ASSESSING AND IMPROVING SECURITY AWARENESS AND CONCERNS IN TELEWORKING

by

Biliangyu Wu

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology

West Lafayette, Indiana

May 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Ida Busiime Ngambeki

Department of Computer and Information Technology

Prof. Jeffrey L. Brewer

Department of Computer and Information Technology

Prof. Kevin C. Dittman

Department of Computer and Information Technology

Approved by:

Dr. John A. Springer

ACKNOWLEDGMENTS

I would like to thank my advisor Dr. Ida Ngambeki providing guidance and feedback throughout my graduate study and my project. Thanks also to Prof. Kevin Dittman and Prof. Jeffrey Brewer for giving advice and support to my project. Lastly, I would like to thank my family for their understanding and support to my graduate study.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

The unexpected and unprecedented global pandemic of COVID-19 has brought dramatic changes to the whole world. As a result of social distancing instituted to slow the pandemic, teleworking has become the new norm in many organizations. The prevalence of teleworking has brought not only benefits to organizations, but also security risks. Although teleworking has existed for decades and many security related issues have been studied by previous research, the researcher didn't find any studies that have assessed organization employee's security awareness and concerns in teleworking. Considering the vital importance of human security awareness in protecting information security, it is necessary to learn the security awareness situation in teleworking. Furthermore, employees with low security awareness should be trained to improve the awareness level. Therefore, this research intends to examine the current teleworking security awareness and concerns in organizations by conducting a survey of workers. Through the survey answers, the researcher found that the security awareness varies in groups of teleworkers who are at different ages, from different industries and different-sized organizations. Meanwhile, the researcher also found that COVID-19 pandemic does not have much impact on people's security concern in teleworking scenarios.

INTRODUCTION

Described as remote working supported by information technology (Gray et al., 1993), telecommuting has begun to gain more and more attention in academia and industry since the 80s (Daniels et al., 2001). The rapid development in information technology had made working at home or other places possible for the first time after the industrial revolution when factory work became the norm. Meanwhile, because of societal development, white-collar jobs that mainly deal with information and communications instead of manufacturing and manual labor, have gradually become one of the biggest working groups (Haddon & Silverstone, 1992). Therefore, more and more organizations tried adopting this approach. However, the number was very small at the time according to Daniels et al.(2001): the percentage of teleworkers was less than 5 percent in Western Europe and the US in the 1990s even though most people were optimistic about the future of teleworking. As one of the most significant components that support teleworking, information technologies are continuously evolving to meet the requirements and drive changes. In the 1990s, text-based communication systems such as E-mail and Internet Relay Chat were the most common means for communicating in teleworking because of the cost and technology restrictions (Wellman et al., 1996). Though multi-media communication technologies such as videoconferencing, tele-writing and fax were invented at that time, they could only be found in the meeting rooms of organizations (Nakamura et al, 1995). With the advent of the new millennium, more technologies were created or adapted to support teleworking. The introduction of virtual private network (VPN) made it easy and secure to access organization's internal resources from anywhere (Scarfone & Souppaya, 2007). Also, the rise of enterprise instant messaging software such as MSN Messenger greatly improved the efficiency and experience of synchronous communication and thus made teleworking accepted by more organizations.

The unexpected and serious global pandemic of COVID-19 brought significant changes to the workplace and pushed teleworking into the spotlight. Under the threat of the virus, companies, schools, and other organizations are trying to keep running while protecting individuals from infection. Voluntarily or not, more and more organizations began to adapt to this unprecedented situation with the support of information technology, making teleworking a new norm for the first time in the history. Because of the rapid growth in teleworking, more and more security issues are emerging . 46% of global businesses have encountered at least one cybersecurity scare since shifting to a remote working model during the COVID-19 lockdown (Till, 2020), 71% of business decision makers believe that the shift to fully remote working during the Covid-19 crisis has increased the likelihood of a cyber breach (SME, 2020). Therefore, it is necessary to examine the security risks in teleworking scenarios.

CHAPTER I: LITERATURE REVIEW

Development of Teleworking

Teleworking emerged in the 1980s and developed alongside the Internet. Teleworking is defined as “a work flexibility arrangement under which an employee performs the duties and responsibilities of the employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work” in Telework Enhancement Act of 2010 (Congress, 2010). Before the explosion of teleworking triggered by the COVID-2019 pandemic in 2020, most workers were required to report to a fixed workplace. As the number of organizations gets bigger and they grow in size, more management and communication related workers are required, creating a large number of white-collar workers (Haddon & Silverstone, 1992). Unlike workers in factories, stores, or construction sites, most of their time is spent on communicating and document processing in the office. White-collar jobs can be summarized as information exchanging and processing. Thanks to the development of the information technology industry, information is able to flow through the Internet and be processed by personal computing devices. These two factors have made teleworking possible. Although some pioneer organizations started adopting teleworking and more attentions was put on this promising working style since the 90s (Daniels et al., 2001), it wasn’t a common practice until the outbreak of COVID-19 (Close et al., 2020).

Looking back at the history of teleworking, all kinds of technologies were utilized for better information exchange and processing. In the early stages when the Internet was not as fast and powerful as it today, telephone was mostly used for communication and simple arrangements. As for more sophisticated multi-media information like images and documents, fax and email were the main channels. On the other hand, although other technologies like videoconferencing and tele-writing boards were available at that time, the cost was so high that only organizations could afford it (Gray et al., 1994. Nakamura et al, 1995). At that time, teleworking was thus more like “telecommuting”, because the system supported mainly simple information exchange from peer to peer, and the penetration rate of the personal computer was not high enough (Alsop, 2010). In the late 90s, virtual private networking (VPN) was invented and then became one of the most important technologies for teleworking in the 21st century. By encrypting data at a low level, VPN protects information from access by any other interconnection nodes in the Internet including the Internet service provider (Bucşa, 2020), allowing employees to easily and securely access the internal resources of their organization via public network from anywhere. At the beginning of the second decade of 21st century, Google released a set of web-based applications: Docs, Sheets, Slides, and Forms, which allow multiple users to edit files at the same time and see the changes made by others synchronously (2012). What's more, the improvement in the penetration rate of the PC and smartphone and the performance of these devices allows more versatile software to run. Communication platforms such as Slack and Microsoft Teams were also created. These platforms consist of built-in functionalities such as instant messaging, scheduling and videoconferencing, while also allow users to customize their software with add-ins developed by third-party developers. This makes the software so versatile that people can do a variety of things in teleworking with it.

Benefits and Challenges of Teleworking

The increasing number of organizations and individuals that are practicing teleworking indicates how attractive this new technology is, and the many benefits it brings to workplaces. The benefits of teleworking include:

- Better flexibility. One of the most important benefits of teleworking is flexibility. The loose bond between employer and employee created by this flexibility allows not only employers to source task to on-demand workers, but also employees to better balance their work and life (Morgan 2004, Fílardí & Zaníní 2020).
- Reduced cost. With less employees onsite, organizations can save part of the cost for utilities and rent to support the office. On the other hand, the time and money spent on commuting are also saved by the employee (Pérez et al. 2002).
- Higher employee satisfaction. Thanks to the flexibility of teleworking, employees have more autonomy over themselves. As a consequence, they have higher morale, higher productivity and thus, lower turnover (Bailey & Kurland 1999, Fílardí & Zaníní 2020).
- Social responsibility. As teleworking reduces traffic caused by commuting, it is also beneficial to society, for example by reducing traffic congestion and air pollution. Therefore, it can help with improving companies' relationships with communities (Bailey & Kurland, 1999).

However, at the same time, teleworking also introduces issues that are worth noting. Here are some challenges posed by teleworking:

- Difficulties in management. Since users are not onsite, it is very difficult for managers to monitor and control employees. For organizations that are at the beginning of adapting to teleworking, big organizational structural changes are necessary that can also be challenging. (Pérez et al. 2002)
- Difficulties in teamwork. When team members are geographically distributed, interaction, communication and collaboration become very difficult. If people do not meet each other, trust and team culture can be hard to establish. What is worse, the differences in schedule and working habits make the teamwork even harder (Bailey & Kurland, 1999).
- Security risks. To support teleworking, all kinds of technologies including software and hardware are used. While generating benefits, these technologies also generate new information security risks, threatening organizational success (Yang, 2012).
- Productivity. Since management cannot monitor workers and home environments often introduce distractions, teleworking can sometimes result in a reduction in productivity.

Security Issues in Teleworking

By allowing employees to work from places other than the office, and to access organizational information from external sites, teleworking greatly improved working efficiency and flexibility, but also introduced serious security risks. Therefore, in the past decades of teleworking, some studies were conducted to identify the security issues in teleworking and find the solutions to them.

To identify security issues, the famous CIA triad model provides a good framework to start. The letters C, I and A refer to confidentiality, integrity, and availability respectively. Confidentiality means that only authorized people are able to access sensitive information. The failure in confidentiality means that information is accessed by unauthorized people who may take advantage of it or sell it for profit. Integrity requires maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle (Rouse, 2019). It guarantees that information cannot be added, modified, or removed inadvertently or maliciously. Lastly, availability suggests whether people can access the services and resources of a system as needed at any time from any place. The system's availability is ensured by adequate capability to handle legitimate requests and resist malicious requests and failsafe mechanisms to deal with all kinds of potential halting. Yang et al. summarized the three dimensions as disclosure, modification, and destruction of data (2012).

Based on the cause of the security issues, they can be categorized into three types: i) personal, ii) technical, and iii) organizational.

- Personal security issues:
  - Lack of security awareness. Humans are probably the weakest point in a system and is also very difficult to reinforce. Most security breaches are caused by lack of security awareness (Peltier, 2013), and many teleworkers do not realize that they can become the source of threats to information security (Ampomah et al., 2013).
  - Unauthorized access. It is very common that household members borrow each other's computers for temporary use. Software that allows employees to work remotely also increases the chance that unauthorized access happen in this situation, and thus increases the risk of inadvertent corruption of files and the introduction of malware (Carnahan & Guttman, 1998). Another example is that an employee might leave the device unlocked in a cafeteria when he/she goes to restroom, which presents an opportunity to an unauthorized person to access device (Yang et al., 2012).
  - The lack of responsibility and self-discipline. With the flexible access to internal resources from almost anywhere, teleworkers are more likely to be motivated by economic or ethical reasons to hand over sensitive information to external persons (Sturgeon, 1996 and Ampomah et al., 2013).
  - Identification compromised. With less supervision of organizations in teleworking, it is hard to tell whether the person behind an internal ID is himself/herself (Ampomah et al., 2013). Therefore, once a teleworker's identification is compromised, it will take longer for the organization to react and take countermeasures.
  - Interruption. A teleworker's workplace, in comparison to official workplaces, is more susceptible to be interrupted by environment factors such as power failure and competing calls for attention (Sturgeon, 1996 and Ampomah et al., 2013). When teleworkers have to stop their job to deal with other things, unsaved documents, unsent emails and other interrupted jobs might cause data loss and communication failure.
  - Theft. Similar to the risk of interruption, teleworking also increases the risk of being a

target of theft. Considering the data saved in all kinds of digital devices, once the devices with important data are stolen, it means a loss of control of the assets and information (Sturgeon 1996). Since offices usually have better security guards and other monitors, teleworkers are facing more challenges to protect their devices from theft, especially for those who telework in public places.

  - COVID specific attacks. During the past several months, COVID-19 has become a continuously important topic around the world. While the researcher is paying so much attention to all kinds of information related to the pandemic, attackers are also leveraging the public's insatiable desire for news and advice related to Covid-19 (Evangelakos, 2020). It is reported that email scams related to COVID-19 surged 667% in March 2020 (Shi, 2020), and users are three times more likely to click on pandemic-related phishing scams (Verizon, 2020).

- Technical security issues:
  - More access to devices by intruders. Working outside the workplace gives more opportunities for intruders to access the corporate system without being onsite (Carnahan & Guttman, 1998). Without the protection of enterprise security technologies such as firewalls, threats such as eavesdropping and man in the middle attacks might be conducted where the victim does his/her job remotely. In addition, portable devices often connect the Internet through WIFI, which adds risks to information security especially when it's public WIFI such as those in hotels (Yang et al. 2012 and Scarfone et al. 2009).
  - Inadequate IT support. With people distributed in different places, organizational IT engineers cannot provide as much support as they do on-site. Therefore, device and network problems might become a serious obstacle in some situations, leading to delay in progress or resource inaccessibility (Carnahan & Guttman, 1998).

- Organizational security issues:
  - Inadequate security policy and procedures. Some organizations do not have adequate security policy and procedures to guide and discipline their employees.
  - Lack of organizational commitment. Teleworkers may not be able to receive as much security support as their colleagues who are working on-site because IT engineers tend to give priority to those who are physically visible (Ampomah et al., 2013).

- Difficulties in monitoring and control. When employees are working onsite, their behavior and traffic on the Internet can be easily monitored and controlled. While for teleworkers who are considered potential insider threats (Yang et al. 2012), monitoring and controlling their activities can become very difficult and expensive (Peacey, 2006).

Facing so many security issues in teleworking, some researchers have proposed measures targeting specific problems (e.g. Sturgeon, 1996 and Chávez, 2020), while others try to develop solutions from a systematic perspective. James studied 4 typical security models used in the traditional working paradigm to examine whether these existing security models are still suitable for teleworking (2011). The Chinese-Wall model deals with confidentiality and integrity by separating data of two different users (Brewer and Nash, 1989) deals, the Clark-Wilson model uses role-based mechanism to ensure data integrity and availability(Clark and Wilson, 1987), the Eggshell model focuses on protecting information from unauthorized network access to enforce confidentiality and availability (Bragg et al, 2004), and the Onion model defines layers of control to preserve the confidentiality and availability of information (Bragg et al, 2004). Based on security threats in teleworking, James listed security policy enforcement mechanisms against the threats, and proposed a secure teleworking model which uses these mechanisms to enforce confidentiality, integrity and availability in teleworking. By considering the existing model with defined telework security model and policy enforcement mechanisms, he found that none of the four can fully support the attributes of secure teleworking model. Thus, a security model that suits the needs of teleworking should be designed and applied.

Aiming at protecting individuals and organizations from social engineering (SE) attack, Abukari and Kwedzo Bankas proposed a set of comprehensive cybersecurity protocols for individuals and organizations who are using teleworking. This protocol uses three levels of protocol to enhance the security: organizational level, individual level, and policy level (2020). On the organizational level is training protocol. It improves organizational SE performance in SE awareness, SE penetration strategy, safe behavior, and reporting channel by assessing and training. As for individual level which is education protocol, it focuses on teleworkers' knowledges on internet ethics, recent dangers, deceptive approach, and best behavior during attacks. Lastly for policy protocol, it enhances the policy by addressing the necessary parts for a strong security policy, including personnel behavior, punitive measures, social engineering measures, preventive measures, desk policy, caller IDs, monitoring, social media, auditing and compliance. Across the three levels of protocols, an assessment-problem-training model is used, which means the object of the protocol will first be assessed to identify the problem or weakness, and then training targeting at specific problem or weakness is conducted. Since assessment indicates what should be improved and determines what training the objective will receive, the assessment of teleworking plays a significant role.

In terms of approaches to improve security awareness and capabilities, Evangelakos introduced breach and attack simulation (BAS) platform to launch continuous attacks that simulate the likely techniques and paths used by malicious actors (2020). By introducing BAS, Evangelakos wants to build employee's mindset and tactics against attackers under a controlled environment.

CHAPTER II

Research Justification

Thanks to the high-speed and low-latency network applied by more organizations, information technologies that allows employees to work from home or anywhere with Internet access is becoming increasingly attractive. While teleworking brings benefits as motivator, morale booster, and environmentally friendly alternative to ensure companies' success in conquering the virtual workplace (Godlove, 2012), it also introduces new security challenges into the system. As the weakest point of a system, security awareness plays a vital role (Peltier,2006). After reviewing more than thirty papers related to security awareness in teleworking, which were acquired through Google Scholar and Purdue University Library, the researcher found that although many literatures have addressed the challenges brought by teleworking and discussed the approaches to assess and improve security awareness, no one has done an assessment of employee's security awareness in teleworking.

Under the huge impact of COVID-19 pandemic, social distancing practice has transformed teleworking from an alternative to a new norm, and even necessity in certain conditions. The rapid increase of teleworkers attracts more attention than ever before, leading to higher risk of being target of cyberattack. Therefore, assessing and improving teleworking security awareness has become necessary to prevent and mitigate security threats. Through this research, the researcher hopes to add knowledges in following aspects:

- The security awareness level of teleworkers
- The gaps in teleworker's security awareness
- The security issues that concern teleworkers

Research Objectives

The research will be focused on assessing security awareness and concerns. So, the research objectives are:

- To assess employee's security awareness in teleworking
- To assess employee's security concern about teleworking.
- To identify the factors that influence security awareness.

- To assess teleworker’s concerns on different types of security issues.

Research Question and Hypothesis

This study aims at assessing employee’s security awareness and concerns about teleworking. Security awareness consists of three dimensions: attitude, knowledge, and behavior (Hassanzadeh et al. 2014). Each of these dimensions should be studied in order to assess the security awareness. Therefore, three research questions are proposed for security awareness assessment:

- What is employee’s attitude towards security in teleworking?
- What is the level of employee’s security knowledge in teleworking?
- What actions are teleworkers taking to ensure information security?

Besides, in order to identify the factors that influence security awareness, the following hypotheses will be tested:

H1: The level of security awareness in teleworking varies from one industry to another.

H2: The level of security awareness in teleworking has a positive correlation with age.

H3: The level of security awareness in teleworking has a positive correlation with education level.

H4: The level of security awareness in teleworking has a positive correlation with income level.

H5: The level of security awareness in teleworking has a positive correlation with teleworking experience.

H6: The level of security awareness in teleworking has a positive correlation with organization size.

For those who are aware of the importance of information security in teleworking, their concerns about security risks vary from one person to another, but some generality might exist. Thus, an additional research question should also be answered by extracting information from the assessment:

- What are teleworkers most concerned security risks related to teleworking?

CHAPTER III: METHODOLOGY

This research was conducted in a quantitative way based on survey used to assess employee's awareness and concerns related to teleworking. The survey was conducted by distributing online questionnaires with Qualtrics, an online survey platform. Through Amazon Mechanic Turk, a crowdsourcing website that is commonly used for on-demand tasks such as survey, participants from different industries will be recruited to take the survey. To acquire a comprehensive and sufficient dataset, the planned sample size was 450. Since the research aimed at assessing security awareness and concerns, the acquired data would be analyzed to examine the related hypotheses. This questionnaire had three sections: profile section, security awareness section, and security concerns section. The first section collected demographic information and teleworking related working experience. The second section was further divided into three parts based on the three dimensions of security awareness. The last section addressed the security concerns by asking questions about attitudes.

The assessment of security awareness was based on the awareness measuring tool proposed by Kruger & Kearney (2006). The original concept of the idea is to assess participants awareness about so-called "Golden Rules", six critical security risks, by measuring the three dimensions of awareness: attitude, knowledge, and behavior. However, these "Golden Rules" are, in fact, insufficient for addressing the security issues in teleworking. Therefore, the teleworking security issues identified in the literature review are adopted as the factors for assessment. In addition, Kruger & Kearney's original design (2006) was intended for an international gold mining company, thus, a weighting system was introduced to reflect the various situations and needs of divisions located at different places. As for this research, because it focused on the overall awareness and does not do any location-based comparative study, the weighting system was removed. In security awareness section, the researcher carefully designed the 19 questions to fully address and assess participant's awareness on each of the eight factors in three dimensions. Although these questions could not cover all security issues in teleworking, it covered the major security issues and risks in teleworking and can, thus, reflected the overall security awareness. The following table shows what survey questions are addressing each factors and dimensions.

Table 1 Question Association with Security Issues

	Attitude	Knowledge	Behavior
Access Control	23	22, 23	24, 40
Self-Discipline	25, 26, 35	25	35, 39, 40
Account Protection	30, 31	28, 29, 31	29
Interruption	33	33	32
Physical Access	34, 35	27, 37	34, 35
Lack of IT Support	36	31	36
Theft	27	37	27
COVID Specific	39	38	39

The format of the question was also adopted from Kruger& Kearney's design. Firstly, all questions were multichoice questions. Secondly, the questions for testing awareness, attitude and behavior had 3 choices: true, false, and do not know. Every correct answer was counted as 1 point, and the total points in this section indicates participant's awareness level.

While the second section provided insights about teleworker's security awareness objectively, assessing their security concerns revealed the perceived significance and severity of different types of security issues in teleworking. In this section of the questionnaire, all questions were answered on a scale of 1 to 5, or "do not know". For each question, one type of attack was addressed. On a certain question, 1 means "I don't worry about this type of attack at all", 5 means "I extremely worry about this type of attack". To answer the research question "What are teleworkers most concerned security risks related to teleworking?", the researcher ranked different types of attack based on their mean points.

CHAPTER IV: RESULTS

Participants

The population of this study included adults who are working in organizations, in other words, not self-employed, no matter whether they have teleworking experience or not. To estimate the teleworking awareness of the population, the survey was created with Qualtrics, distributed through Amazon Mechanic Turk. In total, the researcher collected 441 responses, 135 of them are self-employed, 2 of them don’t consent to let us have the data, and 20 of them are invalid, thus eventually the researcher collected 284 valid responses. Table 2 below shows the descriptive demographic information about respondents. The distribution of age and education are showing obvious peak. For age, it’s between 25 and 34, and for education, it’s college level. This distribution reflex the channel the researcher used to access the respondents, because the people who are familiar with the Internet and doing part-time job on crowd sourcing platform are more likely to be younger generation with higher education. It’s surprising that male respondents were twice more than female respondents, though the researcher didn’t have any preferences in sampling process in terms of sex.

Table 2 Respondent Demography

Item	Category	Frequency	％
Age	19-24	16	5.63
	25-34	147	51.76
	35-44	66	23.23
	45-54	36	12.68
	55-64	15	5.28
	65-74	3	1.05
	75 or above	1	0.35
Sex	Male	194	68.31
	Female	88	30.99
	Non-binary/Third gender	2	0.7
Education	Middle School	2	0.7
	High School	21	7.39
	College	189	66.55
	Graduate School	72	25.35
Avg Yearly Income	<$15,000	6	2.11
	$15,000-24,999	23	8.10
	$25,000-34,999	24	8.45
	$35,000-49,999	67	23.59
	$50,000-74,999	90	31.69
	$75,000-99,999	48	16.90
	$100,000-149,999	14	4.93
	$150,000-199,999	7	2.46
	>$200000	2	0.70
	Prefer not to say	3	1.06

In order to know what industries the respondents are from, the researcher uses North American Industry Classification System (NAICS) as the industry taxonomy. According to the data in Table 3, the sample covers all industries except Agriculture, Forestry, Fishing and Hunting. The industry that most respondents belong to are from manufacturing, information, finance and insurance, professional, scientific, and technical services, and education. Four of these five categories are doing jobs collecting, processing, and distributing information, which makes this research more valuable because they can benefit more from improving information security.

Table 3 Respondent Industry Distribution

Category	Frequency	%
Agriculture, Forestry, Fishing and Hunting	0	0.00
Mining, Quarrying, and Oil and Gas Extraction	1	0.35
Utilities	2	0.71
Construction	7	2.47
Manufacturing	38	13.43
Wholesale Trade	8	2.83
Retail Trade	16	5.65
Transportation and Warehousing	10	3.53
Information	55	19.43
Finance and Insurance	37	13.07
Real Estate and Rental and Leasing	9	3.18
Professional, Scientific, and Technical Services	30	10.60
Management of Companies and Enterprises	6	2.12
Administrative and Support and Waste Management and Remediation Services	7	2.47
Educational Services	21	7.42
Health Care and Social Assistance	7	2.47
Arts, Entertainment, and Recreation	8	2.83
Accommodation and Food Services	4	1.41
Other Services (except Public Administration)	11	3.89
Public Administration	6	2.12

Teleworking has become a common way nowadays, as suggested in Table 4 where 90.5% of the respondents have experience of using teleworking technology. Despite the fact that COVID-19 pandemic and social distancing practices have made teleworking an option for many companies and organization, there are already many people are working remotely before the pandemic. More than 56% have started using teleworking technologies before the COVID pandemic giving the survey was completed in March 2021.

Table 4 Teleworking Experience

Item	Category	Frequency	%
Have you used any teleworking technologies in the past?	Yes	257	90.5
	No	27	9.5
When did you started to use teleworking technologies in your work?	Less than 0.5 year ago	26	10.12
	0,5-1 year ago	85	33.07
	1-3 years ago	88	34.24
	More than 3 years ago	58	22.57
How often do you use the teleworking technologies?	0-1day a week	15	5.84
	2-3days a week	88	34.24
	4-5days a week	131	50.97
	6-7days a week	23	8.95

However, the researcher can also see the significant impact on people’s ways of working brought by COVID pandemic. That’s because 43% started using teleworking technologies in the past year when pandemic spread across the world. This observation can be confirmed from another survey question “Why did you use the teleworking technologies” as shown in Table 5. 32.5% respondents mentioned the COVID and social distancing as their reason for using teleworking technologies, making it the most chosen option for this question.

Table 5 Reason for Using Teleworking Technologies

Category	Response Number	Response Percent	Percent of Cases
Improve efficiency	87	16.4	33.9
COVID and social distancing	173	32.5	67.3
Structure of job	140	26.3	54.5
Work-life balance	102	19.2	39.7
Life changes	26	4.9	10.1
Other	4	0.8	1.6

Moreover, Table 4 also suggests 50% teleworkers are using teleworking technologies almost every day, indicating the importance and necessity of teleworking technologies in supporting this way of working. Different needs in working scenarios requires different technologies, thus, people's primary teleworking technologies provide more about how people work remotely. According to Table 6, the top three most used teleworking technologies are video conferencing, email, and shared cloud drive. Thus, it's worth pay more attention to security in these technologies.

Table 6 Primarily Used Teleworking Technology

Category	Response Number	Response Percent	Percent of Cases
Video Conferencing	210	26.85	81.7
Shared Cloud Drive	135	17.26	52.5
Email	175	22.38	68.1
Collaborative Office Suite	108	13.81	42
Instant Message	92	11.76	35.8
Collaboration Platform	62	7.93	24.1

Security Awareness

In the second section of the survey, the respondent's security awareness in teleworking were evaluated with 19 True-False questions that address three dimensions of security awareness: attitude, knowledge and behavior. Each dimension contributes 12 points to the total awareness which is 36 points. To make it easier to read, this 36-point system was scaled to 100. the mean awareness point is 61.17, with standard deviation of 17.83. This is not a good result because the awareness point is much less than 100, and it's even worse considering how much people are relying on teleworking technologies. To be more specific, knowledge part has the highest performance with mean of 22.36 and standard deviation of 8.84, while behavior part has the lowest points with mean of 18.17 and standard deviation of 5.86. In terms of attitude, it has the middle position with mean of 20.72 and standard deviation of 6.50.

Table 7 Teleworking Security Awareness in Teleworking

	N	Minimum	Maximum	Mean	Std. Deviation
Awareness	284	5.55	86.11	61.17	17.83
Attitude	284	0	91.66	20.72	6.50
Knowledge	284	8.33	100	22.36	8.84
Behavior	284	0	83.33	18.17	5.86

Now that the security awareness level of the teleworkers is showing here, the researcher would like to get deeper into it and try to find out if significant differences in teleworking security awareness exist among different groups of people. To compare the means of different groups, one-way analysis of variance (ANOVA) is used, and the result of analysis will be shown in tables. The ANOVA table includes the mean and standard deviation of each group in three dimensions of security awareness as well as the overall awareness. Besides, the f-value and p-value that indicates whether the variance between the means of two groups significantly different are also listed in the tables. In this research, demographic factors including age, income, and education level, as well as work related factors including industry, teleworking experience and organization size are examined. First of all, it is found that teleworking awareness vary in different age groups. Even though the behavior point doesn't show a significant difference(P=0.847>0.05), the attitude and knowledge points make the difference in overall awareness point significant. People in their 25-34 has the lowest awareness, but mid age to senior people have a much better performance (Table 8).

Table 8 Teleworking Security Awareness in Different Age Group

	Awareness		Attitude		Knowledge		Behavior	
	Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation
19-24	63.69	15.86	21.89	4.86	21.69	9.47	55.94	13.66
25-34	58.11	18.81	19.56	6.78	20.81	9.11	49.69	17.67
35-44	62.19	17.31	21.06	6.58	23.14	8.31	50.00	14.97
45-54	68.36	15.53	23.14	5.64	26.39	7.47	52.31	15.74
55-64	66.11	13.11	22.97	5.08	25.19	8.08	49.92	14.51
65-74	68.53	7.00	25.92	1.61	24.08	7.00	51.47	4.48
75 or above	50.00	0.00	13.89	0.00	19.44	0.00	46.30	0.00
F	2.189		2.62		2.485		0.447	
P	0.044		0.017		0.023		0.847	

Based on that, the researcher wants to further test whether positive correlation exists between age and teleworking security awareness. With the correlation analysis, the researcher gets the result, as shown in Table 9, that a significant positive correlation(p=0.01<0.05) is found between the two variables, though the correlation is very weak (0.15). Thus, **the research hypothesis H2 (The level of security awareness in teleworking has positive correlation with age.) is accepted.**

Table 9 Correlation between Age and Teleworking Security Awareness

	Age	Awareness
Age	1	
Awareness	0.15*	1

Secondly, people’s working industry also indicates their average teleworking security awareness. Similar as the effect of age, significant difference is found in both attitude and knowledge but not in behavior, leading to a significant difference in overall awareness. As Table 10 shows, professional, scientific, and technical services industry has the highest performance in overall teleworking security awareness, which has mean of 69.44 and standard deviation of 13.44. On the other hand, wholesale and trade industry get the lowest points with mean of 45.50 and standard deviation of 21.86. However, it is worth note that due to the low sample size, mining, quarrying, and oil and gas extraction, and agriculture, forestry, fishing and hunting are not discussed here. Since the variance of awareness between different industries is significant (p=0.008<0.05), **the research hypothesis H1 (The level of security awareness in teleworking varies from one industry to another) is accepted.**

Table 10 Teleworking Security Awareness in Different Industry

	Awareness		Attitude		Knowledge		Behavior	
	Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation
Agriculture, Forestry, Fishing and Hunting	0		0		0		0	
Mining, Quarrying, and Oil and Gas Extraction	86.11	0.00	27.78	0.00	33.33	0.00	25.00	0.00
Utilities	55.56	39.28	18.06	13.75	19.44	15.72	18.06	9.83
Construction	55.94	21.31	18.64	7.47	22.22	10.53	15.08	6.19
Manufacturing	51.17	18.36	16.75	6.44	17.97	8.58	16.44	6.69
Wholesale Trade	45.50	21.86	17.36	8.50	14.58	7.83	13.56	8.44
Retail Trade	63.36	14.19	22.92	3.58	23.26	8.47	18.58	6.06
Transportation and Warehousing	54.72	20.61	19.44	6.14	20.83	9.36	14.44	8.17
Information	62.17	18.17	20.61	6.61	22.36	8.97	19.19	5.75
Finance and Insurance	60.22	18.86	20.50	6.97	20.86	8.86	18.83	5.64
Real Estate and Rental and Leasing	68.53	16.83	22.53	6.11	26.56	8.00	19.44	4.81
Professional, Scientific, and Technical Services	69.44	13.44	23.97	5.03	25.56	7.72	19.92	4.67
Management of Companies and Enterprises	55.08	14.64	19.44	7.44	18.06	8.00	17.58	5.47
Administrative and Support and Waste Management and Remediation Services	62.69	15.11	22.61	4.67	22.61	10.69	17.47	2.64
Educational Services	65.86	13.86	21.17	6.47	25.28	6.86	19.44	4.56
Health Care and Social Assistance	60.31	25.83	19.06	7.75	25.00	11.33	25.03	7.92
Arts, Entertainment, and Recreation	68.42	12.58	22.22	5.56	26.39	6.64	19.81	5.83
Accommodation and Food Services	64.58	4.75	24.31	2.67	27.08	1.39	13.19	1.39

Table 10 Continued

	Awareness		Attitude		Knowledge		Behavior	
	Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation
Other Services (except Public Administration)	64.64	12.50	22.22	6.08	22.97	8.53	19.44	2.47
Public Administration	68.06	8.92	23.61	3.39	28.69	5.75	15.75	4.19
F	2.022		1.92		1.977		1.593	
P	0.008		0.013		0.01		0.058	

Lastly, organization size is also found related to teleworking security awareness. According to the data in Table 11, significant difference is also found in attitude and knowledge but not in behavior. The mid-sized organizations with 501-5000 employees have the lowest performance in teleworking security awareness with mean at 55.88 and standard deviation at 19.00, while small organization with less than 50 employees performed the best with mean at 66.92 and standard deviation at 13.11.

Table 11 Teleworking Security Awareness in Different Organization Size

	Awareness		Attitude		Knowledge		Behavior	
	Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation
Less than 50	66.92	13.11	22.89	4.78	25.81	6.22	18.22	4.58
51-500	62.11	17.81	20.94	6.61	22.72	8.92	18.47	5.97
501-5000	55.89	19.00	19.11	6.89	19.78	9.19	17.25	6.58
5001-50000	65.08	16.25	21.22	6.06	23.92	8.89	19.94	4.33
More than 50000	63.50	14.28	22.03	5.92	23.22	6.69	18.25	4.31
I don't know	68.97	22.19	23.61	6.28	26.86	9.42	18.53	7.58
F	3.04		2.33		3.30		1.03	
P	0.01		0.04		0.01		0.40	

After analyzing the correlation between organization size and teleworking security awareness, a negative correlation is found, but this correlation is not significant (p=0.59>0.05). Therefore, **research hypothesis H6 (The level of security awareness in teleworking has positive correlation with organization size) is rejected.**

Table 12 Correlation between Organization Size and Teleworking Security Awareness

	Organization Size	Awareness
Organization Size	1	
Awareness	-0.32	1

Similarly, the researcher also did ANOVA on other factors including education level, yearly income and teleworking experiences. However, no statistical evidence indicates that significant variance exists between different groups that are divided by these factors (Table 13). Therefore, **research hypothesis H3 (The level of security awareness in teleworking has positive correlation with education level), H4 (The level of security awareness in teleworking has positive correlation with income level), and H5 (The level of security awareness in teleworking has positive correlation with teleworking experience) are rejected.**

Table 13 Between-Group Variance of Awareness by Factors

Factor	MS	F	P
Education level	22.32	0.54	0.66
Yearly Avg. Income	61.24	1.51	0.14
Teleworking Experience	63.60	1.68	0.17

Security Concerns

The survey questionnaire consists of three section. The first one is profile section that collects the demographic information, teleworking and security experience, and the second section assesses participant’s security awareness. As for the third section, participant’s concern on different types of security issues in teleworking are explored with scaling questions.

Since the question in security concern section are in the form of Likert scaling, reliability and validity should firstly ensure the questions are reliable and valid before any further analysis. As indicated in Table 14 below, the Cronbach’s Alpha is 0.893 (higher than 0.7). Therefore, it’s confident to say that this section that consists of 9 questions is reliable. Furthermore, the validity is also examined.

Table 14 Teleworking Security Concern Question Reliability

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.891	0.892	8

With the exploratory factor analysis, each of the 8 questions’ validity are checked, and the result is as shown below in Table 15. The load of each of them is higher than 0.5, indicating that all of them can be considered as valid.

Table 15 Teleworking Security Concern Question Validity

Question	Component
How much do you worry about security problems related to physical access in teleworking?	0.783
How much do you worry about security problems related to self-discipline or computer knowledge in teleworking?	0.778
How much do you worry about security problems related to theft in teleworking?	0.769
How much do you worry about COVID specific security problem in teleworking?	0.757
How much do you worry about security problems related to account protection in teleworking?	0.751
How much do you worry about security problems related to access control in teleworking?	0.748
How much do you worry about security problems related to service interruption in teleworking?	0.728
How much do you worry about security problems related to inadequate IT support in teleworking?	0.721

In this section, every question is answered on a scale of 1-5 where 1 means a great deal of concern, while 5 means not concern at all. Therefore, the lower points the question gets, the more people concern about it. The security issues can be divided into 4 tiers based on the mean value. The most concerned teleworking security issue is account protection related issues (2.743± 1.14). On tier 2, service interruption(2.81±1.15), access control(2.82±1.15), and self-discipline or computer knowledge(2.83±1.2) received pretty close concerns by teleworkers. On the third tier, physical access(3.06±1.28) and inadequate IT support (3.07±1.29) also get similar results. Surprisingly, COVID specific teleworking (3.39±1.28) security problem is the least concerned one, giving the long-lasting, wide-spread and significant impact of the epidemic. Alongside with COVID specific teleworking, theft(3.11±1.25) become the other one in the fourth tier security problems that people concerns in teleworking.

Table 16 Teleworking Security Concern

Question	N	Minimum	Maximum	Mean	Std. Deviation
How much do you worry about security problems related to access control in teleworking?	284	20	100	56.4	22.92
How much do you worry about security problems related to self-discipline or computer knowledge in teleworking?	284	20	100	56.6	24.06
How much do you worry about security problems related to account protection in teleworking?	284	20	100	54.6	22.82
How much do you worry about security problems related to service interruption in teleworking?	284	20	100	56.2	23
How much do you worry about security problems related to physical access in teleworking?	284	20	100	61.2	25.58
How much do you worry about security problems related to inadequate IT support in teleworking?	284	20	100	61.4	25.76
How much do you worry about security problems related to theft in teleworking?	284	20	100	62.2	25.04
How much do you worry about COVID specific security problem in teleworking?	284	20	100	67.8	25.64

More about Security Concern and Awareness

Now that the researcher have some data regarding teleworker's security awareness and concerns, it is not enough to study them separately. If one has concern on certain thing, that's because he/she knows the negative impact on him/her, which suggests his/her knowledge about it. To prevent unwanted things from happening, people take actions. Thus, it is likely that correlation exists between teleworkers security awareness and concerns, and the researcher might even predict security awareness level based on how much people concern on different security issues. With awareness as the dependent variable and all 8 security issues mentioned in the survey as independent variables, the multiple linear regression analysis is summarized as the table below.

Table 17 Regression Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
.374a	0.14	0.114	6.03833	0.311

More details about the coefficients are also listed below. As you can see from the table, the concerns as independent variables don't have statistically significant influence on the dependent variable, awareness, except the COVID specific security issues. Therefore, the researcher cannot predict one’s awareness based on how much he/she worries about the following 8 security issues in teleworking.

Table 18 Regression Model Coefficients

Teleworking Security Concerns	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	17.798	1.226		14.518	0		
Access control	0.123	0.434	0.022	0.283	0.778	0.521	1.918
Self-discipline or computer knowledge	−0.387	0.44	−0.073	−0.88	0.379	0.46	2.172
Account protection	−0.611	0.44	−0.109	−1.387	0.167	0.511	1.958
Service interruption	−0.562	0.412	−0.101	−1.365	0.173	0.575	1.74
Physical access	0.574	0.41	0.114	1.398	0.163	0.468	2.136
Inadequate IT support	−0.357	0.367	−0.072	−0.971	0.332	0.576	1.736
Theft	0.278	0.401	0.054	0.693	0.489	0.512	1.954
COVID specific	1.976	0.403	0.395	4.901	0	0.482	2.075

CHAPTER V: DISCUSSION AND CONCLUSION

Discussion

The data extracted from the survey provided us with a chance to dig into the security awareness and concern of teleworkers. Based on the data analysis, the researcher can try answering the research questions. First of all, the overall awareness in teleworking security across different industries is far away from the ideal level, because the mean of awareness point is only 61.17 which is much less than 100 total points(Table 7). Furthermore, teleworkers have better performance in knowledge (22.36±8.83) than attitude(20.72±6.50) and behavior(18.17±5.86). This result helps us to answer the first three research questions that further discuss the security awareness from three perspectives. Under the scaled points, the full point for each dimension is 33.33. Although knowledge achieved the highest among three dimensions, the mean point is only 67.09% of the full point of a single dimension. Obviously, a considerable gap exists in teleworker's security knowledge. As for attitude and behavior, situation is worse. In these two parts, participants got only 62.17% and 54.52% of the full point, respectively. On one hand, this tells us that teleworkers are not taking information security serious enough, even though they do have a little sense of protecting themselves. On the other hand, as a result of insufficient knowledge on and inactive attitude to teleworking security, only small part of security measures and actions are taken, leading to significant teleworking security risk. Therefore, it is critical to learn the fact that even though teleworking is now becoming prevalent around the world due to COVID pandemic, the development of employee's security awareness is not catching up. Fortunately, there are many studies working on improving people's information security awareness and ability, such as the security training protocol created by Abukari and Kwedzo Bankas in 2020.

Secondly, the researcher found security awareness of teleworkers vary from different groups that are divided by working industry, age, and organization size. In the 22 industry categories in NASIC standard, wholesale trade, manufacturing, and transportation and warehousing are the industries that have the lowest teleworking security performance. On the other hand, professional, scientific and technical services, real estate, rental and leasing, and arts, entertainment and recreation performed the best. This difference reflects the how jobs are different between the industries. For the least industries with lowest points, most of the jobs require manpower and thus hiring mainly blue-collar employees who directly interact with people and stuff. Naturally, most of their jobs cannot be done remotely through the Internet, and thus rely less on teleworking, and have less awareness on information security in this scenario. On the opposite, the industries with highest teleworking security awareness mainly dealing with information that is creating, organizing, distributing, and analyzing information. This type of job requires less physical interaction but higher flexibility. Thus, employees in these industries can benefit more from teleworking and, meanwhile, accumulate more knowledge and experience in teleworking information security. Age, as another factor that influences teleworkers security awareness, is found a positive correlation with it, meaning that people's teleworking security awareness increases as they grow older. This might be due to the increased experiences and the small sample size of people who are older than 64. Unlike age, although significant variance is found in different employees from different sized organizations, no statistical evidence suggests correlation between organization size and teleworking awareness. As for other potential correlators the researcher has in hypothesis: education level, income level, and teleworking experiences, no significant statistical evidence that indicate their correlation with teleworking security awareness was found in the data.

Last but not the least, the data also provides us with some insight about people's concern in teleworking security. Despite the huge impact on the ways people work and live brought by COVID pandemic, teleworkers don't consider COVID related security problems as their major concern. In contrary, common security issues related to account protection, service interruption and access control concern teleworkers the most. The potential explanation for this is that even though the pandemic induces the massive application of teleworking around the world, most of the teleworking technologies and paradigm already exists before the pandemic. Thus, people are still mainly facing security challenges exist before COVID eruption. If this is true, improving teleworker's general awareness and capability in information security does not only meet the long-term needs of organization, but also relieve people's concern in short term.

On the other hand, if we look at the top issues people concern, they correspond with James' research on teleworking security (2011) where he proposed a conceptual model of teleworking security. In James’s model, he describes confidentiality as the primary security objective, and uses multiple mechanisms such as network encryption, authentication, and access control. The most concerned security issues are as well as the most fundamental security requirements in teleworking. This does not only suggest how important they are, but also to certain extent indicates that the current security mechanisms and policies are not providing secure feeling for teleworkers, and thus more works are required to improve the access control and account protection as well as users’ perception of security. Tryfonas and his research team defines availability from macroscopic and real-time perspective (2000). In their definition, the macroscopic part of availability refers to permanence of services including physical resources, personnel, and guarantying procedures. Service interruption, as one of the most concerned security issues in teleworking, apparently shows people’s concern on availability. Therefore, though breach of confidentiality is seen as the main information security threat in teleworking (Deloitte, 2011), availability threat has close impact on people’s security perception and that might result from the fact that teleworkers rely more on the Internet to connect to other people or services.

However, there are many limitations that might weaken the findings of this article. On one hand, the valid sample of this survey is only 284, which can hardly guarantee large amount in different sample groups. For example, we don’t have any participants working in agriculture, forestry, fishing and hunting industry, and have only one participant from mining, quarrying, and oil and gas extraction industry. Therefore, there is gap between research findings and reality. Besides the sample size, this gap also results from the channel used to distribute the questionnaire. Since MTurk is a crowd sourcing platform which attracts people who have easy Internet access and are seeking part-time income, the sample is relatively special compared to the population, so we see uneven distribution in sex, education, income etc. On the other hand, the survey questionnaire consists only 19 and 8 questions for security awareness assessment and concern evaluation respectively due to the limitation of questionnaire length. Although these questions have covered the essential dimensions of teleworking security awareness and concerns, it can be more specific and extensive. With questions that are more fine-grained and comprehensive, the assessment and evaluation should better suggest participants real security awareness level and concerns.

Conclusion

In conclusion, this research found that security awareness of teleworkers is not good, and it requires more training programs for better performance. Among the three dimensions of awareness, people need most improvement in behavior. Secondly, the result shows that teleworkers in labor-intensive industry, at younger age, and from mid-sized organization tend to have lower performance in security awareness. Lastly, availability related security concerns are given more attention in teleworking while COVID-19-specific security issues are not concerned much. Thus in teleworking, more efforts and attention should be put on improving teleworker’s general awareness and capability in information security especially the availability part, because it does not only meet the long-term needs of organization, but also relieve people’s concern in short term.

REFERENCES

Abukari, A. M., & Kwedzo Bankas, E. (2020). Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond Article in. International Journal of Scientific and Engineering Research, 11(4), 1401–1407. http://www.ijser.org

Alsop, T. (2010, February). Percentage of U.S. households with a computer 1984-2010. Retrieved October 13, 2020, from https://www.statista.com/statistics/184685/percentage-of-households-with-computer-in-the-united-states-since-1984/

Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & security, 26(4), 276-289.

Ampomah, M., Silva, Y. De, Li, H., Pahlisa, P., Yang, Q., & Zhang, Q. (2013). Information Security Strategy and Teleworking (In) security. 11. http://hdl.handle.net/11343/33341

Bailey, N. B. K. D. E., & Kurland, N. B. (1999). The advantages and challenges of working here, there, anywhere, and anytime. Organizational dynamics, 28(2), 53-68.

Blau, I., & Caspi, A. (2009). What type of collaboration helps? Psychological ownership, perceived learning and outcome quality of collaboration using Google Docs. In Proceedings of the Chais Conference on Instructional Technologies Research, 48–55.

Bucşa, R. C. (2020). Teleworking and Securing Data with VPN Technology. Economy Transdisciplinarity Cognition, 23(1), 78-85.

Carnahan, L., & Guttman, B. (1998). Security Issues for Telecommuting. Edpacs, 26(4), 1–8. https://doi.org/10.1201/1079/43242.26.4.19981001/30226.1

Chávez, J. D. (2020). Key considerations for ensuring the security of organisational data and information in teleworking from home. April, 1–6.

Close, K., Grebe, M., Andersen, P., Khurana, V., Franke, M., &amp; Kalthof, R. (2020, July). The Digital Path to Business Resilience. Retrieved from https://www.bcg.com/publications/2020/digital-path-to-business-resilience

Congress, U. S. (2010). Telework Enhancement Act of 2010. In 111th Congress, HR (Vol. 1722).

Daniels, K., Lamond, D., & Standen, P. (2001). Teleworking: frameworks for organizational research. Journal of management studies, 38(8), 1151-1185.

Deloitte Access Economics. (2011). Next Generation Telework: A Literature Review.

Evangelakos, G. (2020). Keeping critical assets safe when teleworking is the new norm. Network Security, 2020(6), 11–14. https://doi.org/10.1016/S1353-4858(20)30067-2

Fílardí, F., CASTRO, R. M. P., & Zaníní, M. T. F. (2020). Advantages and disadvantages of teleworking in Brazilian public administration: analysis of SERPRO and Federal Revenue experiences. Cadernos EBAPE. BR, 18(1), 28-46.

Godlove, T 2012, 'Examination of the factors that influence teleworkers' willingness to comply with information security guidelines', Information Security Journal: A Global Perspective, vol. 21, no. 4, pp. 216 -229.

Gray, M., & Hodson, N. G. Gordon. 1994. Teleworking explained.

Haddon, L., & Silverstone, R. (1992). Information and communication technologies in the home: the case of teleworking. University of Sussex, PICT.

Hassanzadeh, M., Jahangiri, N., & Brewster, B. (2014). A conceptual framework for information security awareness, assessment, and training. In Emerging Trends in ICT Security (pp. 99-110). Morgan Kaufmann.

James, P. (2011). Are existing security models suitable for teleworking? Proceedings of the 9th Australian Information Security Management Conference, 130–139. https://doi.org/10.4225/75/57b533efcd8c0

Katane, J. (2017). The influence of organizational culture and project management maturity in virtual project teams. University of Johannesburg, Johannesburg, Gauteng, South Africa, September, 1–10. https://www.researchgate.net/publication/319528141

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & security, 25(4), 289-296.

Kuhn, D. R., Frankel, S., Tracy, M., & National Institute of Standards and Technology (U.S.). (2002). Security for telecommuting and broadband communications recommendations of the National Institute of Standards and Technology. 1 v. (various pagings). http://purl.access.gpo.gov/GPO/LPS70000

McGregor, S. E., Watkins, E. A., & Caine, K. (2017). Would you slack that? The impact of security and privacy on cooperative newsroom work. Proceedings of the ACM on Human-Computer Interaction, 1(CSCW). https://doi.org/10.1145/3134710

Morgan, R. E. (2004). Teleworking: an assessment of the benefits and challenges. European Business Review.

Nosek, B. A., Banaji, M. R., & Greenwald, A. G. (2002). E-research: Ethics, security, design, and control in psychological Research on the internet. Journal of Social Issues, 58(1), 161–176. https://doi.org/10.1111/1540-4560.00254

Nakamura, K., Masuda, Y., & Kiyokane, Y. (1995, January). Roles of communication media in telework environments. In Proceedings of the Twenty-Eighth Annual Hawaii International Conference on System Sciences (Vol. 4, pp. 446-455). IEEE.

Nakayama, M., & Chen, C. C. (2019). Length of Cloud Application Use on Functionality Expectation, Usability, Privacy, and Security: A Case of Google Docs. Pacific Asia Journal of the Association for Information Systems, 11(3), 5–27. https://doi.org/10.17705/1pais.11302

Peacey, A. (2006). Teleworkers–extending security beyond the office. Network Security, 2006(11), 14-16.

Peltier, TR 2013, "Remote Access Security Issue", Information Systems Security, vol.10, no. 6, pp.31- 36

Pérez, M. P., Sánchez, A. M., & de Luis Carnicer, M. P. (2002). Benefits and barriers of telework: perception differences of human resources managers according to company's operations strategy. Technovation, 22(12), 775-783.

Rouse, M. (2019). What is the CIA Triad? Retrieved from https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availabilityCIA

Scarfone K, Hoffman P, & Souppaya, M 2009, "Guide to Enterprise Telework and Remote Access Security, Recommendations of the National Institute of Standards and Technology", NIST Special Publication, 800-46 Revision 1.

Scarfone, K., & Souppaya, M. (2007). User's Guide to Securing External Devices for Telework and Remote Access. NIST Special Publication, 800, 114.

Shi, F. (2020). Threat Spotlight: Coronavirus-Related Phishing. Retrieved from https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

SME. (2020, April). Remote working has increased risk of a cyber breach, say businesses. Retrieved from https://www.smeweb.com/2020/04/06/remote-working-has-increased-risk-of-a-cyber-breach-say-businesses

Sturgeon, A 1996, "Telework: threats, risks and solutions", Information Management & Computer Security, vol.4, no.2, pp.27–38

Till, N. (2020, May). Half of global businesses have already encounted a cyber scare since shifting to remote working during COVID-19. Retrieved from https://bdaily.co.uk/articles/2020/05/06/half-of-global-businesses-have-already-encounted-a-cyber-scare-since-shifting-to-remote-working-during-covid-19

Tryfonas, T., Gritzalis, D., & Kokolakis, S. (2000, August). A qualitative approach to information availability. In IFIP International Information Security Conference (pp. 37-47). Springer, Boston, MA.

Verizon. (2020). 2020 Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/?CMP=OOH_SMB_OTH_22222_MC_20200501_NA_NM20200079_00001

Wellman, B., Salaff, J., Dimitrova, D., Garton, L., Gulia, M., & Haythornthwaite, C. (1996). Computer networks as social networks: Collaborative work, telework, and virtual community. Annual review of sociology, 22(1), 213-238.

Yang, H., Zheng, C., Zhu, L., Chen, F., Zhao, Y., & Valluri, M. (2012). Security Risks in Teleworking : A Review and Analysis. 1–15.

APPENDIX A. SURVEYS

1. What is your age?
    a) Under 18 years old
    b) 19-24
    c) 25-34
    d) 35-44
    e) 45-54
    f) 55-64
    g) 65-74
    h) 75 years or above
    i) Prefer not to say

2. What is your sex?
    a) Male
    b) Female
    c) Prefer not to say

3. What is your education level?
    a) Elementary school
    b) Middle school
    c) High school
    d) College
    e) Graduate school
    f) Prefer not to say

4. What is your average yearly income?
    a) Less than $15,000
    b) 15,000-24,999
    c) 25,000-34,999
    d) 35,000-49,999

e) 50,000-74,999

f) 75,000-99,999

g) 100,000-149,999

h) 150,000-199,999

i) 200,000 or above

j) Prefer not to say

5. What industry does your job belong to?

a) Agriculture, Forestry, Fishing and Hunting

b) Mining, Quarrying, and Oil and Gas Extraction

c) Utilities

d) Construction

e) Manufacturing

f) Wholesale Trade

g) Retail Trade

h) Transportation and Warehousing

i) Information

j) Finance and Insurance

k) Real Estate and Rental and Leasing

l) Professional, Scientific, and Technical Services

m) Management of Companies and Enterprises

n) Administrative and Support and Waste Management and Remediation Services

o) Educational Services

p) Health Care and Social Assistance

q) Arts, Entertainment, and Recreation

r) Accommodation and Food Services

s) Other Services (except Public Administration)

t) Public Administration

6. Are you self-employed?

a) Yes

b) No

7. How many employees does your organization have?

a) Less than 50
b) 51-500
c) 501-5000
d) 5001-50000
e) More than 50000

8. How long have you been working for this organization?

a) Less than 1 year
b) 1-3 years
c) 4-5 years
d) 6-10 years
e) More than 10 years

9. Have you used any teleworking technologies in the past?

a) Yes
b) No

10. When did you started to use teleworking technologies in your work?

a) Less than half a year ago
b) Less than one year ago
c) Less than three years ago
d) More than three years ago

11. Why did you use the teleworking technologies?

a) Volunteered to use it to improve efficiency
b) Influenced by the COVID pandemic and social distancing practice
c) Structure of my job
d) Work-life balance
e) Life changes

f) Other: ___________________________________

12. What are your primarily used teleworking technologies (**Multiple answers are allowed**)?

a) Email

b) Video conferencing (e.g. Zoom)

c) Shared cloud drive (e.g. Google Drive)

d) Instant message (e.g. GroupMe)

e) Collaborative office suite (e.g. Google Docs)

f) Collaboration platform (e.g. Microsoft Teams)

13. How many hours do you spend daily in average on the following tools (**Multiple answers are allowed**)?

a) Email: ______

b) Video conferencing (e.g. Zoom): _______

c) Shared cloud drive (e.g. Google Drive): _______

d) Instant message (e.g. GroupMe): _______

e) Collaborative office suite (e.g. Google Docs): _______

f) Collaboration platform (e.g. Microsoft Teams): _______

14. How often do you use the teleworking technologies?

a) 0-1 days a week

b) 2-3 days a week

c) 4-5 days a week

d) 6-7 days a week

15. Do you have any experience of being a victim of security issues?

a) Yes

b) No

16. Do you have any experience of being a victim of security issues related to these teleworking technologies?

a) Yes.

b) No.

17. What kind of incident were you facing (**Multiple answers are allowed**)?

a) Data breach

b) Data loss

c) Phishing

d) Malware

e) Account compromised

f) Denial of service

g) Other: ____

18. What teleworking technologies caused the incident?

a) Email

b) Instant message

c) Online conferencing

d) Shared cloud drive

e) Collaborative office suite

f) Collaboration platform

g) Other: ____

19. How much was the cost of the incident to your organization?

a) Less than $100

b) $100-$500

c) $501-$1000

d) $1,001-$5,000

e) $5,001-$10,000

f) $10,001-$50,000

g) More than $50,000

h) I don't know

20. what was the consequence of the incident to you?

a) Economical loss

b) Demotion

c) Dismissal

d) Reputation damage

e) Privacy violation

f) Other_______

g) Prefer not to say

21. How often have you encountered with security issues related to teleworking technologies?

a) Only once

b) Yearly

c) Monthly

d) Weekly

e) Daily

22. Any users can edit my shared documents on Google Drive

a) True

b) False

c) Do not know

23. It is okay to post the link of shared documents to public

a) True

b) False

c) Do not know

24. I only give edit permission of shared documents to people who must edit the document.

a) True

b) False

c) Do not know

25. The organizational security policy is not always correct, so it is okay not to follow sometimes

if I’m away from office.

a) True

b) False

c) Do not know

26. It is unethical to give away organizational information to outsider no matter how much he/she is willing to pay for.

a) True

b) False

c) Do not know

27. I usually leave my laptop or cellphone on the table in library when I’ll be back in few minutes.

a) True

b) False

c) Do not know

28. Using one complex password on all my different account is convenient and secure.

a) True

b) False

c) Do not know

29. I use multi-factor authentication to protect my important accounts (e.g. Google account, iCloud account, enterprise email).

a) True

b) False

c) Do not know

30. I am neither famous nor rich, so I don’t need complex password for my accounts.

a) True

b) False

c) Do not know

31. If my account is compromised, I should tell organizational IT department immediately.

   a) True
   b) False
   c) Do not know

32. I save my progress frequently when I’m working on a task

   a) True
   b) False
   c) Do not know

33. It is okay to let my kids use my work computer

   a) True
   b) False
   c) Do not know

34. I am willing to help stranger who wants to use my computer to download a file to her USB flash drive.

   a) True
   b) False
   c) Do not know

35. I never talk about details of my work in public.

   a) True
   b) False
   c) Do not know

36. I know how to contact the IT support department.

   a) True
   b) False
   c) Do not know

37. Others can’t do anything to the data in my computer or laptop if they don’t know the password.
    a) True
    b) False
    c) Do not know

38. It is okay to provide my information for COVID control purpose, if it is required by an email sent from a person who claimed to be WHO employee.
    a) True
    b) False
    c) Do not know

39. I generally trust emails sent to my work email.
    a) True
    b) False
    c) Do not know

40. I always use different devices for working and doing personal stuff.
    a) True
    b) False
    c) Do not know

41. On a scale of 1 to 5, how much do you think new security risks are introduced by teleworking.
    1: Not at all,
    5: Definitely

42. On a scale of 1 to 5, how much do you worry about security problem related to **access control** in teleworking?
    1: Not at all,
    5: Extremely worry

43. On a scale of 1 to 5, how much do you worry about security problem related to **self-discipline** in teleworking?

    1: Not at all,

    5: Extremely worry

44. On a scale of 1 to 5, how much do you worry about security problem related to **account protection** in teleworking?

    1: Not at all,

    5: Extremely worry

45. On a scale of 1 to 5, how much do you worry about security problem related to **interruption** in teleworking?

    1: Not at all,

    5: Extremely worry

46. On a scale of 1 to 5, how much do you worry about security problem related to **physical access** in teleworking?

    1: Not at all,

    5: Extremely worry

47. On a scale of 1 to 5, how much do you worry about security problem related to **inadequate IT support** in teleworking?

    1: Not at all,

    5: Extremely worry

48. On a scale of 1 to 5, how much do you worry about security problem related to **theft** in teleworking?

    1: Not at all,

    5: Extremely worry

49. On a scale of 1 to 5, how much do you worry about **COVID specific** security problem in teleworking?

    1: Not at all,

    5: Extremely worry

50. What other security concerns about teleworking do you have? On a scale of 1 to 5, how much do you worry about it

    ____

    1: Not at all,

    5: Extremely worry