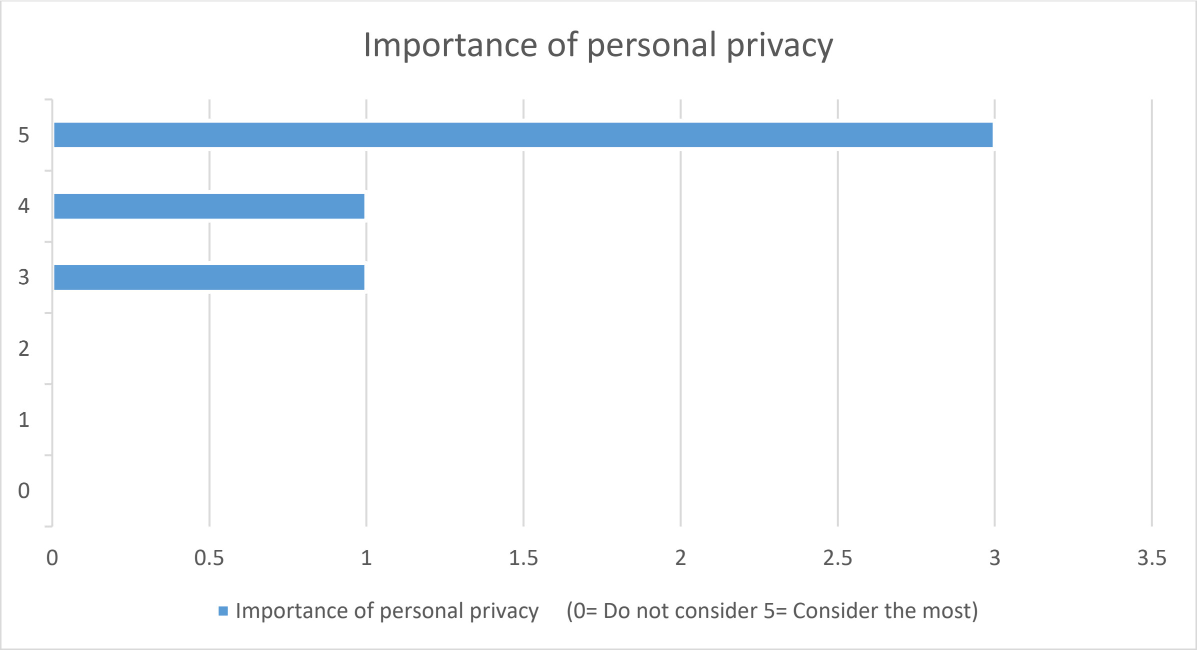


Figure E.576: Importance of personal privacy (Media-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 100 percent of the respondents have endorsed (See figure E.565). The other notable factors that have come out of the survey are organisational support, budget allocation, social differences, personal privacy, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies, mutual trust between countries and previous experience with other countries in developing policies (See figure E.554-564) (See figure E.566-576).

United Kingdom – Charity and Voluntary work

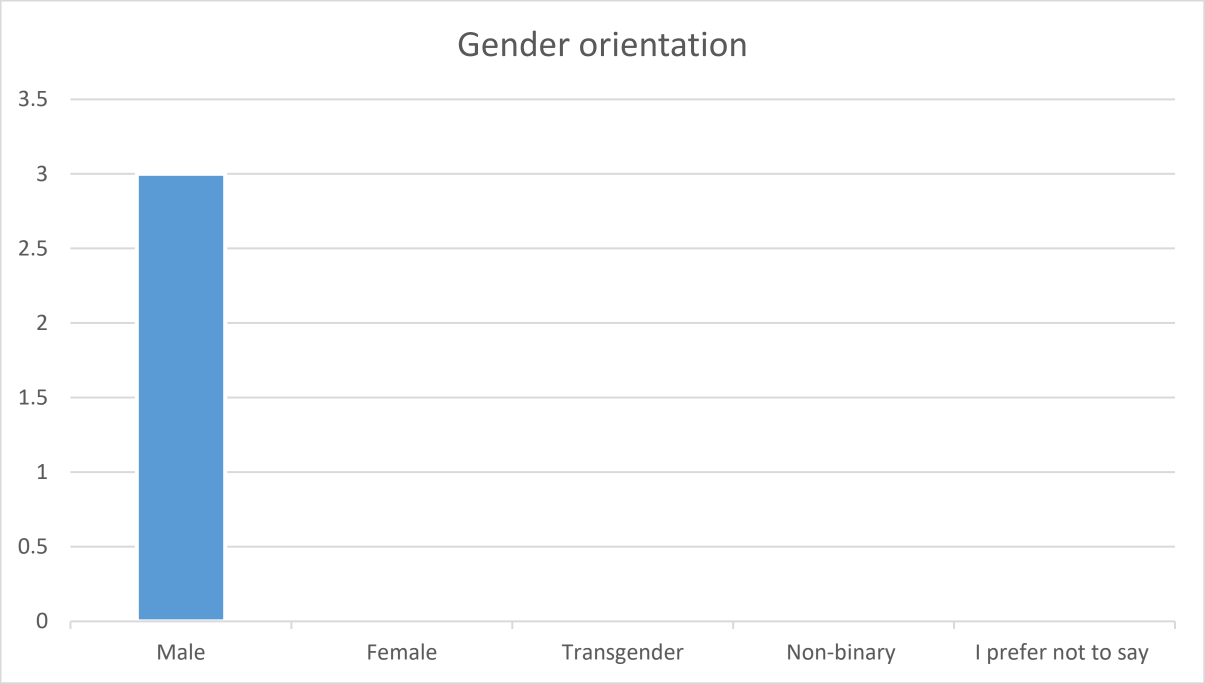


Figure E.577: Gender orientation (Charity and Voluntary work-UK)

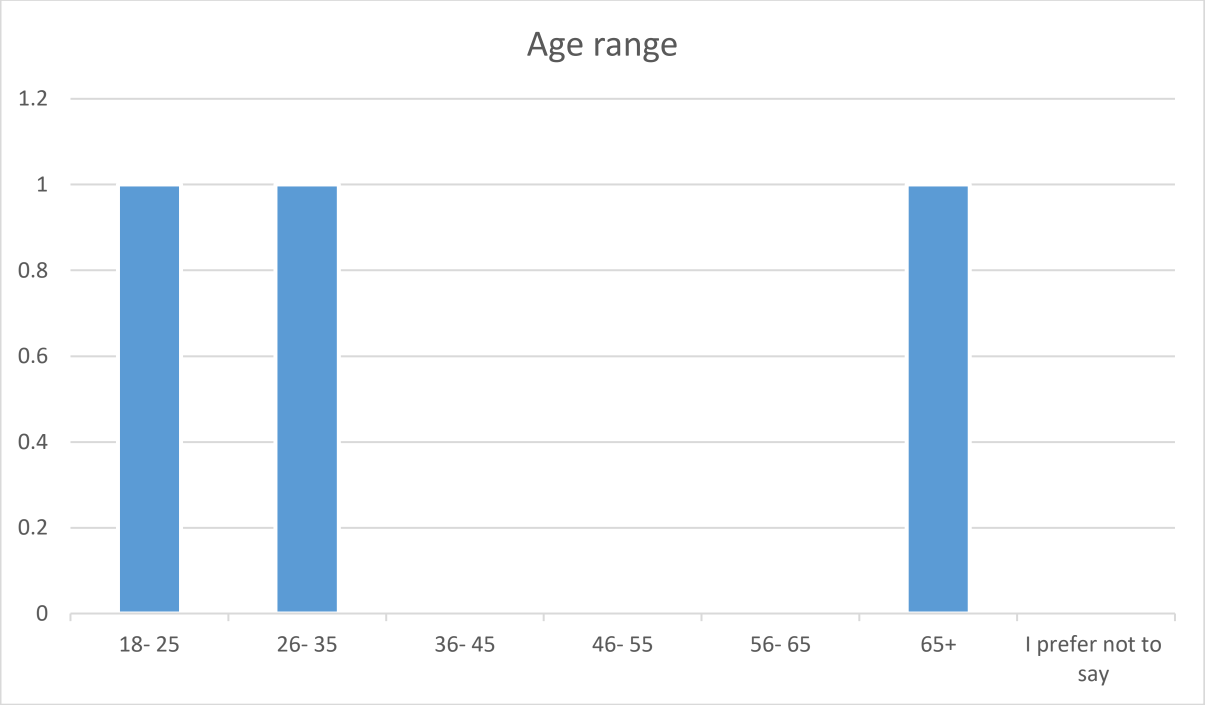


Figure E.578: Age range (Charity and Voluntary work-UK)

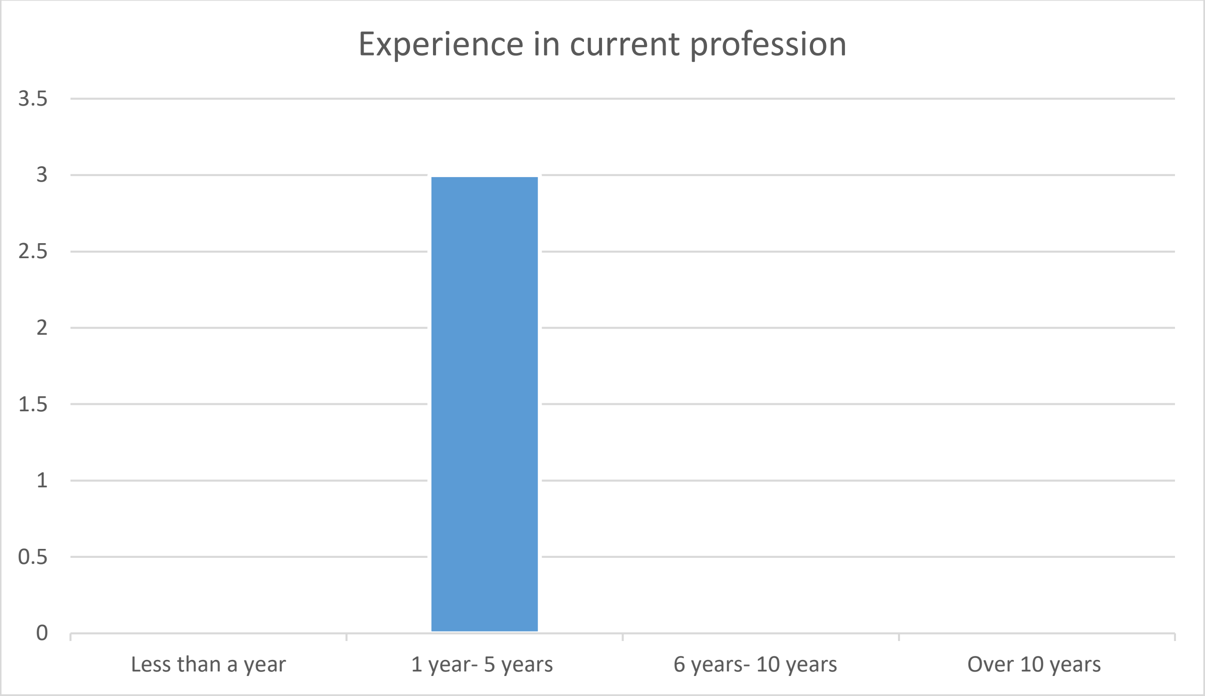


Figure E.579: Experience in the current profession (Charity and Voluntary work-UK)

This analysis is based on the responses received from United Kingdom participants in charity and voluntary work. There were 3 participants and all of them were males (See figure E.577). They were within the 18-65+ age range out of which 1 in the 18-25, 1 in the 26-35, and 1 in the 65+ range (See figure E.578). All the participants employed in the industry for between 1 and 5 years (See figure E.579).

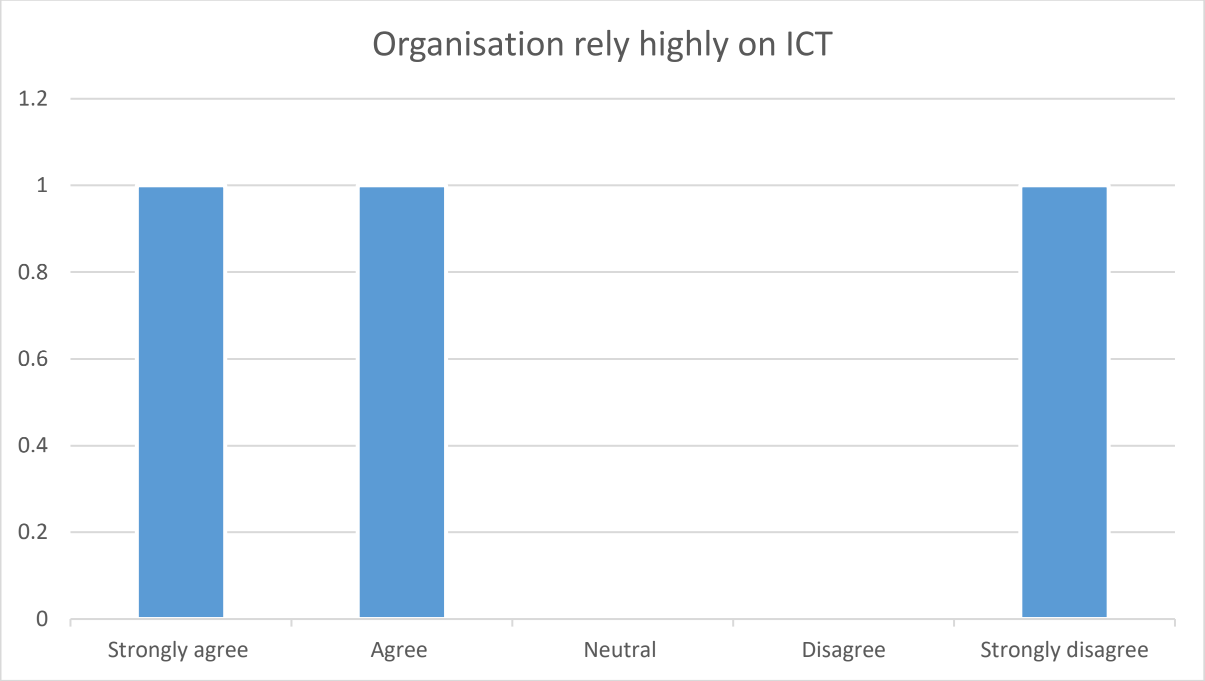


Figure E.580: Organisation rely highly on ICT (Charity and Voluntary work-UK)

Out of the 3 the respondents, 2 have worked in a technology reliance working environment, and 1 have marked ‘disagree’ on ICT (See figure E.580). This indicates a majority of those involved in charity and voluntary work have a high reliance on ICT.

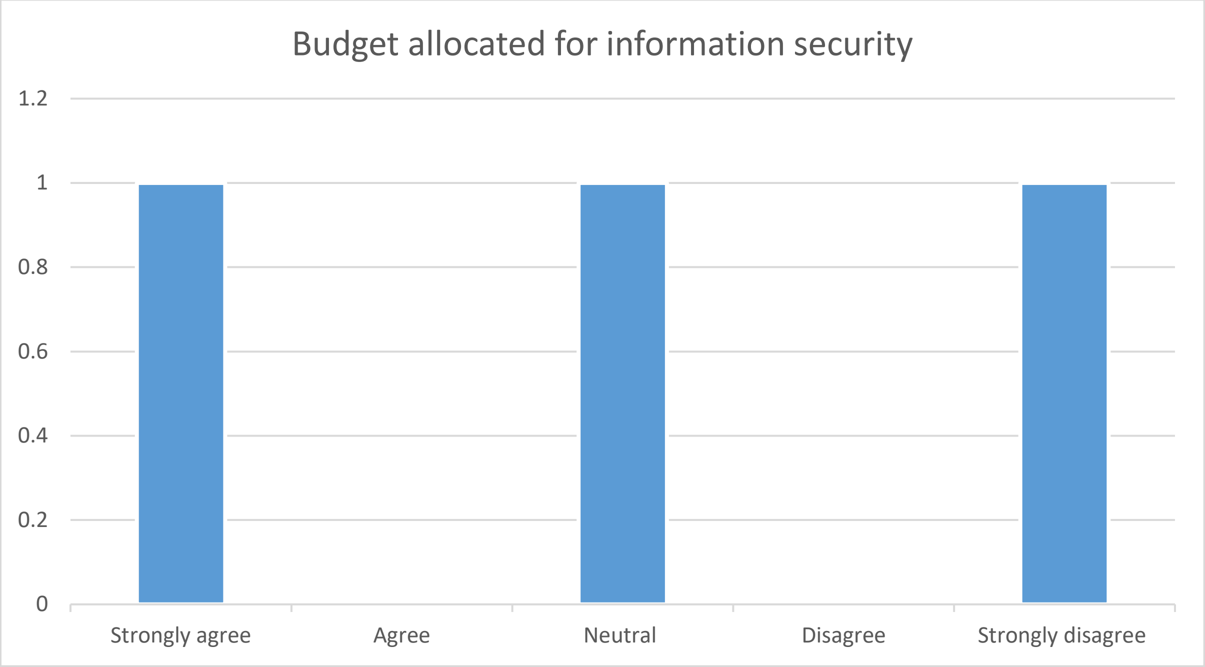


Figure E.581: Budget allocated for information security (Charity and Voluntary work-UK)

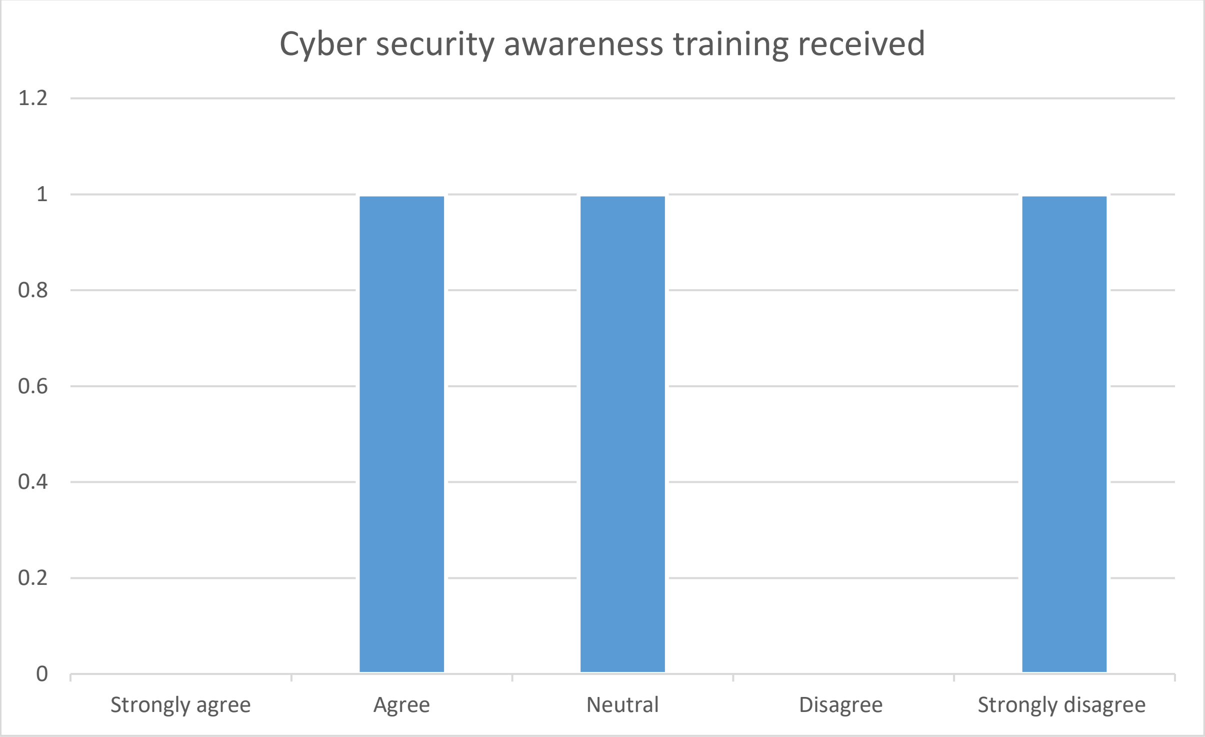


Figure E.582: Cyber security awareness training received (Charity and Voluntary work-UK)

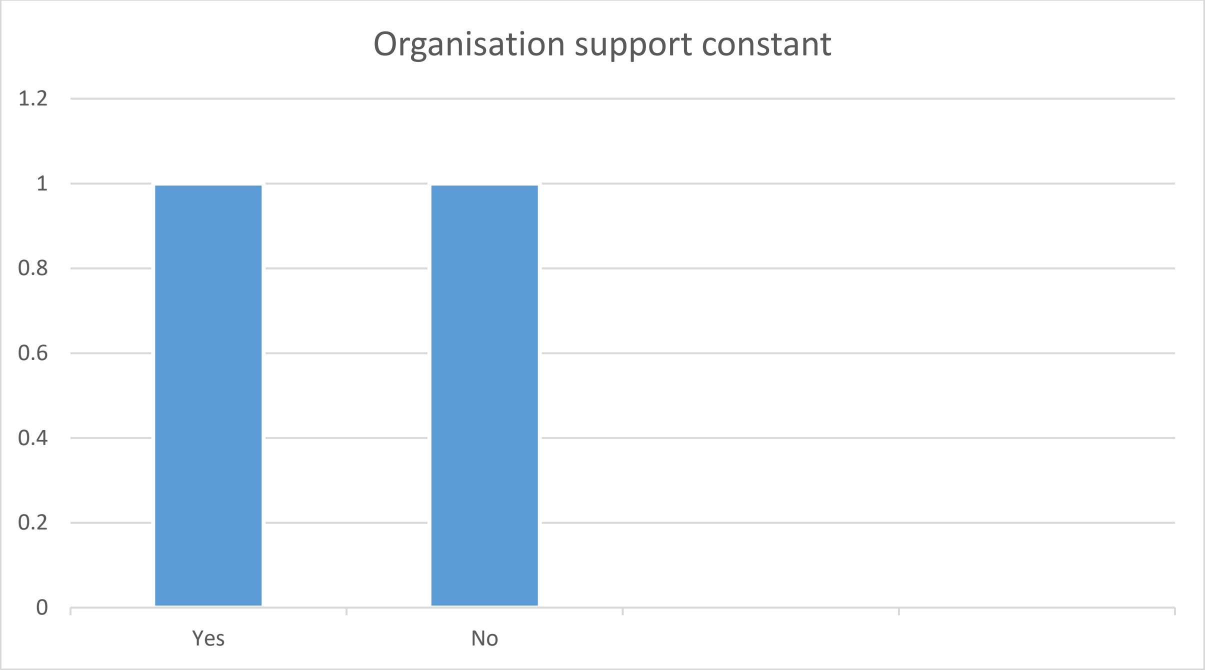


Figure E.583: Organisation support constant (Charity and Voluntary work-UK)

Funding allocation is not up to a satisfactory level. 1 out of the 3 have indicated that their organisations had an allocated budget for information security, whilst 1 had not expressed an opinion either way and notably according to the 1 disagreed, their organisations had no budget allocation for information security (See figure E.581). Some of the participants made the point that regular security awareness training that they received was also inadequate. Only 1 participant has received regular cybersecurity awareness training, whilst 1 neither agreed nor disagreed, and 1 participant had not regularly received security awareness training (See figure E.582). In addition, only 1 participant had received support from the organisation to protect personal information (See figure E.583). This clearly show that despite the high reliance of technology, there is no apparent budget allocation, as a result the employees did not receive regular security awareness training and support to towards protecting personal information.

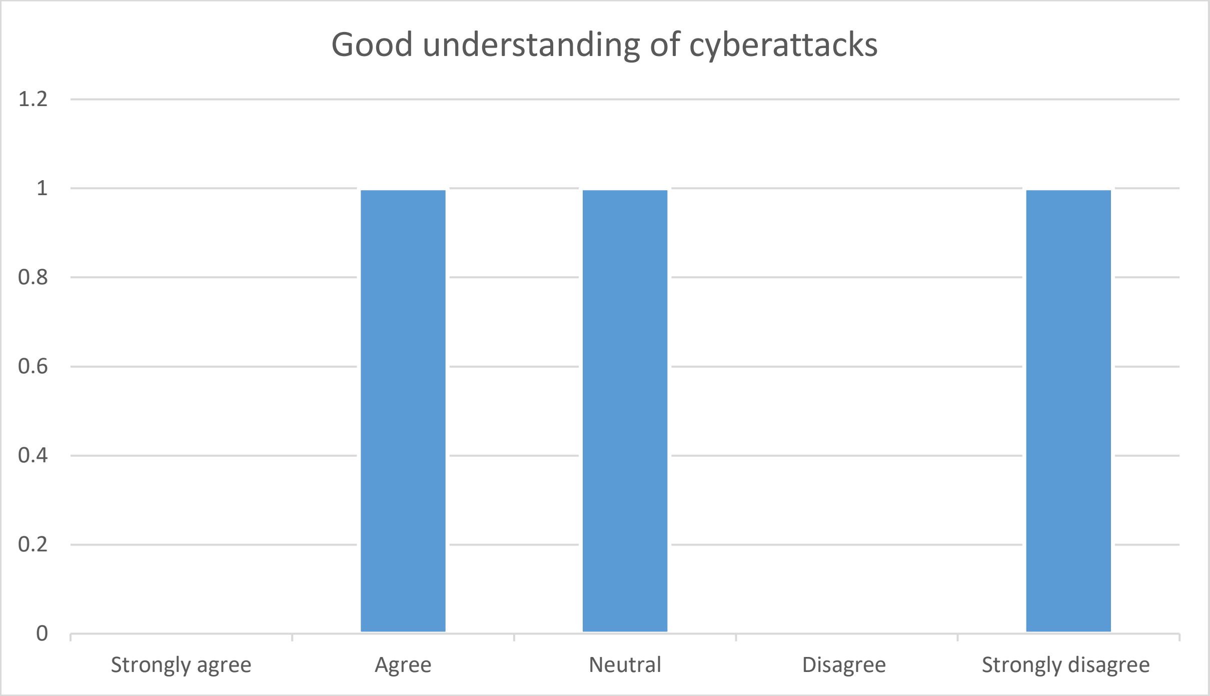


Figure E.584: Good understanding of cyberattacks (Charity and Voluntary work-UK)

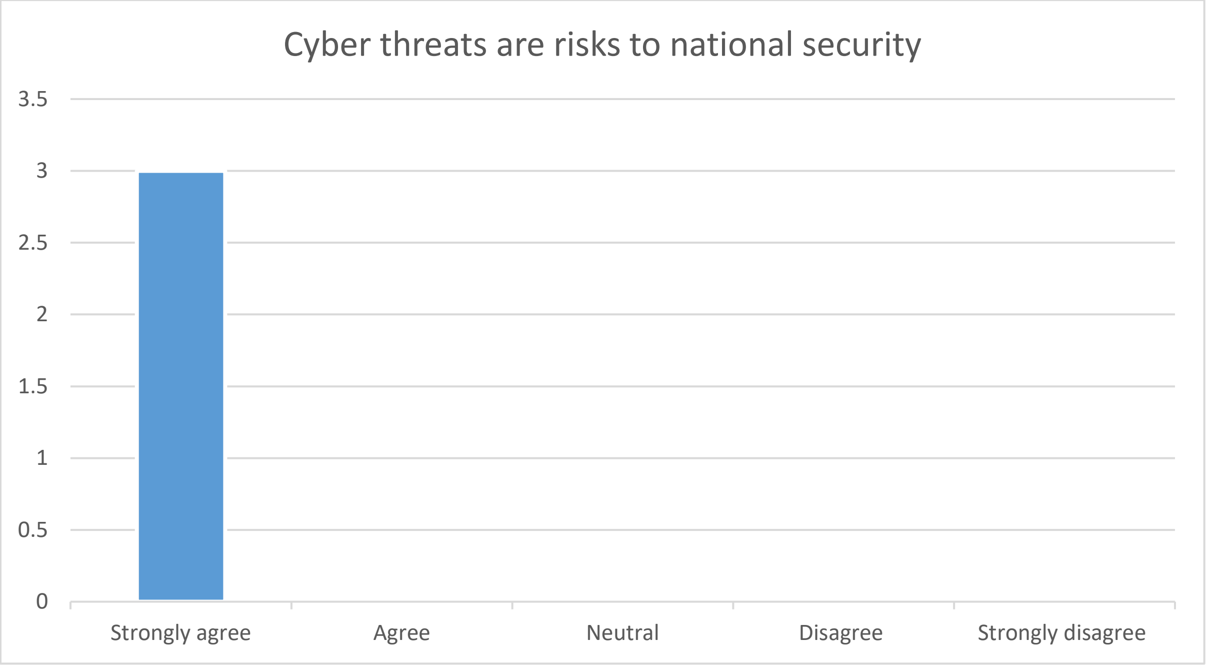


Figure E.585: Cyber threats are risks to national security (Charity and Voluntary work-UK)

The participants do not appear to have a high understanding of the impact of cyber-attacks on the public and the organisation. Only 1 participant does, 1 expressed no opinion either way, and 1 participant have no understanding (See figure E.584). Furthermore, 100 percent of the participants realise the potential threats to national security from cyber-attacks (See figure E.585). In general, understanding cyber threats and their impact on national security will make people act responsibly to minimise end-user errors, and in the longer term, their voice would be an influencing factor in accepting and implementing a national, regional and global level mechanism.

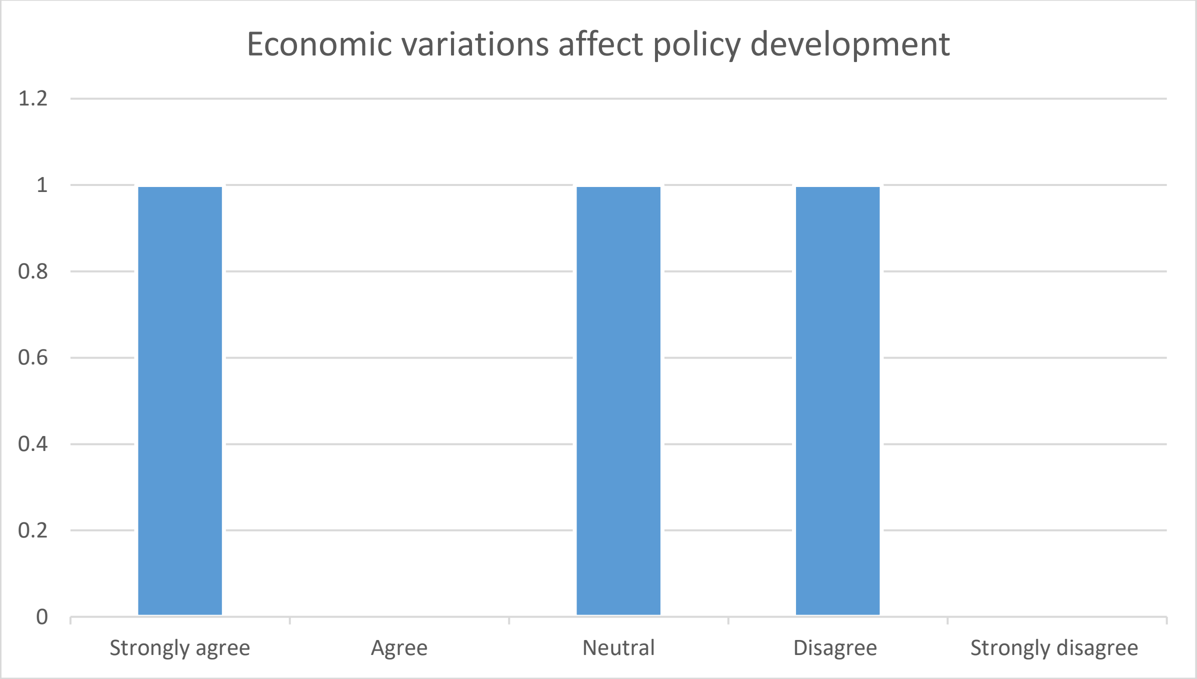


Figure E.586: Economic variations affect policy development (Charity and Voluntary work-UK)

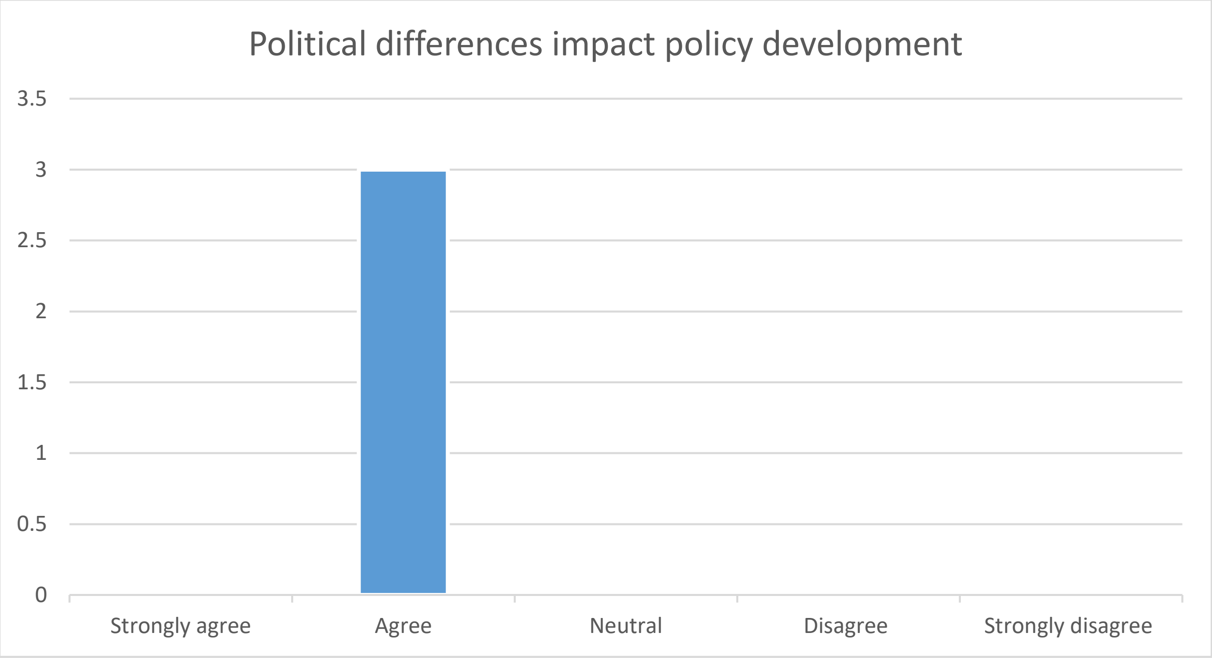


Figure E.587: Political differences impact policy development (Charity and Voluntary work-UK)

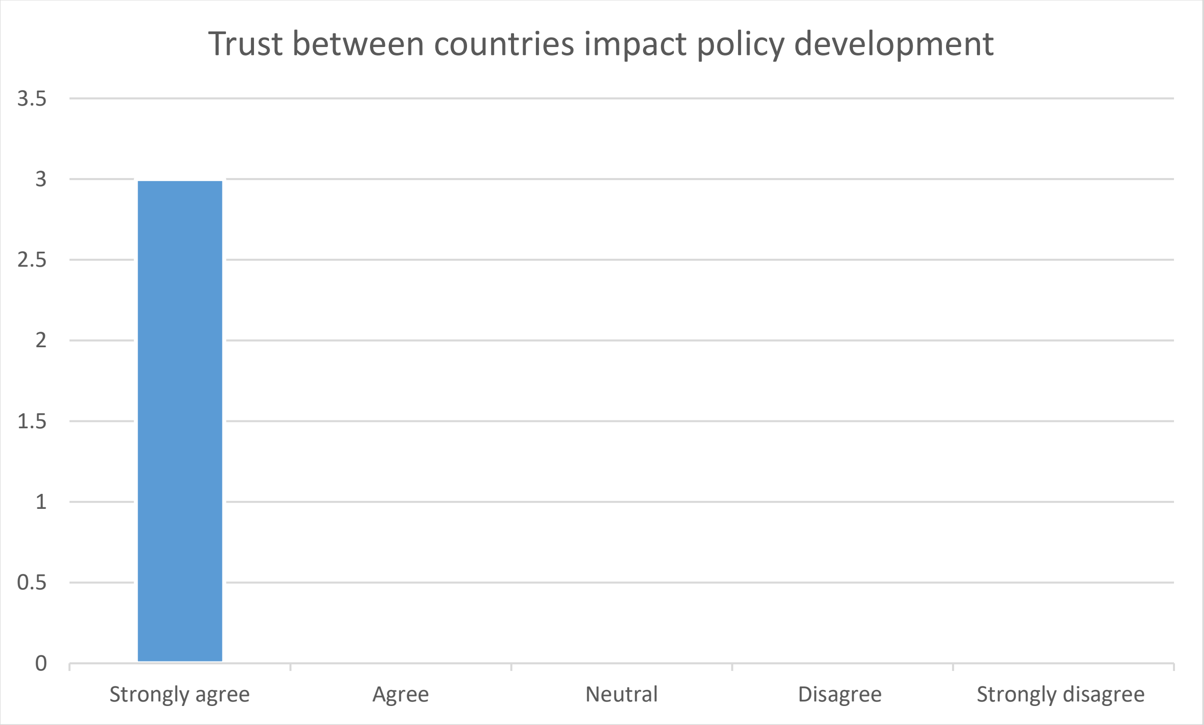


Figure E.588: Trust between countries impact policy development (Charity and Voluntary work-UK)

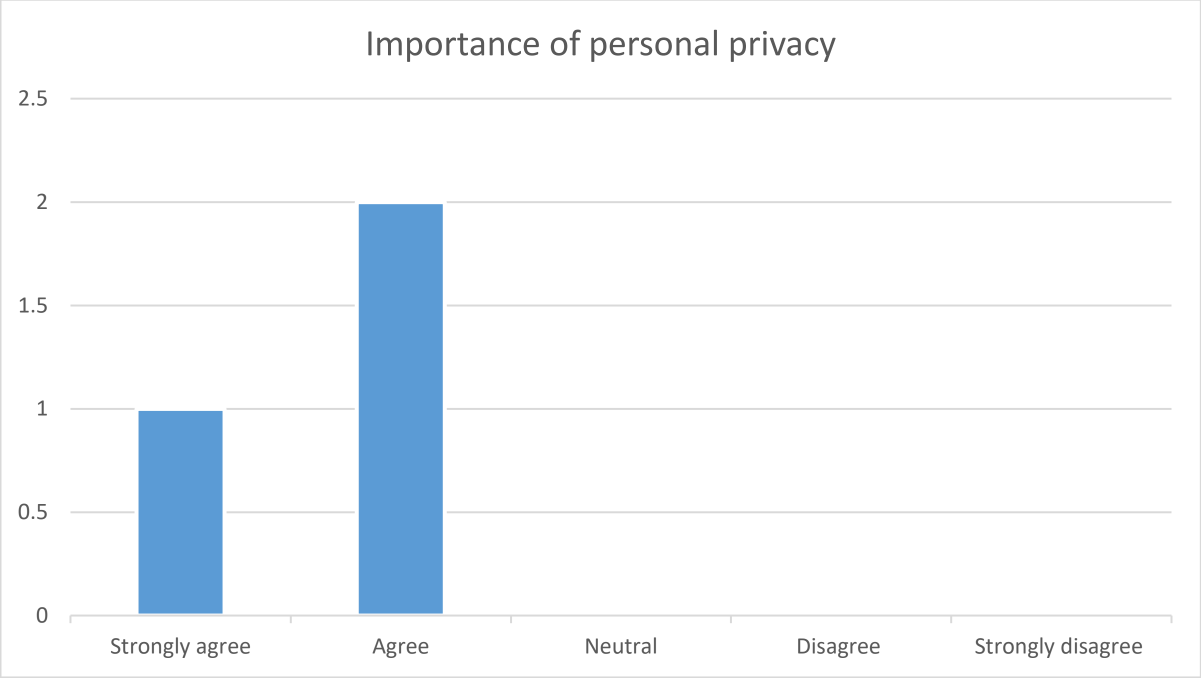


Figure E.589: Importance of personal privacy (Charity and Voluntary work-UK)

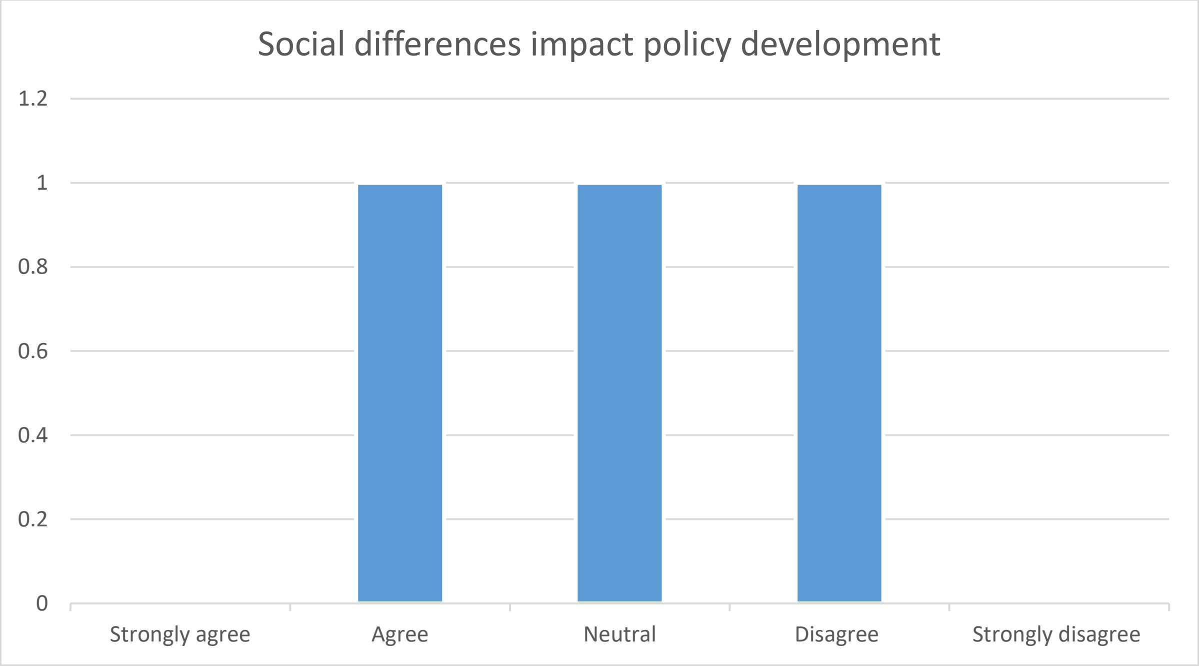


Figure E.590: Social differences impact policy development (Charity and Voluntary work-UK)

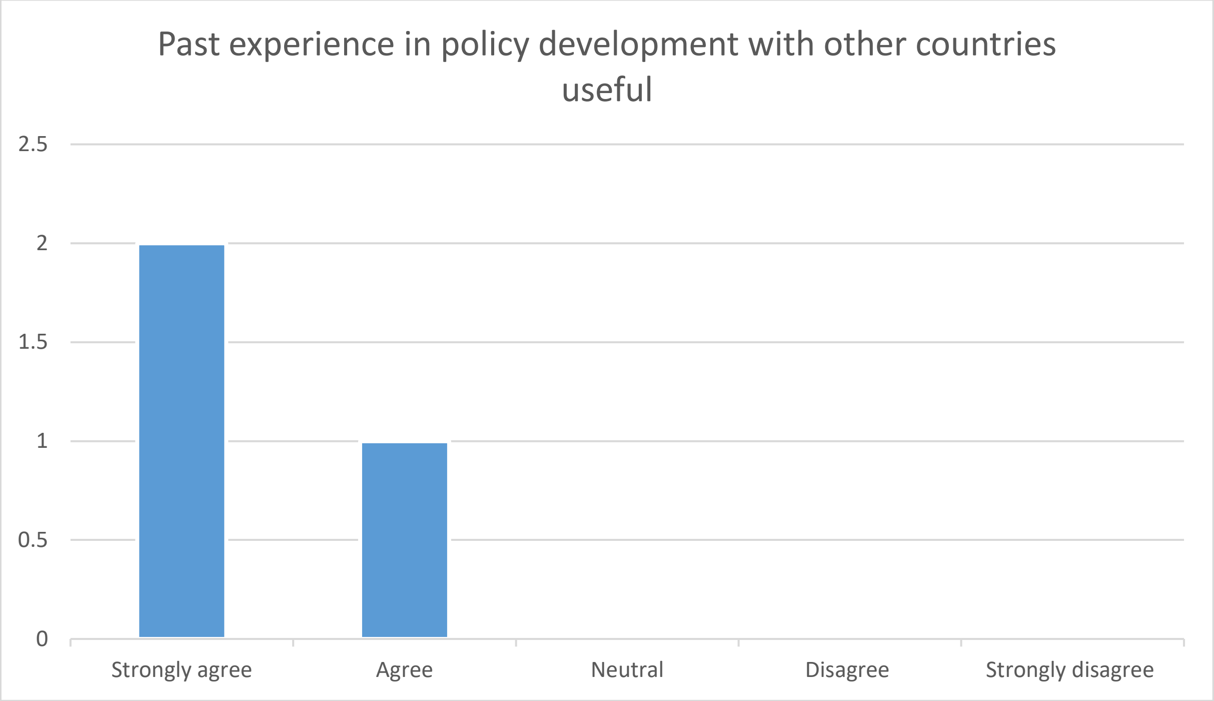


Figure E.591: Past experience in policy development with other countries useful (Charity and Voluntary work-UK)

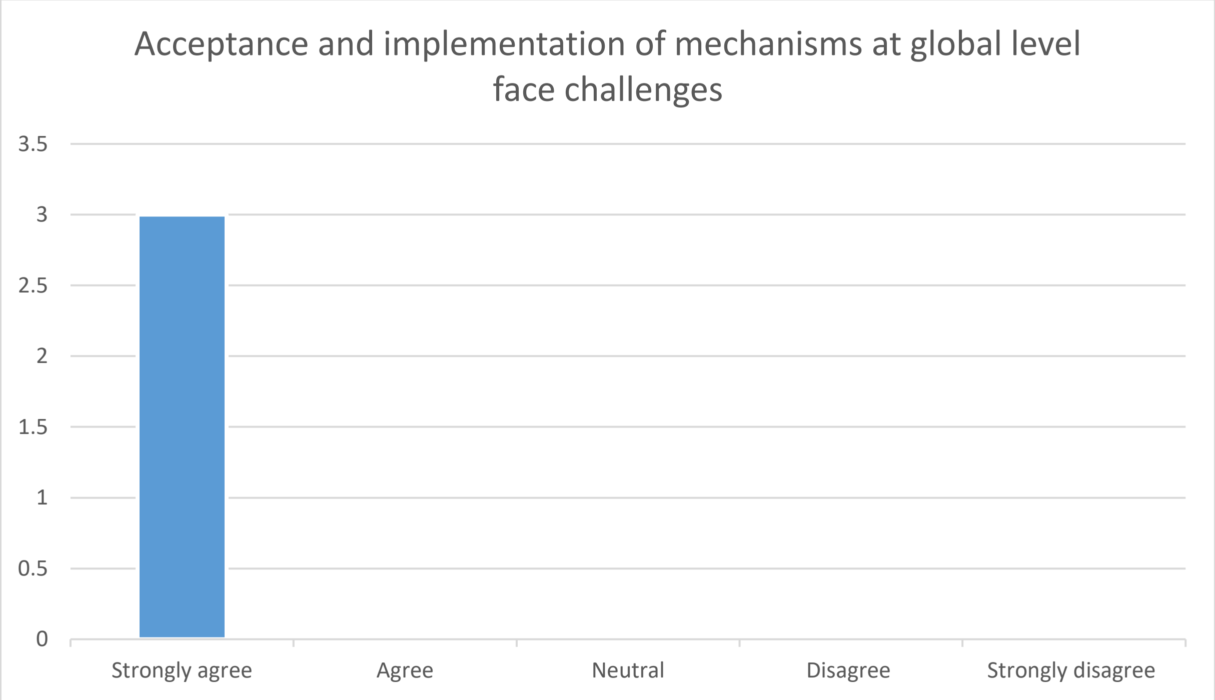


Figure E.592: Acceptance and implementation of mechanisms at global level face challenges (Charity and Voluntary work-UK)

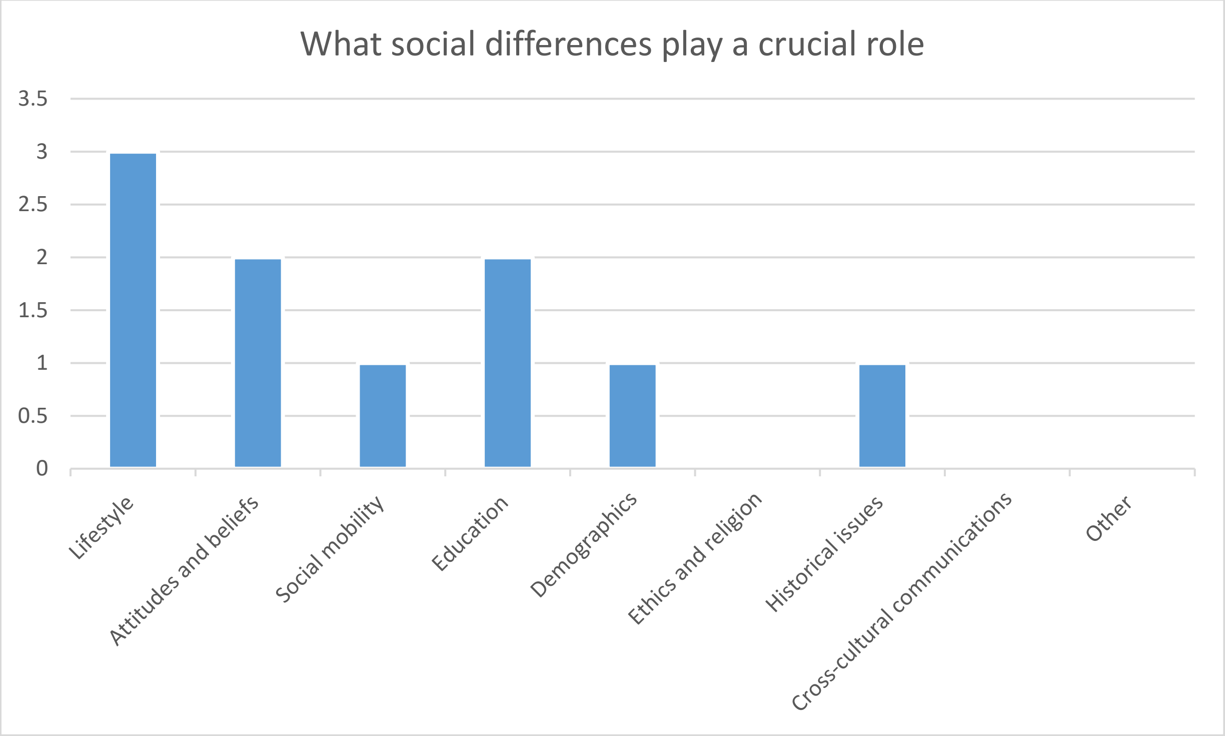


Figure E.593: What social differences play a crucial role (Charity and Voluntary work-UK)

The response to the social differences listed in the questionnaire, the majority has highlighted the importance of education, lifestyle and attitude and beliefs (See figure E.593). Knowledge of and familiarity with potential cyber threats, their impact on people and national security is crucial in accepting and implementing data privacy and security policies. Therefore, it is important to conduct cybersecurity awareness training at schools and at the organisational level. It becomes clear that educational training can be an effective way to make people understand the importance of privacy and the implications associated with privacy violations. People will have to make a crucial choice in their lifestyles when considering reliance on technology at the workplace. If there is a high reliance on technology in sharing or handling personal information, the demand for accepting and implementing policies associated with data privacy and security also should be high. Believing in privacy and respecting the privacy of self and others are contributory factors that have been discussed under attitude and believes.

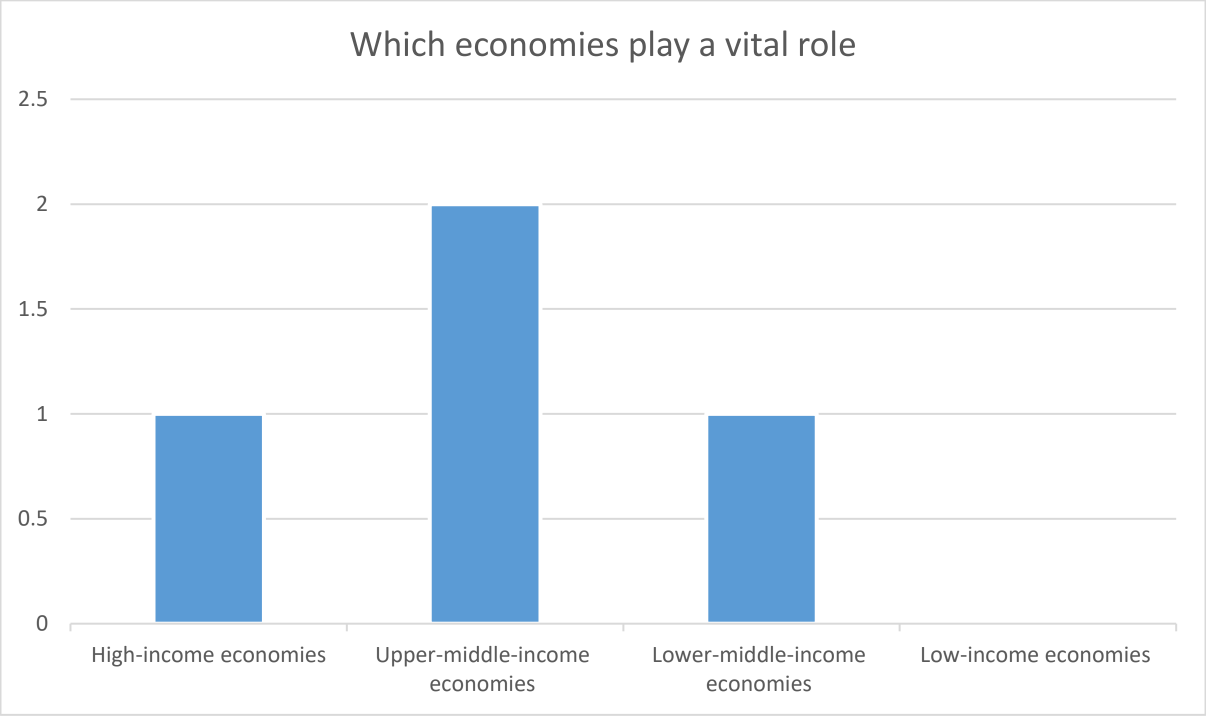


Figure E.594 Which economies play a vital role (Charity and Voluntary work-UK)

In the questionnaire, majority has stated that the upper-middle-income countries play a vital role. Interestingly the participants working in the charity and voluntary sector choose upper middle income economies over high income economies (See figure E.594). There are key stages in policymaking. This includes identifying policymaker aims, identifying policies to achieve those aims, select a policy measure, identify the necessary resources, implement and then evaluate the policy. These stages need time, money, and resources. Therefore, the financial stability of a country counts as a crucial factor in policymaking.

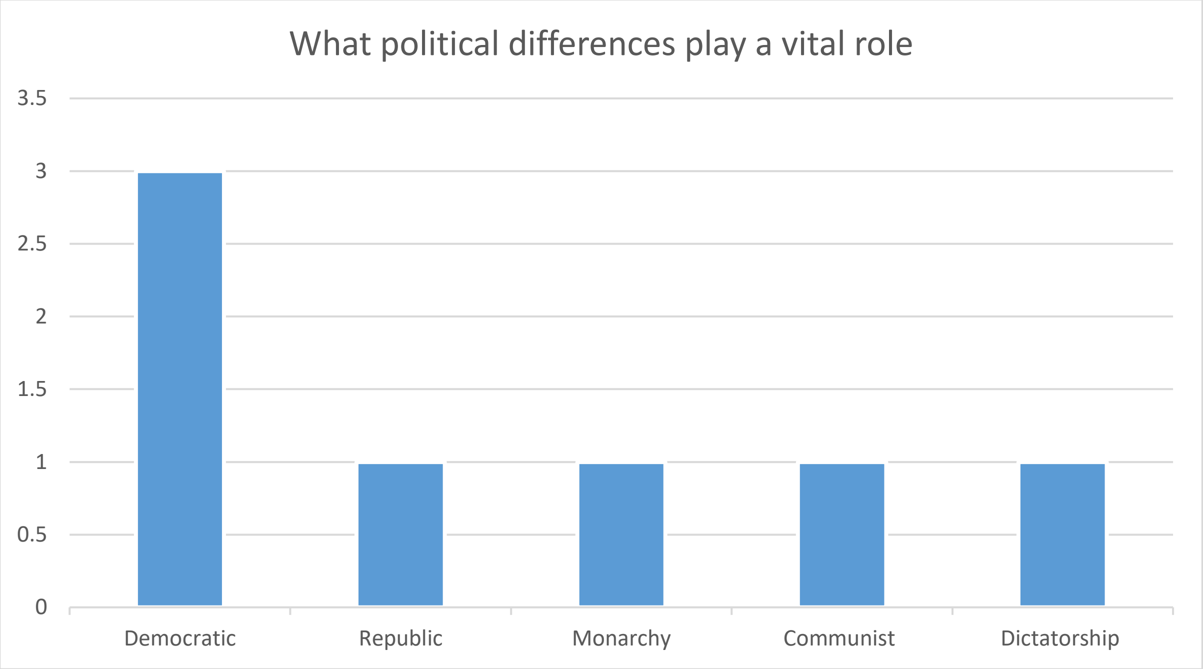


Figure E.595: What political differences play a vital role (Charity and Voluntary work-UK)

The majority have chosen a democratic political system (See figure E.595), in preference to others because it allows a public voice to influence the process of policy development and facilitates a consensus and collective responsibility for their actions . This forms the basis for developing trust and between the organisations, and coherence and transparency in the policy development process.

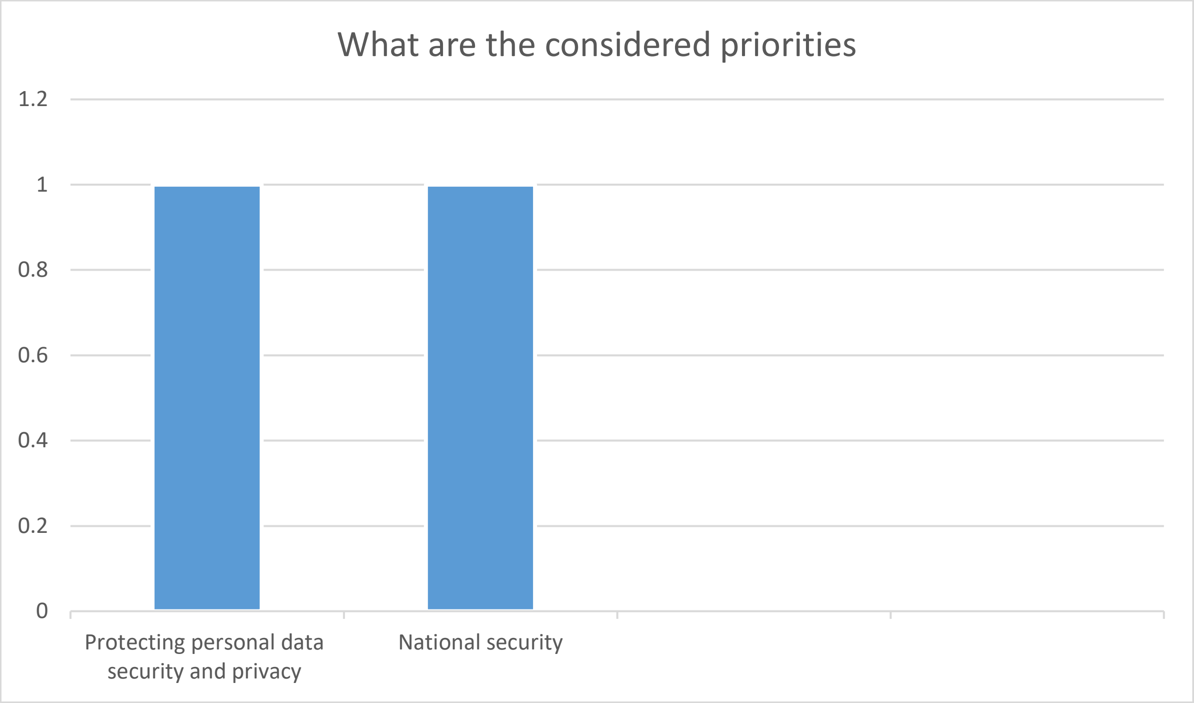


Figure E.596: What are the considered priorities (Charity and Voluntary work-UK)

The majority not considered either the importance of protection of personal data security and privacy or protection of national security, in accepting and implementing a global data privacy and security policies (See figure E.596).

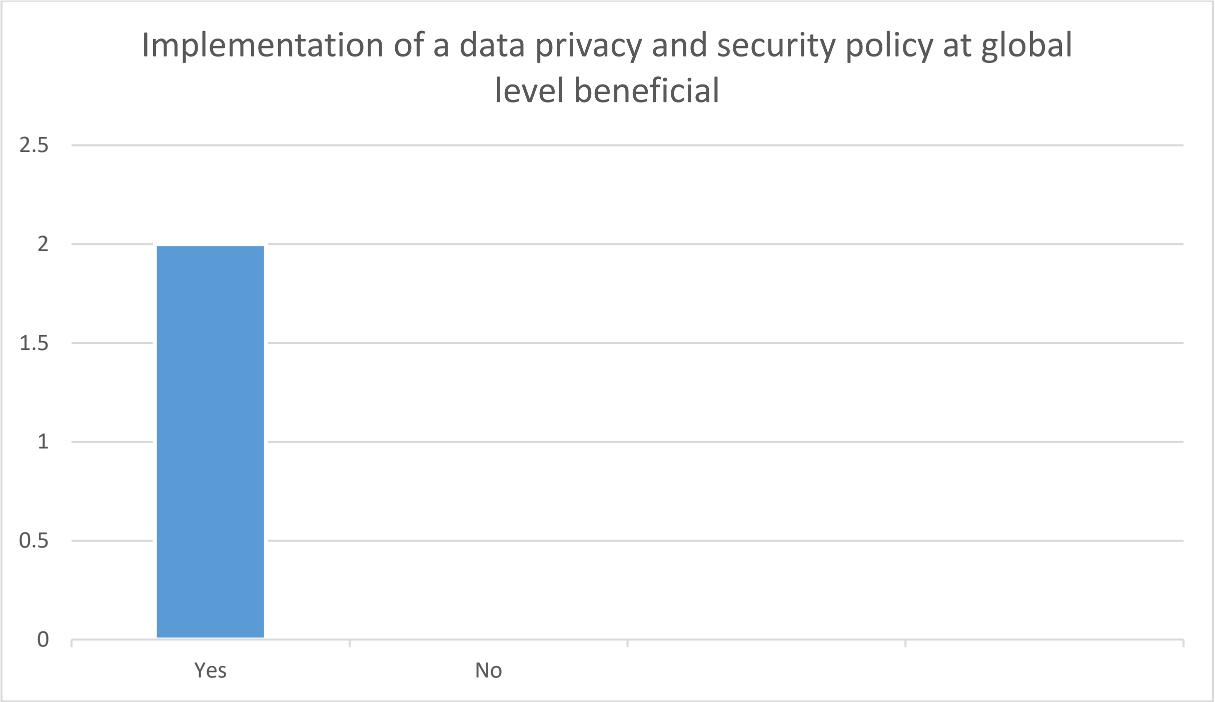


Figure E.597: Implementation of a data privacy and security policy at global level beneficial (Charity and Voluntary work-UK)

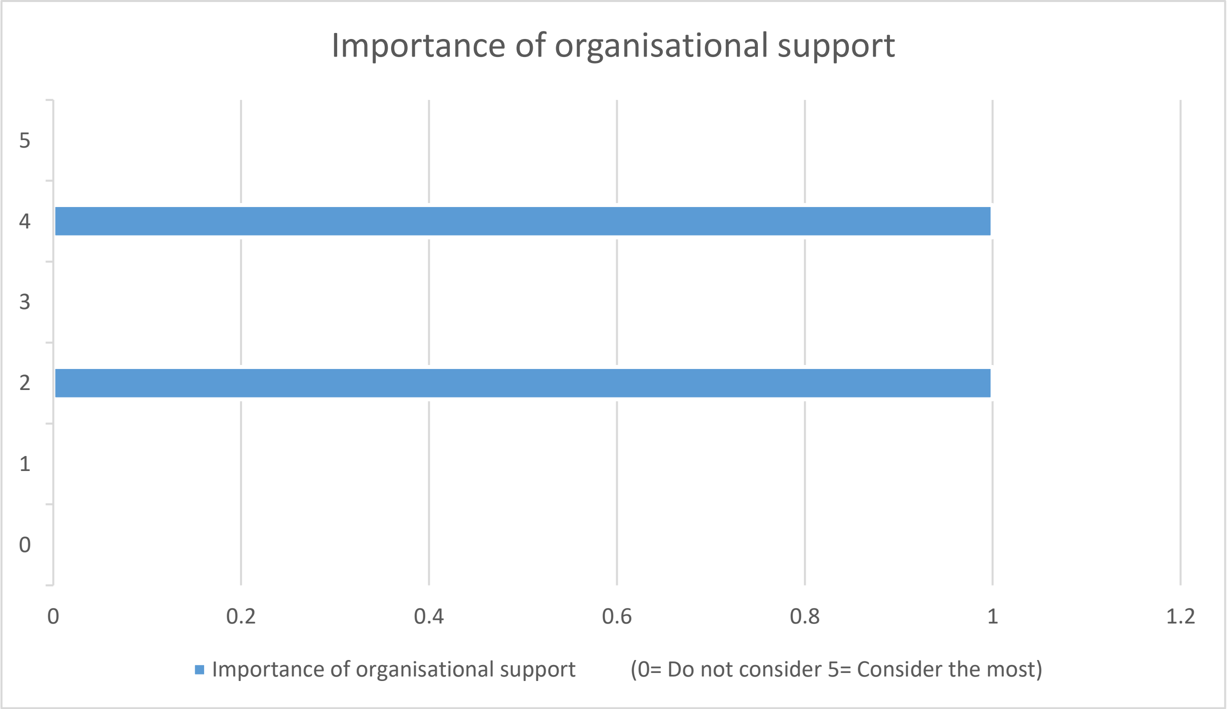


Figure E.598: Importance of organisational support (Charity and Voluntary work-UK)

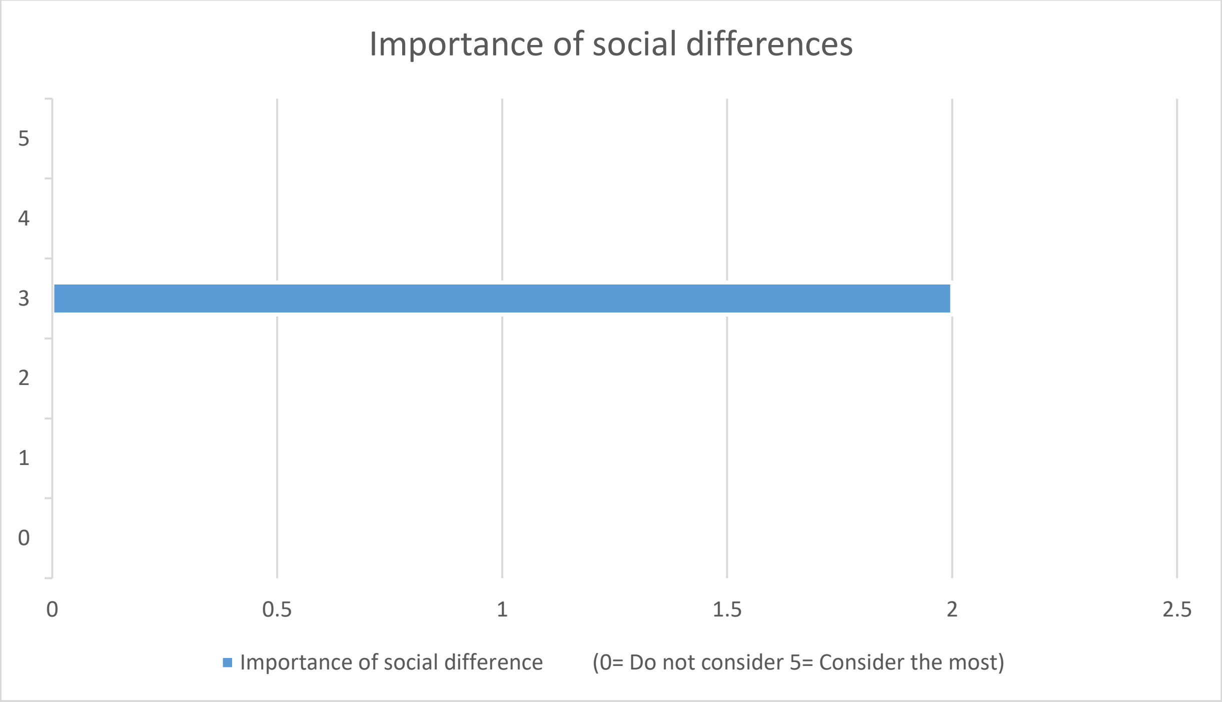


Figure E.599: Importance of social differences (Charity and Voluntary work-UK)

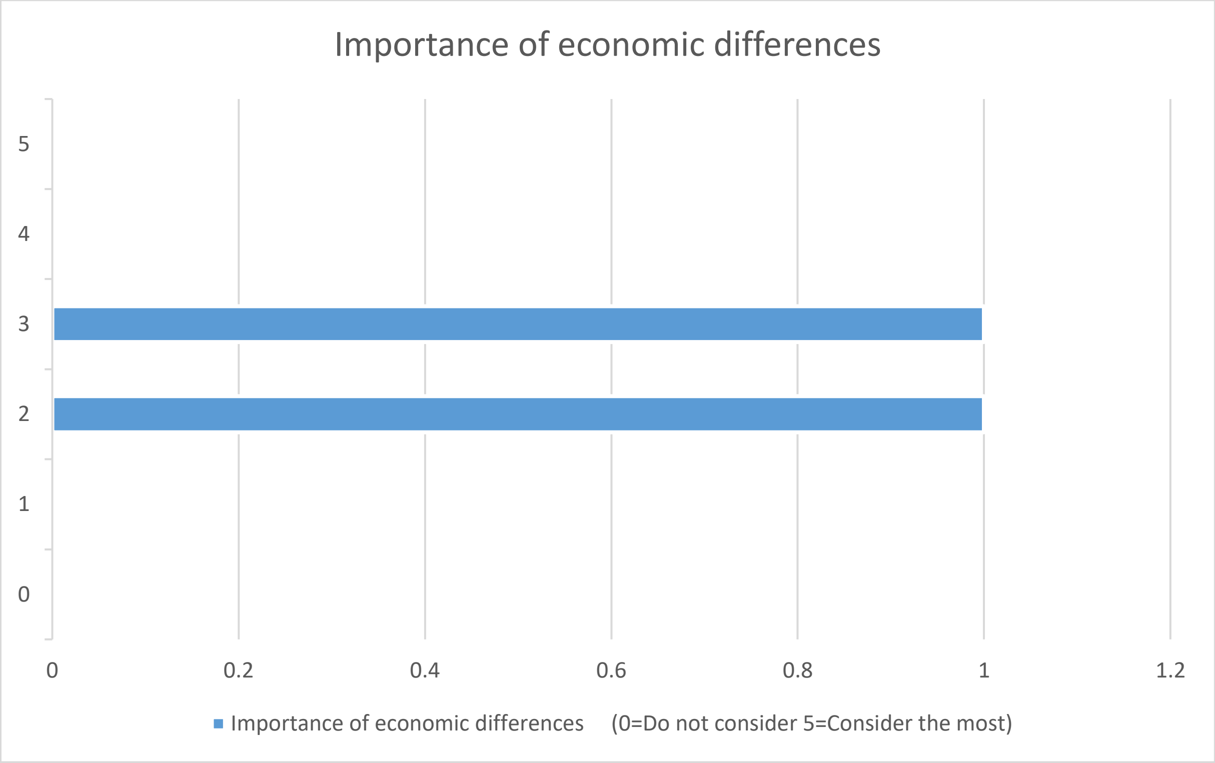


Figure E.600: Importance of economic differences (Charity and Voluntary work-UK)

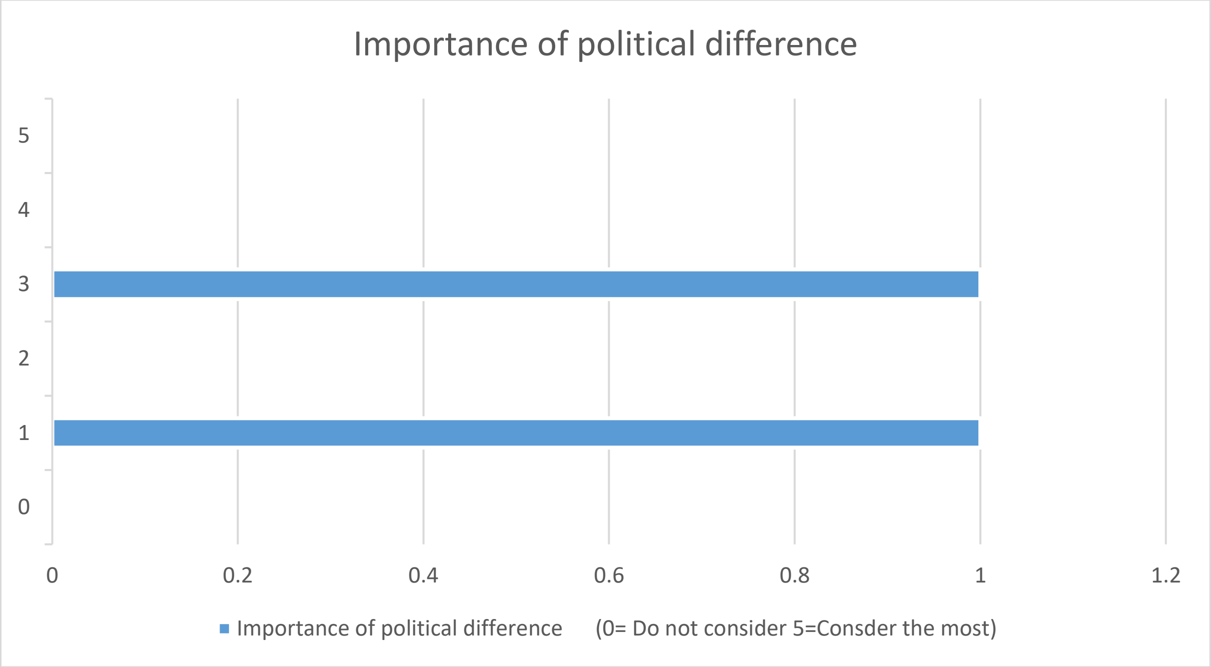


Figure E.601: Importance of political difference (Charity and Voluntary work-UK)

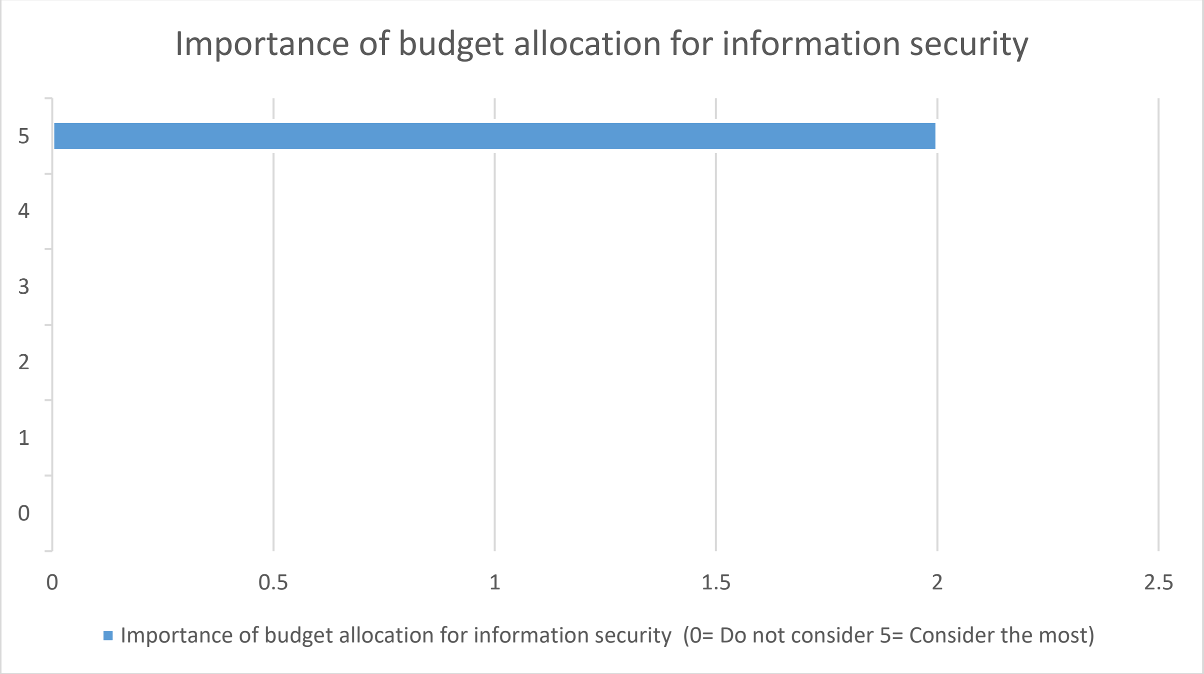


Figure E.602: Importance of budget allocation for information security (Charity and Voluntary work-UK)

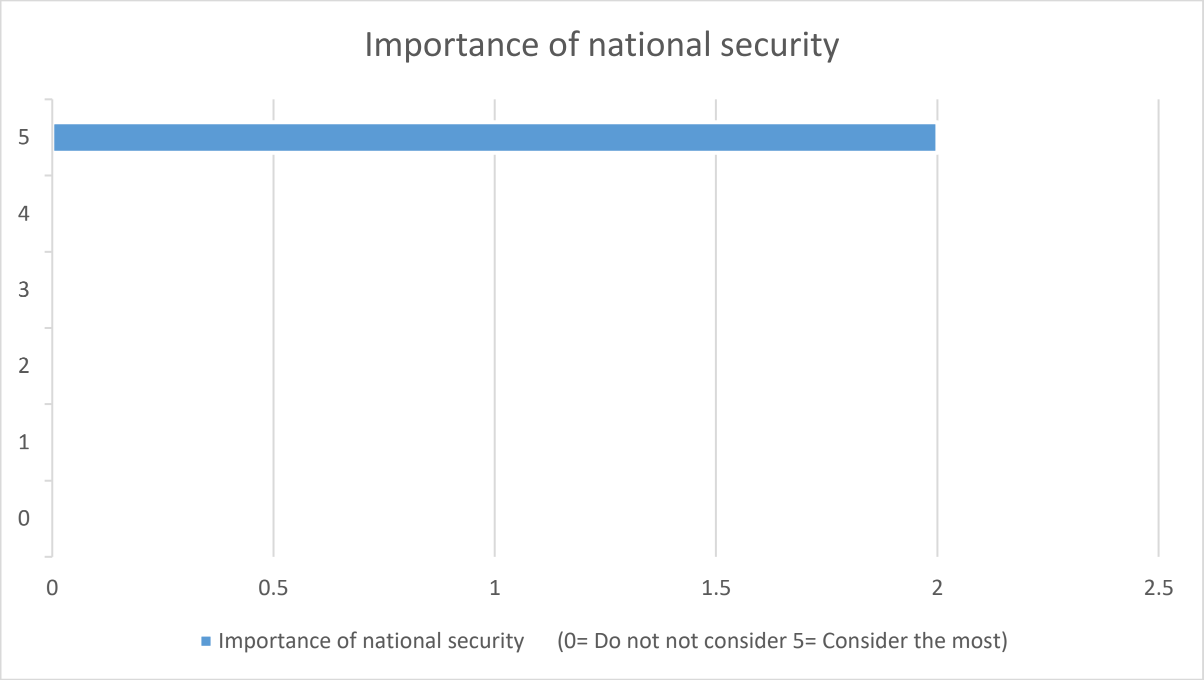


Figure E.603: Importance of national security (Charity and Voluntary work-UK)

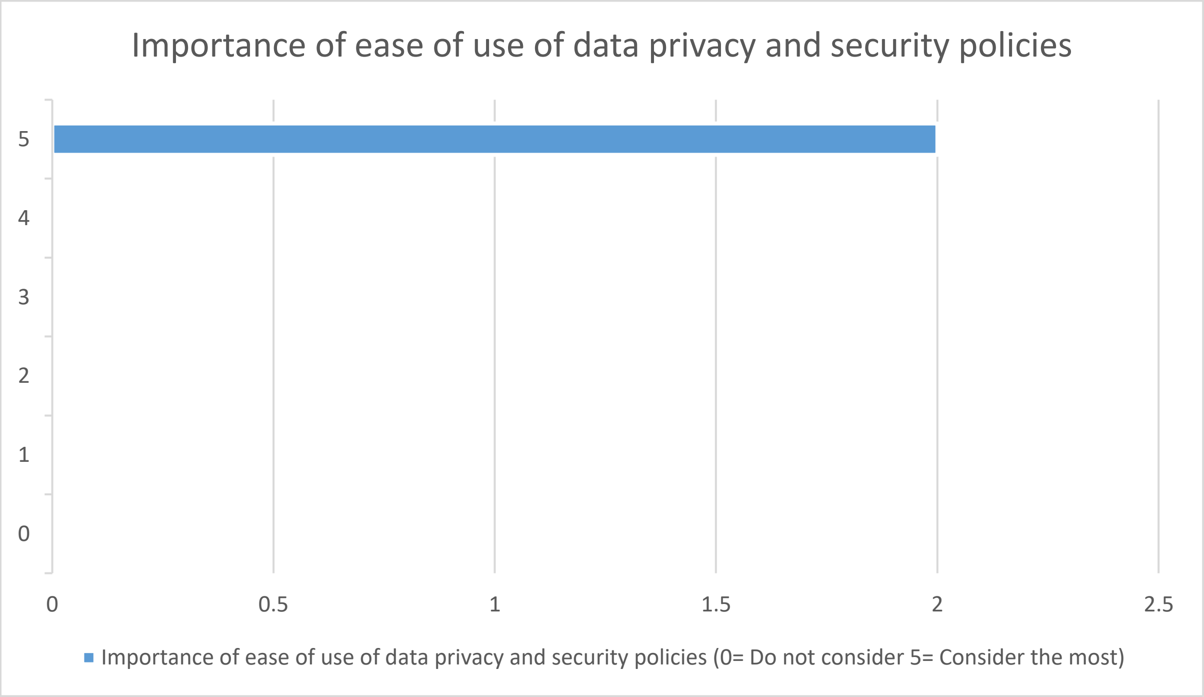


Figure E.604: Importance of ease of use of data privacy and security policies (Charity and Voluntary work-UK)

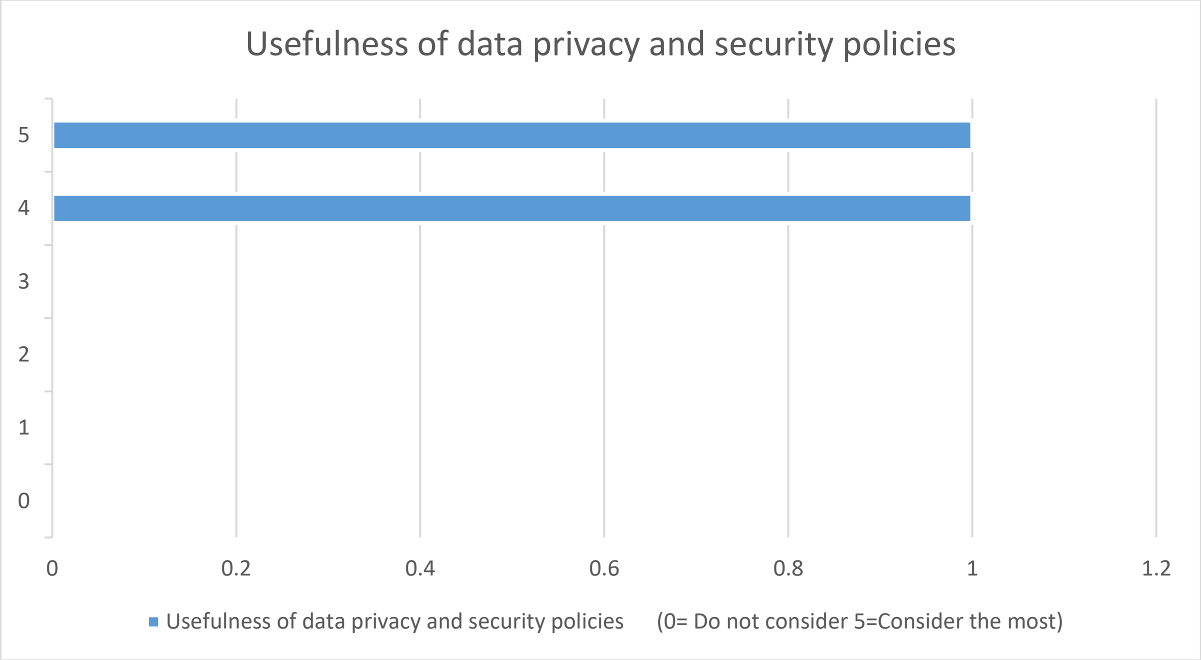


Figure E.605: Usefulness of data privacy and security policies (Charity and Voluntary work-UK)

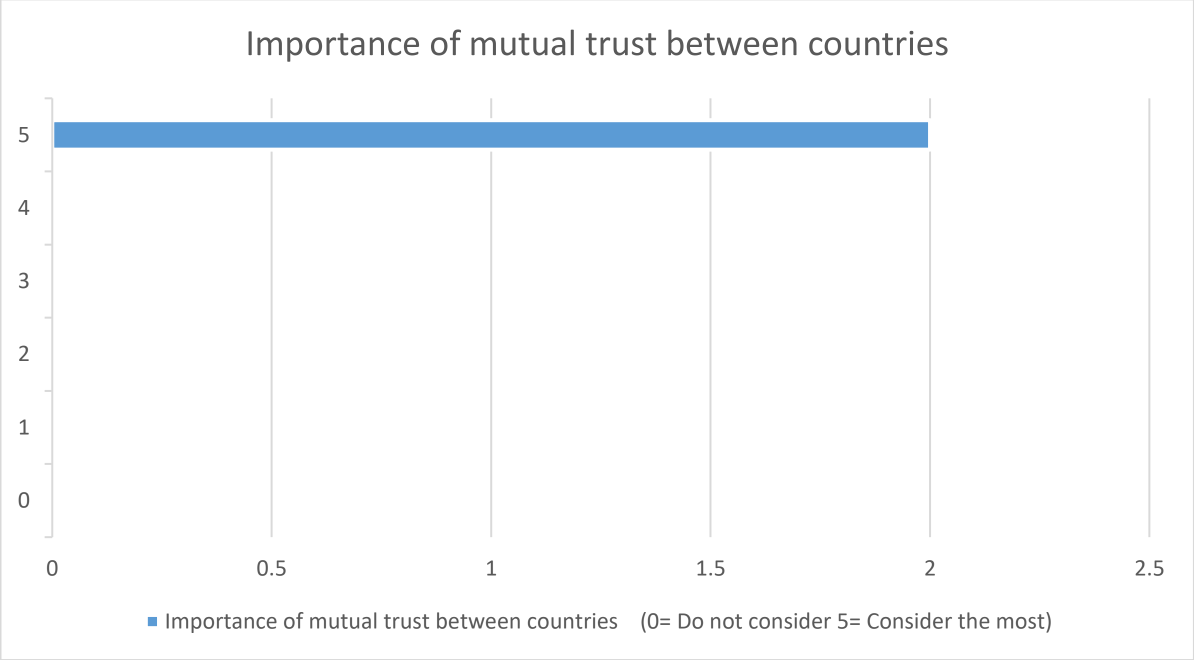


Figure E.606: Importance of mutual trust between countries (Charity and Voluntary work-UK)

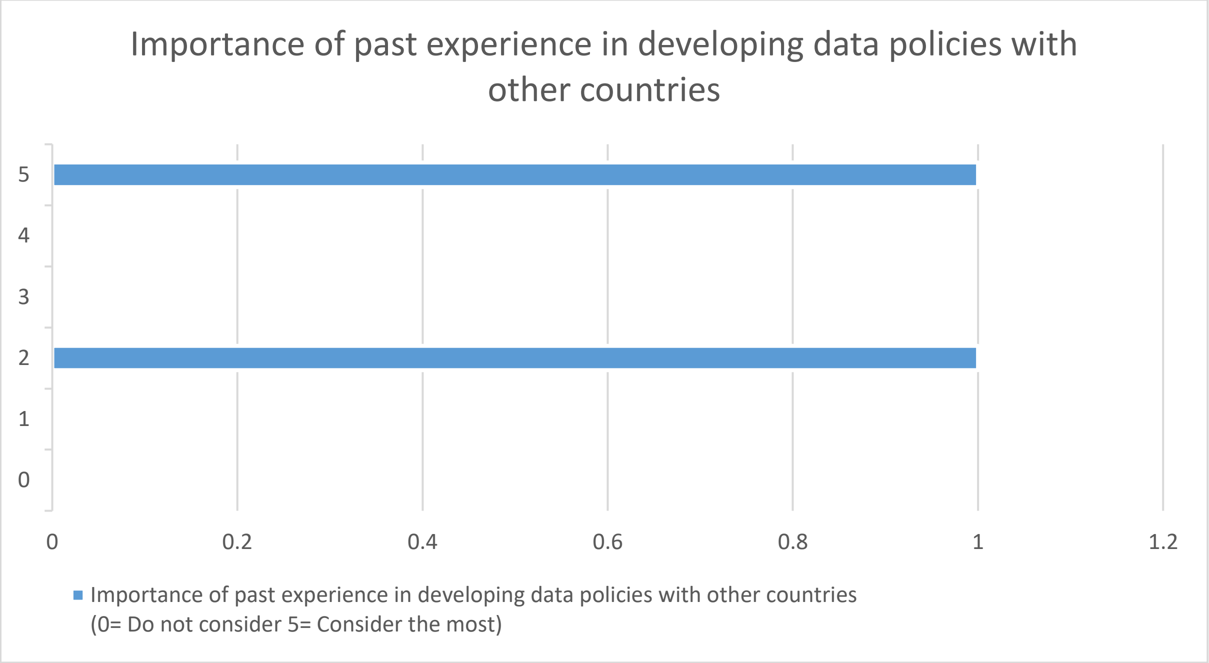


Figure E.607: Importance of past experience in developing data policies with other counties (Charity and Voluntary work-UK)

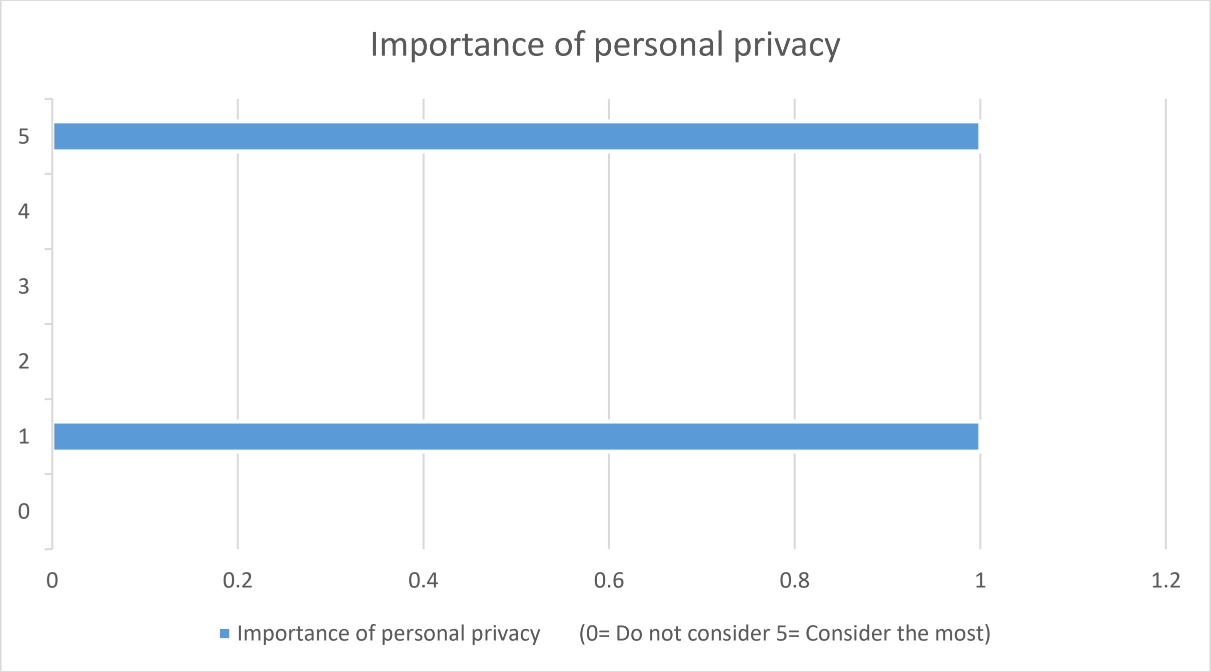


Figure E.608: Importance of personal privacy (Charity and Voluntary work-UK)

The message from the respondents is clear. The significance of the message derived from the research survey is the imperative need to have a global level data protection mechanism, which 67 percent of the respondents have endorsed (See figure E.597). The other notable factors that have come out of the survey are budget allocation, social differences, national security, ease of use of data privacy and security policies, the usefulness of data privacy and security policies and mutual trust between countries. (See figure E.586-596) (See figure E.598-608).