

**T.C.
BAHÇEŞEHİR UNIVERSITY**

**THE OUTBREAK OF COVID-19: A WAKEUP CALL
TO EXPLORE INFORMATION SECURITY POLICIES,
TRAINING AND AWARENESS FROM
TELEWORKERS' PERSPECTIVE IN THE CONTEXT
OF SAUDI ARABIA**

Master's Thesis

ASMAA EL KHATIB

ISTANBUL, 2021

**T.C.
BAHÇEŞEHİR UNIVERSITY**

**GRADUATE SCHOOL
MASTER IN CYBER SECURITY**

**THE OUTBREAK OF COVID-19: A WAKEUP
CALL TO EXPLORE INFORMATION
SECURITY POLICIES, TRAINING AND
AWARENESS FROM TELEWORKERS'
PERSPECTIVE IN THE CONTEXT OF SAUDI
ARABIA**

Master's Thesis

ASMAA EL KHATIB

**Thesis Advisor: ASST.PROF.DR. ORHAN GÖKÇÖL
ISTANBUL, 2021**

THE REPUBLIC OF TURKEY
BAHÇEŞEHİR UNIVERSITY

GRADUATE SCHOOL
MASTER OF SCIENCE PROGRAM IN CYBER SECURITY

Title of the Thesis:

Name and Surname of the Student:

Date of Thesis Defense:

The thesis has been approved by the Graduate School of _____.

Title, Name and LAST NAME
Graduate School Director
Signature

I certify that this thesis meets all the requirements as a thesis for the degree of Master of Science.

Title, Name and LAST NAME
Program Coordinator
Signature

This is to certify that we have read this thesis and we find it fully adequate in scope, quality and content, as a thesis for the degree of Master of Arts.

Jury Members

Signature

Thesis Supervisor
Title, Name and SURNAME

Thesis Co-supervisor
Title Name and SURNAME

Member
Title Name and SURNAME

Member
Title Name and SURNAM

ACKNOWLEDGEMENTS

First, I want to express my gratitude to my supervisor Dr. Orhan Gökçöl, Asst. Prof. at Bahçeşehir University for his support, guidance and constructive feedback. Secondly, I want to thank my parents, Nassir Elkhatab and Rabia Almasri, and my siblings, Amne, Mohammad and Abdullah, for their love and support throughout this journey. I also wish to take this opportunity to thank the research participants who agreed to take part in in this study. Indeed, this project would not have been possible without their cooperation.

ISTANBUL, 2021

Asmaa El khatib

ABSTRACT

THE OUTBREAK OF COVID-19: A WAKEUP CALL TO EXPLORE INFORMATION SECURITY POLICIES, TRAINING AND AWARENESS FROM TELEWORKERS' PERSPECTIVE IN THE CONTEXT OF SAUDI ARABIA

Asmaa El khatib

Master in Cyber Security

Thesis Supervisor: ASST.PROF.DR. ORHAN GÖKÇÖL

April 2021, 76 pages

The lockdown due to the outbreak of COVID-19 has forced many employees to continue working remotely from their homes which poses threats and risks on information security. Therefore, this study aims at exploring the perspectives of teleworkers in the Kingdom of Saudi Arabia on three areas: their awareness of the existence of information security policy (ISP) and remote security policy in the organizations they work for; whether their organizations have provided training and awareness programs to maintain information security in general and while working from their homes; and whether their behaviour reflects awareness of information security. In addition, this study aims to explore whether there are any significant differences among respondent groups regarding information security policies, training and information security awareness. To explore these areas, a closed-ended self-administered questionnaire was designed based on extensive literature review. A total of 155 questionnaires were collected and analysed using the Statistical Package for Social Sciences (SPSS).

The reported findings indicate that the majority of teleworkers are aware of the existence of ISP and remote security policy in the organizations they work for. Over one half of the participants have received some form of training or guidelines to maintain information security in general and merely half of them reported receiving specific training to maintain information security while working from home. Moreover, the reported behaviours indicate that on average, teleworkers have fairly good ISA with some areas in need of enhancements. When analysing the data by the size of the organization and sector, it was found that in regards to security policies and training, there are significance differences between teleworkers sub-groups based on the size of the organization. However, no sufficient statistical differences in regards to security policies and training were found based on the sector. Finally, in regards to ISA, significant statistical differences were detected based on both the size of the organization and sector.

Keywords: Home-telework, Information security policies, Remote security policy, Security training, Information security awareness.

ÖZET

COVID-19 SALGINI SONRASINDA SUUDİ ARABİSTAN'DAKİ KURULUŞLARDA UZAKTAN ÇALIŞANLARIN BAKIŞ AÇISINDAN BİLGİ GÜVENLİĞİ POLİTİKALARI, EĞİTİM VE FARKINDALIKLARININ DEĞERLENDİRİLMESİ

Asmaa El khatib

Siber Güvenlik Bilimleri Yüksek Lisans Programı

Tez Danışmanı: ASST.PROF.DR. ORHAN GÖKÇÖL

Nisan 2021, 76 Sayfa

Covid-19'un salgınından dolayı kilitlenme, birçok çalışanı, bilgi güvenliği konusunda tehdit ve risk teşkil eden uzaktan çalışma koşullarında devam etmesini sağlamıştır. Bu nedenle, bu çalışma, Suudi Arabistan Krallığı'ndaki uzaktan çalışanların bakış açılarını üç alanda keşfetmeyi amaçlamaktadır: Bilgi Güvenliği Politikası'nın varlığının farkındalığı ve çalıştıkları kuruluşlarda uzaktan çalışma güvenliği politikası; kuruluşlarının genel olarak bilgi güvenliğini sağlamak için eğitim ve farkındalık programları sağlayıp evlerinden çalışırken bilgi güvenliğini sağlayıp sağlamadıkları; ve davranışlarının bilgi güvenliği bilincini yansıtır yansıtmadığı. Buna ek olarak, bu çalışma, katılımcı gruplar arasında bilgi güvenliği politikaları, eğitim ve bilgi güvenliği bilinci konusunda önemli bir fark olup olmadığını keşfetmeyi amaçlamaktadır. Bu alanları keşfetmek için, kapalı uçlu bir kendi kendine uygulanan anket, kapsamlı literatür taramasına göre tasarlanmıştır. Toplam 155 anket toplanmış ve sosyal bilimler için istatistiksel paket (SPSS) kullanılarak analiz edilmiştir.

Rapor edilen bulgular, uzaktan çalışanların çoğunluğunun, çalıştıkları kuruluşlarda bilgi güvenliği politikaları ve uzaktan çalışma politikasının varlığının farkındalığını göstermektedir. Katılımcıların yarısından fazlası, genel olarak bilgi güvenliğini sağlamak için bir miktar eğitim veya kuruma ait direktifler almıştır. Katılımcıların yalnızca yarısı evden çalışırken bilgi güvenliğini sağlamak için belirli bir eğitim aldığını belirtmiştir. Dahası, bildirilen davranışlar ortalama olarak, uzaktan çalışanların, geliştirmelere ihtiyacı olan bazı alanlarda oldukça iyi bir farkındalığa sahip olduğunu göstermektedir. Verileri organizasyonun ve sektörün büyüklüğüyle analiz ederken, güvenlik politikaları ve eğitime ilişkin olarak, kuruluşun büyüklüğüne dayanan uzaktan çalışan alt grupları arasında farklılıklar gözlemlenmiştir. Bununla birlikte, sektöre dayanarak güvenlik politikaları ve eğitim konusunda yeterli istatistiksel fark bulunamamıştır. Son olarak, bilgi güvenliği ile ilgili olarak, hem organizasyonun hem de sektörün büyüklüğüne göre anlamlı farklılıklar tespit edilmiştir.

Anahtar Kelimeler: Evden çalışma, Bilgi güvenliği politikaları, Uzaktan çalışma güvenliği politikası, Güvenlik eğitimi, Bilgi güvenliği farkındalığı.

TABLE OF CONTENTS

TABLES	viii
FIGURES	ix
ABBREVIATIONS	x
1.INTRODUCTION.....	1
1.1 RESEARCH QUESTIONS	4
1.2 RESEARCH CONTEXT.....	4
1.3 DISSERTATION OVERVIEW	5
2.LITERATURE REVIEW.....	6
2.1 TELEWORK.....	6
2.1.1 Telework from Home: Definition and Overview.....	6
2.1.2 Security Risks Generated in Teleworking	7
2.1.3 Information Security in Home Teleworking Environment	11
2.2 INFORMATION SECURITY POLICIES	12
2.2.1 Importance.....	13
2.2.2 Uptake	13
2.2.2.1 Internationally	14
2.2.2.2 In KSA.....	15
2.3 INFORMATION SECURITY TRAINING AND AWARENESS 	16
2.3.2 In KSA.....	17
2.3.3 Measuring Information Security Awareness (ISA)	18
2.3.3.1 Human aspects of information security questionnaire (HAIS-Q).....	18
2.4 GAP OF KNOWLEDGE.....	20
3.DATA AND METHOD.....	23
3.1. SAMPLE	23
3.2. RESEARCH DESIGN	24
3.3. DATA-COLLECTION PROCEDURES	25
3.2.1. Designing the Survey.....	25

3.2.2. Piloting the Survey	33
3.2.3. Administrating the Survey	33
3.4. ETHICAL CONCERNS.....	34
3.5. VALIDITY and RELIABILITY.....	34
4.FINDINGS	36
4.1 DATA ANALYSIS	36
4.2 FINDINGS	38
4.2.1 Teleworkers Group Differences.....	57
4.2.1.1 Teleworkers group differences (by size)	57
4.2.1.1.1 Security policies and training	57
4.2.1.1.2 Information security awareness	58
4.2.1.2 Teleworkers group differences (by sector)	61
4.2.1.2.1 Security policies and training	61
4.2.1.2.2 Information security awareness	62
5.DISCUSSION AND CONCLUSION	66
5.1 DISCUSSION	66
5.1.2 Policies.....	66
5.1.2 Training and Awareness.....	67
5.1.3 Teleworkers Group Differences.....	70
5.2 LIMITATIONS AND SUGGESTIONS FOR FUTURE RESEARCH	72
5.2.1 Research Tool	72
5.2.2 Sample	73
5.2.3 Scope.....	74
5.3 CONCLUSION.....	74
REFERENCES.....	77
Books	77
Periodicals	79
Other Publications	87
APPENDICES	89
ANNEX 1: Questionnaire in English..Hata! Yer işareti tanımlanmamış.	
ANNEX 2: Questionnaire in Arabic...Hata! Yer işareti tanımlanmamış.	

ANNEX 3: WhatsApp Message Hata! Yer işareti tanımlanmamış.

ANNEX 4: Screenshots from bitly.com..... Hata! Yer işareti tanımlanmamış.

ANNEX 5: HAIS-Q Items Hata! Yer işareti tanımlanmamış.

ANNEX 6: Participants Results - Reverse Scoring Applied -

Descriptive Statistics Hata! Yer işareti tanımlanmamış.

ANNEX 7: Descriptive Statistics of All Focus Areas .. Hata! Yer işareti tanımlanmamış.

ANNEX 8: ISA Score - Percentage of Favourable Responses Hata! Yer işareti tanımlanmamış.

ANNEX 9: Mann Whitney U Test Results - by Size ... Hata! Yer işareti tanımlanmamış.

ANNEX 10: Mann Whitney U Test Results - by Sector Hata! Yer işareti tanımlanmamış.

TABLES

Table 3.1: Description of the Population and Sample.....	24
Table 3.2: Focus Areas and Sub-Areas with the Corresponding Statements.....	31
Table 4.1: Normal VS. Revers Scoring.....	37
Table 4.2: Information about the Research Participants	42
Table 4.3: Existence of ISP & Remote Security Policy.....	43
Table 4.4: Information Security Training in General and for Remote Working	45
Table 4.5: Descriptive Statistics of Sub-Areas in Password Management	46
Table 4.6: Descriptive Statistics of Sub-Areas in Email Use.....	47
Table 4.7: Descriptive Statistics of Sub-Areas in Internet Use.....	48
Table 4.8: Descriptive Statistics of Sub-Areas in Social Media Use.....	49
Table 4.9: Descriptive Statistics of Sub-Areas in Mobile Devices.....	50
Table 4.10: Descriptive Statistics of Sub-Areas in Information Handling	51
Table 4.11: Descriptive Statistics of Sub-Areas in Incident Reporting	52
Table 4.12: Summary of Descriptive Statistics for All Sub-Areas	53
Table 4.13: Descriptive Statistics for All Focus-Areas.....	54
Table 4.14: Percentage of Favourable Responses.....	55
Table 4.15: Information Security Awareness Level	56
Table 4.16: Information Security Awareness Level	56
Table 4.17: Cross-tabulation of Survey Sample by Sector and Size.....	57
Table 4.18: Questions 6, 7, 8 and 9 by Organization Size	58
Table 4.19: Average Scores for All Focus Areas.....	58
Table 4.20: Average Scores for All Sub-Areas.....	59
Table 4.21: Questions 6, 7,8 and 9 by Organization Sector.....	61
Table 4.22: Average scores for all focus area	62
Table 4.23: Average Scores for All sub-areas	63
Table 4.24: Test Results for Email Use Focus Area	64

FIGURES

Figure 2.1: Focus Areas with Representative Areas	19
Figure 3.1: Cronbach's Alpha for the KAB Survey Components	35
Figure 4.1: Responses to the First Questionnaire Item	39
Figure 4.2: Responses to the Second Questionnaire Item.....	39
Figure 4.3: Responses to the Third Questionnaire Item.....	40
Figure 4.4: Responses to the Fifth Questionnaire Item.....	41
Figure 4.5: Responses to the Sixth Questionnaire Item	42
Figure 4.6: Responses to the Seventh Questionnaire Item.....	43
Figure 4.7: Responses to the Eighth Questionnaire Item	44
Figure 4.8: Responses to the Ninth Questionnaire Item	44
Figure 4.9: Answers to Focus Area: Password Management	46
Figure 4.10: Answers to Focus Area: Email Use	47
Figure 4.11: Answers to Focus Area: Internet Use	48
Figure 4.12: Answers to Focus Area: Social Media Use	49
Figure 4.13: Answers to Focus Area: Mobile Devices	50
Figure 4.14: Answers to Focus Area: Information Handling.....	51
Figure 4.15: Answers to Focus Area: Incident Reporting	52

ABBREVIATIONS

CIA	:	Confidentiality, Integrity, and Availability
COVID-19	:	Coronavirus Disease of 2019
DCMS	:	Department for Digital, Culture, Media and Sport
HAIS-Q	:	Human Aspects of Information Security Questionnaire
ICT	:	Information and Communications Technology
ILO	:	International Labour Organization
ISA	:	Information Security Awareness
ISP	:	Information Security Policy
KAB	:	Knowledge-Attitude-Behaviour
KSA	:	Kingdom of Saudi Arabia
NIST	:	National Institute of Standards and Technology
SAR	:	Saudi Arabian Riyal
SME	:	Small and Medium-sized Enterprises
SPSS	:	Statistical Package for Social Sciences
UK	:	United Kingdom

1. INTRODUCTION

On March 11th 2020, the World Health Organization classified the novel Coronavirus outbreak (also known as COVID-19) as a pandemic.¹ To slow down the spread of the virus, governments worldwide were urged to take urgent and drastic measures. Among these measures was the nationwide lockdowns in many countries. As the lockdown measures came into effect, many businesses and organizations instructed their employees to stay home and continue to work remotely. Although the concepts of working remotely and at home are not new phenomena, many organizations have no previous experience of telework; even organizations that were previously familiar with the concept were struggling with the abrupt shift of mass employees from working in the office to working at home (Curran 2020). However, this is not the first time a disaster disrupts the nature of work creating the need to shift towards teleworking.

Natural disasters (such as; fires, earthquakes, tsunamis, hurricanes, etc.), security threats, terrorist attacks and many other disasters have been forcing workplaces to be closed; sometimes for extended periods of time. For example, a series of earthquakes between 2010 and 2012 in Christchurch, New Zealand, forced many organizations to shut down and operate remotely (Donnelly & Proctor-Thomson 2015). The terrorist attack on the World Trade Center and the Pentagon followed by the discovery of anthrax in Washington, DC and several other cities emphasized the importance of telework for organizations as well as employees (Potter, 2003). In a Congress committee hearing on *The Heightened Need for Telework Opportunities in the Post-9/11 World*, Congressman, Tom Davis indicated that telework is “an essential component of any continuity of operations plan. Something we once considered advantageous and beneficial has evolved into a cornerstone of emergency preparedness” (US House 2004). In an analogous statement, Donnelly and Proctor-Thomson identify home telework as an “essential component of continued organizational operation in times of disaster” (2015 p. 50).

¹ WHO 2020, <https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020> [Accessed 18 November 2020].

Whilst organizations have had their hands full managing the social and economic impact of the Coronavirus pandemic, there has been an unprecedented increase in the indiscriminate as well as targeted cyber-attacks targeting the general public along with the legions of home teleworkers (Lallie et al. 2020). Many entities have reported a growth in the frequency and severity of cyber-attacks. Google alone reported blocking 18 million phishing emails and malware associated with COVID-19 daily during the month of April, 2020.² In addition to the observed growth of cyber-attacks, additional security threats and risks have been introduced with the sudden shift of workforces to working from home; as “working at home en-masse has realised a level of cyber security concerns and challenges never faced before by industry and citizenry” (Lallie et al. 2020, p. 1). Besides the already existing security threats and risks, organizations nowadays have to deal with the added risks and threats associated with employees operating outside the organization safety net. Under these circumstances governing information security is more essential than ever.

Information security is defined by the National Institute of Standards and Technology (NIST) as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability” (2017, p. 2). As indicated in the definition, information security is the preservation of three main components or characteristics known as the CIA triad which are confidentiality (i.e. accessibility to information is only granted to authorized personnel); integrity (i.e. confirming that information is accurate and not accidentally or maliciously modified); and availability (i.e. ensuring reliable and timely access to information when required by authorized users) (Peltier 2013).

To maintain information security and to protect information assets from security threats and risks, organizations have equipped themselves with various administrative, technical and physical information security controls. Nevertheless, information security policy is one of the most essential information security controls (Schneier 2015, Höne & Eloff 2002). Information security policy is the “cornerstone” for any efficient information security architecture; it acts as a foundation on which all other security standards, procedures and guidelines are based, and it defines employees’ roles and responsibilities

² Google Cloud 2020, <https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond> [Accessed 20 September 2020].

(Hone & Eloff 2002, Peltier 2013). However, relying completely on information security policy is insufficient; another equally significant safeguard is information security training and awareness programs (Sturgeon 1996). Undoubtedly, employees are one of the indispensable factors of organizational information security. The actions of an individual employee could enhance organizational security posture, or could endanger the security of the entire organization (Rao & Nayak, 2014). Therefore, it is essential for organizations to provide organization wide security training and awareness programs (Rao & Nayak 2014).

As indicated earlier, due to the outbreak of COVID-19, employers were suddenly required to allow their workforce to operate remotely from their homes without thoroughly considering security threats and risks and the safety of teleworkers home environment (Abukari & Bankas 2020). Nevertheless, what motivated this study and especially in the context of the Kingdom of Saudi Arabia (KSA) is the fact that when the lockdown took place and employees started working from home, I have noticed lack of information security awareness among family members and friends who have worked or still working from home. There was no consideration for the security of information they were handling, there were lack of awareness of the organizational security policies and their roles and responsibility in safeguarding information security. However, to maintain information security, combat cybercrimes and the threats and risks associated with the innovative way of working from home, it is crucial for employees to be aware of the security policies present at the organizations they work for and to be aware of and trained to follow the best security practices and how they can maintain information security regardless of the work setting. In other words, a lot of these measures were even necessary before the outbreak of COVID-19 and the shift to telework.

In order to explore this phenomenon further, an exploratory study have been carried out. Indeed, conducting this study does not only help in exploring employees' awareness of the existing of security policies at the organizations they work for, but it also examines if employees have had information security training and if they have information security awareness. This study will pave the way and draw researchers' awareness to the

importance of investigating this area in-depth. Having said this, the aim of this study is clarified in the research questions below.

1.1 RESEARCH QUESTIONS

- i. To what extent are teleworkers in KSA aware of the existence of information security policies in the organizations they work for? And to what extent are these teleworkers aware of the existence of remote work policies in the organizations they work for?
- ii. Are teleworkers at these organizations trained to maintain information security in general and while working remotely?
- iii. To what extent does their behaviour reflect awareness of information security while working remotely?
- iv. Are there any significant differences among respondent groups regarding information security policies, training and information security awareness?

1.2 RESEARCH CONTEXT

The context of the study is KSA. KSA is one of the developing countries and it has the largest economy of the Middle East,³ and it is one of the G20 members.⁴ According to Al-Harethi and Al-Amoodi (2019), the Middle East attracts many cyber-attacks because the area has over half of the world's oil and gas supplies and with the emergence of COVID-19, the Middle East is experiencing a "cyber pandemic" (Murphy 2020). In the same vein, the United States Department of defense has indicated that when it comes to cyber-security, gulf countries are "in good shape, [but] Saudi Arabia is not" (cited in Al-Harethi & Al-Amoodi 2019). KSA has, therefore, launched a new vision 2030 that aims at enhancing many aspects in the public and private sectors including the development and usage of IT, and creating "Resilient, secure and trusted Saudi cyberspace".⁵

³ World Bank (n.d.), https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true&year_high_desc=true [Accessed 10 June 2020].

⁴ G20 Foundation (n.d.), <https://www.g20foundation.org/g20/what-is-the-g20> [Accessed 23 July 2020].

⁵ National Cybersecurity Authority (NCA) (n.d.), <https://nca.gov.sa/en/index.html> [Accessed 5 January 2021].

1.3 DISSERTATION OVERVIEW

The remaining of this paper is structured as follows. After this introduction, the second chapter is the review of literature which focuses on telework, information security policies, information security training and awareness and ends with the gap of knowledge. The third chapter sheds the light on the adopted methodology to answer the research questions, which includes research design and data collection procedures. Chapter four focuses on data analysis and reported the findings. The last chapter includes a discussion of the findings, the limitations, recommendations for future researches and a conclusion.



2. LITERATURE REVIEW

There are three main sections in this chapter; each section addresses an important aspect of the study. The literature review commences with the definition and overview of home telework, security risks generated in teleworking and information security in home teleworking environment. The second section tackles the literature on information security policies, their importance and uptake internationally and in KSA. The third section addresses information security training and awareness, information security, training and awareness in the context of KSA and methods to measure Information Security Awareness (ISA). The literature review concludes with the gap of knowledge.

2.1 TELEWORK

2.1.1 Telework from Home: Definition and Overview

Telework -also known as teleworking or telecommuting- has been defined as “working outside the conventional workplace and communicating with it by way of telecommunications or computer-based technology” (Bailey & Kurland 2002, p. 384). The definition indicates that telework can be distinguished by two main aspects: (a) the work location; and (b) the use of Information and Communications Technology (ICT) which refers to all hardware and software components related to computer and digital technologies; such as, smartphones, tablets, laptops, desktop computers, network infrastructure and so on.

With regard to the first aspect, telework can be used to describe any work that takes place outside the specified place of business which includes a wide range of work arrangements; however, the focus of this study is teleworking in the context of the employee’s own dwelling. In other words, teleworking from home “comprises workers who carry out work defined as telework in their own residence” (International Labour Organization (ILO) 2020a). It should be noted that, “teleworking”, “remote working”, “working at home”, “home-based work” and the different combinations of the four terms including “remote

work from home”, “home-based telework” and “telework from home” are often used interchangeably due to their interrelated and overlapped nature; however, the terms are not synonymous (ILO 2020a). Defining these terms and the difference between them is beyond the scope of this study, nevertheless, across the course of the study the terms “telework from home” and “home telework” are used exclusively to refer to the above stated definition.

Teleworking has been extensively discussed and increasingly advocated for its positive impact on individuals, organizations and even on the society as a whole (e.g. Day & Burbach 2011, Lister & Harnish 2011, Mello 2007, Kurkland & Bailey 1999, Niles 1997). Moreover, at time of risks and unexpected events (e.g., natural disasters, terrorist attacks, outbreak of epidemic and/or pandemic), teleworking practices and policies play a main role in the continuity plan of any business (ILO 2020b). Aside from its desirable benefits, teleworking raises challenges that are not usually present in ordinary work arrangements (Greer & Payne 2014). These challenges may be related to the fact that working at a distance from the core organization does not only affect where teleworkers conduct their work, it also alters the physical surroundings; the change in physical location and surroundings may also affect working practices and the tools and methods teleworkers use to perform their work (Sardeshmukh et al. 2012 cited in Greer & Payne 2014).

2.1.2 Security Risks Generated in Teleworking

The majority of literature on teleworking tends to focus on different aspects of telework with less attention given to data security. Nevertheless, most examinations identified data security as a source of concern for organizations. In a study of teleworking adoption and how it is more influenced by the attitudes of management, autonomy of workers and flexibility of employment than technology establishment; Clear and Dickson (2005) list data security risks as one of the major disadvantages of telework adoption in small and medium-sized enterprises (SMEs). Niles (1997) in a study on the success factors and implementation challenges of telework, identifies unauthorized access to organizations’ sensitive information as one of the barriers for adopting telework. Illegems and Verbeke (2003) also argue that concerns for the security of internal data is one of the holdbacks in

adopting telework. Similarly, in a study on the benefits and limitations associated with telework, Mello (2007) notes security of sensitive information as a reason for the limited diffusion of the concept. In the United States, the General Accounting Office (2001) conducted a study to investigate possible barriers facing employers when adapting teleworking programs. Concerns for the security of sensitive data was among the barriers reported by employers. Although the topic of data security in relation to telework is not adequately addressed in literature, some researchers have directly examined data security threats associated with teleworking.

In a growing body of literature, telework is perceived as a source of threat to the confidentiality, integrity and availability of data. Among the perceived security risks is the risk of data disclosure. Spinellis et al. (1999) conducted a study on the security requirements and risks in small enterprises and home offices. The study did not address teleworking in specific; however, it examined security issues and threats present in home-office environments. One of the major security threats mentioned in the study is the unauthorized disclosure of data. Rikitake et al. (2001) also identified data security issues while home teleworking over the internet and other technologies. Among the risks mentioned is the risk of other family members sharing the same equipment (such as computer devices) which may lead to sensitive data leakage. Sharing computer devices and other telecommuting equipment is not the only source of data leakage. Unattended work devices and printed documents may be vulnerable to unauthorized access by teleworker's family or anyone able to access the home office (Sturgeon 1996).

Data could also be susceptible to eavesdropping while in transit over unprotected networks and communication channels (Okereafor & Manny 2020, NIST 2016, Ernst & Young 2008). Although it is more common in other forms of teleworking than in home telework settings, data disclosure could also occur through the loss or theft of devices or other tangible assets which may hold sensitive data (Ernst & Young 2008). All mentioned scenarios indicate accidental data leakage, whereas, data leakage could also be deliberate. Without proper monitoring and deterring measurements, employees who have access to confidential data may leak it to competitors causing vital damage to their organizations (Niles 1997, Sturgeon 1996). Indeed, confidential data loss could have a negative impact

on organizations especially if the data leakage was from top level management (Lim & Teo 2000).

Modification of data is another security threat associated with teleworking. Sturgeon (1996) described modification as the unintended or deliberate change to information or systems leading to integrity loss. As mentioned earlier, the use of unsecure networks and communication channels which are beyond the organization's control does not only make data vulnerable to unauthorized access but also increases the risk of data being intercepted and tampered with (NIST 2016). Moreover, data modification may be the result of malicious software or technical and human errors. Likewise, information modification may lead to substantial financial damages for organizations (Spinellis et al. 1999).

Another data security threat is the threat of data interruption. Interruption is identified as the loss of availability of information, IT systems or any asset required by authorized employees leading to productivity loss (Sturgeon 1996). Interruption may be the result of unexpected power failure since home environments lack the capability to provide sufficient power supplies (Risktaker et al. 2001). A natural disaster, accidental system errors or malicious software (malware) could also lead to data interruption and even data destruction. However, the temporary cut of service or loss of access to data or systems is not as crucial as data destruction. The destruction of critical organizational data maintained by home teleworkers without having proper backups might have severe impact on the organization (Sturgeon 1996).

Security breaches regarding sensitive information are not the only risks generated in home telework environment. A number of studies have identified other issues of information security related to teleworking. Among the identified issues is the lack of organizational commitment to teleworking. Ernst and Young (2008) reported that although companies are aware of the risks present in telework arrangements, they choose to put off the topic in the favour of handling more immediate challenges and risks; and as a result, teleworkers may receive less technical support than employees who are physically present at the workplace. With no specialist IT support on-hand, teleworkers may seek technical assistance elsewhere leading to all sorts of security threats (Ampomah et al. 2013).

Another point worth mentioning is that, telework eliminates the boundaries between different departments within an organization, creating a cooperate ownership vagueness whilst managing security risks (Ernst & Young 2008). Another issue is the inability or inefficiency in monitoring teleworkers' activities and environments. Peacey (2006) noted that it is more challenging to monitor and control teleworker's environment outside the organization's premises as compared with the central workplace. Despite the abundance of tools and software available to track and monitor teleworkers, there is an increasing concern for teleworker's privacy due to the intrusive nature of these tools and software (ILO 2020b, GAO 2001).

Home teleworkers are less prepared to handle security risks because home environments lack the technologies and methods (e.g. VPN, firewalls, anti-virus, DNS filtering and proxies) needed to mitigate security threats that are usually available within organizations (Evangelakos 2020). Moreover, teleworkers setup their equipment and network connections and use their personal equipment for telecommuting which could lead to various security issues (Peltier 2002). In addition, many teleworkers use remote access technologies to access organization's resources. Since home equipment do not have the same level of protection as organization's equipment; the nature of telework and remote access technologies could expose the organization to more threats compared to technologies only accessed from within the organization (NIST 2016).

Lack of awareness is another security threat; many studies identify teleworkers as a source of threat or potential threat to information security. Teleworkers often do not fully understand information security risks, the importance of the data they are processing, the consequences of their actions on information security or how to sustain data securely in a teleworking environment (NIST 2016). Teleworkers as well lack security and privacy related practices while using portable devices, wireless networks and internet downloads which may compromise the security of sensitive data (Ernst & Young 2008). Another significant threat to information security is the lack of efficiency in monitoring employees' compliance to technology related policies specially when they use their personal devices while teleworking (Ernst & Young 2008).

Furthermore, the propagation of COVID-19 pandemic has generated a significant security risks and threats (Evangelakos 2020, Lallie et al. 2020). Cyber-criminals are leveraging the current circumstances, preying on public's disruption, fear and the desire for news to conduct a range of COVID-19-related cyber-attacks (Evangelakos 2020, Lallie et al. 2020, Okereafor & Manny 2020). Attackers are impersonating as government entities, public authorities and healthcare representatives, penetrating systems and stealing information by conducting phishing and malware attacks (Evangelakos 2020). These attacks are targeting the general public alongside home teleworkers who are operating outside their organizations' protective zones (Evangelakos 2020, Lallie et al. 2020).

The list of identified security issues is inclusive but not an exhaustive one, nevertheless, the key threat to information security is the lack of security policies and the lack of information security training and awareness programs. A survey conducted by Ernst and Young and the Center for Democracy and Technology (2008) on 73 government and corporate organizations from 10 industries in Canada, the United States and Europe showed surprising findings. The survey identified lack of policies, procedures and training programs among these organizations. Only around half of the organizations surveyed had written policies or training programs in place to handle the privacy and security of information for home telework settings.

2.1.3 Information Security in Home Teleworking Environment

Information security is vast; it cannot be achieved with a single solution because different risks require different security strategies. A number of studies have looked at administrative, technical and physical safeguards and controls to overcome teleworking-related security threats and risks. Proposed safeguards and measures incorporate the protection of teleworkers' devices, networks, remote access technologies and communication channel through the use of encryption, backups, VPN technology, strong authentication and access control, antivirus software, firewalls, IDSs/IPSs and many other measures (NIST 2016, Ernst & Yong 2008, Peacey 2006, Sturgeon 1996).

As indicated earlier, the technologies and methods for protecting information security are various; however, maintaining a secure work environment for home teleworkers can be a complicated task. Organizations have different security requirements and objectives, not to mention that every home teleworking situation is different. Nonetheless, “as a necessary minimum, an organization should develop and maintain an appropriate data-security policy if it aspires to advance telework” (Pyöriä 2011, p. 9). Similarly, Sturgeon (1996) established the need for security policy and procedures before organizations adapt any teleworking agreement with employees. Just as vulnerabilities associated with home teleworking are most likely different from those present at traditional workplace; the policies in place may or may not be transportable and sufficient to home teleworking settings. Ernst & Yong (2008) indicated that organizations should develop and enforce policies, tools and controls that are specific to teleworking arrangements.

Another point that is equally important, is to ensure teleworkers awareness and compliance with security policies and guidelines. As mentioned earlier, employees are considered a substantial aspect in security; teleworkers need to be aware of security risks, the purpose of security policies and the critical need to comply with them to safeguard against security risks and threats (Sturgeon 2008, 1996). Organizations will be held accountable for data breaches occur due to a lack of adherence to policies and procedures. Therefore, organizations need to communicate the security policies clearly and regularly conduct awareness and training programs (Day & Burbach 2011, Peltier 2002).

2.2 INFORMATION SECURITY POLICIES

Peltier (2013) defines policy as “a high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area” (p. 2). Security policies are established at many levels varying from the broad organizational policy to the explicit operational constraints (NIST 2015). Remote security policies on the other hand, are often part of the ISP or created as a separate policy within the main document of the information security framework. The aim of a remote security policy is to identify appropriate measures and controls to protect and maintain information security while conducting work from a remote location (NIST 2016).

2.2.1 Importance

The importance of a policy to the information security of an organization is indisputable. Many authors have written extensively on the indispensable role a policy plays for organizations' information security (Schneier 2015, Höne & Eloff 2002, King et al. 2001, Higgins 1999). As Peltier stated in his book *Information Security Fundamentals*, "the cornerstone of effective information security architecture is a well written policy statement" (2013, p. 2). The importance of information security policy emerges from the fact that it contributes to the organization as a whole, demonstrating organizational interest in safeguarding information security and coordinating security efforts (Barman 2001, Lee 2001). It also acts as a foundation on which all other security standards, procedures and guidelines are based; and correspondingly directing employees' actions (Peltier 2013, Höne and Eloff 2002). As the availability of a policy could positively enhance employee's behaviour towards information security risks (Li et al. 2014). Moreover, oftentimes the existence of a policy indicates that the risk assessment process has already taken a place. Therefore, if organizations payed a considerable attention while setting up their security policies, they could accomplish a stronger and more secure IT environment (Abu-Musa 2010).

2.2.2 Uptake

Although information security policies are widely acknowledged for their importance; this significance has not been translated into ground. Many organizations are still lacking formal information security policies (Arnott 2002); and even where they do exist, they sometimes are considered insufficient (Höne & Eloff 2002, Moule & Giavara 1995). Whitman and Mattord (2005) also argue that despite of the fact that information security policy may be the most cost-effective security measure, however, it is the most difficult to establish adequately.

2.2.2.1 Internationally

Internationally, there are many studies and surveys which have distinct foci other than policies, but which investigate the uptake level of security policies among organizations as part of their examinations. An example of such survey is the annual *Cyber Security Breaches Survey* conducted by the Department for Digital, Culture, Media and Sport (DCMS) in the United Kingdom. The main focus of the survey is to investigate how UK organizations handle cyber security, and the impact of breaches; however, survey results indicates that only four in ten businesses (38 percent) and charities (42 percent) have a formal policy in place. The DCMS study further reports that although most of these organizations have certain technical controls (e.g. malware protection); they are lacking cyber security policies, specifically policies covering home and mobile working (DCMS 2020). Fulford and Doherty (2003) conducted a questionnaire to examine the uptake, content, dissemination and impact of information security policies in large organization in UK; results indicates that 76 percent of the sample have information security policy whereas 24 percent do not have information security policy in place (Fulford & Doherty 2003). Lopes and Sá-Soares (2010) as well examined the adoption of information systems security policies, however, in the context of Portuguese public administration. The authors reported low adoption of security policies among City Councils.

Alqahtani (2017) examined information security policies (ISPs) sufficiency in a large organization within an Arab gulf country. The study evaluated the adequacy of ISPs by examining the maturity level of focused domains such as; password management, mobile computing and email use. The findings reveal a variety in the maturity levels of the investigated elements; however, only three out of the 16 investigated areas had a good maturity level, three were average and the remaining 10 scored below average or poor. Information security policies and telework/remote security policies have also been an essential part of various commercial surveys. A survey by Ernst & Young and the Center for Democracy and Technology (CDT) of 73 government and corporate organizations from 10 industries in the United States, Canada and Europe examined organizational policies, practices and techniques in regards to teleworking; the survey identified lack of policies, procedures and training programs among these organizations. Only around half

of the organizations surveyed had written policies or training programs in place to handle the privacy and security of information for home telework settings (Ernst & Young 2008).

2.2.2.2 In KSA

There is a small number of studies that investigate the prevalence and the adoption of information security policies within organizations in KSA. In a study to explore the existence and implementation of information security governance (ISG) in KSAs' organizations; the author reported that the majority of Saudi organizations do not have a clear written information security policy, information security strategies or disaster recovery plans (Abu-Musa 2010). In addition, procedures for risk assessment are not conducted effectively and responsibilities and roles are not distinctly defined and communicated to employees (Abu-Musa 2010). Alsaif et al. (2015) conducted a survey on multiple organizations in Saudi Arabia to investigate how these organizations deal with the issues of deterrence for information security violation; with an emphasize on information security policies efficiency and awareness among employees. The authors stated that although organizations have informed their employees of information security policies, survey results indicate that only 61 percent of the participants are aware of these policies; besides that, 18 percent of participants frequently take company's information or use computers to conduct work from home; and 44 percent do the same occasionally. In addition, 33 percent of the participants process confidential organization information using their mobile phones and other personal devices.

On the other hand, Alzamil (2018), reported that the majority of surveyed organizations in KSA have information security policy in place and have established appropriate technology; nevertheless; these policies are not implemented and circulated adequately which decreases the efficiency of the deployed technology. Al-Harethi and Al-Amoodi (2019) reported that although there is a positive correlation between security policies and information security management, organizations within private sector in Saudi Arabia do not give adequate attention to information security policies. Thakur et al. (2016) examined information security policy in E-government in KSA while considering the effectiveness, threats and vulnerability involved. Alzahrani et al. (2018) on the other

hand, investigated the aspects that influence employees' compliance with their organization's ISPs.

2.3 INFORMATION SECURITY TRAINING AND AWARENESS

Information security threats cannot be eliminated by simply adopting a security policy or certain technical controls (Parsons et al. 2014). Policies, procedures and controls could be ignored or misused by employees who are not fully aware of their importance (Kruger & Kearney 2006); therefore, employees are considered the most vulnerable factor in information security (Fertig & Schütz 2020, Li et al. 2014, Furnell & Clarke 2012). Lack of awareness among employees of the security requirements of the organization is one of the main factors leading to security breaches (Parsons et al. 2014, Rao & Nayak 2014). Many studies identify unintentional or naive mistakes by uninformed, or non-compliant employees as the main threat to information security (Rao & Nayak 2014).

On the other hand, employees who are aware of their organization's security objectives and further follow the information security policies and regulations determined by their organizations can greatly improve the overall level of security in the organization (Bulgurcu et al. 2010, Siponen 2010). Therefore, to mitigate information security risks associated with the human factor, organizations need to train their employees on what is acceptable, unacceptable, what is anticipated from them to ensure security of information and what possible risks and threats that they might face. Gardner and Thomas (2014) define security awareness training as a "formal program with the goal of training users of the potential threats to an organization's information and how to avoid situations that might put the organization's data at risk." (p. 1).

Information security awareness can be the result of life experiences, or acquired from external sources such as journals and newspapers, or can be gained through organizational electronic and physical learning resources such as; workshops, quizzes, and simulated phishing and different awareness materials (Bulgurcu et al. 2010). Training and awareness programs ensure that the vulnerability and threats associated with the human aspects are reduced considerably (Rao & Nayak 2014). Organizations could enhance

information security awareness by frequently training their employees (Pattinson et al. 2018). As simply reading the ISP has been proved to significantly enhance the information security culture of employees compared with employees who had not read it (Da Veiga 2016). For all of these reasons, it is crucial for organizations to conduct organization wide security training and awareness programs. These programs must be conducted in a regular basis and cover various aspects of information security (Rao & Nayak 2014).

2.3.2 In KSA

While numerous studies have examined information security training and awareness, few studies have explicitly considered information security training and awareness in the context of KSA. Al-Harethi and Al-Amoodi (2019) conducted a quantitative survey to examine the information security element in technical IT departments at private organizations in KSA. The survey results indicate that the increase of awareness among staff members could reflect positively on the overall information security policies of the organization, which in result decreases the damages in the organization. Alsaiif's et al. (2015) study of five organizations in Saudi Arabia indicate that only 40 percent of employees are trained to maintain information security, and in regards to attacks and threats awareness, only 43 percent of employees open their email attachment with due care, awareness of fishing attacks and email spams among participants was also low (42 percent and 33 percent respectively).

Alarifi et al., (2012) collected data using an online questionnaire from 462 Saudis to examine the level of information security awareness among the general public in KSA. The online survey asked participant about different aspects of information security such as, password practices, password sharing, the frequently the change their passwords, awareness of information threats, incident reporting and other. The survey reported low level of ISA among survey participants in KSA. AlMindeel and Martins (2020) examined how information security awareness influence employees' behaviour in a government sector setting in Saudi Arabia. Innab et al. (2018) conducted a survey to examine employees' security training and awareness in the context of Riyadh, KSA while focusing

on the area of electronic mail phishing. The study concluded that employees in the government sector have more effective anti-phishing training compared to employees in the private sector.

2.3.3 Measuring Information Security Awareness (ISA)

Kruger and Kearney (2006) defined ISA as “the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organisation, their individual security responsibilities, and acts accordingly” (p. 289). The majority of the studies and surveys that attempt to measure ISA have focused on measuring one component or aspect of ISA or tend to measure information security in general means (Parsons et al. 2014). Moreover, most of the models used are adapted and derived from other fields (e.g. health and environmental psychology) (Parsons et al. 2014); which may present a biased viewpoint because studies that are based on these models tend to focus solely on proving or verifying the theory in use (Karjalainen 2011). Examples of such studies and models include, Mylonas et al. (2013) who examined security awareness in smartphone platforms; and Kruger and Kearney (2006) who measured ISA of an international mining company using the Knowledge-Attitude-Behaviour (KAB) model.

2.3.3.1 Human aspects of information security questionnaire (HAIS-Q)

The Human Aspects of Information Security Questionnaire (HAIS-Q) is arguably more accurate to test aspects of interest than any other information security questionnaire (Parsons et al. 2014). The HAIS-Q attempts to examine the overall ISA of participants while taking into consideration the unique nature of information security and the different factors that may affect participant’s knowledge, attitude and behaviour. The HAIS-Q is a self-report measure designed to assess information security awareness within an organization (Parsons et al. 2014). The instrument can be used by organizations to assess employee knowledge, attitude and behaviour which in turn might be used as an indicator of the overall security posture of an organisation, to test the efficiency or effectiveness of various controls, training and awareness program, or/and to justify the need to enforce

certain controls, training or awareness programs (McCormac et al. 2017, Parsons et al. 2017, 2014). This tool has been tested and validated by several studies as an effective instrument for measuring ISA among different populations, such as; employees, students and the general public (e.g. Mahardika et al. 2020, Takens 2020, Ikhsan & Ramli 2019, Pattinson et al. 2018, 2016, McCormac et al. 2017, Wahyudiwan et al. 2017, Mäses 2015, Parsons et al. 2017, 2015, 2014).

Figure 2.1: Focus Areas with Representative Areas

Focus area	Sub-area
Password management	Using the same password Sharing passwords Using a strong password
Email use	Clicking on links in emails from known senders Clicking on links in emails from unknown senders Opening attachments in emails from unknown senders
Internet use	Downloading files Accessing dubious websites Entering information online
Social media use	SM privacy settings Considering consequences Posting about work
Mobile devices	Physically securing mobile devices Sending sensitive information via Wi-Fi Shoulder surfing
Information handling	Disposing of sensitive print-outs Inserting removable media Leaving sensitive material
Incident reporting	Reporting suspicious behaviour Ignoring poor security behaviour by colleagues Reporting all incidents

Source: Parsons et al. 2017, p. 45.

The tool is designed to measure employee' behaviours that is unintentional or correlated with lack of awareness rather than intended harm or misuse which is identified by the authors as 'Neutral Behaviours (Accidental)' (Parsons et al. 2014). The instrument includes 63 statements designed to test three dimensions; which are knowledge (what do the participants know), attitude (how they conceptualize the topic) and behaviour (what the participants do). Each of these dimensions is subdivided into seven focus areas; these areas are password management, email use, internet use, social media use, mobile devices, information handling and incident reporting. These seven focus domains are developed to demonstrate the areas of information security policy that are more relatable to employees; and which are most susceptible to non-compliance (Parsons et al. 2014). Furthermore, each of the seven areas are further subdivided into three representative areas

leading to 21 areas of interest, (check Figure 2.1 for the focus areas and sub-areas). For each of these areas, there is one statement on knowledge, one on attitude and another on behaviour (see Annex 5). These three statements are formatted differently but they are all measuring the same thing (same sub-area). Finally, 29 statements out of 63 statements are negatively phrased (denoted by ^ in Annex 5) and all statements are measured on a 5-point Likert-type scale (strongly agree to strongly disagree).

2.4 GAP OF KNOWLEDGE

In the wake of COVID-19, massive movement to home telework adoption is observed among organizations worldwide. As of today, there have not been major cases of telework adoption among organization; however, the devastating nature of COVID-19 pandemic has necessitated this massive movement. Whilst the importance of telework as an alternative work arrangement is indisputable; as can be inferred from the above stated literature, the nature of telework amplifies existing risks and adds new challenges and threats that are not usually present in ordinary work arrangements (Greer & Payne 2014, Ernst & Young 2008).

Although each organization has different security requirements and objectives and every home teleworking situation is different, the review of the literature has indicated the importance of security policies, employees' security training and awareness in protecting information security in different work arrangements. This unprecedented situation calls for investigating information security policies and remote security policies awareness among teleworkers. Policies acts as the foundation on which all other security standards, procedures and guidelines are based (Peltier 2013, Höne & Eloff 2002); however, having an adequate ISP would not be effective without communicating it to all employees. Employees need to be aware of the policy and have an understanding of how to follow it (Da Veiga 2016).

Besides security policies, another point that is equally important is to ensure teleworkers' awareness and compliance with security policies and guidelines. As mentioned earlier, employees are considered a substantial aspect in security; employees need to be aware of

security threats, the purpose of security policies and the critical need to comply with them to safeguard against security risks and threats (Sturgeon, 1996). Organizations will be held accountable for any data breaches that may occur as a result of a lack of adherence/compliance to policies and procedures. Therefore, organizations need to clearly convey its security policies and regularly conduct training and awareness programs (Day & Burbach 2011, Peltier 2002).

The review of literature has also indicated that limited research had been published in the context of KSA. The studies that do focus on KSA context, however, do not explore the areas addressed in this study in the same manner; for example, the survey conducted by Al-Harethi and Al-Amoodi (2019) examined ISPs in private sector organizations; nonetheless, the study focused on one city only (Jeddah) without indicating the size of organizations investigated. Furthermore, Alsaif et al. (2015) mainly focused on understanding deterrence in ISPs in KSA's organizations while limiting their participants to a set of organizations (King Faisal University (KFU), Saudi Telecom Company (STC), ARAMCO, Zain and SABIC). Alarifi et al. (2012) investigated information security awareness, but among the general public in KSA and not among employees. On the other hand, AlMindeel and Martins (2020) examined how information security awareness influence employees' behaviour but within the government sector. Furthermore, none of these studies explored the areas addressed in this study all together.

Moreover, none of these studies explored teleworkers awareness of the existence of remote security policies in KSA. In addition, the majority of these studies and surveys are mostly conducted formally with the organizations' representatives or conducted solely with IS managers, IT staff or individuals who are responsible for information security within these organizations. Although information security professionals typically have more detailed knowledge of the situation of information security in an organization and the information supplied by them can reveal significant information about the investigated area, the supplied information may not reflect the opinions or experiences of the majority of individual employees (technical and non-technical) and may not yield a realistic assessment of the situation (Parsons et al. 2014). Investigating the situation from employees' perception may yield different results (Alzamil 2018).

In light of all of these considerations, there is a compelling need to examine teleworkers' awareness of the existence of information security and remote security policies in KSA, other aspects of security policies such as, scope, content, dissemination and impact are, however, beyond the scope of this study. Moreover, since employees are repeatedly viewed as the weakest factor in information security (Li et al. 2014, Furnell and Clarke 2012), there is a necessity to investigate whether employees undertake any kind/form of educational, training or awareness programs to maintain information security in general and while they are working from home. In addition, the study aims to measure the level of ISA among employees who are working from home. Finally, the study attempts to explore whether there are any significant differences among respondent groups regarding information security policies, training and information security awareness.

3. DATA AND METHOD

This chapter focuses on the methodology I have used to collect data and answer the early mentioned research questions: (i) to what extent are teleworkers in KSA aware of the existence of information security policies in the organizations they work for? And to what extent are these teleworkers aware of the existence of remote work policies in the organizations they work for? (ii) are teleworkers at these organizations trained to maintain information security in general and while working remotely? (iii) to what extent does their behaviour reflect awareness of information security while working remotely? And (iv) are there any significant differences among respondent groups regarding information security policies, training and information security awareness? The chapter is divided into five sections following the outline suggested by Burgess (2001): sampling, research design, data collection procedures, ethical issues and the last section focuses on validity and reliability.

3.1. SAMPLE

Under this section, I will focus on the targeted population, defined as “all the members of the group that you are interested in” (Burgess 2001, p. 4), sampling procedure and research participants/actual sample, which refers to the “sub-set of the population that is usually chosen” (Burgess 2001, p. 4). I will also focus on the reason for choosing them. As this research concerns itself with home teleworkers in KSA, the larger population includes all employees in KSA who worked or still working from home during the period of the lockdown due to the outbreak of COVID-19. Therefore, to collect as much responses as possible to explore the area under study, I have used nonprobability sampling procedure, to be more specific I have used snowball sampling, which is “identifying one participant who meets your inclusion criteria. This first individual is then asked to refer someone else for the survey; then, you ask this second individual to refer someone else, and so on” (Sue & Ritter 2007, p. 8). 155 participants were identified using this sampling strategy. The main limitation with this sampling procedure is that the identified sample

“may or may not represent the population well” (Sue & Ritter 2007, p. 33) which was a main concern when using this sampling strategy.

Therefore, to ensure that the sample represents the population, I have summarized the characteristics of both in Table 1, and it will be noticed from the table that the sample was indeed representable of the population. To avoid this problem, I have also followed the technique suggested by Burgess (2001) which is “to look for about 20-30 responses in each of the major sub-categories of the sample” (p. 4). Another main concern was related to the chosen sampling procedures; a main limitation when using the snowball sampling is that the research participants are not obliged to take part in the study and therefore, many research participants might withdraw from the study or not return their responses. Elaborating on this issue, Burgess (2001) explains that the response rate for surveys is 20 percent. Therefore, he suggests to send five times as the researcher wants to be returned. Indeed, this problem was one of the limitations of this study due also to reasons related to the procedure used to administrate the research tool (section 3.2.3).

Table 3.1: Description of the Population and Sample

Description of population	Description of sample
Employees in KSA	155 research participants indicated that they work in KSA
Home teleworkers (people who have been working from home during the lockdown and using ICTs to carry out their work remotely)	129 research participants indicated that they worked or still working from home due to the outbreak of COVID-19 (the actual final sample).

3.2. RESEARCH DESIGN

Quantitative tool, a questionnaire, was used to conduct this exploratory study. The use of surveys has many advantages and limitations at the same time. As for the advantages, according to Walliman (2011), surveys are faster in collecting big amount of data from large number of participants in a shorter period of time, they are cheap and they remove the effect the researcher might have on the research participants. Mathers and Hunn

(2007) add that as surveys do not put the research participants to any harm or danger, they are considered more ethical than other research tools (e.g. experimental tools). However, this research tool has two main limitations. They do not provide an in-depth data about “why people think and act in the way they do” and the questions in the tool depend mainly on the skills of the researcher in designing and wording his/her questions (Mathers & Hunn 2007, p. 8).

3.3. DATA-COLLECTION PROCEDURES

3.2.1. Designing the Survey

The questions in the survey were written based on the review of literature, and as the data were collected from people in KSA, the questionnaire was designed in two language, English (Annex 1) and then translated into Arabic by a professional translator (Annex 2). Due to restrictions in time, all the questions in the survey were closed-ended. It has to be acknowledged that although this type of questions is easier to analyse, faster to answer by the research participants and require no writing skills from the research participants (Walliman 2011), some researchers consider closed-ended questions a “source of bias” (Akbayrak 2000, p. 5) because the research participants cannot put their own thoughts and answers and they are restricted to the options the researcher includes in the tool. When designing the survey, I have followed the guidelines provided by Burgess (2001):

- i. Keeping the survey clear and short;
- ii. Avoiding the use of unnecessary headings, double questions;
- iii. Starting with a short introductory statement;
- iv. Including contact information of the researcher;
- v. Numbering the questions to make it easy for the research participant to follow the questions and they helpful for the researcher during the data analysis;
- vi. Making use of different font sizes (I have used **bold** font to draw peoples’ attention to definitions);
- vii. Starting with the easiest questions; and
- viii. Grouping questions relating to the same area.

I had two options when designing the survey, Google Forms or Microsoft Forms. Nevertheless, after piloting the tool, I decided to use Google Forms because the people participated in the piloting stage reported that question related to Likert scale were easier to answer on Google Forms. The questionnaire was divided into three main sections (Annex 1 and 2). The first section gathered general characteristics of the research sample, demographics. The second section collected data on the extent of employees' awareness on the existence of both information security policy and remote security policy at the organizations they work for. The third and last section collected data regarding security training and awareness and included a self-report questions to measure the level of ISA among teleworkers. Although the questions are different from one another, they provided a shared holistic view of the researched subject. The next section goes into the details of each item in the questionnaire.

Section 1: Demographics (5 questions):

The first page included an introductory section (introducing the research, aim of the study, assurance for anonymity, estimated time to complete the survey, a thank you and the research email) and five questions. The wording and justification of using these questions are addressed below.

Q1. At any stage, did you work from home due to the outbreak of COVID-19?

- a) Yes
- b) No

Q2. Before the pandemic, did you work from home?

- a) Yes
- b) No

Q3. Did you use a computer, smartphone, tablet or any other electronic device to carry out your work at home during COVID-19?

- a) Yes
- b) No

For an employee to be defined as a home teleworker two aspects were investigated: (a) the work location; and (b) the use of ICTs. Starting with the first aspect, the work location, telework is often linked with teleworker own residences (Van Oostendorp et al. 2005); however, teleworking in its general definition is not necessarily restricted to employee's

home, it also includes working at any alternative worksite other than the default workplace; such as, satellite offices, telework centres, hotels, cafés, airports, public transportation etc. Nevertheless, this survey was targeting employees teleworking from home. This element was investigated using question (Q1). Moreover, to get a better understanding and insight if the concept of telework is new in KSA or is known to people even before the pandemic, (Q2) was used. These two questions were adopted from ILO guide for labour statistics data collection (ILO 2020a); however, to elicit a better understanding, the wording of the questions was slightly changed.

The second element to distinguish a home teleworker is the usage of ICTs. This element was investigated using the third question (Q3). This question was also adopted from the ILO guide for labour statistics data collection (ILO 2020a). To elicit a better understanding, the wording of the question was slightly modified. Although the list of ICT components is exhaustive, I have kept the same list of devices mentioned in the original question because the devices listed are familiar to employees in general (technical and non-technical); and listing other technologies might have confused the research participants. Lastly, it should be noted that telework can also be defined with regards to time or the frequency in which the employee teleworks from home (ILO 2020a), nevertheless, it is irrelevant and beyond the scope of this study.

Q4. I work at ...

- a) Government sector
- b) Private sector
- c) Non-profit/Charities

Q5. Including yourself, what is the approximate total number of employees at your organization?

- a) 1 – 5 employees
- b) 6 – 49 employees
- c) 50 – 249 employees
- d) 250 or more

The purpose of the above two questions was to determine the demographics of the organizations the research participants work for which will help in answering the fourth research question. The first question (Q4) was used to determine the type of organizations.

Organizations can be classified into three sectors; government, private and non-profit/charities.⁶ The second question (Q5) was used to determine the size of the organization. The widely-accepted classification of organizations is based on the number of employees and annual revenue. In KSA, according to the Small and Medium Enterprises General Authority, a micro enterprise has between one and five employees and has a turnover of three million Saudi Riyal (SAR) or less, a small enterprise has between six and 49 employees and has a turnover between three to 40 million SAR, a medium-sized enterprise has between 50 and 249 employees and has a turnover between 40 to 200 million SAR and finally a large enterprise has 250 employees or above and has a turnover of more than 200 million SAR.⁷ However, as this study was targeting employees who might not have enough information about the revenue of the organizations they work for, the classification in this survey was based solely on the number of employees.

Section 2: Information Security Policy (2 questions):

This section aimed at answering the first research question, to what extent are teleworkers in KSA aware of the existence of information security policies in the organizations they work for? And to what extent are these teleworkers aware of the existence of remote work policies in the organizations they work for? The majority of organizations have either formal (written) or informal ISP. The aim of this section was to determine if teleworkers are aware of information security policies in general and remote security policies in specific at the organizations they work for. Since the questionnaire was targeting a diverse audience (technical and non-technical employees) for whom the term *Information Security Policy* might be a foreign concept, it was therefore essential that the questionnaire includes a short and clear definition of ISP to ensure that participants understand the concept. The definition did not truly capture all the aspects and components of the term, but I have listed the items that might be understood and

⁶ Saudi vision 2030 (n.d.), https://www.vision2030.gov.sa/sites/default/files/attachments/NTP%20English%20Public%20Document_2810.pdf [Accessed 3 January 2021].

⁷ Small and Medium Enterprises General Authority (Monsha'at): <https://www.monshaat.gov.sa/ar/SMEs-definition>

recognized by the participants. After listing the definition, the participants were presented with the following question:

Definition: It is a document stating organization's general goals and objectives in terms of information security. It offers a detailed clarification of what is suitable, unsuitable, what is anticipated from employees to ensure security of information; and what disciplinary actions can be taken against violation of policy.

Q6. In light of the previous definition, does your organization have an information security policy?

- a) Yes
- b) No
- c) Don't know

Q7. Does your organization have a remote security policy? (a remote security policy ensures security of information while working from alternative worksite such as; your home, hotel etc.)

- a) Yes
- b) No
- c) Don't know

Section 3: *Information Security Training & Awareness (2 questions):*

This section focused on answering the second research question, are teleworkers at these organizations trained to maintain information security in general and while working remotely? And the third research question, to what extent does their behaviour reflect awareness of information security while working remotely? To answer research question number two, two questions were used:

Q8. Does your organization provide any form of training or guidelines in regards to information security?

- a) Yes
- b) No

Q9. Did your organization provide any form of training or guidelines on how to maintain information security while working from home?

- a) Yes
- b) No

The first question was to determine if the organizations provide any form of training or guidelines in regards to information security in general regardless of the work settings. This because information security training is a continuous process and knowledge; skills or practices obtained from training should be transferable to other settings. The second question was to explore if employee got specific training on how to maintain information security while working from home.

Q10. I use a different password for my social media and work accounts.

Q11. I share my work passwords with colleagues.

Q12. I use a combination of letters, numbers and symbols in my work passwords.

Q13. I don't always click on links in emails just because they come from someone I know.

Q14. If an email from an unknown sender looks interesting, I click on a link within it.

Q15. I don't open email attachments if the sender is unknown to me.

Q16. I download any files onto my work computer that will help me get the job done.

Q17. When accessing the internet at work, I visit any websites that I want to.

Q18. I assess the safety of websites before entering information.

Q19. I don't regularly review my social media privacy settings.

Q20. I don't post anything on social media before considering any negative consequences.

Q21. I post whatever I want about my work on social media.

Q22. When working in a public place, I leave my laptop unattended.

Q23. I send sensitive work files using a public Wi-Fi network.

Q24. I check that strangers can't see my laptop screen if I'm working on a sensitive document.

Q25. When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.

Q26. I wouldn't plug a USB stick found in a public place into my work computer.

Q27. I leave print-outs that contain sensitive information on my desk when I'm not there.

Q28. If I saw someone acting suspiciously in my workplace, I would do something about it.

Q29. If I noticed my colleague ignoring security rules, I wouldn't take any action.

Q30. If I noticed a security incident, I would report it.

Table 3.2: Focus Areas and Sub-Areas with the Corresponding Statements

Focus area	Sub-area	Statements
Password management	Using the same password	Q10. I use a different password for my social media and work accounts.
	Sharing passwords	Q11. I share my work passwords with colleagues.
	Using a strong password	Q12. I use a combination of letters, numbers and symbols in my work passwords.
Email use	Clicking on links in emails from known senders	Q13. I don't always click on links in emails just because they come from someone I know.
	Clicking on links in emails from unknown senders	Q14. If an email from an unknown sender looks interesting, I click on a link within it.
	Opening attachments in emails from unknown senders	Q15. I don't open email attachments if the sender is unknown to me.
Internet use	Downloading files	Q16. I download any files onto my work computer that will help me get the job done.
	Accessing dubious websites	Q17. When accessing the internet at work, I visit any websites that I want to.
	Entering information online	Q18. I assess the safety of websites before entering information.
Social media use	SM privacy settings	Q19. I don't regularly review my social media privacy settings.
	Considering consequences	Q20. I don't post anything on social media before considering any negative consequences.
	Posting about work	Q21. I post whatever I want about my work on social media.
Mobile devices	Physically securing mobile devices	Q22. When working in a public place, I leave my laptop unattended.
	Sending sensitive information via Wi-Fi	Q23. I send sensitive work files using a public Wi-Fi network.
	Shoulder surfing	Q24. I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Information handling	Disposing of sensitive print-outs	Q25. When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
	Inserting removable media	Q26. I wouldn't plug a USB stick found in a public place into my work computer.
	Leaving sensitive material	Q27. I leave print-outs that contain sensitive information on my desk when I'm not there.
Incident reporting	Reporting suspicious behaviour	Q28. If I saw someone acting suspiciously in my workplace, I would do something about it.
	Ignoring poor security behaviour by colleagues	Q29. If I noticed my colleague ignoring security rules, I wouldn't take any action.
	Reporting all incidents	Q30. If I noticed a security incident, I would report it.

Statements from 10 to 30 were used to measure teleworkers' information security awareness; which answers the third research question. To get an accurate evaluation of teleworkers' ISA, the statements came from a reliable source that was previously tested for its validity and accuracy in measuring participants' ISA as formerly stated in section 2.3.3.1. Thus, the Human Aspects of Information Security Questionnaire (HAIS-Q) was used (Parsons et al. 2017). HAIS-Q is a flexible self-report measure/instrument that according to Parsons et al. (2017) might be used for various purposes. The tool consists of 63 statements designed to test the knowledge, attitude and behaviour of respondents in seven main focus areas or domains: password management, email use, internet use, social media use, mobile devices, information handling and incident reporting. Parsons et al. (2017) indicate that studies using this tool will get better measures when using all 63 items; they acknowledge, however, that they might be too long to include in one study. Therefore, they suggest that researchers can use the tool, vertically or horizontally, by focusing on specific domain(s) or modular(s). Example of studies that adapted one or two parts of the components include Pattinson et al. (2016), where the authors only used knowledge and attitude modular; Takens (2020) utilized both attitude and behaviour and 5 out of the 7 focus areas; and Ikhsan and Ramli (2019) where they solely used the knowledge modular (Table 3.2).

Having said this, in this study, only 21 statements (see Table 3.2 to know which statement represent which focus area) were chosen focusing on the aspect of behaviour. The choice of behaviour domain instead of knowledge or attitude is due to the fact that although there is a positive correlation between knowledge of policy and procedures and information security behaviour, better knowledge of policy and procedures does not necessarily ensure sufficient information security behaviour (Parsons et al. 2014). Moreover, Hänsch and Benenson (2014) divided security awareness into three categories; perception, protection, and behaviour; however, they reported that only behaviour is perceived to have a positive impact on information security within an organization. Similarly, Sari and Trianasari (2014) indicated that behaviour is the only valuable measure to understand ISA, as compliant behaviour is the product of ISA and therefore, can be used as an accurate measure of ISA (Fertig & Schütz 2020). Thus, when responding to the 21 statements, the research participants had to choose from a five-point Likert scale, rated

from “Strongly Agree” to “Strongly Disagree”. The responses were given values from one to five, which means that the more suitable the response, the higher the value given to it.

3.2.2. Piloting the Survey

Walliman (2011) explains that the aim of piloting the survey “is to detect any flaws in ... questioning and correct these prior to the” administrating the survey (p. 16). He adds that piloting questions also help the researcher to make necessary changes to the tool “to maximise ... response rate and minimise ... error rate on answers” (Walliman 2011, p. 16). Thus, because of time constraints and given the importance of this stage, the survey was piloted on seven colleagues (one Information Security Specialist who speaks English and Arabic fluently, three English native speakers and three Arabic natives). One received the Arabic and English versions, three received the Arabic version of the survey and the other three received the English version, and they were asked to contact the researcher whenever facing a difficulty understating or responding to any of the questions. Moreover, I have asked each one of them to provide a feedback about the clarity, organization and the overall structure of the survey. Their feedback was helpful and based on it I made the following changes to the tool:

- i. Using Google Forms instead of Microsoft Forms because the Likert Scale questions (Q10-30) were easier to answer on Google Forms;
- ii. Modifying the wording of the translated, Arabic, version of the survey (questions 13, 17 and 30).

3.2.3. Administrating the Survey

The survey was administrated electronically via WhatsApp (Annex 3). The message used to send the survey via WhatsApp included a short introduction inviting people to take part in the study, and two links, one for the Arabic version of the survey and the second one for the English version. Administrating the research tool in this way helped me to reach more research participants, but it had some limitations. Firstly, I could not know who responded to the survey and who did not which means that I could not send a follow up

reminder to those who did not. Secondly, the number of replies has dropped which is a problem inherited in this type of instruments administration; according to Sekaran and Bougie (2016), 30 percent is considered an acceptable response rate when administrating questionnaires online. To keep track of the actual number of people who opened the survey and the actual number of returned responses, I have used bitly.com. The number of people who opened the questionnaire was 221, and only 155 responses were returned (Annex 4).

3.4. ETHICAL CONCERNS

Dörnyei explains that ethical issues “are more in QUAL than in QUAN approaches because qualitative research often intrudes into the human private sphere” (2007, p. 64). However, I have paid attention to ethics throughout all the stages of the research. As the first page of the research tool (Annex 1 and 2) is the consent and information sheet, an ethical approval was obtained from all research participants. The form included an explanation of the aims of the study and assurance for confidentiality. Moreover, the research tool did not include any question that might identify any of the research participants. This means that both anonymity and confidentiality were achieved. Finally, to ensure data security, all responses were stored on a computer protected with a two-factor authentication password, and all data was deleted two months after submitting the paper.

3.5. VALIDITY and RELIABILITY

To ensure validity, I have first focused on face validity, “evaluates the appearance of the questionnaire in terms of feasibility, readability, consistency of style and formatting, and the clarity of the language used” (Taherdoost 2016, p. 29). To achieve this type of validity, the research tool was piloted (section 3.2.2.). Another type of validity I have focused on was content validity. To ensure this type of validity, I have followed three of the steps suggested by Taherdoost (2016). Firstly, the research tool was designed after a careful review of literature. Secondly, “A content validity survey ... [was] generated (each item is assessed using three-point scale (not necessary, useful but not essential and essential))”

(Taherdoost 2016, p. 30). The third step suggested by Taherdoost (2016) is to have the document evaluated by an expert in the field. Indeed, before distributing the survey and before piloting, the survey was sent to an Information Security Specialist and his evaluation, comments and feedback were considerate to increase the quality of the questionnaire.

In addition, to ensure reliability, “Internal Consistency or Homogeneity” (Fink 2003, p. 49) which means that all the question in the research tool focus on a certain issue was used. This was achieved by confirming that all the questions in the survey focus on the areas under study. Furthermore, each section of the questionnaire focused on a certain theme; the first section focused on demographics, the second section focused on policies, and the last one focused on training and awareness. Most importantly, to ensure internal reliability/consistency, I have calculated Cronbach’s alpha for questionnaire items 10 to 30 and compared the calculations with Cronbach’s (1951) recommended value (which indicates that items measure the same phenomena must have a Cronbach’s alpha value over 0.70) and with calculations reported in Parsons et al. (2014), (Cronbach’s alpha for self-reported behaviour was 0.918 (Figure 3.1)). Cronbach’s alpha for this study is 0.753 which is less than Parsons et al. (2014) but has exceeded the 0.70 value which indicates that the study has an internal consistency.

Figure 3.1: Cronbach's Alpha for the KAB Survey Components

Constructs	Cronbach’s alpha
Knowledge of policy and procedures	0.844
Attitude towards policy and procedures	0.884
Self-reported behaviour	0.918

Source: Parsons et al. (2014, p. 171).

4. FINDINGS

4.1 DATA ANALYSIS

The first 3 questions of the survey were to filter the data collected and identify the answers of the targeted sample (home teleworkers who work in KSA). To analyse these questions, I used descriptive statistical analysis which according to Edgar and Manz (2017) refers to “ways at evaluating and exploring the results of one variable at a time” (p. 123). This type of analysis is useful and effective to “provide simple summaries about the sample and the measures” (Trochim 2006). The same analysis procedure was also used to analyse questions 6, 7, 8 and 9. However, as questions 6 and 7 are targeted to answer research question number one, to what extent are teleworkers in KSA aware of the existence of information security policies in the organizations they work for? And to what extent are these teleworkers aware of the existence of remote work policies in the organizations they work for? And as questions 8 and 9 focus on answering the second research question, are teleworkers at these organizations trained to maintain information security in general and while working remotely? These four questions were analysed using proportions.

Another part of the analysis focuses on data collected to answer the third research question, to what extent does their behaviour reflect awareness of information security while working remotely? Out of the 30 questions, 21 questions are dedicated to measuring ISA. The nature of the questions used in the questionnaire to measure ISA (Likert- scale questions) requires a different way of analysis. After excluding the responses that did not fulfil the requirements of this survey and prior to data analysis several steps have been taken. First, the quality of the participants’ responses was examined. As the case with any questionnaire, some participant may not answer the questions with regards to their content (content non-responsivity), choosing the same answer for all statements. This behaviour has been identified by some of the authors using the HAIS-Q tool. For example, Parsons et al. (2017) excluded 26 responses because the authors detected a pattern in the responses as some participants selected the same answer to all the statements (e.g., selecting “Strongly Agree” as an answer for all statements). The same examination was applied to

all responses, and none of them have chosen the same uniform response for all the statements. Thus, none of the answers were excluded. This is probably due to the fact that I have used only one domain (21 statements) which is a considerable length compared to Parsons et al. (2017) where they used all three domains (63 statements).

Secondly, reverse scoring was conducted on the answers. As mentioned earlier, some of the statements in the questionnaire are negatively worded or phrased (Parsons et al. 2014; 2017) which means that there is a difference in the direction of scales in use. A statement which is “positively” worded will indicate a more positive attitude (awareness) when going higher on the scale. On the other hand, with “negatively” worded statements, a strong agreement with the statement reflects a low level of awareness. Therefore, it is essential to ensure that all statements are consistent with the way they are being measured. Out of the 21 statements, 10 statements are negatively phrased (11, 14, 16, 17, 19, 21, 22, 23, 27 and 29).

Table 4.1: Normal VS. Revers Scoring

5-point Likert Scale	Normal	Revers
Strongly Disagree	1	5
Disagree	2	4
Neutral	3	3
Agree	4	2
Strongly Agree	5	1

After reverse scoring the negatively phrased statements, descriptive statistics (specifically mean, standard deviation, minimum and maximum) were conducted for each statement (21 statements representing the 21 sub-areas). After that, descriptive statistics was also calculated for the seven main focus areas (Annex 6 and 7). In addition, the level of ISA was calculated and interpreted using different approaches (Annex 8).

The last part of the analysis focuses on answering the fourth research question, are there any significant differences among respondent groups regarding information security policies, training and information security awareness? Prior to data analysis, survey

questions number 4 and 5 were used to characterise the data collected in terms of both the size of the organization teleworkers work for and the sector they are employed at. After that, to investigate the significant differences among respondent groups, a series of chi-square tests were conducted on questions 6, 7, 8, and 9. Nevertheless, the nature of the questions used in the questionnaire to measure ISA requires a different way of analysis. As a result, a non-parametric test (Mann-Whitney U test) was carried out on the questionnaire items 10-30. Finally, all the data were analysed using the Statistical Package for Social Sciences (SPSS). The following section reports the findings from the data collected.

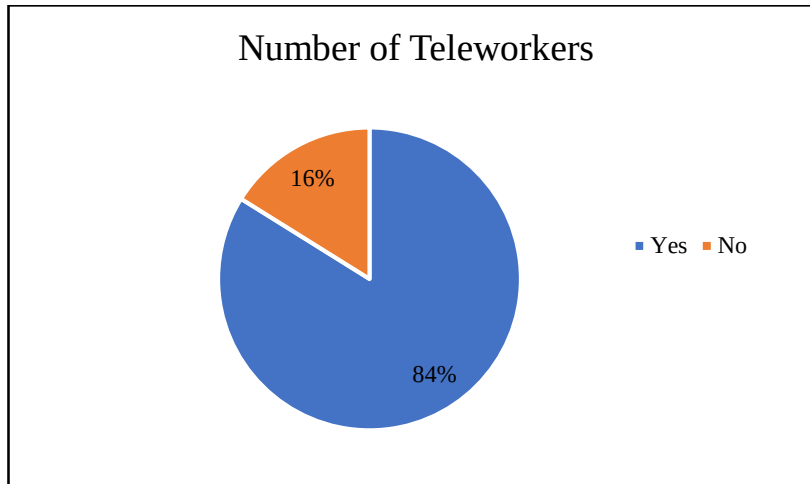
4.2 FINDINGS

The questionnaire links for both versions, English and Arabic, were clicked 221 times (English= 26 times and Arabic= 195 times). However, the returned responses were 155 (English= 20 responses and Arabic= 135 responses); this means that there are 64 people who clicked the links without answering the questionnaires; 2 clicks were subtracted from the total number of clicks as the supervisor has opened both links once from Turkey (Annex 4). It has to be noted, that as all the questions in the tool were mandatory, all 155 research participants answered all the questions in the tool. To organize this section, I will include the question from the questionnaire followed by the findings.

Q1. At any stage, did you work from home due to the outbreak of COVID-19?

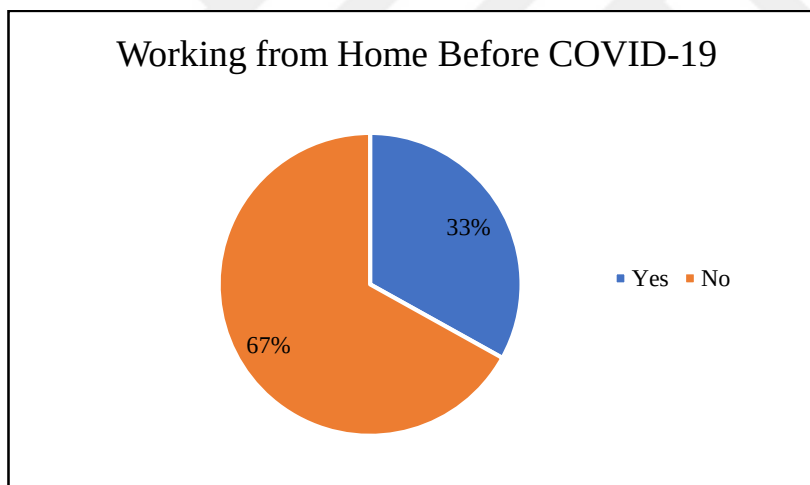
Research participants had two options when answering this question “Yes” or “No”. Out of the 155 research participants, 130 answered “Yes” which represents 83.87 percent of the sample, and only 25 research participants answered “No” which represents 16.13 percent of the sample (Figure 4.1). As this question is one of two questions aimed at identifying teleworkers, the target sample of the study, the responses of the 25 participants were eliminated. Therefore, the analysis for the subsequent questions will be based on the answers of the 130 participants.

Figure 4.1: Responses to the First Questionnaire Item



Q2. Before the pandemic, did you work from home?

Figure 4.2: Responses to the Second Questionnaire Item



In this question, too, the research participants had two options to choose from “Yes” or “No”. Out of the 130 participants, 43 (33.1 percent) participants answered that they have worked from home before the pandemic, and the majority of the participants 87 (66.9 percent) answered “No” (Figure 4.2). As this question was solely to get better insight and understanding if the concept of telework is new in KSA or it has existed before the outbreak of COVID-19, no research participants were removed based on their answers to this question. Although 33.1 percent of the participants reported working from home before the pandemic, the question is not enough to accurately measure the phenomena. Different questions need to be asked to determine the frequency they telework from

home. Thus, the only insight from this question is that employees were given the chance to telework from home before and that it is not a new concept in Saudi Arabia.

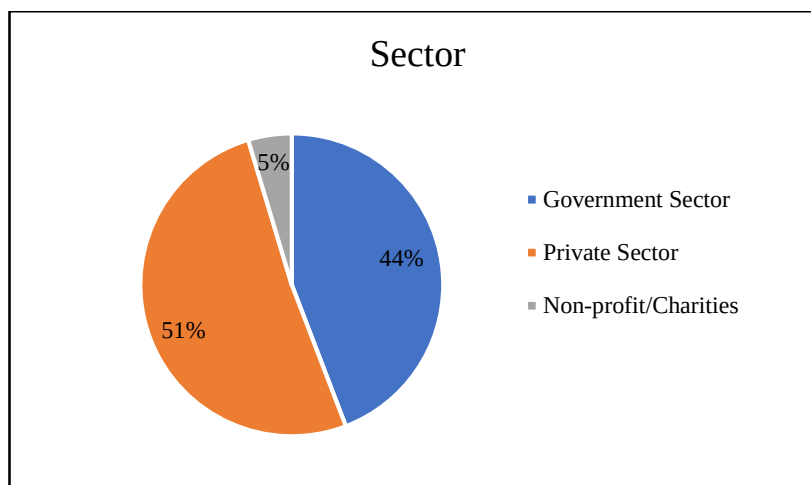
Q3. Did you use a computer, smartphone, tablet or any other electronic device to carry out your work at home during COVID-19?

This is a third question that had two answers only, “Yes” or “No”, that the research participants could choose from. Interestingly, out of the 130 participants, 129 (99.2 percent) answered “Yes” to this question, and only one participant (0.8 percent) said “No”. Therefore, the responses of this one research participant were removed from the rest of the data analysis, as this question is the second of two questions aimed at identifying teleworkers only. The analysis in the coming sections will be based on the responses of the 129 participants.

Q4. I work at the ...

When answering this question, the research participants had three answers to choose from: “government sector”, “private sector” and “non-profit/charities”. Figure 4.3 shows that more than half of the participants, 66 (51.61 percent), indicated that they work at the private sector. Out of the 129 participants, 57 (44.19 percent) said that they work for the government sector and 6 (4.65 percent) said that they work at non-profit/charities.

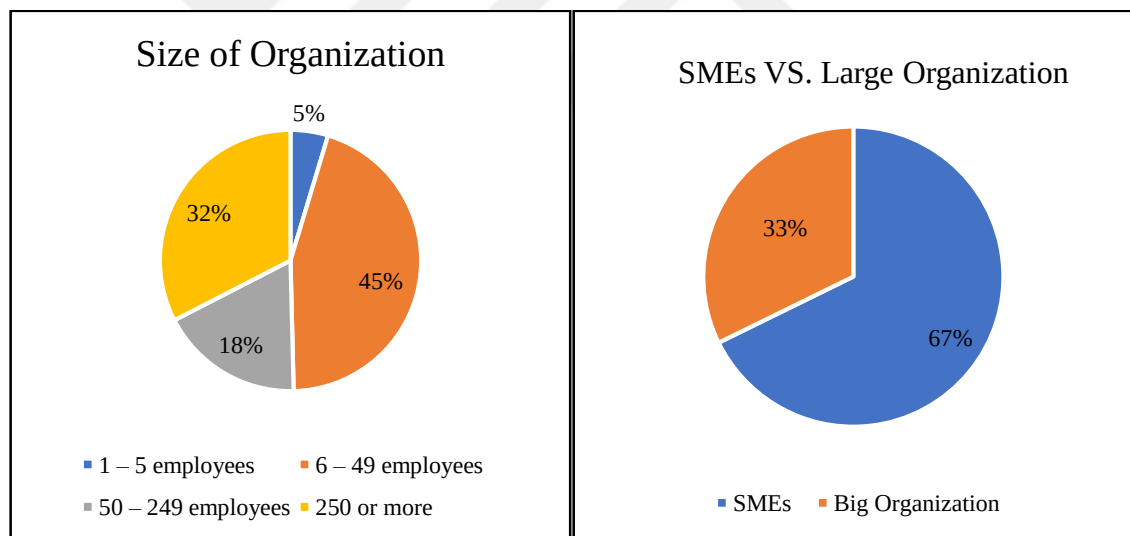
Figure 4.3: Responses to the Third Questionnaire Item



Q5. Including yourself, what is the approximate total number of employees at your organization?

This was the last question in the first section of the questionnaire. The participants had four options to choose from when answering this question: (a) “1 – 5 employees”, (b) “6 – 49 employees”, (c) “50 – 249 employees” and (d) “250 or more”. As can be seen in Figure 4.4, out of the 129 participants, 6 (4.7 percent) chose the first option, “1 – 5 employees”, 58 (45 percent) selected the second option, “6 – 49 employees”, and 23 (17.8 percent) chose the third option, “50 – 249 employees”. This means that 87 (67.4 percent) participants work for small and medium-sized enterprises (SMEs). Whereas, the number of research participants who work for large organizations is 42 (32.6 percent) (Figure 4.4). These results were anticipated given the fact that the majority of organizations in KSA are SMEs (Monsha’at 2017).

Figure 4.4: Responses to the Fifth Questionnaire Item



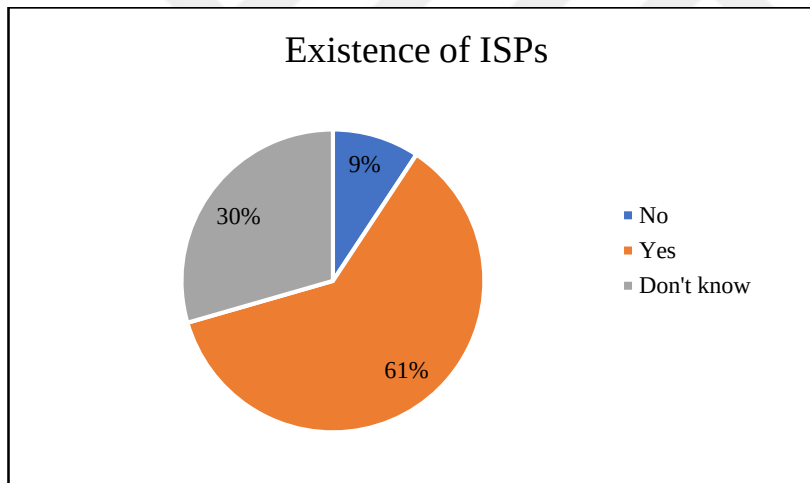
Q6. In light of the previous definition, does your organization have an information security policy?

Research participants had three options when answering this question: (a) “Yes”; (b) “No” and (d) don’t know. More than half of the respondents, 79 (61.2 percent), indicated that their organizations have information security policy, 12 (9.3 percent) said that their organization does not have a policy and 38 (29.5 percent) of the participants indicated that they do not know (Figure 4.5).

Table 4.2: Information about the Research Participants

Variables	Response Options	Responses %
Working from home during the pandemic	Yes	130 (83.87%)
	No	25 (16.13%)
Working from home before the pandemic	Yes	43 (33.1%)
	No	87 (66.9%)
Use of electronic devices	Yes	129 (99.2%)
	No	1 (0.8%)
Sector	government sector	57 (44.19%)
	private sector	66 (51.16%)
	non-profit/charities	6 (4.65%)
Size of the organization	1 – 5 employees	6 (4.7%)
	6 – 49 employees	58 (45%)
	50 – 249 employees	23 (17.8%)
	250 or more	42 (32.6%)

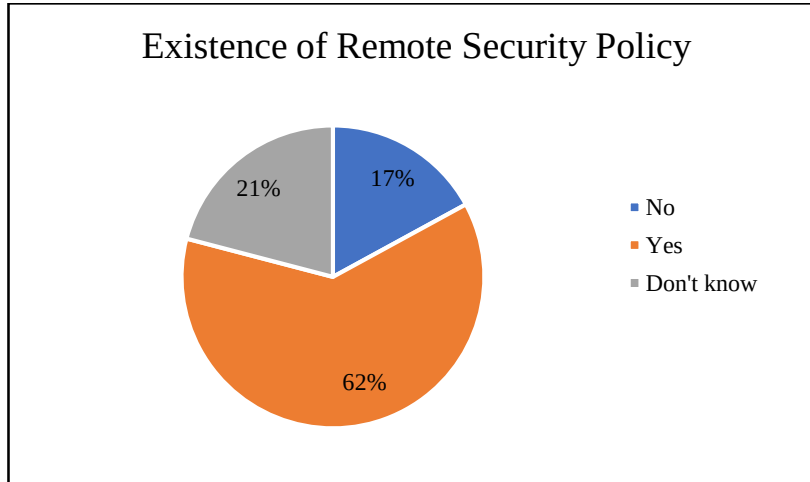
Figure 4.5: Responses to the Sixth Questionnaire Item



Q7. Does your organization have a remote working security policy? (a remote security policy ensures security of information while working from alternative worksite such as; your home, hotel etc.).

Similar to the previous question, research participants had three answers to choose from, “Yes”, “No” and “Don’t know”. Based on the responses of the 129 research participants, 80 (62 percent) indicated that their organizations have a remote security policy, 22 (17.1 percent) answered no, and 27 (20.9 percent) reported that they don’t know (Figure 4.6).

Figure 4.6: Responses to the Seventh Questionnaire Item



When comparing the responses for the above two questions (numbers 6 and 7), it was found that out of the 129 participants, 67 (51.9 percent) are aware that their organizations have an ISP and a remote security policy. On the other hand, 7 (5.4 percent) reported that their organizations have an ISP, but they do not know if their organizations have a remote security policy, 5 (3.9 percent) reported that their organizations have an ISP but not a remote security policy. Moreover, 2 (1.6 percent) reported that their organizations have a remote security policy but not an ISP and 10 (8 percent) participants said that their organizations have neither. In addition, 11(8.5 percent) participants reported that their organizations have a remote security policy but they don't know if their organizations have an ISP. Interestingly, 20 (15.5 percent) reported that they do not know if their organizations have either, and finally, 7 (5.4 percent) indicated that they don't know if their organizations have an ISP but they believe that their organizations do not have a remote security policy (Table 4.3).

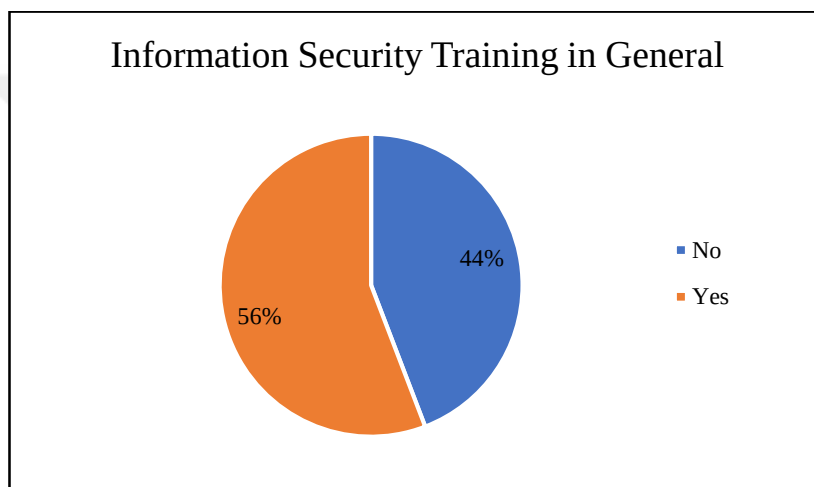
Table 4.3: Existence of ISP & Remote Security Policy

<i>Remote Security Policy?</i>	<i>ISPs?</i>				
		Yes	No	Don't know	Total
	Yes	51.9%	1.6%	8.5%	62.0%
	No	3.9%	7.8%	5.4%	17.1%
	Don't know	5.4%	0%	15.5%	20.9%
	Total	61.2%	9.3%	29.5%	100%

Q8. Does your organization provide any form of training or guidelines in regards to information security?

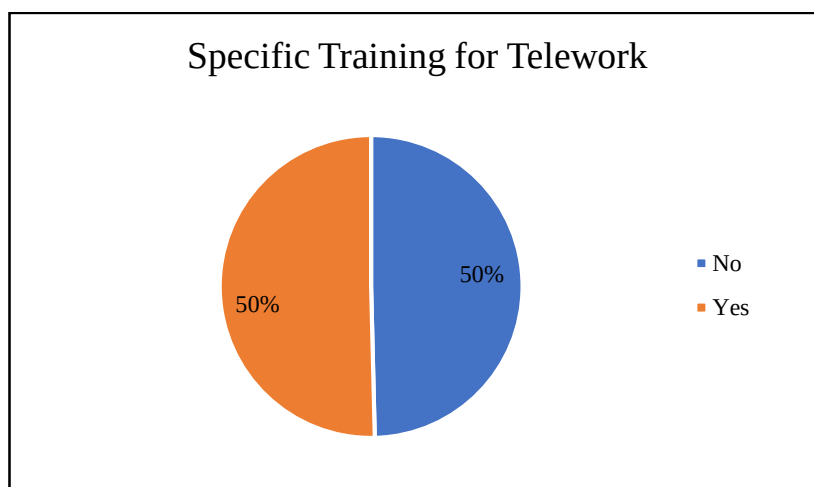
This question was designed to allow participants to choose from two answers only, “Yes” or “No”. The data collected is presented in Figure 4.7 show that more than half of research participants, 72 (55.8 percent), have received some form of training or guidelines about information security, and 57 (44.2 percent) participants reported that their organizations do not provide any type of training or guidelines about information security.

Figure 4.7: Responses to the Eighth Questionnaire Item



Q9. Did your organization provide any form of training or guidelines on how to maintain information security while working from home?

Figure 4.8: Responses to the Ninth Questionnaire Item



Answers to this question were also based on two options only “Yes” or “No”. Out of the 129 participants, 65 (50.4 percent) reported that they have received specific training or guidelines for working from home, and 64 (49.6 percent) answered no; this reveals that the rate of responses for both choices is almost equal (Figure 4.8).

When comparing the responses of the 129 research participants for questions 8 and 9, it was noticed that 59 (45.7 percent) participants received some form of training or guidelines in regards to information security in general and on how to maintain information security when working from home. In addition, 13 (10.1 percent) participants said that they have received training or guidelines in regards to information security in general, but did not receive any form of training or guidelines to maintain information security when working from home, and 6 (4.7 percent) participants said that their organizations did not provide any form of training or guidelines in general, but provided training in regards to maintaining information security when working from home. Nonetheless, 51(39.5 percent) participants did not receive any form of training or guidelines (Table 4.4).

Table 4.4: Information Security Training in General and for Remote Working

	IS training in general?			
		Yes	No	Total
	Yes	59 (45.7%)	6 (4.7%)	50.4%
	No	13 (10.1%)	51(39.5%)	49.6%
	Total	55.8%	44.2%	100%

Questions 10-30: Information security awareness (ISA)

Password Management focus area:

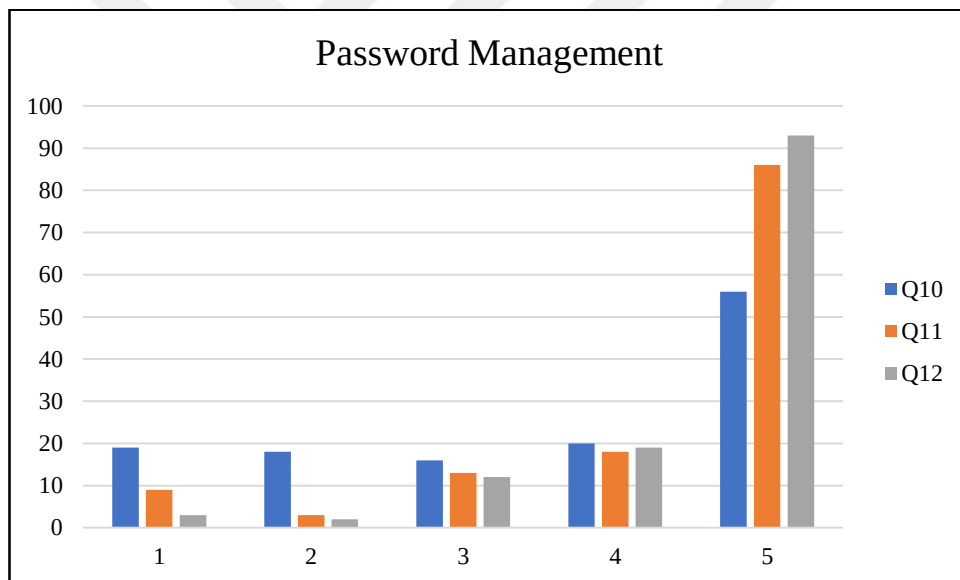
The first focus area is password management. The sub-areas measured are the usage of the same password, password sharing and the usage of strong password. Within these sub-areas, the participants scored the highest in “using a strong password” sub-area (M = 4.53, SD = 0.9). This behaviour indicates that the majority of respondents are highly aware of the importance of using letters, numbers and symbols in their work passwords. The second highest sub-area is password sharing (M = 4.31, SD = 1.2). Finally,

participants scored the lowest in using the same password for social media and work accounts ($M = 3.59$, $SD = 1.5$). Figure 4.9 demonstrates the range of answers each statement has received.

Table 4.5: Descriptive Statistics of Sub-Areas in Password Management

Sub-area	Statements	Min	Max	Mean	SD
Using the same password	10. I use a different password for my social media and work accounts.	1	5	3.59	1.51
Sharing passwords	11. I share my work passwords with colleagues.	1	5	4.31	1.18
Using a strong password	12. I use a combination of letters, numbers and symbols in my work passwords.	1	5	4.53	.9

Figure 4.9: Answers to Focus Area: Password Management



Email Use focus area:

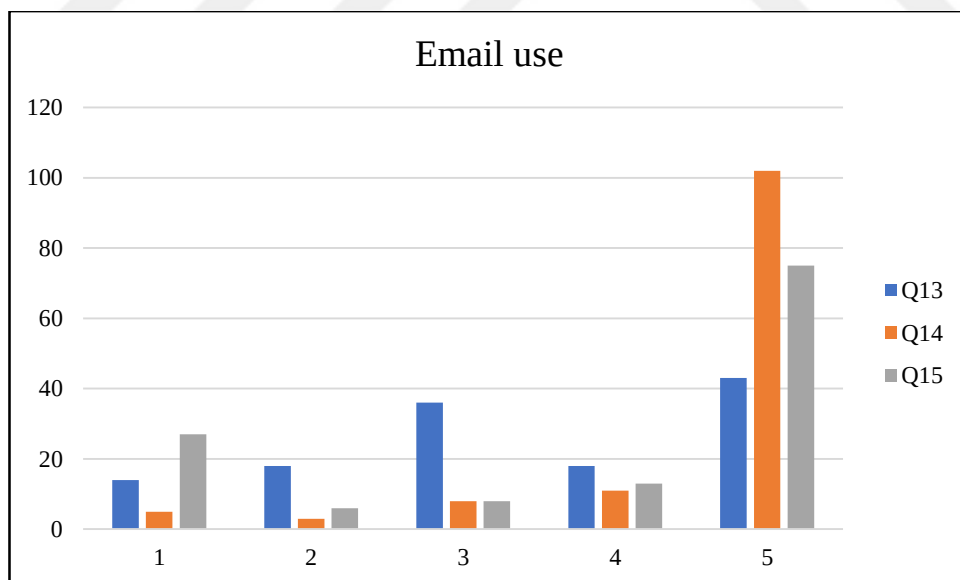
The second focus area is email use. The sub-areas measured are, clicking on links in emails from known senders, unknown senders and opening attachments in emails from unknown senders. Within these sub-areas, participants scored the highest in “clicking on links in emails from unknown senders” sub-area ($M = 4.57$, $SD = 0.99$), which shows that the majority of research participants are aware of the risk of clicking on links coming from unknown senders. The second highest sub-area is “opening attachments in emails from unknown senders” ($M = 3.8$, $SD = 1.64$). Finally, participants scored the lowest in

“clicking on links in emails from known senders” sub-area ($M = 3.45$, $SD = 1.36$), which means that participants are most likely to click on links in emails if they are coming from someone they know. However, emails coming from known senders could also be phishing emails (Parsons et al. 2017). Figure 4.10 demonstrates the range of answers each statement has received.

Table 4.6: Descriptive Statistics of Sub-Areas in Email Use

Sub-area	Statements	Min	Max	Mean	SD
Clicking on links in emails from known senders	13. I don't always click on links in emails just because they come from someone I know.	1	5	3.45	1.36
Clicking on links in emails from unknown senders	14. If an email from an unknown sender looks interesting, I click on a link within it.	1	5	4.57	.99
Opening attachments in emails from unknown senders	15. I don't open email attachments if the sender is unknown to me.	1	5	3.8	1.64

Figure 4.10: Answers to Focus Area: Email Use



Internet Use focus area:

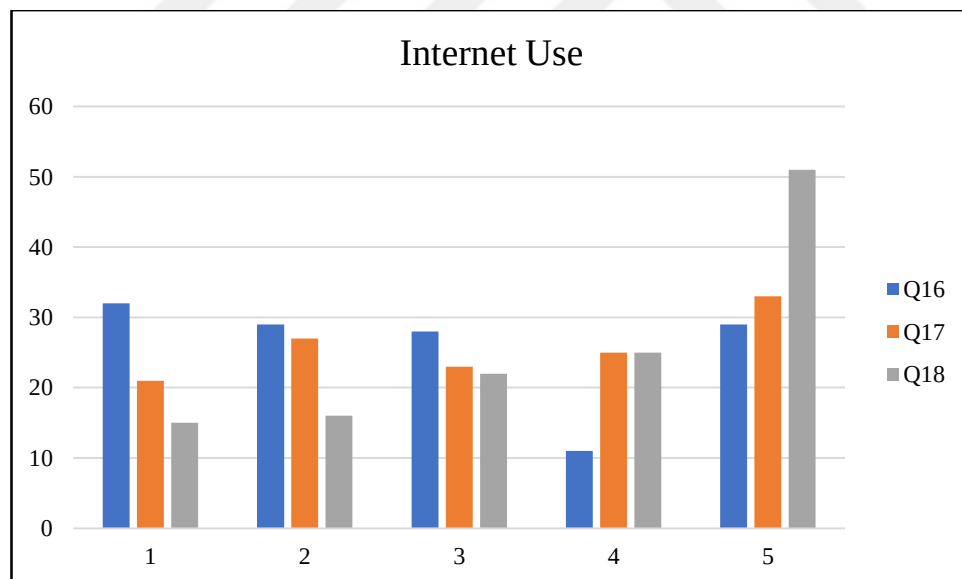
The third focus area is internet use. The sub-areas measured are, files downloading, accessing dubious websites and entering information online. Within these sub-areas, participants scored the highest in “entering information online” sub-area ($M = 3.63$, SD

= 1.41). Participants' scores for the other two sub-areas are ($M = 3.17$, $SD = 1.44$ and $M = 2.81$, $SD = 1.48$) which indicate that participants do not fully recognize the danger associated with accessing dubious websites or the risk of downloading any file onto their work computers. Figure 4.11 demonstrates the range of answers each statement has received.

Table 4.7: Descriptive Statistics of Sub-Areas in Internet Use

Sub-area	Statements	Min	Max	Mean	SD
Downloading files	16. I download any files onto my work computer that will help me get the job done.	1	5	2.81	1.48
Accessing dubious websites	17. When accessing the internet at work, I visit any website that I want to.	1	5	3.17	1.44
Entering information online	18. I assess the safety of websites before entering information.	1	5	3.63	1.41

Figure 4.11: Answers to Focus Area: Internet Use



Social Media Use focus area:

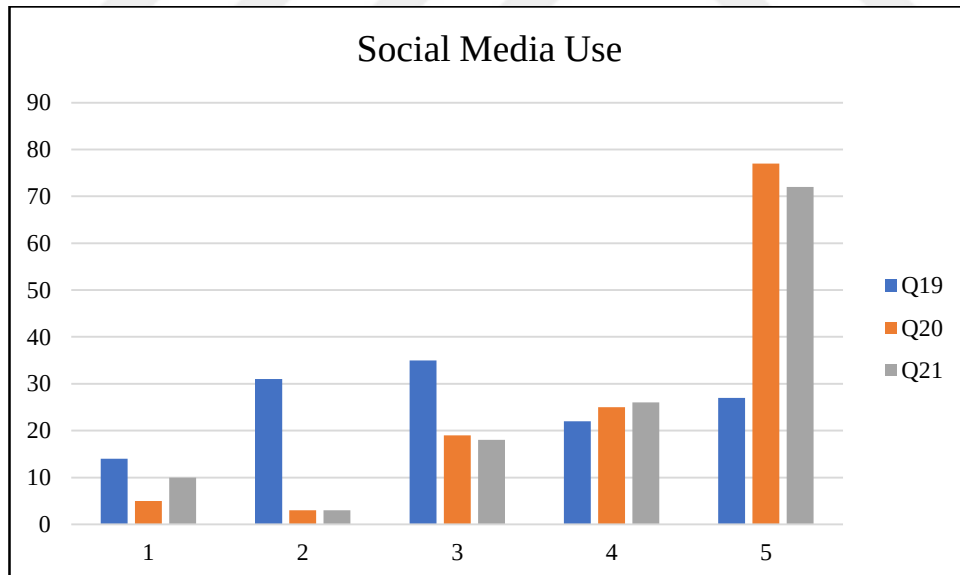
The fourth focus area is social media use. The sub-areas measured are, SM privacy settings, considering consequences and posting about work. Within these sub-areas, the statement that received the most positive responses is the statement regarding if participants post anything on social media before considering any negative consequences.

($M = 4.29$, $SD = 1.05$). The second highest sub-area is “posting about work” ($M = 4.14$, $SD = 1.22$), which indicates that the majority of respondents are aware that they should not post about their work on social media and that they consider the negative impact before posting. Finally, participants scored the lowest in how often they review SM privacy settings” ($M = 3.13$, $SD = 1.3$). Figure 4.12 demonstrates the range of answers each statement has received.

Table 4.8: Descriptive Statistics of Sub-Areas in Social Media Use

Sub-area	Statements	Min	Max	Mean	SD
SM privacy settings	19. I don't regularly review my social media privacy settings.	1	5	3.13	1.3
Considering consequences	20. I don't post anything on social media before considering any negative consequences.	1	5	4.29	1.05
Posting about work	21. I post whatever I want about my work on social media.	1	5	4.14	1.22

Figure 4.12: Answers to Focus Area: Social Media Use



Mobile Devices focus area:

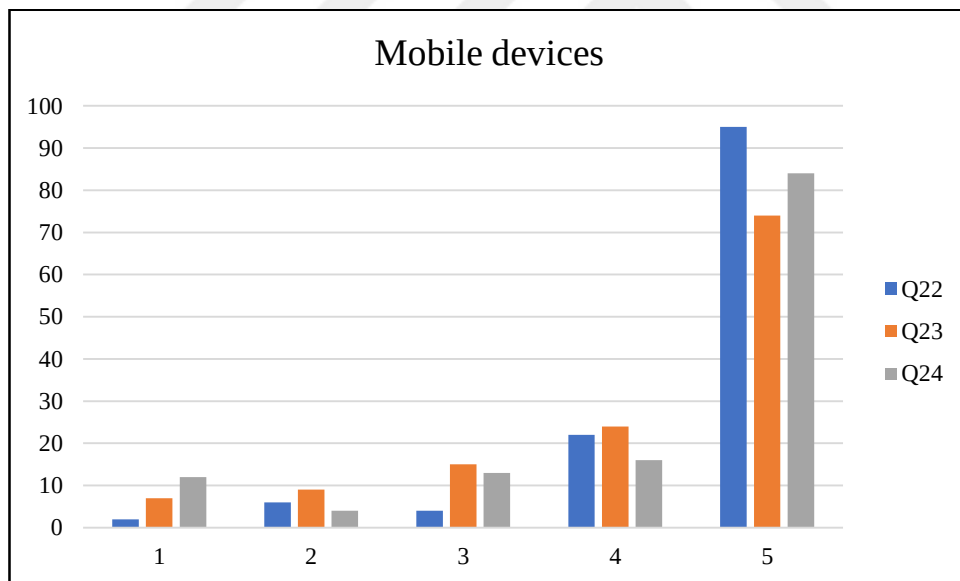
The fifth focus area is mobile devices. The sub-areas measured are, physically securing mobile devices, sending sensitive information via Wi-Fi and shoulder surfing. The statement that received the most positive answers was about securing mobile devices when working in a public place ($M = 4.57$, $SD = .88$). Participants also reported high

scores in statement number 24, which means they are aware of the risk of shoulder surfing ($M = 4.21$, $SD = 1.3$). Lastly, participants scored the lowest in “sending sensitive information via Wi-Fi” sub-area ($M = 4.16$, $SD = 1.2$). Figure 4.13 demonstrates the range of answers each statement has received.

Table 4.9: Descriptive Statistics of Sub-Areas in Mobile Devices

Sub-area	Statements	Min	Max	Mean	SD
Physically securing mobile devices	22. When working in a public place, I leave my laptop unattended.	1	5	4.57	.88
Sending sensitive information via Wi-Fi	23. I send sensitive work files using a public Wi-Fi network.	1	5	4.16	1.2
Shoulder surfing	24. I check that strangers can't see my laptop screen if I'm working on a sensitive document.	1	5	4.21	1.3

Figure 4.13: Answers to Focus Area: Mobile Devices

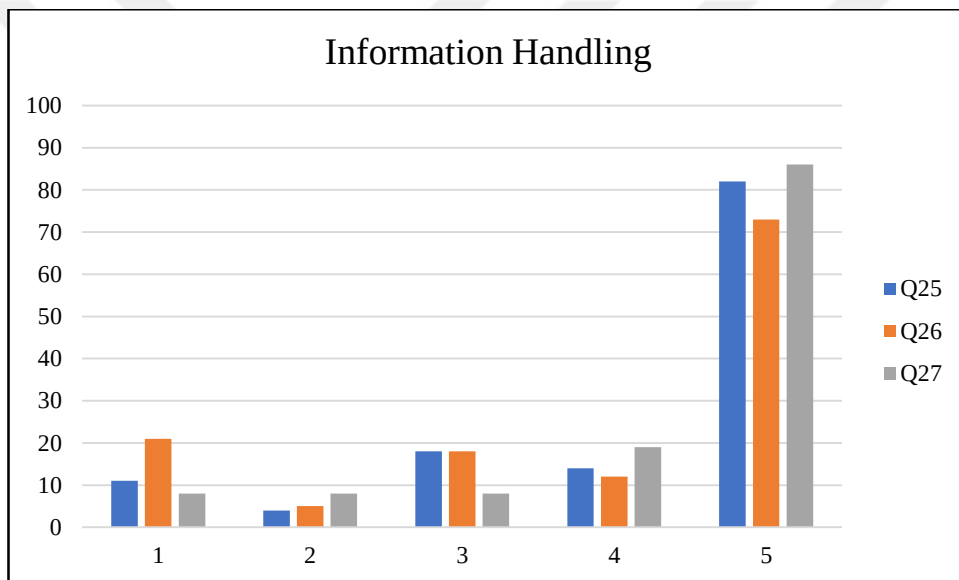


Information Handling focus area:

Another focus area is information handling. The sub-areas measured are, disposing of sensitive print-outs, inserting removable media and leaving sensitive material. Overall, participants reported positive behaviour regarding these sub-areas as they respectively scored ($M = 4.18$, $SD = 1.28$, $M = 3.86$, $SD = 1.52$ and $M = 4.29$, $SD = 1.21$). Figure 4.14 demonstrates the range of answers each statement has received.

Table 4.10: Descriptive Statistics of Sub-Areas in Information Handling

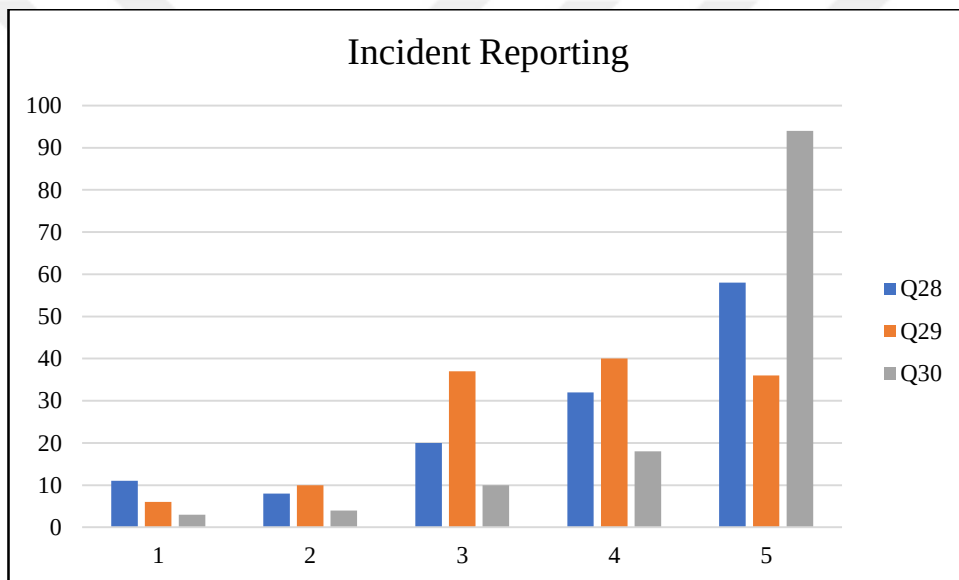
Sub-area	Statements	Min	Max	Mean	SD
Disposing of sensitive print-outs	25. When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.	1	5	4.18	1.28
Inserting removable media	26. I wouldn't plug a USB stick found in a public place into my work computer.	1	5	3.86	1.52
Leaving sensitive material	27. I leave print-outs that contain sensitive information on my desk when I'm not there.	1	5	4.29	1.21

Figure 4.14: Answers to Focus Area: Information Handling**Incident Reporting focus area:**

The last area under investigation is related to incident reporting. The sub-areas measured are, ignoring poor security behaviour by colleagues, reporting suspicious behaviour and reporting all incidents. Participants indicated that they are most likely to report incidents ($M = 4.52$, $SD = 0.94$) than to report a suspicious behaviour ($M = 3.91$, $SD = 1.27$). In addition, apparently some participants do not find themselves obliged to report poor security behaviour of other colleagues ($M = 3.7$, $SD = 1.1$). Figure 4.15 demonstrates the range of answers each statement has received. Table 4.12 is a summary of the descriptive statistics for all sub-areas.

Table 4.11: Descriptive Statistics of Sub-Areas in Incident Reporting

Sub-area	Statements	Min	Max	Mean	SD
Reporting suspicious behaviour	28. If I saw someone acting suspiciously in my workplace, I would do something about it.	1	5	3.91	1.27
Ignoring poor security behaviour by colleagues	29. If I noticed my colleague ignoring security rules, I wouldn't take any action.	1	5	3.7	1.1
Reporting all incidents	30. If I noticed a security incident, I would report it.	1	5	4.52	0.94

Figure 4.15: Answers to Focus Area: Incident Reporting

Overall, the participants demonstrated a good level of ISA on all focus areas. Table 4.13 shows that participants' scores were highest for the focus area "Mobile devices" ($M=12.93$, $SD=2.14$) which indicates a high level of awareness regarding mobile devices. Similarly, participants' scores for the "Password management" focus area were high ($M = 12.43$, $SD = 2.47$). "Information handling" focus area scores were the third highest ($M = 12.33$, $SD = 2.74$). The answers for the sub-areas "Clicking on links in emails from unknown senders" and "Physically securing mobile devices" were the highest ($M= 4.57$) among all other sub-areas across the different focus areas (Table 4.12); where the majority of participants selected 4 "Disagree" or 5 "Strongly disagree" (Figure 4.10 and 4.13).

Table 4.12: Summary of Descriptive Statistics for All Sub-Areas

Statements	Min	Max	Mean	SD
10. I use a different password for my social media and work accounts.	1	5	3.59	1.51
11. I share my work passwords with colleagues.	1	5	4.31	1.18
12. I use a combination of letters, numbers and symbols in my work passwords.	1	5	4.53	0.9
13. I don't always click on links in emails just because they come from someone I know.	1	5	3.45	1.36
14. If an email from an unknown sender looks interesting, I click on a link within it.	1	5	4.57	0.99
15. I don't open email attachments if the sender is unknown to me.	1	5	3.8	1.64
16. I download any files onto my work computer that will help me get the job done.	1	5	2.81	1.48
17. When accessing the internet at work, I visit any website that I want to.	1	5	3.17	1.44
18. I assess the safety of websites before entering information.	1	5	3.63	1.41
19. I don't regularly review my social media privacy settings.	1	5	3.13	1.3
20. I don't post anything on social media before considering any negative consequences.	1	5	4.29	1.05
21. I post whatever I want about my work on social media.	1	5	4.14	1.22
22. When working in a public place, I leave my laptop unattended.	1	5	4.57	0.88
23. I send sensitive work files using a public Wi-Fi network.	1	5	4.16	1.2
24. I check that strangers can't see my laptop screen if I'm working on a sensitive document.	1	5	4.21	1.3
25. When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.	1	5	4.18	1.28
26. I wouldn't plug a USB stick found in a public place into my work computer.	1	5	3.86	1.52
27. I leave print-outs that contain sensitive information on my desk when I'm not there.	1	5	4.29	1.21
28. If I saw someone acting suspiciously in my workplace, I would do something about it.	1	5	3.91	1.27
29. If I noticed my colleague ignoring security rules, I wouldn't take any action.	1	5	3.7	1.1
30. If I noticed a security incident, I would report it.	1	5	4.52	0.94

On the other hand, participants' scores were the lowest for the "internet use" focus area (M = 9.61, SD = 2.97). In addition, the sub-area "Downloading files" scored the lowest among all other sub-areas across the different focus areas (Table 4.12). This is also the only sub-area where the mean of the participants' scores is below the average (with the average being 3); which shows that respondents have low awareness of this sub-area and are less likely to pay attention to type of files they are downloading to their work computer.

Table 4.13: Descriptive Statistics for All Focus-Areas

Focus area	Min	Max	Mean	SD
Password management	3	15	12.43	2.47
Email use	7	15	11.81	2.55
Internet use	3	15	9.61	2.97
Social media use	5	15	11.56	2.23
Mobile devices	7	15	12.93	2.14
Information handling	4	15	12.33	2.74
Incident reporting	4	15	12.13	2.46

After completing the descriptive statistics, a further step was calculating the ISA score. Pattinson et al. (2016 cited in Takens 2020, p. 21) suggest formula 4.1 which calculates the percentage of "favourable responses" of each focus domain. The formula is based on the concept of measuring the favourable responses only, by accumulating the responses marked as 'Strongly agree' and 'Agree'; then, expressing the result as a percentage of the sum of responses for each focus area (Table 4.14).

$$ISA \% = \frac{\text{Strongly agree answers} + \text{Agree answers}}{\text{Number of responses} - \text{Not applicable answers}}$$

The percentage of "favourable responses" reported in Table 4.14 indicates that "Mobile devices" focus area received the highest percentage compared to other focus-areas (81 percentage). On the other hand, the lowest percentage was recorded in "Internet use" focus-area (45 percentage). This focus area scored almost 20 percent less than all other focus areas which demonstrates a gap between it and all other domains (see Annex 8 for

the detailed calculations). To further interpret the implication of the calculated percentage, the percentage in Table 4.14 were compared with the range suggested by Kruger and Kearney (2006, cited in Ikhsan & Ramli 2019) in Table 4.15.

Table 4.14: Percentage of Favourable Responses

Statement	Sub-area	% per sub-area	% per focus-area
Q.10	Using the same password	59%	75%
Q.11	Sharing passwords	81%	
Q.12	Using a strong password	87%	
Q.13	Clicking on links in emails from known senders	47%	68%
Q.14	Clicking on links in emails from unknown senders	88%	
Q.15	Opening attachments in emails from unknown senders	68%	
Q.16	Downloading files	31%	45%
Q.17	Accessing dubious websites	45%	
Q.18	Entering information online	59%	
Q.19	SM privacy settings	38%	64%
Q.20	Considering consequences	79%	
Q.21	Posting about work	76%	
Q.22	Physically securing mobile devices	91%	81%
Q.23	Sending sensitive information via Wi-Fi	76%	
Q.24	Shoulder surfing	78%	
Q.25	Disposing of sensitive print-outs	74%	74%
Q.26	Inserting removable media	66%	
Q.27	Leaving sensitive material	81%	
Q.28	Reporting suspicious behaviour	70%	72%
Q.29	Ignoring poor security behaviour by colleagues	59%	
Q.30	Reporting all incidents	87%	
Overall			69%

Although Kruger and Kearney (2006) examined ISA using different focus areas than the ones used in Parsons et al (2017, 2014), many studies have used the scale (Table 4.15) developed by Kruger and Kearney (2006) as a way to interpret results obtained using Parsons et al (2017, 2014) tool. For example, Ikhsan and Ramli (2019) measured ISA of government employees using the knowledge approach from Parsons et al (2017, 2014) and then calculated the level of ISA using Kruger and Kearney's (2006) scale. Mahardika

et.al (2020) and Wahyudiwan et al. (2017) as well used the three variables of the KAB model and matched it with Kruger and Kearney's (2006) criteria to calculate the level of ISA. Therefore, this approach has been used as an additional method to further interpret the findings and to better recognize the focus area that need improvements. Table 4.16 demonstrates ISA level based on matching the percentage of favourable responses Table 4.14 with the criteria in Table 4.15.

Table 4.15: Information Security Awareness Level

Category	Percentage (%)	Action Plan
Good	80 – 100	No need for action
Average	60 – 79	Action potentially required
Poor	≤ 59	Action required

Source: Kruger and Kearney 2006 cited in Ikhsan & Ramli 2019, p. 3

Table 4.16: Information Security Awareness Level

Focus area	Awareness level per focus-area	Overall Awareness level
Password management	75%	69%
Email use	68%	
Internet use	45%	
Social media use	64%	
Mobile devices	81%	
Information handling	74%	
Incident reporting	72%	

The findings reported in Table 4.16 indicate that only the “Mobile devices” focus area is classified as “good” which means that *no need for action*. On the other hand, the majority of the focus areas (“password management”, “Email use”, “Social media use”, “Information handling”, and “Incident reporting”) are classified as “average” which indicates that *action potentially required* to enhance these areas. Moreover, the worst score was recorded in the “Internet use” focus-area (45 percentage). In addition, ISA level for the internet use focus-area is classified as “poor” and *action required* to increase the level of ISA. Finally, it was found that the overall awareness level of teleworkers in all focus areas is within the “average” range (69 percentage).

4.2.1 Teleworkers Group Differences

Table 4.17 demonstrates the breakdown of the survey sample by sector and size. The sample is composed of 66 (51.16 percent) teleworkers from the private sector, 57 (44.19 percent) teleworkers from the government sector, and only 6 (4.65 percent) teleworkers from non-profit/charities. By size the collected data shows that 42 (32.56 percent) of teleworkers work for large organizations (250 or more employees), 23 (17.83 percent) work for medium organizations (50-249 employees), 58 (44.96 percent) work for small organizations (6-49 employees), and 6 (4.65 percent) of respondents work for micro-organizations (1-5 employees). The data examined in the previous part shows findings on the basis of the whole sample. The coming section, however, assess the data by breaking down the sample into subcategories by the size of the organization (large/SMEs) and then followed by the sector (private/government). The analysis by sector is limited to private and government sectors because the sample size of non-profit/charities is comparatively too small to be included.

Table 4.17: Cross-tabulation of Survey Sample by Sector and Size.

		Organization Size				
		SMEs			Large (250 or more)	Total
		Micro (1 – 5 employees)	Small (6 – 49 employees)	Medium (50 – 249 employees)		
Sector	Private Sector	5	19	11	31	66
	Government Sector	0	37	9	11	57
	Non-profit/charities	1	2	3	0	6
	Total	6	58	23	42	129

4.2.1.1 Teleworkers group differences (by size)

4.2.1.1.1 Security policies and training

The sample was first examined by the size of the organization, dividing the whole sample into two subgroups, large organizations and SMEs. Table 4.18 shows frequency of response to questions 6, 7, 8 and 9 for teleworkers who work for large organizations as

well as teleworkers who work for SMEs. To determine whether there are significant differences between the two groups in regards to questions 6, 7, 8 and 9, a series of Chi-square tests were conducted. The results of the Chi-square test show significant differences among the two groups regarding ISPs ($\chi^2 = 26.27$; $df = 2$; $p < .001$), remote security policy ($\chi^2 = 9.54$; $df = 2$; $p = .008$), training in general ($\chi^2 = 15.96$; $df = 1$; $p = < .001$), and training for remote work ($\chi^2 = 8.67$; $df = 1$; $p = .003$).

Table 4.18: Questions 6, 7, 8 and 9 by Organization Size

		Large Organizations	SMEs
Q6. Information security policies?	Yes	39 (93%)	40 (46%)
	No	1 (2%)	11 (13%)
	Don't know	2 (5%)	36 (41%)
Q7. Remote Security Policy?	Yes	34 (81%)	46 (53%)
	No	4 (10%)	18 (21%)
	Don't know	4 (10%)	23 (26%)
Q8. IS training in general?	Yes	34 (81%)	38 (44%)
	No	8 (19%)	49 (56%)
Q9. IS training for remote work?	Yes	29 (69%)	36 (41%)
	No	13 (31%)	51 (59%)

4.2.1.1.2 Information security awareness

At this point, consideration is turned into ISA. As can be seen in Table 4.19, across all focus areas, the average scores of teleworkers at large size organizations are higher than the average scores of teleworkers at SMEs.

Table 4.19: Average Scores for All Focus Areas

Focus area	Teleworkers at Large Organizations	Teleworkers at SMEs
Password management	12.86	12.22
Email use	12.62	11.43
Internet use	10.21	9.32
Social media use	12.19	11.25
Mobile devices	13.14	12.83
Information handling	13.36	11.84
Incident reporting	12.24	12.08

4.2.1.1.2.1 Teleworkers group differences on sub-area level

Table 4.20: Average Scores for All Sub-Areas

Sub-areas	Teleworkers at Large Organizations	Teleworkers at SMEs
Using the same password	3.67	3.55
Sharing passwords	4.36	4.29
Using a strong password	4.83	4.38
Clicking on links in emails from known senders	3.79	3.29
Clicking on links in emails from unknown senders	4.76	4.47
Opening attachments in emails from unknown senders	4.07	3.67
Downloading files	3.21	2.62
Accessing dubious websites	3.33	3.09
Entering information online	3.67	3.61
SM privacy settings	3.21	3.09
Considering consequences	4.33	4.26
Posting about work	4.64	3.9
Physically securing mobile devices	4.57	4.56
Sending sensitive information via Wi-Fi	4.31	4.08
Shoulder surfing	4.26	4.18
Disposing of sensitive print-outs	4.29	4.13
Inserting removable media	4.4	3.6
Leaving sensitive material	4.67	4.11
Reporting suspicious behaviour	3.98	3.89
Ignoring poor security behaviour by colleagues	3.69	3.7
Reporting all incidents	4.57	4.49

This part of the findings focuses on the individual statements (sub-areas) under study. As shown in Table 4.20, the average scores of teleworkers at large organizations for all sub-areas are higher than the average scores of teleworkers at SMEs. The Mann Whitney U test was performed on each statement of every focus area. Out of the 21 statements, a significant difference was found between the two groups in regards to five statements. These five statements relate to password management, internet use, social media use and information handling focus areas. On the other hand, there is no significant difference between the two groups within the three focus areas: email use, mobile devices and

incident reporting. Annex 9 demonstrates the full results obtained from the Mann Whitney U test where the statements with a significant difference have been highlighted.

Password Management:

Within the password management focus area, a significant difference was found in “Using a strong password” sub-area presented with the following statement:

Q12. I use a combination of letters, numbers and symbols in my work passwords.

The results of Mann Whitney U test indicate that the information security awareness levels of teleworkers that work for large organizations (N = 42; Mean Rank =75.6) are considerably higher than the awareness levels of teleworkers that work for SMEs (N = 87; Mean Rank =59.89), (U = 1382; Z = -2.837; p = 0.005).

Internet Use:

In this focus area, a significant difference was detected in the following statement which is part of the “Downloading files” sub-area.

Q16. I download any files onto my work computer that will help me get the job done.

Based on the results obtained from Mann Whitney U test, the awareness levels of teleworkers at large organization (N = 42; Mean Rank = 74.64) are higher than those of teleworkers at SMEs (N = 87; Mean Rank = 60.34), (U = 1422; Z = -2.087; p = 0.037).

Social Media Use:

There is also a significant difference in the statement belonging to “Posting about work” sub-area:

Q21. I post whatever I want about my work on social media.

The finding of the test indicates that the awareness levels of teleworkers at SMEs (N = 87; Mean Rank = 58.32) are significantly lower than the awareness levels of teleworkers at large organizations (N = 42; Mean Rank = 78.85). As can be seen in Annex 9, the p-value reported here is the lowest among all other values (U = 1245.5; Z = -3.238; p = 0.001).

Information Handling:

Within this focus area, two sub-areas are showing significant differences “Inserting removable media” and “Leaving sensitive material”.

Q26. I wouldn't plug a USB stick found in a public place into my work computer.

Teleworkers working for large organizations reported a higher level of information security awareness (N = 42; Mean Rank = 78.05) than teleworkers working for SMEs (N = 87; Mean Rank = 58.7), (U = 1279; Z = -3.059; p = 0.002).

Q27. I leave print-outs that contain sensitive information on my desk when I'm not there.

The results of this statement as well indicate a significant difference in the awareness levels between the two groups with the teleworkers at large organizations having higher awareness levels (N = 42; Mean Rank = 73.9) than teleworkers at SMEs (N = 87; Mean Rank = 60.7), (U = 1453; Z = -2.247; p = 0.025).

4.2.1.2 Teleworkers group differences (by sector)

4.2.1.2.1 Security policies and training

After examining the sample by size, attention was shifted to the sector. The sample was classified into teleworkers who work for private or government organizations. As mentioned earlier, the sample of teleworkers who work for non-profit/charities was not included in the analysis due to the small sample size (6 respondents). Table 4.21 shows frequency of responses to questions 6, 7,8 and 9 for both groups.

Table 4.21: Questions 6, 7,8 and 9 by Organization Sector

		Private Organizations	Government Organizations
Q6. Information security policies?	Yes	44 (67%)	33 (58%)
	No	8 (12%)	3 (5%)
	Don't know	14 (21%)	21 (37%)
Q7. Remote Security Policy?	Yes	43(65%)	34 (60%)
	No	15(23%)	6 (11%)
	Don't know	8(12%)	17 (30%)
Q8. IS training in general?	Yes	38 (58%)	34 (60%)
	No	28 (42%)	23 (40%)
Q9. IS training for remote work?	Yes	29 (44%)	35 (61%)
	No	37 (56%)	22 (39%)

In this part as well, to determine whether there are significant differences between the two groups in regards to questions 6, 7, 8 and 9, a series of chi-square tests were conducted. The results of chi-square test indicates that there are no significant differences among the two groups regarding ISPs ($\chi^2 = 4.610$; $df = 2$; $p = .100$), training in general ($\chi^2 = 0.054$; $df = 1$; $p = 0.816$), and training for remote work ($\chi^2 = 3.738$; $df = 1$; $p = .053$). However, there is a significant difference among the two groups in regards to remote security policy ($\chi^2 = 7.531$; $df = 2$; $p = .023$).

4.2.1.2.2 Information security awareness

As demonstrated in Table 4.22, the average scores vary between the two groups. Teleworkers at private sector have higher levels of awareness than teleworkers at government sector in password management, email use, social media use and information handling focus areas. On the other hand, teleworkers at government organizations reported higher levels of information security awareness in internet use, mobile devices and incident reporting focus areas.

Table 4.22: Average scores for all focus area

Focus area	Teleworkers at Private Sector	Teleworkers at Government Sector
Password management	12.67	12.12
Email use	12.92	10.42
Internet use	9.52	9.61
Social media use	11.3	9.61
Mobile devices	12.67	13.21
Information handling	12.67	11.89
Incident reporting	12.06	12.16

4.2.1.2.2.1 Teleworkers group differences on sub-area level

This part focuses on the individual statements (sub-areas). Table 4.23 shows the average scores for both groups across all sub-areas. As indicated earlier, the level of information security awareness varies between the two sub groups which is also reflected on the individual statements. The Mann Whitney U test was conducted on each statement of

every focus area. Out of the 21 statements, a significant difference was found between the two groups in seven statements. The statements with a significant difference are part of email use, social media use, mobile devices, information handling and incident reporting focus areas. Nevertheless, no significant differences were found between the two groups in password management and internet use focus areas. Annex 10 shows the complete test results obtained from the Mann Whitney U test where the statements with a significant difference have been highlighted.

Table 4.23: Average Scores for All sub-areas

Sub-areas	Teleworkers at Private Sector	Teleworkers at Government Sector
Using the same password	3.71	3.53
Sharing passwords	4.35	4.21
Using a strong password	4.61	4.39
Clicking on links in emails from known senders	3.86	2.96
Clicking on links in emails from unknown senders	4.76	4.3
Opening attachments in emails from unknown senders	4.3	3.16
Downloading files	2.85	2.77
Accessing dubious websites	3.15	3.14
Entering information online	3.52	3.7
SM privacy settings	3.12	3.16
Considering consequences	4.08	4.47
Posting about work	4.11	4.23
Physically securing mobile devices	4.47	4.67
Sending sensitive information via Wi-Fi	3.92	4.42
Shoulder surfing	4.27	4.12
Disposing of sensitive print-outs	4.18	4.23
Inserting removable media	4.11	3.49
Leaving sensitive material	4.38	4.18
Reporting suspicious behaviour	3.83	3.93
Ignoring poor security behaviour by colleagues	3.52	3.95
Reporting all incidents	4.71	4.28

Email Use:

In this focus area, significant differences were observed in all three statements.

Q13. I don't always click on links in emails just because they come from someone I know.

Q14. If an email from an unknown sender looks interesting, I click on a link within it.

Q15. I don't open email attachments if the sender is unknown to me.

The three statements belong to the sub-areas “Clicking on links in emails from known senders”, “Clicking on links in emails from unknown senders” and “Opening attachments in emails from unknown senders”. Overall, the test results indicate that teleworkers working for private sector have significantly higher awareness levels than teleworkers working for the government sector. in all three statements. Table 4.24 shows the test results of the three statements respectively for both groups.

Table 4.24: Test Results for Email Use Focus Area

Statement	Private Sector		Government Sector		Test Results		
	N	Mean Rank	N	Mean Rank	U	Z	P (2-tailed)
13	66	72.74	57	49.56	1172	-3.716	<.001
14	66	67.48	57	55.65	1519	-2.538	0.011
15	66	72.64	57	49.68	1179	-3.991	<.001

Social Media Use:

Within the social media use focus area, a significant difference was found in the following statement:

Q20. I don't post anything on social media before considering any negative consequences.

The finding of the test indicates that teleworkers at government sector have significantly higher awareness levels (N = 57; Mean Rank = 71.33) regarding “Considering consequences” than teleworkers at private sector (N = 66; Mean Rank = 53.94), (U = 1349; Z = -3.039; p = 0.002).

Mobile Devices:

In this focus area, a significant difference was observed in the following statement which is part of the “Sending sensitive information via Wi-Fi” sub-area.

Q23. I send sensitive work files using a public Wi-Fi network.

According to the test results, the awareness levels of teleworkers at government sector (N = 57; Mean Rank = 68.88) differ significantly from the awareness levels of teleworkers at private sector (N = 66; Mean Rank = 56.06), (U = 1489; Z = -2.224; p = 0.026).

Information Handling:

There is also a significant difference in the statement belonging to “Inserting removable media” sub-area:

Q26. I wouldn't plug a USB stick found in a public place into my work computer.

Teleworkers working at private organizations reported a higher level of information security awareness (N = 66; Mean Rank = 67.66) than those working at government organizations (N = 57; Mean Rank = 55.45), (U = 3160.5; Z = -2.099; p = 0.036).

Incident Reporting:

The last focus area with a significant difference between the two groups is incident reporting. Similar to social media use and mobile devices focus areas, teleworkers working at government organizations demonstrated higher ISA levels (N = 57; Mean Rank = 69.4) than teleworkers working at private organization (N = 66; Mean Rank = 55.61), (U = 1459; Z = -2.225; p = 0.026) in “Ignoring poor security behaviour by colleagues” sub-area measured using the following statement:

Q29. If I noticed my colleague ignoring security rules, I wouldn't take any action.

5. DISCUSSION AND CONCLUSION

The chapter begins with a discussion of the findings reported in this research in the context of the literature review presenting the meaning, relevance and importance of the findings regarding the research questions. The comparison in the discussion is between the results of this research and the results of other studies in the context of KSA and other countries. Section two of the chapter focuses on the limitations of this study and recommendations for further researches. The last section is a conclusion.

5.1 DISCUSSION

The section is divided into three sections based on the research questions. The first section discusses the first research question, the second one addresses questions two and three, while the findings of research question number four are discussed in the final section.

5.1.2 Policies

As mentioned in Chapter 2, in order to harness the benefits of security policies, employees first need to be aware of these policies and have an understanding of how to follow them (Da Veiga 2016). The second section of the questionnaire aimed at collecting data to answer research question number one; to what extent are teleworkers in KSA aware of the existence of information security policies in the organizations they work for? And to what extent are these teleworkers aware of the existence of remote work policies in the organizations they work for?

More than half of the respondents (61.2 percent) in this study were aware of the existence of ISP in their organizations, and about 62 percent of the participants indicated that their organizations have a remote security policy in place. This indicates that teleworkers in KSA are equally aware of the existence of ISPs and remote security policies. The results also reveal that policies are common, at least among the sample which aligns with the findings of Alzamil (2018) and Alsaif (2015). Alzamil (2018) reported that the majority

of the surveyed organizations both in public and private organizations in KSA have ISP in place. While the findings reported in Alsaif's (2015) study on five organizations in KSA show that 61 percent of the employees are aware of the existence of security policy within their organizations.

Nevertheless, these findings contradict with the results of Abu-Musa (2010) who reported that the majority (58.1 percent) of Saudi organizations have no clear written ISPs. The variance in the reported percentages is because of differences in time and targeted contexts in these studies. The relatively high percentages reported in the current study, in Alsaif (2015), and Alzamil (2018) is due to the increased attention given to the area by the Saudi government which can be seen for example in the establishment of the National CyberSecurity Authority (2017).⁸ Another interesting remark is that almost one-third of the total respondents indicated that they *don't know* if their organizations have an ISP and more than one quarter of them indicated the same regarding having remote security policy. This implies that even if these organizations had security policies in place, they are insufficient given that employees are not aware of them (Da Veiga 2016).

5.1.2 Training and Awareness

The data obtained from the third section of the questionnaire is dedicated to answering the second and third research questions. Starting with the second question, are teleworkers at these organizations trained to maintain information security in general and while working remotely? The results reveal that more than half of the participants (55.8 percent) have received some form of training or guidelines regarding information security and half of them (50.4 percent) reported receiving training or guidelines on how to maintain information security while working remotely.

These results can also be compared with the ones reported in Alsaif et al. (2015). Alsaif and her colleagues indicate that less than 40 percent of the employees who work at KSA's organization are trained to maintain information security. This study and Alsaif et al.

⁸ Center for International Communication 2017, <https://cic.org.sa/2017/11/saudi-arabia-sets-up-cyber-security-authority-to-boost-national-security/> [Accessed 22 January 2021].

(2015) show that there is an increase in percentages which might be also due to the early mentioned reason, the increased attention given by the government in KSA. Another critical finding is that a relatively high number (39.5 percent) of teleworkers indicated that they did not receive any form of information security training or guidelines from their organization which may make them less secure and more vulnerable to threats and risks present in home environment settings. It also has to be acknowledged that there is a scarcity of research conducted around this area.

At this point, the discussion is focused on ISA. In the questionnaire the statements from 10 to 30 were to answer the third research question; to what extent does their (teleworkers) behaviour reflect awareness of information security while working remotely? The mean scores of the answers for all sub-areas, except one, were above the average (Table 4.12). On focus area level, teleworkers' scores were the lowest for the "Internet use" focus area. Two of its three sub-areas, however, were still above the average. The main concern is in regards to "Downloading files" sub-area because it was the only sub-area where the scores were below the average. These results suggest that teleworkers do not fully recognize the risks of downloading any file onto their work computers. This was emphasized by Parsons et al. (2017), who suggest that employees tend to prioritize their needs "to get the job done" (p. 45) over the risks posed by downloading such files. To avoid this problem, organizations can setup a Group Policy control to block certain file extensions that are potentially malicious from being downloaded.

In contrast, the scores were the highest in the "Mobile devices" focus area. On sub-area level, two sub-areas achieved equally high scores. The first sub-area is "clicking on links in emails from unknown senders". This indicates that the majority of teleworkers are aware of the risks of clicking on links coming from unknown senders. These results are promising; especially, that phishing emails are one of the main attack vectors (Alabdan 2020) which had significantly increased during the outbreak of COVID-19 (Abukari & Bankas 2020, Evangelakos 2020, Lallie et al. 2020). The second sub-area that received the most positive answers was about physically securing mobile devices when working in a public place.

In the context of KSA, when comparing my findings with the ones of Alarifi's et al. (2012), we are to notice that ISA level of teleworkers is higher than ISA level among the general public in KSA. In regards to physically securing mobile devices, Alarifi and colleagues (2012) reported that only 29 percent of the respondents keep their devices secure all the time and 43.1 percent of them sometimes do. Moreover, the authors reported that merely 29.7 percent of their sample were aware of the risks of phishing attacks. The differences in the results can be understandable given the difference between the two studies in both the time and context; this study focuses on teleworkers' ISA in workplace contexts, whereas Alarifi's et al. (2012) survey is to measure the general public ISA with almost nine-year difference.

Internationally, a comparison is made with the findings of Parsons et al. (2017) and other studies that adapted Parsons's et al. (2017) method as a way of measuring ISA. It should be noted, however, that the results may not be accurately comparable because I have only used one of the three aspects (behaviour) while the majority of the compared to studies used all three aspects (knowledge, attitude and behaviour) to measure ISA. Parsons's et al. (2017) survey of 505 working Australians indicates that the lowest average scores were for the "Internet use" focus area followed by "Email use" and "Incident reporting" focus areas which is in line with the findings of this study. The highest focus areas in Parsons's et al. (2017) study were the "Information handling", "Password management" and "Mobile devices" which is also consistent with the findings reported in this study. Nonetheless, it should be reported that there are differences in the order of these focus areas in Parsons's et al. (2017) compared to this study. The authors indicated that the results of ISA may vary based on the cultures and countries where the study is to be conducted (Parsons et al. 2017). For example, working Australians reported high level of ISA in "incident reporting" focus area which according to Parsons et al. is a "reflection of Australia's 'anti-dobbing' culture" (2017, p. 49).

In addition, based on the calculated percentages of "Favourable Responses" of each focus area, it was found that "Mobile devices" is the only focus area classified as "good" which means that this area is in a good shape and *no actions are needed* to enhance it. On the other hand, the lowest scores were recorded in the "Internet use" focus-area. Thus, ISA

level for this area is classified as “poor” and *actions are required*. The rest of the focus areas are classified as “average” which means that *actions are potentially required* to enhance teleworkers’ ISA. Finally, it was found that the overall awareness level of teleworkers in all focus areas is within the “average” range (69 percentage). These results can be compared to Mahardika’s et.al (2020) and Wahyudiwan’s et al. (2017); the first reported 77.09 percent and the later 79.02 percent for the Behaviour domain, compared to 69 percent reported in this study. This means that the ISA score for these three studies is quite similar as all of them are classified to set within the “average” range.

To conclude, the three areas under investigation are related to each other. Given the level of awareness of security policies and training reported by the research participants, it is not surprising that the overall ISA among participants is in an acceptable range. Parsons et al. (2014) stated that better knowledge of policy and procedures can improve employees’ attitudes towards information security which is translated into better information security behaviour. In addition, although the study did not examine the efficiency of the policies or training reported by the participants, the aspects/domains investigated in the ISA is designed based on a review of several information security policies and might be used to evaluate the efficiency or effectiveness of different controls, training and awareness programs (Parsons et al. 2014). Thus, the level of ISA reported in the different focus areas may give some insights into the efficiency of the security policies or training programs within these organizations. For example, the low level of awareness in the area of “Internet use” suggests that the participants are either unaware of the recommended security policies or procedures when using the internet or they did not have adequate training and awareness programs.

5.1.3 Teleworkers Group Differences

The last part of the discussion focusses on the fourth research question; are there any significant differences among respondent groups regarding information security policies, training and information security awareness? Starting with security policies, the statistical results of Chi-square tests based on the size of the organization teleworkers work for show significant differences among the two groups regarding ISPs ($p < .001$), and remote

security policy ($p=.008$). The majority of teleworkers at large organizations are aware of the existence of ISP (93 percent) and remote security policy (81 percent), while only 46 percent of teleworkers at SMEs are aware of ISP and 53 percent of them are aware of remote security policy. These results were expected given the fact that large organizations are more likely to have security policies compared to SMEs (Clear 2007, Fulford & Doherty 2003). On the other hand, the statistical results of Chi-square tests based on the sector reveal that there is no significant difference between the two groups in regards to ISP ($p=.100$); however, there is a significant difference in their responses regarding remote security policy ($p=.023$).

As for security training, when examining the sample based on the size of the organization, the results of Chi-square tests show significant differences between the two groups regarding training in general ($p <.001$) and training for remote work ($p=.003$). The majority (81 percent) of teleworkers at large organizations had some form of training or guidelines about information security, whereas less than half (44 percent) of teleworkers at SMEs reported receiving such training. Moreover, more than half (69 percent) of the teleworkers at large organizations indicated that their organization provided information security training for remote work; nevertheless, only (41 percent) of teleworkers at SMEs reported receiving training or guidelines on how to maintain information security while working from home. On the contrary, no significant differences were observed in the answers of teleworkers in different sectors regarding training in general ($p = 0.816$) and training for remote work ($p=.053$).

These results suggest that teleworkers' awareness of security policies and having training is statically associated with the size of the organization they work for. These results were anticipated given the fact that "smaller organization place limited value on information and its security" (Smith & Rupp 2002). Moreover, compared to large organizations, SMEs face constraints in resources. Among these constraints are the lack of personnel with security expertise and the lack of financial and managerial resources to recruit specialist and/or train their employees (Senarathna et al. 2018, Clear 2007, Gupta & Hammond 2005). However, there is no sufficient statistical evidence to associate these two variables with the sector teleworkers work at.

The final aspect is ISA. When characterising the sample by size, across all focus areas, the average scores of teleworkers at large organizations are higher than the average scores of teleworkers at SMEs. Moreover, the results obtained from Mann Whitney U test indicate significant differences in five sub-areas. These belong to password management, internet use, social media use and information handling. However, no significant differences were detected within the three other focus areas: email use, mobile devices and incident reporting. The most significant difference between the two groups is in the “Posting about work” sub-area ($p = 0.001$). The awareness level of teleworkers at SMEs is significantly lower than the awareness level of teleworkers at large organizations.

Based on the sector, teleworkers at the private sector have higher ISA levels in password management, email use, social media use and information handling focus areas. Whereas, teleworkers working for the government sector reported higher levels of ISA in internet use, mobile devices and incident reporting focus areas. However, out of the 21 sub-areas, the results of Mann Whitney U test indicated a significant difference in seven sub-areas: email use, social media use, mobile devices, information handling and incident reporting focus areas. Interestingly, significant differences were observed (in favour of the private sector teleworkers) on all sub-areas under email use focus area. This is the only focus area that shows significant differences on all sub-areas which suggest that teleworkers working for the government sector have lower ISA regarding email use, and as a result they are less likely to recognise the risks associated with this area.

5.2 LIMITATIONS AND SUGGESTIONS FOR FUTURE RESEARCH

The limitations of this study and suggestions can be categorized under three main sections: research tool, sample and scope.

5.2.1 Research Tool

To answer the research questions, a questionnaire with closed-ended items was adapted and administrated online. The use of this tool had many limitations. First, I have used a quantitative tool, a questionnaire, to investigate behavioural aspects which might not give

accurate and/or in-depth data on employees' actual behaviour. Elaborating on this issue, Kruger and Kearney (2006) explain that "actual behaviour may not be measured accurately by a questionnaire alone as respondents do not necessarily tell the truth when asked about their behavior" (p. 292). Parsons et al. (2014) add that "the HAIS-Q is a self-report measure" (p. 173) which means that people might not provide accurate measures about their behaviours. Nevertheless, Parsons et al. (2014) indicate that self-report tools can be very effective and powerful when studying areas similar to the one addressed in the research. Having said this, it is suggested that future studies investigate this area using mixed-methods (e.g. interviews, observations, etc.) to provide in-depth data about the areas under study.

Secondly, due to time constraints, the tool focused on one (behaviour) of the three aspects (knowledge, attitude and behaviour) designed by Parsons et al. (2014) to measure ISA which according to Parsons et al. (2017) may result in "a less comprehensive measure of ISA" (p. 48). Future studies, therefore, are encouraged to devise research tools that focus on all three aspects suggested by Parsons et al. (2014). Finally, the tool was administrated online. It has to be noted, however, that although some researchers (e.g. Johnson 2005) argue that the lack of communication between the researcher and research participants might influence the quality and accountability of the data and research, Reips (2005) responding to this concern notes that the increased anonymity of the research participants increases the authenticity of the data.

5.2.2 Sample

It has to be acknowledged that the sample might be considered small due to three main reasons. First, this is a small scale exploratory-based study. This means that the researcher was trying to provide a "greater understanding and insight into the phenomena or situation under study" (Edgar & Manz 2017, p. 98). Secondly, due to time constraints, the researcher had limited time to collect the data. Thirdly, the study was conducted under the name of a Turkish university in the context of KSA which affected the number of responses returned. Indeed, a number of people have restrained from responding to the questionnaire due to this problem.

Furthermore, as this study focused on the prospective of employees about the areas under study, the field could benefit from collecting data from research participants focusing on variables (e.g. gender, job-description, etc.) that might influence the findings. For example, McCormac et. al (2017) indicated that there is a connection between personality characteristics and ISA. It will also be interesting for future research to use the tool to measure the phenomena within specific organizations.

5.2.3 Scope

Although the numbers reported by the participants regarding security policies are considered reasonable, given the indisputable importance of a policy to the information security of an organization, the slow uptake of security policies by the Saudi organizations must be investigated. In addition, more research needs to be done to investigate the effectiveness of security policies as well as other aspects related to it such as, scope, and content in the context of KSA. Furthermore, the level of ISA reported in this study can be used as an indication of the quality of the training these teleworkers may have had. However, as ISA can also be the result of life experience or obtained from external resources (Bulgurcu et al. 2010), future studies should investigate the different aspects of training such as scope, content and frequency within the organizations in KSA.

5.3 CONCLUSION

The emergence of COVID-19 has affected individuals and organisations worldwide. The unprecedented event mandated the sudden shift to adapt teleworking as the *new-normal* way of working. Given the surge in COVID-19 related cyber-attacks in addition to the threats and risks associated with home telework environments, governing information security is more crucial than ever. The importance of security policies, information security training and awareness in safeguarding the information security of an organization is indisputable. The human factor is arguably the weakest link in the information security of an organization, especially, when operating outside the organization premises. Under these circumstances, it is essential for teleworkers to be

aware of their organizations' security policies and to be trained and aware of how to maintain information security.

This research aims to examine these areas from the employee's (teleworker's) perspective. Moreover, it attempts to help in filling the gap in the academic literature regarding these areas because limited research had been published in the context of KSA. With that being said, this study has been driven by four questions: (i) to what extent are teleworkers in KSA aware of the existence of information security policies in the organizations they work for? And to what extent are these teleworkers aware of the existence of remote work policies in the organizations they work for? (ii) Are teleworkers at these organizations trained to maintain information security in general and while working remotely? (iii) To what extent does their behaviour reflect awareness of information security while working remotely? And (iv) are there any significant differences among respondent groups regarding information security policies, training and information security awareness? It has to be noted that this study is one of the first to examine security policies, training and ISA from teleworkers' perspectives within different organizational sizes and sectors in the context of KSA during the outbreak of COVID-19.

To answer these questions, an exploratory study was conducted using a closed-ended questionnaire to examine these areas. The research tool was designed to collect data from home teleworkers in KSA. The findings reported in chapter four indicate that more than half of the research participants are aware of the existence of ISPs (61.2 percent) and remote security policy (62 percent) in the organizations they work for. Moreover, the findings reported about security training show that 55.8 percent of the participants have received some form of training to maintain information security compared to 50.4 percent of home teleworkers who have received specific training to maintain information security when working remotely. In addition, to answer the third research questions, the data collected reflect that the average teleworker has a fairly good ISA, but there are some areas that might need improvement. The data also reflect that the sample have high awareness in the domain of "Mobile Devices" and low awareness in the domain of "Internet Use". Finally, the analysis of the data by size has shown that there are significant

differences between the sub-groups (large/SMEs) in regards to security policies and training. This implies that teleworkers working for large organizations are more likely to be aware of security policies and are more likely to receive a security training compared to teleworkers working for SMEs. However, when examining the sample by the sector, there is no sufficient statistical evidence to associate security policies and training with the sector teleworkers work at.

When examining teleworkers group differences in regards to ISA, significant statical differences were detected based on the size of the organizations. Teleworkers working at large organizations had higher ISA level than teleworkers working at SMEs in five sub-areas under password management, internet use, social media use and information handling focus areas. By sector, significant differences were observed in seven sub-areas. Within these areas, teleworkers at the private sectors had higher ISA levels in the statements that relate to email use and information handling focus areas; while teleworkers at the government sector demonstrated higher ISA in statements belonging to social media use, mobile devices and incident reporting focus areas. The findings obtained from this study provide an insight to the current situation which will hopefully inform future academic research and practice.

REFERENCES

Books

- Barman, S., 2001. *Writing information security policies*. Indianapolis: New Riders Publishing.
- Burgess, T. 2001. *General introduction to the design of questionnaires for survey research*. Leeds: University of Leeds.
- Dörnyei, Z. 2007. *Research methods in Applied Linguistics: Quantitative, Qualitative, and Mixed Methodologies*. Oxford: Oxford University Press.
- Edgar, T.W. & Manz, D.O., 2017. *Research methods for cyber security* 1st ed., Cambridge, England: Syngress.
- Fink, A 2003. Reliable and valid survey instruments, in *The survey handbook*, 2nd ed., SAGE Publications, Inc., Thousand Oaks, CA, pp. 47-54.
- Gardner, B. and Thomas, V., 2014. *Building an information security awareness program: defending against social engineering and technical threats*. 1st ed., Waltham, Massachusetts: Elsevier.
- Illegems, V. and Verbeke, A. 2003. *Moving Towards the Virtual Workplace: Managerial and Societal Perspectives on Telework*. Cheltenham: Edward Elgar.
- King, C.M., Dalton, C. and Foreword By-Beck, S.H., 2001. *Security Architecture: Design, Deployment, and Operations*. Berkeley: McGraw-Hill Professional.
- Mathers, N., Fox, N. and Hunn, A. 2007. *Surveys and Questionnaires*. The NIHR RDS for the East Midlands/Yorkshire & the Humber.
- Nilles, J. M. 1994. *Making Telecommuting Happen: A Guide for Telemanagers and Telecommuters*. New York: Van Nostrand Reinhold.
- Peltier, T.R., 2013. *Information security fundamentals*. 2nd ed. CRC press.
- Rao, U.H. and Nayak, U. 2014. *The InfoSec handbook: An introduction to information security*. Apress.
- Schneier, B., 2015. *Secrets and lies: digital security in a networked world*. 15th ed. John Wiley & Sons.
- Sekaran, U., and Bougie, R. 2016. *Research methods for business: a skill-building approach*. 7th ed. Chichester, West Sussex, United Kingdom: John Wiley & Sons.

Sue, V. M., & Ritter, L. A. 2007. *Conducting online surveys*. Thousand Oaks, CA: SAGE Publications.

Van Oostendorp, H., Breure, L. and Dillon, A. 2005. *Creation, use, and deployment of digital information*. Routledge.

Walliman, N. 2018. *Research Methods: The Basics*. 2nd ed. London: Routledge.

Whitman, M.E. and Mattord, H.J., 2005. *Principles of information security*. 2nd ed. Boston: Cengage Learning.



Periodicals

- Abu-Musa, A., 2010. Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security*. **18**(4), pp. 226-276.
- 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.
- Akbayrak, B., 2000. A comparison of two data collecting methods: interviews and questionnaire. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, (18), pp. 1-10.
- Alabdan, R., 2020. Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 12(10), p.168.
- Alarifi, A., Tootell, H. and Hyland, P., 2012, June. A study of information security awareness and practices in Saudi Arabia. In *2012 International Conference on Communications and Information Technology (ICCIT)* (pp. 6-12). IEEE.
- Al-Harethi, A. and Al-Amoodi, A., 2019. Organizational Factors Affecting Information Security Management Practices in Private Sector Organizations. *International Journal of Psychology and Cognitive Science*. **5**(1), pp.9-23.
- AlMindeel, R. and Martins, J.T., 2020. Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. *Information Technology & People*.
- Almubayedh, D., khalis, M. A., Alazman, G., Alabdali, M., Al-Refai, R. and Nagy, N., 2018. Security Related Issues In Saudi Arabia Small Organizations: A Saudi Case Study, *2018 21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh, 2018, pp. 1-6.
- Alqahtani, F.H., 2017. Developing an information security policy: a case study approach. *Procedia Computer Science*. **124**, pp.691-697.
- Alsaif, M., Aljaafari, N. and Khan, A.R., 2015. Information security management in Saudi Arabian organizations. *Procedia Computer Science*. **56**, pp.213-216.
- Alzahrani, A., Johnson, C. and Altamimi, S., 2018. Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation. In *2018 4th International Conference on Information Management (ICIM)* (pp. 125-132). IEEE.

- Alzamil, Z.A., 2018. Information security practice in Saudi Arabia: case study on Saudi organizations. *Information & Computer Security*. **26** (5), pp.568-583
- Arnott, S. 2002. "Strategy Paper", *Computing*, 28th February, 16.
- Bailey, D.E. and Kurland, N.B. 2002. A review of telework research: Findings, new directions, and lessons for the study of modern work. *Journal of Organizational Behavior*. **23**(4), pp.383-400.
- Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*. **34**(3), pp.523-548.
- Clear, F., 2007. SMEs, electronically-mediated working and data security: cause for concern?. *International Journal of Business Science & Applied Management (IJBSAM)*, **2**(2), pp.1-20.
- Clear, F. and Dickson, K., 2005. Teleworking practice in small and medium-sized firms: management style and worker autonomy. *New Technology, Work and Employment*. **20**(3), pp.218-233.
- Cronbach, L.J., 1951. Coefficient alpha and the internal structure of tests. *Psychometrika*. **16**(3), pp.297-334.
- Curran, K., 2020. Cyber security and the remote workforce. *Computer fraud & security*. **2020**(6), pp.11–12.
- Day, F.C. and Burbach, M.E., 2011. Telework considerations for public managers with strategies for increasing utilization. *Communications of the IBIMA*. pp.1-18.
- Da Veiga, A. 2016. Comparing the information security culture of employees who had read the information security policy and those who had not. *Information & Computer Security*. **24**(2), pp.139-151.
- Department for Digital, Culture, Media and Sport (DCMS). 2020. Cyber Security Breaches Survey 2020. [Online]. London. [Accessed 18 November 2020]. Available from: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019>
- Department for Digital, Culture, Media and Sport (DCMS). 2019. Cyber Security Breaches Survey 2019. [Online]. London. [Accessed 18 November 2020]. Available from: <https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020>

- Donnelly, N. and Proctor-Thomson, S. 2015. Disrupted work: home-based teleworking (HbTW) in the aftermath of a natural disaster. *New Technology, Work and Employment*. **30**(1), pp.47-61.
- Ernst and Young. 2008. *Risk at Home: Privacy and Security in Telecommuting*. [pdf] Available at:
https://iapp.org/media/pdf/knowledge_center/EYCDTRiskatHomePrivacyandSecurityinTelecommuting.pdf [Accessed 30 September 2020].
- Evangelakos, G. 2020. Keeping critical assets safe when teleworking is the new norm. *Network security*. **2020**(6), pp.11-14.
- Fertig, T. and Schütz, A., 2020. About the Measuring of Information Security Awareness: A Systematic Literature Review. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*. 7, January, 2020. [Online]. [Accessed 17 October 2020]. Available from:
https://www.researchgate.net/publication/338630876_About_the_Measuring_of_Information_Security_Awareness_A_Systematic_Literature_Review
- Fertig, T., Schütz, A.E. and Weber, K., 2020. Current Issues of Metrics for Information Security Awareness. In: *Twenty-Eighth European Conference on Information Systems (ECIS2020) – A Virtual AIS Conference* (2020).
- Fulford, H. and Doherty, N.F., 2003. The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*. **11**(3), pp.106-114.
- Furnell, S. and Clarke, N. 2012. Power to the people? The evolving recognition of human aspects of security. *computers & security*. **31**(8), pp.983-988.
- Godlove, T. 2012. Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines. *Information Security Journal*. **21**(4), pp216-229.
- Greer, T. and Payne, S. 2014. Overcoming Telework Challenges: Outcomes of Successful Telework Strategies. *The psychologist-manager journal*. **17**(2), pp.87-111.
- Hänsch, N. and Benenson, Z., 2014. Specifying IT security awareness. In *2014 25th International Workshop on Database and Expert Systems Applications*,

- September, 2014, Munich. [Online]. pp.326-330. [Accessed 5 October 2020]. Available from: <https://ieeexplore.ieee.org/abstract/document/6974870>
- Higgins, H. N., 1999. Corporate system security: towards an integrated management approach. *Information Management & Computer Security*. **7**(5), pp. 217-222.
- Höne, K. and Eloff, J., 2002. Information security policy — what do international information security standards say? *Computers & Security*. **21**(5), pp. 402-409.
- Ikhsan, M.G. and Ramli, K. 2019, June. Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment. In 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC) (pp. 1-4). IEEE.
- ILO. 2020a. *Defining and measuring remote work, telework, work at home and home-based work*. [Online]. [Accessed 28 October 2020]. Available from: https://www.ilo.org/global/statistics-and-databases/publications/WCMS_747075/lang--en/index.htm
- ILO. 2020b. *Practical Guide on Teleworking during the COVID-19 pandemic and beyond*. [Online]. [Accessed 26 October 2020]. Available from: https://www.ilo.org/travail/whatwedo/publications/WCMS_751232/lang--en/index.htm
- Innab, N., Al-Rashoud, H., Al-Mahawes, R. and Al-Shehri, W., 2018, April. Evaluation of the Effective Anti-Phishing Awareness and Training in Governmental and Private Organizations in Riyadh. In *2018 21st Saudi Computer Society National Computer Conference (NCC)* (pp. 1-5). IEEE.
- Iscan, O.F. and Naktiyok, A. 2005. Attitudes towards telecommuting: the Turkish case. *Journal of Information Technology*. **20**(1), pp. 52-63.
- Kruger, H.A. and Kearney, W.D. 2006. A prototype for assessing information security awareness. *Computers & security*. **25**(4), pp.289-296.
- Kurkland, N.B. and Bailey, D.E. 1999. Telework: The advantages and challenges of working here, there, anywhere, and anytime. *Organizational Dynamics*. **28**(2), pp.53-68.
- Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., 2020. Cyber security in the age of covid-19: A timeline and

- analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv preprint arXiv:2006.11929*.
- Lee, D., 2001. Developing Effective Information Systems Security Policies. *SANS Institute*.
- Li, L., He, W., Xu, L., Ivan, A., Anwar, M. and Yuan, X., 2014. Does explicit information security policy affect employees' cyber security behavior? A pilot study. In *2014 Enterprise Systems Conference, August, 2014. Shanghai*. [Online]. pp.169-173. [Accessed 17 October 2020]. Available from: <https://ieeexplore.ieee.org/abstract/document/6997038/>
- Lim, V. and Teo, T. 2000. To work or not to work at home - An empirical investigation of factors affecting attitudes towards teleworking. *Journal of Managerial Psychology*. **15**(6), pp.560-586.
- Lister, K. and Harnish, T. 2011. The shifting nature of work in the UK: bottom line benefits of Telework. *Telework Research Network*.
- Lopes, I. and Sá-Soares, F. 2010. Information systems security policies: a Survey in Portuguese public administration. Paper presented at the IADIS International Conference Information Systems (2010), pp. 61-69
- Mahardika, M.S., Hidayanto, A.N., Paramartha, P.A., Ompusunggu, L.D., Mahdalina, R. and Affan, F., 2020. Measurement of Employee Awareness Levels for Information Security at the Center of Analysis and Information Services Judicial Commission Republic of Indonesia. *Advances in Science, Technology and Engineering Systems*. **5**(3), pp.501-509.
- McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T. and Pattinson, M., 2017. A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses. *Australasian Journal of Information Systems. Australia*. **21**, [no pagination].
- Mello, J.A., 2007. Managing Telework Programs Effectively. *Employee Responsibilities and Rights Journal*. **19**(4), pp. 247-261.
- Moule, B. and Giavara, L. 1995. Policies, procedures and standards: an approach for implementation. *Information Management and Computer Security*, **3** (3), pp.7-16.
- Murphy, D. 2020. Middle East facing 'cyber pandemic' as Covid exposes security vulnerabilities, cyber chief says. *CNBC*. [Online]. 6 December. [Accessed 1 April

2021]. Available from: <https://www.cnn.com/2020/12/06/middle-east-facing-cyber-pandemic-amid-covid-19-uae-official-says.html>

- Mylonas, A., Kastania, A. and Gritzalis, D. 2013. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*. **34**, pp.47-66.
- National Institute of Standards and Technology (NIST). Nieves, M., Dempsey, K. and Pillitteri, V., 2017. *An introduction to information security* (No. NIST Special Publication (SP) 800-12 Rev. 1 (Draft)). National Institute of Standards and Technology.
- National Institute of Standards and Technology (NIST). Souppaya, M. and Scarfone, K. 2016. *Guide to enterprise telework, remote access, and bring your own device (BYOD) security* (No. NIST Special Publication (SP) 800-46 Rev. 2 (Draft)). National Institute of Standards and Technology.
- National Institute of Standards and Technology (NIST). Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A. 2015. *Guide to Industrial Control Systems (ICS) Security*. (No. NIST Special Publication (SP) 800-82 Rev. 2). National Institute of Standards and Technology.
- Nilles, J. 1997. Telework: Enabling Distributed Organizations: Implications for IT Managers. *Information Systems Management*. **14**(4), pp.7–14.
- Okerefor, K. and Manny, P. 2020. Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the COVID-19 Pandemic. *Journal Homepage: http://ijmr.net*. in, **8**(6).
- Olson, M.H. and Primps, S.B. 1984. Working at home with computers: Work and nonwork issues. *Journal of Social Issues*, **40**(3), pp.97-112.
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T., 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*. **66**, pp.40-51.
- Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R. and Jerram, C., 2015. The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*. **9**(2), pp.117-129.

- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C., 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*. **42**, pp.165-176.
- Pattinson, M.R., Butavicius, M.A., Ciccarello, B., Lillie, M., Parsons, K., Calic, D. and McCormac, A., 2018. Adapting Cyber-Security Training to Your Employees. In *Human Aspects of Information Security & Assurance (HAISA)*. pp. 67-79
- Pattinson, M.R., Butavicius, M.A., Parsons, K., McCormac, A., Calic, D. and Jerram, C., 2016. The Information Security Awareness of Bank Employees. In *Human Aspects of Information Security & Assurance (HAISA)*. pp. 189-198.
- Peacey, A. 2006. Teleworkers – extending security beyond the office. *Network Security*. **2006**(11), pp.14–16.
- Peltier, T. 2002. Remote Access Security Issues. *Information Systems Security*. **10**(6), pp.31–36.
- Potter, E.E. 2003. Telecommuting: The future of work, corporate culture, and American society. *Journal of labor research*. **24**(1), pp.73–84.
- Pyöriä, P. 2011. Managing telework: risks, fears and rules: MRN. *Management Research Review*. **34**(4), pp. 386-399.
- Rikitake, K., Kikuchi, T., Nagata, H., Hamai, T. and Asami, T. 2001. Security Issues on Home Teleworking over Internet. *IEICE Technical Report IA2001-20*. **101**(440), pp.9-16.
- Sardeshmukh, S.R., Sharma, D., and Golden, T.D. 2012. Impact of telework on exhaustion and job engagement: A job demands and job resources model. *New Technology, Work and Employment*. **27**(3), pp.193-207.
- Sari, P.K. and Trianasari, N., 2014, May. Information security awareness measurement with confirmatory factor analysis. In *2014 International Symposium on Technology Management and Emerging Technologies (ISTMET 2014)*, May 27-29, 2014, Bandung, Indonesia. [Online]. pp.218-223. [Accessed 1 October 2020]. Available from: <https://ieeexplore.ieee.org/abstract/document/6936509>
- Senarathna, I., Wilkin, C., Warren, M., Yeoh, W. and Salzman, S., 2018. Factors that influence adoption of cloud computing: An empirical study of Australian SMEs. *Australasian Journal of Information Systems*, 22.

- Siponen, M., Pahlila, S. and Mahmood, M.A. 2010. Compliance with information security policies: An empirical investigation. *Computer*. **43**(2), pp.64-71.
- Smith, A.D. and Rupp, W.T. 2002. Issues in cybersecurity; understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security*. **10**(4), pp.326-40.
- Spinellis, D., Kokolakis, S. and Gritzalis, S. 1999. Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management and Computer Security*. **7**(3), pp.121-128.
- Sturgeon, A. 1996. Telework: threats, risks and solutions. *Information Management and Computer Security*. **4**(2), pp.27-38.
- Taherdoost, H. 2016. Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research. *International Journal of Academic Research in Management*. (5), pp. 28-36.
- Thakur, K., Ali, M.L., Gai, K. and Qiu, M. 2016. Information security policy for e-commerce in Saudi Arabia. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 187-190). IEEE.
- Tung, L., Palvia, S., Huei, L., Ye-Meng, L. and Yee, T., 1995. A study of telecommuting in Singapore: current status and future prospects. *Pacific Asia Conference on Information Systems (PACIS)1995 Proceedings, Singapore*. [Online]. [no publisher], p.79. [Accessed 20 October 2020]. Available from: <https://aisel.aisnet.org/pacis1995/79>
- United States. General Accounting Office. 2001. *Telecommuting: Overview of Potential Barriers Facing Employers*. [Online]. United States: General Accounting Office. [Accessed 21 October 2020]. Available from: <https://digital.library.unt.edu/ark:/67531/metadc300383/>
- Wahyudiwan, D.D.H., Sucahyo, Y.G. and Gandhi, A., 2017, October. Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education. In *2017 3rd International Conference on Science in Information Technology (ICSITech)* (pp. 654-658). IEEE

Other Publications

Ampomah, M., De Silva, Y., Li, H., Pahlisa, P., Yang, Q. and Zhang, Q., 2013.

Information security strategy and teleworking (in) security. The University of Melbourne.

Argaam. 2018. Mataa tuetabar kabir? Wamataa tuetabar saghiratan 'aw mutwst?

[Online]. [Accessed 30 November 2020]. Available from:

<https://www.argaam.com/ar/article/articledetail/id/582861>

G20 Foundation. (n.d.). *What is the G20*. [Online]. [Accessed 23 September 2020].

Available from: <https://www.g20foundation.org/g20/what-is-the-g20>

Google Cloud. 2020. *Protecting businesses against cyber threats during COVID-19 and beyond*. [Online]. [Accessed 25 October 2020]. Available from:

<https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond>

Karjalainen, M., 2011. *Improving employees' information systems (IS) security behavior*. PhD. Thesis. University of Oulu.

Mäses, S., 2015. *Evaluation method for human aspects of information security*. Master thesis. Tallinn university of technology.

Saudi vision 2030. 2018. National Transformation Program: Delivery Plan. [Online].

[Accessed 26 October 2017]. Available from:

https://vision2030.gov.sa/sites/default/files/attachments/NTP%20English%20Public%20Document_2810.pdf

Small and Medium Enterprises General Authority (Monsha'at). No date. Taerif

Almunshat. [Online]. [Accessed 29 November 2020]. Available from:

<https://www.monshaat.gov.sa/ar/SMEs-definition>

Small and Medium Enterprises General Authority (Monsha'at). 2017. [Online].

[Accessed 20 December 2020]. Available from:

<https://www.monshaat.gov.sa/ar/news/174>

Takens, N.D. 2020. *Information Security Awareness of bank employees: how differences between headquarter and branch employees affect ISA program design*. Master's Thesis. Open University of the Netherlands.

The General Authority for Statistics (GaStat). 2019. *The National Classification of Economic Activities*. [Online]. [Accessed 26 November 2020]. Available from:

https://www.stats.gov.za/sites/default/files/the_national_classification_of_economic_activities_aug-2019_isic4.pdf

Trochim, W., 2006. Web center for social research methods. Retrieve from <https://socialresearchmethods.net/kb/statdesc.php>

US House. Committee on Government Reform. 2004. *Beneficial or Critical? The Heightened Need for Telework Opportunities in the Post-9/11 World*. Hearing, 8 July. Washington: Government Printing Office

World Bank 2019. GDP (current US\$) | Data. [Accessed 23 September 2020]. Available from: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true&year_high_desc=true.

World Health Organization (WHO). 2020. *WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020*. [Online]. [Accessed 27 October 2020]. Available from: <https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020>

APPENDICES



