SOLENT UNIVERSITY

MSc COMPUTER ENGINEERING

AJAZALI SAIYED

MAA111 Pilot Project

14th December

Report 1: HOME WORKING: MANAGING THE CYBER RISKS

Table of Contents

1. Introduction and Background Report

1.1 Introduction

Work-from-home or home working has become predominant in current age due to introduction of COVID-19. However, with increase of home working individuals, cyber-crimes have reached new heights along with concurrent cyber-security initiatives. Cyber-security plays a massive role in most organisations due to prevalence of sensitive data and resources. In current paradigm of technology, it has become increasingly simple to infiltrate other networks or systems and cause substantial damage. This damage can be in the form of data theft, privacy exploitation, system crashing, phishing and more. Despite recent resurgence of cyber-threats, this issue originated from nominal research projects.

This program and technology speeded like a wildfire and introduction of antivirus became an absolute necessity due to increased exposure of cyber-threats and cyber-criminals. Cyber-security became an important concept late 20th century after discovery of *"creeper"* virus; in this time ***ARPANET*** was more prevalent, which is an earlier form of internet (Lexisnexis.co.uk, 2020). This virus had ability to infiltrate a system and duplicate itself within any system and spreads to other systems as well. However, after introduction of *"Rivest-Shamir-Adleman (RSA) Algorithm"*, cryptography came into light.

This cryptography became foundation of modern cyber-security practices. However, in current generation, with an immense amount of cyber-security improvements, cyber-thefts and criminal activities regarding digital interface have improved as well. Nevertheless, in current atmosphere COVID-19, cyber-crime has reached its peak due to increased involvement of people in digital atmosphere.

COVID-19 forced most geopolitical regions to maintain social distancing and go into lockdown situations. This situation and gradual increase of infected patients afflicted mind of people with fear. This fear acts as a catalyst for cyber-criminals, which enables them to use it as a bait and introduce malware to individual systems. Cyber-criminals are using scam emails, websites and providing thumbnail bait to lure people into digital traps, which allows different forms of virus to enter individual systems; current pandemic accelerated digitalisation in UK and in different other geopolitical regions such as US, China, Russia and more.

In prime time of lockdown, cyber-crimes such as spam messages, malware attacks, ransomware infiltration and more reached its highest peak in UK. Approximately 907,000 messages and 737 malware incidents were spotted in UK (Lexisnexis.co.uk, 2020). Furthermore, this situation indicates an increase in malicious *Uniform Resource Locators (URLs)* to almost 48,000 cases. Thus, this discussion provides an overall idea regarding current situation of cyber-threats in pandemic. Akin to UK, other geopolitical regions faced similar problems as well. Increased internet traffic has made this task of safeguarding systems from potential cyber-threats a massively complex task.

Work-from-home has become common in this pandemic, which is effectively increasing internet traffic and employees of different organisations are using systems from their homes without using proper security protocols. Businesses and charities are providing adequate service regarding cyber-security measures and current increase of cyber-threats elevated them further as well. Figure 1 indicates such elevation in efforts from organisations in UK, in 2019, 78% of UK businesses used cyber-security measures and in 2020, this statistics increased to 80% (Assets.publishing.service.gov.uk, 2020). However, this increment is not enough since a considerable percentage of UK businesses are not using cyber-security measures and in current elevation of cyber-theft cases, ignorance can become a major issue.

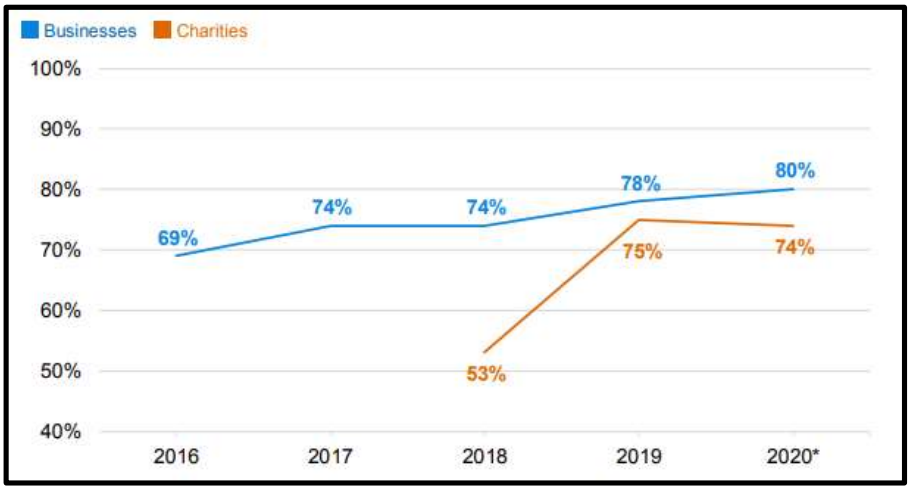

Figure 1: Cyber-Security Initiatives by UK Businesses and Charities

(Source: Assets.publishing.service.gov.uk, 2020)

This study aims at providing a clearer outlook on current situation and possible gateways to improve cyber-security measures. This research provides background about external literature findings as well to encompass a strong base for current research. In addition, this background

analysis is done through a systematic review structure. This structure aims at providing better transparency in learning and provides a strong structural design to encompass all key features in external pieces of literature. Furthermore, below section encompasses research question for this research study and provides a guide path for this research.

1.2 Research Question

Aim of this study is to find impact of increasing cyber-crime activities in UK over home working individuals due to COVID-19 lockdown and provide possible ways to restrict adverse impact. Research question for current study is mentioned below.

- What is the impact of increasing cyber-crime activities in UK over home working individuals due to COVID-19 lockdown and possible ways to restrict these adverse impacts?

1.3 Background

This section provides in-depth analysis regarding external literature findings and encompasses key features identified in this research. Systematic review focuses on building a structured analysis regarding current literature findings and provides concurrent evaluation regarding present research prospects. Table below illustrates a systematic review regarding current research topics and provides relevance of each article regarding current research.

Author	Aim	Method	Outcome	Limitation	Relevance
1. Abukari, and Bankas, 2020	Current article aims to identify cyber-security hygiene protocols for	Method used in this article is secondary data collection method. Nevertheless, this research	This article proposes different protocols and strong emergence of security tools is	This study provides a clear suggestion regarding protocol required to follow in	Current article finds strong relevance to present research topic. This research

	teleworkers in current generation of COVID-19.	addresses different remote access methods for teleworkers to work smoothly.	evident as well. Nevertheless, strict usage of proposed protocol in this article can help in reducing cyber-crime.	current atmosphere. However, this study does not focus on any particular geopolitical region, which increases its potential of general discussion rather than critical discussion.	focuses on finding impact of increasing cyber-crime in UK and suggesting possible mitigation methods. Reviewed article provides in-depth analysis regarding different protocols, which can help in reducing cyber-crime threats. However, this study does not focus on UK, making it lose its relevance in some points.

2. Weil and Murugesan, 2020	This article aims to identify different reliable information for software developers and managers of organisations to help them keep track of current technological shifts.	Secondary data collection methodology is used in this article since most data gained for this research is through secondary sources. This article does not provide any specific information regarding its applied methodology; however, judging from analysis, this research uses secondary sources to conduct its analysis.	Current article explores some minor aspects of different Information Technology (IT) risks and various resilience initiatives. This article acts as a strong medium of providing information about current condition of IT industry due to COVID-19 exclusively.	This article does not propose any significant limitation. However, wide scope of this research is one of primary limitation of this research since current research loses its critical aspects.	Current article finds low relevance regarding present research. For example, this article provides impact of COVID-19 in cyber-crimes. However, this information is not focusing on any certain geopolitical region and most data proposed in this article aims at encompassing impact of COVID-19 on IT field. Thus, despite some

					relevance regarding current research, this article fails in finding any strong connection with current research.
3. Okereafor and Adebola, 2020	This article emphasises on reviewing different cyber-security effects of COVID-19 panic on different digital systems and cyberspace.	This article focuses on secondary sources from trusted locations such as *"World Health Organisation (WHO)"* and more. Nevertheless, this article discusses different factors of COVID-19 in cyber-security through a	Current article emphasises on cyber-security importance and indicates different activities, which can help individuals to reduce overall cyber-threats such as not clicking URLs of unauthorised websites and more.	Present study indicates different factors of COVID-19 and its influence of cyber-security; however, it fails in identifying any particular geopolitical region and provides effects over that region. In addition, this article fails in	This study provides a strong relevance regarding current research topic since both pieces of research focus on increasing cyber-threats due to COVID-19 and its impact. However, this study fails in identifying

		report structure.	Furthermore, this study presents dominating importance of increasing cyber-threats due to current pandemic and indicates that individual panic and anxiety regarding current incident is increasing cyber-threat vulnerability.	providing any direct understanding towards effects of increasing cyber-threats in-home working individuals.	any certain regional context and it does not provide any dedicated findings regarding home working individuals. Research topic of this study focuses highly on home working individuals and effects of COVID-19 over them; this study does not provide any dedicated data regarding that factor, which makes this article reduce its relevance

					regarding current study.
4. Wangila, 2020	Current article aims at evaluating different organisational measures during this COVID-19 epidemic.	This article provides a secondary data analysis interface. Data used for this research are from verified sources and it focuses on different cloud-security sources since this research focuses primarily on cyber-security.	According to outcome of this research article, COVID-19 has certainly affected individual organisations and forced them to take unprecedented methods including higher amounts of digital involvement in both external and internal atmospheres. However, this article states that most organisations are able to	Current article does not propose any significant limitation in its paradigm of research. However, akin to other studies mentioned in this systematic review, this article suffers limitations of being general. This does not focus on any certain geopolitical region, which reduces its critical outlook.	Present article fails in finding strong relevance to current research since it fails in identifying effects of COVID-19 over any certain geopolitical region. Furthermore, aspects of home working are mentioned less in this analysis making it less relevant to current aspects of research.

			hold their position and suffer low consequences in this situation due to current advancement of technology.		
5. Pranggono and Arabo, 2020	This paper aims at studying different effects of COVID-19 pandemic over cyber-security issues. Furthermore, this article provides different viable approaches for home working individuals to reduce	This article applies a secondary research method to collect different data and information required for research. Data sources used in this article are authentic and mostly focus on different cyber-security activities (Borkovich	According to current article, cyber-threats increased massively in current paradigm of COVID-19. This study states that most affected region in this situation is healthcare organisations and they need to imply new systems to	No such limitation is mentioned in this article; however, since this is secondary research, a large portion of this study is dependent upon used data sources. This high dependency is primary limitation of this article.	This article finds strong relevance to current research topic since it provides adequate information regarding cyber-threats due to COVID-19. Furthermore, this study provides data regarding impact of this pandemic over home

	vulnerability towards cyber-threats.	and Skovira, 2020).	overcome this vulnerability. Furthermore, this article provides information about vulnerable individuals becoming prey to cyber threats as well.		working individuals and provides geopolitical region context as well, which increases critical aspect and relevance of this research as well.
6. Hakak *et al*. 2020	This study focuses on evaluating different malicious activities associated with COVID-19 and various mitigation methods.	Research method used in this article is a secondary data collection method and data sources in this article are authentic.	As per current article, different categories of cyber-attacks are present, ranging from disrupting services to information theft. This article concludes adverse	Current research study primarily focuses on cyber-attacks and its increasing factors in current atmosphere of pandemic. Thus, this study has major limitations	Current article finds a low amount of relevance to present research study since all variables do not align perfectly with proposed research topic. Some correlations

			impact of COVID-19 over cyber-security. Nevertheless, current article also claims that mitigation strategies can facilitate cyber-attack prevention planning.	regarding exploring different critical aspects such as regional effects, individual impacts and more.	are present such as increasing cyber-attacks due to COVID-19 and more. Nevertheless, current article does not address specific regional context or effect over home working individuals, which are core points of current research study.
7. Mandal and Khan, 2020	This paper aims to highlight different areas responsible for causing security	Current paper focuses on collecting data through trusted secondary sources such as WHO,	According to current article, social engineering attacks improved by a	Akin to previous articles mentioned in this section, this article fails in identifying	Relevance of this study with proposed research topic is low since this article

	breaches and propose different generic preventive methods.	McAfee Labs and more. Hence, current article focuses on using secondary data collection method.	considerable margin due to introduction of COVID-19. Nevertheless, this paper claims that entire security structure needs reformatting. Furthermore, this article indicates improvement of home working and other remote activities through this resurgence of security infrastructure.	any regional context, which is considered as its primary limitation (Borkovich and Skovira, 2020).	addresses one key aspect of proposed research topic and does not provide a critical outlook about regional or individual aspects.
8. Tan *et al.* 2020	Aim of this research article is to explore	This article undertakes a primary qualitative	According to current article, older people are	Current article focuses on individual	This research has relevance to proposed research

	different cyber-security mindsets of older persons in Malaysia and effect over individual well-being.	research method using semi-structured interviews. This article solely focuses on older people of Malaysia.	extremely vulnerable to cyber-threats since they are a novice in handling cyber-attacks and unwarily attracted to cyber-attack baits. Further analysis suggested that older people in Malaysia are keen to learn different aspects of cyber-security; however, they are restricted due to low governmenta l initiatives.	interviews and provides data regarding each interview result. However, results of this focus primarily on interview results of people having limited knowledge of cyber-security. Thus, misleading data can occur in this research framework.	topic; however, geopolitical region selected in this study is Malaysia and for proposed research, it is UK. Thus, this decreases overall relevance.
9. Borkovich	This article identifies	Primary qualitative	According to outcome of	This article faces a	This study finds strong

and Skovira, 2020	cyber-risks and different additional positive effects of home working.	approach is undertaken for this research, including interviewing participants through a 30-minute zoom video using open-ended questions.	this research, several areas of improvement are necessary rather than improving security infrastructure. Furthermore, this article identifies that home working will continue in future as well; thus, proper training and cautiousness is necessary for each individual.	massive limitation of not addressing any critical aspect of its research topic. Nevertheless, robust design of this study covers up that limitation; however, low number of interviewee is another major limitation in current study.	relevance to proposed research topic since this study addresses all key aspects such as effects of COVID-19 over home working individuals regarding cyber-security issues and more. However, regional context is not evidently making it less relevant.
10. Hoffman, 2020	This article aims at analysing impact of telehealth facilities in	This study focuses on using secondary data collection	According to current condition of COVID-19, telehealth helped in	Limitations of this study include a lower amount of critical outlook.	Low relevance is present since this study primarily focuses on

	COVID-19 and effects of cybersecurity, reimbursement, liability, licensure, technological access and artificial intelligence over it.	methods.	improving overall medical systems. However, it faces cyber-security issues, which can be solved through technological innovation.		telehealth and discusses cyber-security as an ancillary factor.

Table 1: Systematic Review

This study indicates a lower amount of prevalence regarding current research topic. Thus, primary research is necessary to gain adequate data.

Reference list

Abukari, A.M. and Bankas, E.K., 2020. Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *International Journal of Scientific & Engineering Research*, *11*(4), pp.1401-1407.

Assets.publishing.service.gov.uk, 2020. Cyber Security Breaches Survey 2020. Viewed on 10/12/2020 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf>

Borkovich, D.J. and Skovira, R.J., 2020. Working From Home: Cybersecurity In The Age Of Covid-19. *Issues in Information Systems*, *21*(4), pp.1-13.

Hakak, S., Khan, W.Z., Imran, M., Choo, K.K.R. and Shoaib, M., 2020. Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. *IEEE Access*, *8*, pp.124134-124144.

Hoffman, D.A., 2020. Increasing access to care: telehealth during COVID-19. *Journal of Law and the Biosciences*, *7*(1), p.43.

Lexisnexis.co.uk, 2020. About Covid-19. Viewed on 10/12/2020 <https://www.lexisnexis.co.uk/blog/covid-19/accelerated-digitisation-cybercrime-in-a-post-covid-19-world>

Mandal, S. and Khan, D.A., 2020, September. A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 837-842). IEEE.

Okereafor, K. and Adebola, O., 2020. Tackling the Cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. *Journal Homepage: http://ijmr. net. in*, *8*(2), pp.1-14.

Pranggono, B. and Arabo, A., 2020. COVID-19 pandemic cybersecurity issues. *Internet Technology Letters.1*, pp.1-6.

Wangila, F., 2020. Organizational Cyber-Security Measures During COVID-19 Epidemic. *International Journal of Innovative Science and Reserach Technology*, *5*(3), pp.1340-1341.

Weil, T. and Murugesan, S., 2020. IT Risk and Resilience-Cybersecurity Response to COVID-19. *IT Prof.*, *22*(3), pp.4-10.