SOLENT UNIVERSITY

MSc COMPUTER ENGINEERING

AJAZALI SAIYED

MAA111 Pilot Project

18th December

Report 2: HOME WORKING: MANAGING THE CYBER RISKS

Table of Contents

2. Pilot study

2.1. Methodology

Research methods

The methodology section provides a brief outline of used tools and techniques in this research process. The section talks about the consideration of required tools that has helped to complete this pilot research about cyber security management. The use of metrology is proven to be crucial to resolve research oriented issues while conducting the process. This chapter plays its role to select appropriate tools in order to collect adequate data and regards to the chosen topic. Suitable research tools are chosen to perform this study. The section targets to provide the maximum idea of UK cyber crime incidents during these eight long months.

Research onion

Research onion is one of the most suitable ways to select appropriate research tools from this onion-shaped structure. Each step of research onion consists of a plethora of research strategies and philosophies (Apuke, 2017). Each layer of the onion has provided the researchers a general idea of this pilot project. This tool is used to have an empirical understanding of essential research approaches within the study. Research onion is an important tool to select research tools as the onion shaped figure is able to provide a collective look on all other options of research methodologies.

Research philosophy

Research philosophy comes up with an effective method of data collection and analysis. This indicates knowledge development by completing the research process. Significance of research philosophy arrives in helping out individuals by taking assumptions of rich essentials.

Justification

In this assessment the researchers have used ***positivism philosophy*** to conduct this pilot research. The philosophy is adopted to gain actual knowledge of observation. This is chosen based on the limitation of data collection and factual findings of gathered data.

Research approach

The research approach is a plan consisting of each step of broad assumptions in regards to data collection and interpretation (Rutberg, S. and Bouikidis, 2018). This is helpful for the researchers to collect relative data and documentation to the topic.

Justification

Deductive approach has been chosen for the development of hypothetical situations to conduct this pilot research. It has become easier to analyze the real life vulnerabilities of cyber crime very closely by the help of this research approach (Basias and Pollalis, 2018). This approach is chosen as it is constituent to a particular pattern in order to study the data and facts.

Research design

Research Design indicates adopted research strategies to integrate several components of the chosen process. This section of methodology is efficient to address arrived issues of research by outlining congruent structure of data collection and measurement.

Justification

In this research process the researchers have used a descriptive design process to highlight both independent and dependent variables (Ryder *et al.* 2020). This research design has helped the researchers to take part in elementary finding off real life experiences for the given topic.

Data collection process

The data collection process has been conducted based on primary and secondary data analysis in regards to the vulnerable margins of cyber crimes, especially during the pandemic crisis. The selection of research has involved quantitative data analysis by taking part in surveys. Primary data collection comes up with fresh and data secondary data collection includes previously gathered data resources. Needless to mention, that primary data are much more reliable than secondary data. The researchers have made 10 close-ended questions please to conduct the survey.

Data collection tools

Primarily, there are two data collection techniques exist in the process such as quantitative and qualitative, within which the quantitative data collection has been done. The survey has included close ended questionnaires (Ryder *et al.* 2020). Each response is stored in a Likert-scale chart. MS Excel is used to record the survey results. Participants' responses are stored password protected devices. No one has the access to this device apart from the researchers. Audio recording is also made for emergencies. Several features of excel has been used in this project for analysing collected data. This feature plays an essential for creating visual representation of dataset.

Population and sampling

The study has included 17 participants to take part in this research. These individuals are randomly selected from multinational companies who have worked "work from home" during the lockdown period. 10 sets of samples and observations are prepared to satisfy the study needs.

Accessibility issues

It is difficult for the researchers to collect relative information from the employees regarding their difficulties during the WFH period. Most of the cases they have hesitated to respond honestly. Time management has proven to be a critical factor in this research. It has been difficult to convince what's penis to manage their time for the study. Shortage of funding has restricted researchers to purchase important secondary resources online.

Ethical considerations

The research has followed specific ethical code of the UK government and data protection Act, 2018. Each of the responses has been collected securely within a password protected device. No other individuals apart from the researchers will have the access to visualise the gathered primary data (Susilo*et al.* 2019). Participants are assured of not using their responses in commercial applications. The researchers have provided stress on the anonymity of employees.

Limitations

The researchers have faced serious limitations within its process. It has been a challenge researcher to identify sham data within secondary resources. Requirement of excessive time is another challenge for the researchers. Financial constraint has created another limitation while conducting this research process.

2.2. Result and analysis

Q.1) How far do you agree that you have faced most of the WFH issues due to cybercrimes?

Responses	No of Responses	Percentage of responses
1. Strongly agree	7	41.17647059
2. Agree	5	29.41176471

3. Neutral	0	0
4. Disagree	3	17.64705882
5. Strongly disagree	2	11.76470588
TOTAL	**17**	**100**

Table 1: Response on first sample question

The first sample judges employees' opinion about the impact of cyber crimes resulting from their professional issues during the time. 7 of 17% have strongly agreed on this point and only five of them have agreed. This makes more than 50% positive responses on this sample. On the other hand, 3 and 2 participants have put their responses under the "disagree" and "strongly disagree" categories respectively. The sample has not received any neutral responses.

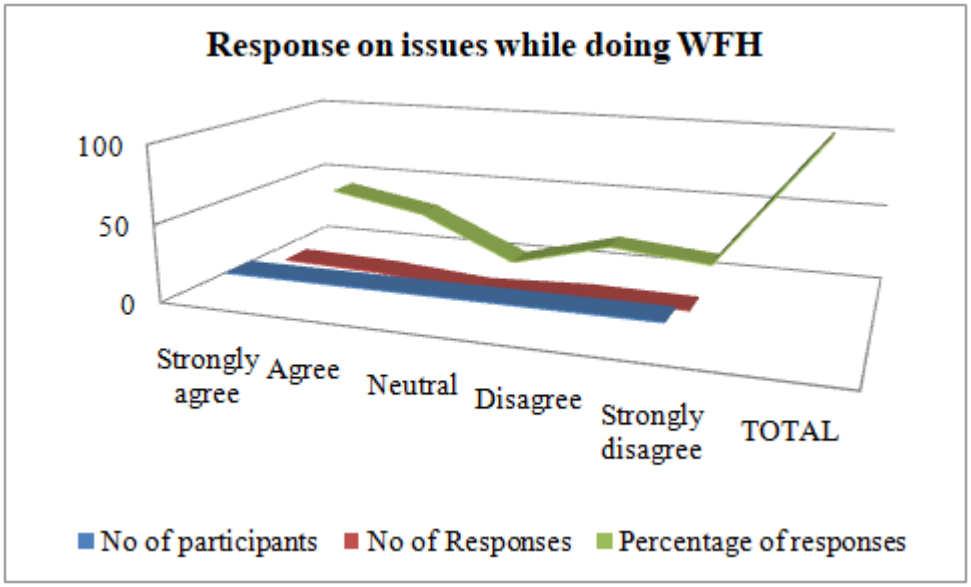

Figure 1: Graphical presentation on "Sample 1" response

Q.2) Do you agree that you have received scam emails?

Responses	No of responses	Percentage of responses
1. Strongly agree	8	47.05882353

2. Agree	5	29.41176471
3. Neutral	1	5.882352941
4. Disagree	2	11.76470588
5. Strongly disagree	1	5.882352941
TOTAL	**17**	**100**

Table 2: Response on second sample question

This analysis shows 13 (8 under "strongly agree" and 3 under "agree" categories) positive responses on the response of participants' scam email receiving. On the other side, nearly 11% and 5% participants have ticked the box of "disagree" and "strongly disagree" categories respectively. One participant has preferred to remain neutral in this section.

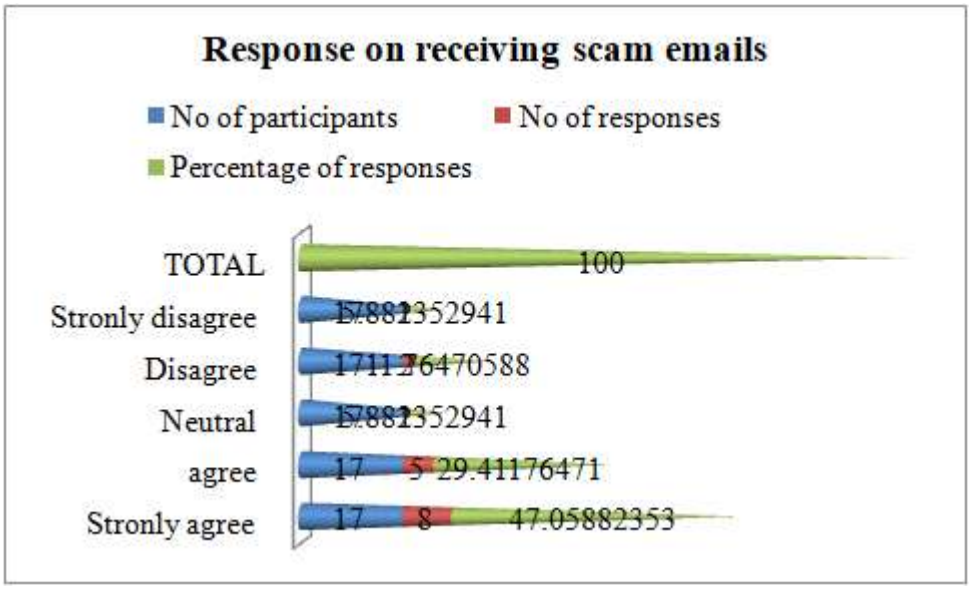

Figure 2: Graphical presentation on "Sample 2" response

Q.3) How far do you agree that you have faced data breaching issues while working in this period?

Responses	No of responses	Percentage of responses
1. Strongly agree	7	41.17647059

2. Agree	4	23.52941176
3. Neutral	2	11.76470588
4. Disagree	2	11.76470588
5. Strongly disagree	2	11.76470588
TOTAL	**17**	**100**

Table 3: Response on third sample question

The sample is made to judge participants' opinion on their experience of data breaching during the lockdown period. Nearly 41% have put their responses under the "strongly agree" category, which shows seven responses in this section. Four of them have put their responses in "agree" making a percentage of 23% to put their response in this category. However, almost 22% of the candidates have provided negative responses that they disagree on this point. The number of participants who have put "disagree" and "strongly disagree" responses are two for each category. Another two have put their response in neutral sections.

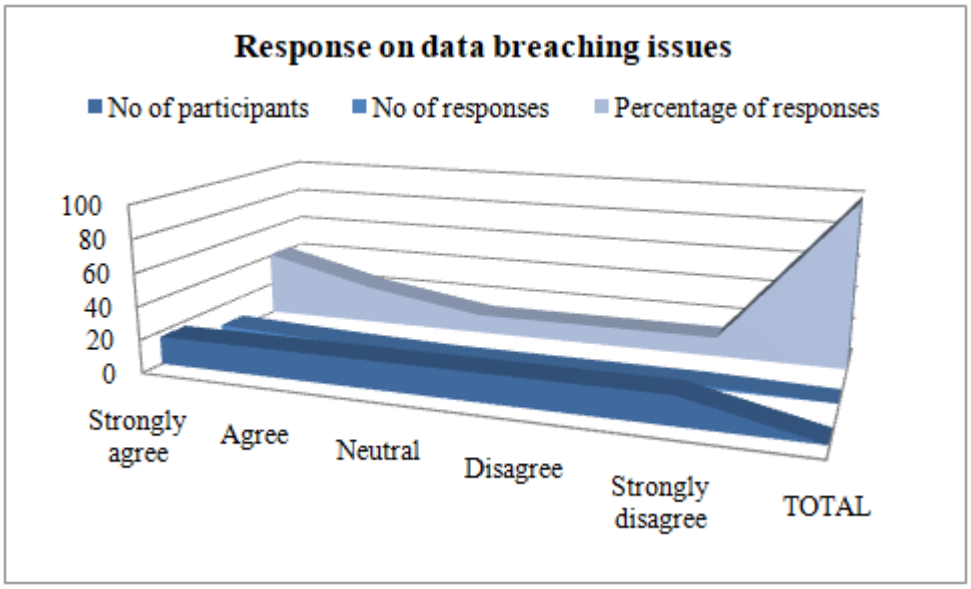

Figure 3: Graphical presentation on "Sample 3" response

Q.4) How far do you agree that your company has helped you to solve this matter?

Responses	No of responses	Percentage of responses

1. Strongly agree	5	29.41176471
2. Agree	5	29.41176471
3. Neutral	0	0
4. Disagree	4	23.52941176
5. Strongly disagree	3	17.64705882
TOTAL	**17**	**100**

Table 4: Response on fourth sample question

This sample contains responses of participants' opinion on their company's contribution in solving these issues. 5 of the participants have put their response and "strongly agree" category while another 5 have decided to go with “agrees". This section has received 7 responses in the "disagree" and "strongly disagree" category making a percentage of nearly 23 and 17 respectively. The sample has received no neutral responses.

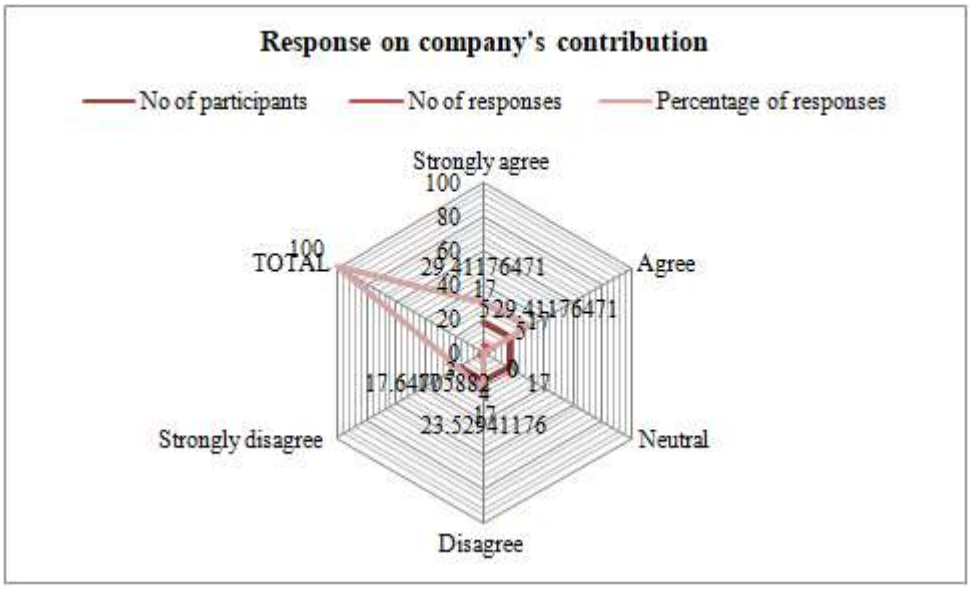

Figure 4: Graphical presentation on "Sample 4" response

Q.5) How far do you agree that your antivirus protection system has protected your device from cyber attack?

Responses	No of responses	Percentage of responses
1. Strongly agree	8	47.05882353
2. Agree	5	29.41176471
3. Neutral	0	0
4. Disagree	1	5.882352941
5. Strongly disagree	3	17.64705882
TOTAL	**17**	**100**

Table 5: Response on fifth sample question

The sample is made to check participants' opinion on their anti-virus's ability to protect against cyber attack. In this regard more than 70% participants have strongly agreed to their anti-virus's capabilities. However, a little number of participants has put their negative responses against this section making a proportion of 22% participants to provide their responses in this one.

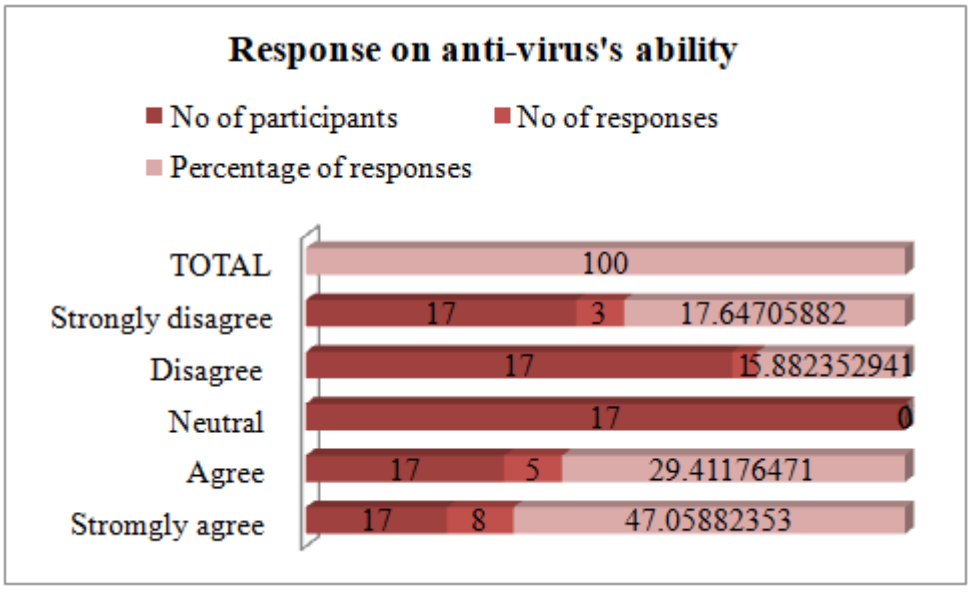

Figure 5: Graphical presentation on "Sample 5" response

Q.6) How far do you agree that your company has investigated earlier cybercrime issues?

Responses	No of responses	Percentage of responses
1. Strongly agree	9	52.94117647
2. Agree	4	23.52941176
3. Neutral	2	11.76470588
4. Disagree	1	5.882352941
5. Strongly disagree	1	5.882352941
TOTAL	**17**	**100**

Table 6: Response on sixth sample question

The sample is designed to judge companies' previous cyber crime cases. The question is asked in a manner so that participants can answer the company's previous attempts to solve cyber security issues. This section has got maximum positive responses making it more than 70% of positive responses. However, this section has received one response for the "disagree" and "strongly disagree" section coming up with nearly 10% of negative responses. The sample has received to neutral responses as well.

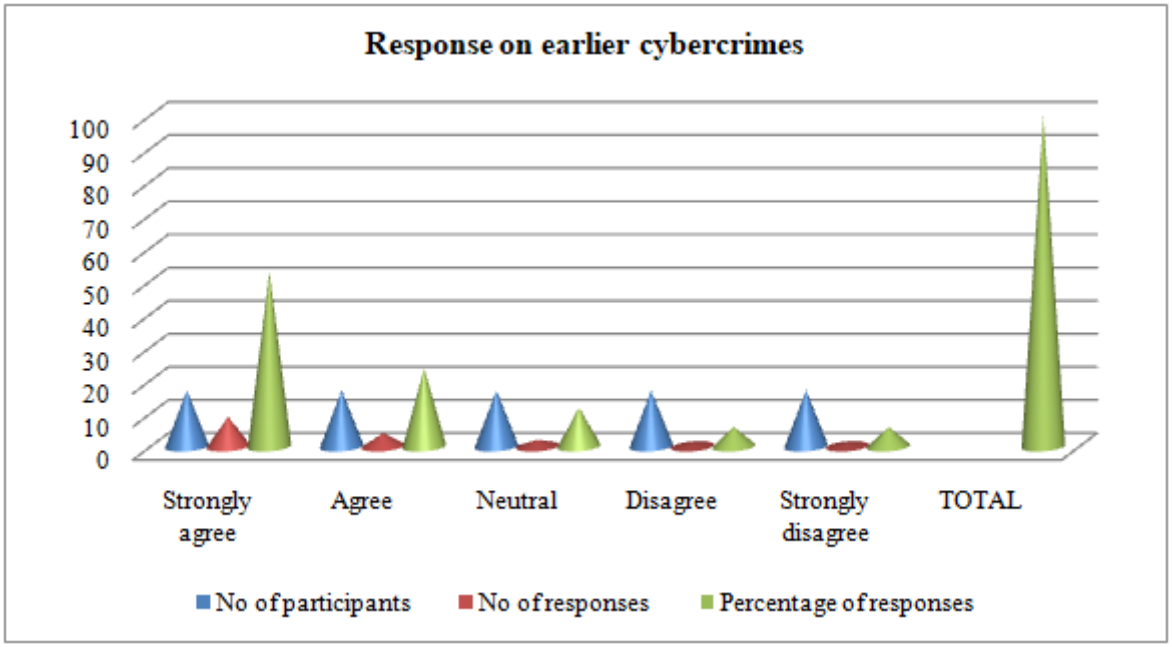

Figure 6: Graphical presentation on "Sample 6" response

Q.7) Do you agree that your device contains several tech-savvy software that can increase the chances of cyber attacks?

Responses	No of responses	Percentage of responses
1. Strongly agree	8	47.05882353
2. Agree	4	23.52941176
3. Neutral	1	5.882352941
4. Disagree	3	17.64705882
5. Strongly disagree	1	5.882352941
TOTAL	**17**	**100**

Table 7: Response on seventh sample question

This sample targets software's ability to increase the chances of cyber attacks. 8 of 17 persons have strongly agreed on this point, while 4 of 17 have agreed on this point. Almost 47% responses are put under the "strongly agree" section and 23% responses are submitted under the "agree" section. 4 of 17 have preferred to go with "disagree" and "strongly disagree" responses making a percentage of nearly 18% and 6% respectively to put their response under these categories. The sample has received one neutral response as well.

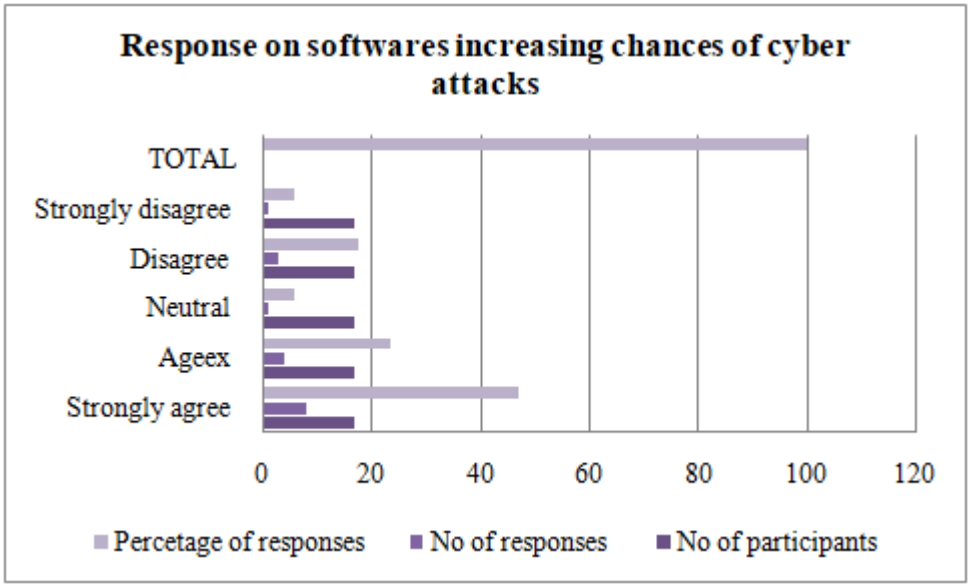

Figure 7: Graphical presentation on "Sample 7" response

Q.8) How far do you agree that you are faced with fraud actions during this period?

Responses	No of responses	Percentage of responses
1. Strongly agree	5	29.41176471
2. Agree	6	35.29411765
3. Neutral	1	5.882352941
4. Disagree	4	23.52941176
5. Strongly disagree	1	5.882352941
TOTAL	**17**	**100**

Table 8: Response on eighth sample question

Question number 8 is made to judge the number of fraud actions during this crisis period. Almost 29% and 35% have put their response against the "strongly agree" and "agree" category. On the other hand 4 participants have disagreed on this point making a percentage of 23.5% responses under the "disagree" option. Only one participant has strong leaders agreed on this point. The sample has received one neutral response as well.

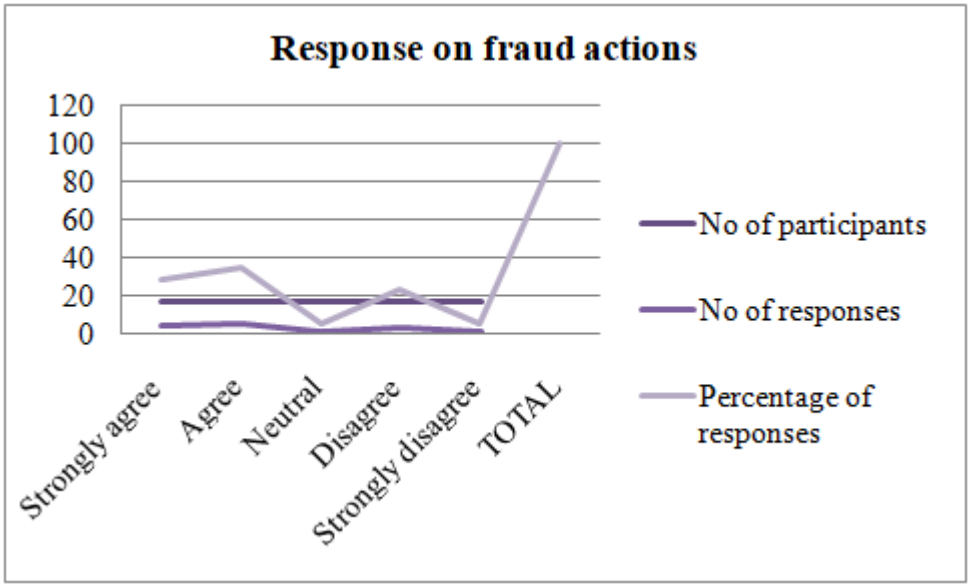

Figure 8: Graphical presentation on "Sample 8" response

Q.9) How far do you agree that your company follows cybercrime regulations to control these incidents?

Responses	No of responses	Percentage of responses
1. Strongly agree	6	35.29411765
2. Agree	5	29.41176471
3. Neutral	0	0
4. Disagree	3	17.64705882
5. Strongly disagree	3	17.64705882
TOTAL	**17**	**100**

Table 9: Response on ninth sample question

This question is made to judge whether companies in the UK follow cyber crime regulations or not. As per the analysis 11 of 17 participants have put their positive responses against the "strongly agree" and "agree" option. Almost 35% responses have gone under the "strongly agree" section while another 29% responses have gone to the "agree" option. However, 9

participants have put their negative responses under "disagree" and "strongly disagree" category respectively. Nearly 17.6 percent have put their responses against these two sections. The section has received no neutral responses.

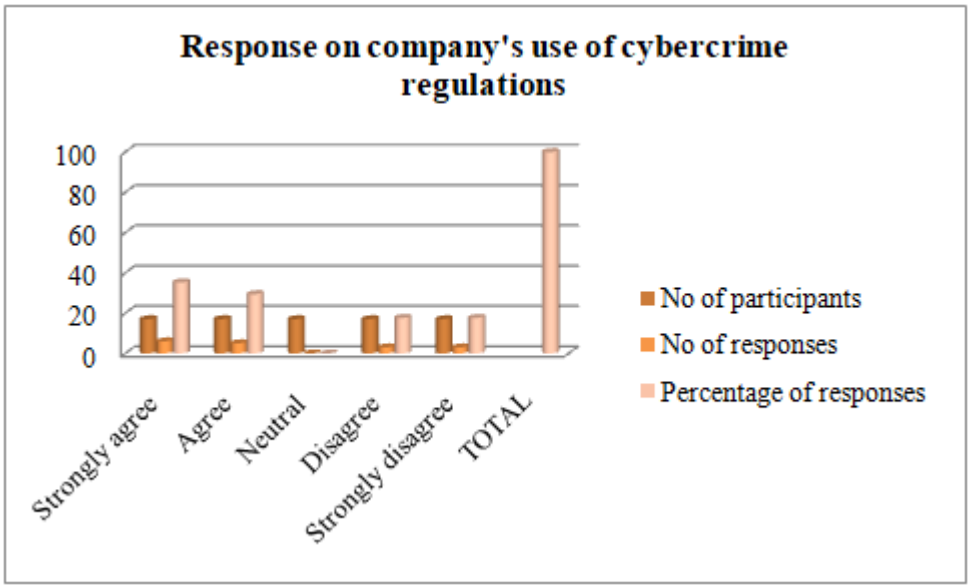

Figure 9: Graphical presentation on "Sample 9" response

Q.10) Do you agree that USB drives are well efficient to provide cyber security?

Responses	No of responses	Percentage of responses
1. Strongly agree	9	52.94117647
2. Agree	5	29.41176471
3. Neutral	0	0
4. Disagree	1	5.882352941
5. Strongly disagree	2	11.76470588
TOTAL	**17**	**100**

Table 10: Response on tenth sample question

This analysis is made to judge USB drives ability to control cyber crimes. 9 12 participants have strongly agreed to this point making almost 53% responses under this category. Another

five persons have agreed on this case making it almost 29% responses under this option. However the section has received three negative responses as well. One of 17 participants has disagreed while another 2 you have strongly disagreed on this point. This number shows almost 6% off of this agreement and 12% of strongly disagreement on this regard. The section has received no neutral responses that has proved that people knows about the problem.

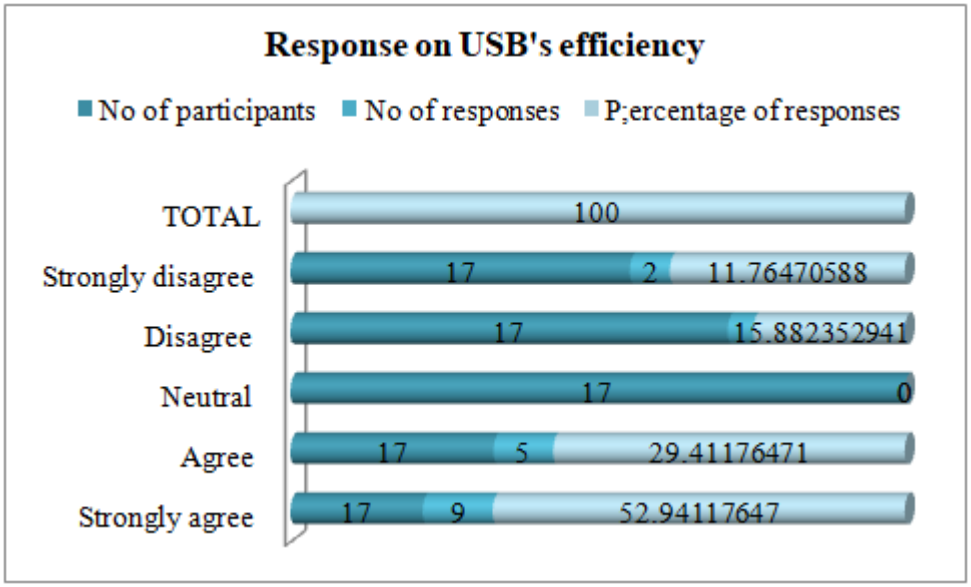

Figure 10: Graphical presentation on "Sample 10" response

2.3. Conclusion

Global pandemic has put the world to work from home during the Coronavirus pandemic situation. However it has been proven that probability of cyber crimes has extensively increased during this period of time. The discussion has provided a detailed understanding of cyber crimes during this period. This section has provided a strong discussion against cyber risk management during the work from home period. The primary analysis troops that most of the employees suffer due to the increasing rates of data breaching issues. During this period, cybercriminals have increased sending scam emails by hacking company's official email IDs. These emails claim to have a virus cure offering financial reward to the users. Once employees click on them the dodgy websites download viruses onto their devices and steal their passwords. The government of the UK has specific regulations to control cyber crimes. The report has scheduled 10 questions to judge the exact condition of cyber crimes during these eight months. The study has received both positive and negative responses from

the. However, in some cases they are observed hesitating while providing honest answers. Proper ethical code is maintained while recording employees' responses.

Reference list

Apuke, O.D., 2017. Quantitative research methods: A synopsis approach.Kuwait Chapter of Arabian Journal of Business and Management Review, 33(5471), pp.1-8.

Basias, N. and Pollalis, Y., 2018. Quantitative and qualitative research in business & technology: Justifying a suitable research methodology.Review of Integrative Business and Economics Research, 7, pp.91-105.

Rutberg, S. and Bouikidis, C.D., 2018.Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research.Nephrology Nursing Journal, 45(2), pp.209-213.

Ryder, C., Mackean, T., Coombs, J., Williams, H., Hunter, K., Holland, A.J. and Ivers, R.Q., 2020. Indigenous research methodology–weaving a research interface. International Journal of Social Research Methodology, 23(3), pp.255-267.

Susilo, H., Lestari, S.R., Lukiati, B. and Sudrajat, A.K., 2019. Enacting Life-Based Learning (LBL) Approach in Quantitative Research Methodology Course: The Case of Biology Education Students.JPP (JurnalPendidikandanPembelajaran), 26(2), pp.66-74.

Tan, S.L., Vergara, R.G., Khan, N. and Khan, S., 2020. Cybersecurity and Privacy Impact on Older Persons Amid COVID-19: A Socio-Legal Study in Malaysia. *Asian Journal of Research in Education and Social Sciences*, *2*(2), pp.72-76.