Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

The Influence of Personal Characteristics and Other Factors on the Susceptibility of Public Sector Employees to Cyber-Social Engineering Through LinkedIn: A Mixed-Methods Sequential Explanatory Study

Mohammed Khaled N. Alotaibi

A thesis submitted for the award of
Doctor of Philosophy
The School of Computer Science and Statistics
Trinity College Dublin
2021

Supervisor
Dr. Aideen M Keaney

DECLARATION

I declare that this thesis has not been submitted as an exercise for a degree at this or any other university and it is entirely my own work.

I agree to deposit this thesis in the University's open access institutional repository or allow the Library to do so on my behalf, subject to Irish Copyright Legislation and Trinity College Library conditions of use and acknowledgement.

I do consent to the examiner retaining a copy of the thesis beyond the examining period, should they so wish (EU GDPR May 2018).

_____

Mohammed K. Alotaibi

31/3/2021

SUMMARY

Social networking sites (SNS) have become ubiquitous in daily life, fulfilling an ever-broader array of uses. However, SNS are a double-edged sword: while a useful means of communicating, networking and self-presentation, they are also a threat to individual and organisational information security. Employees accessing these platforms from their workplaces can unwittingly create opportunities through which infected files and hyperlinks can be introduced, jeopardising employees and putting their organisation's sensitive data at risk. Cyber-social engineering (CSE) employs deceptive and persuasive tactics leveraged by malicious perpetrators over cyberspace to obtain financial gain or sensitive data. CSE can be exploited by these attackers through social media. These cybercriminals use a variety of vectors to carry out cyberattacks. The success of these psychology-based malicious attacks is found to be due to user characteristics and user behaviours. To date, little attention has been paid to the influence of such characteristics and behaviours on employee susceptibility to CSE while using SNS. Much of the research to date has largely focused on Facebook; research on CSE over career-oriented social networking sites (CSNS) such as LinkedIn, is lacking. In addition, this lacuna has a particular significance when it comes to the impact that susceptible employees using CSNS can have on the information security of their organisation.

To date, the few studies which have investigated the human aspects of susceptibility to cyber-social engineering (CSE) victimisation over social media platforms have focused on examining cognition and behaviour of individuals, including level of engagement, risk perception and propensity, perceived control of information, trust, motivation, past experience and competence. Other research has sought to identify user gullibility to maliciously deceptive messages through perceptions of source characteristics, such as perceived worthiness and attractiveness. In addition, some scholars have looked into how personality traits could influence these cognitive and behavioural aspects to being vulnerable to cybercrime victimisation over SNS. However, the limited number and scope of studies on the phenomenon of CSE risks in the context of SNS is a clear indication that much remains to be discovered regarding the factors that influence this phenomenon. The current research comprehensively combines the most salient factors found under five human aspect domains: personality characteristics and the dispositional, behavioural, demographic and motivations of employees in a public sector organisation in Saudi Arabia. The research described contributes to

improving the understanding of this phenomenon, The objective of the research was to gain a deeper understanding of the relationships between these factors and fallibility to CSE attacks. A noticeable gap in knowledge is how and to what extent cultural dimensions (particularly, collectivism and power distance, which are prevalent in Saudi Arabia) and personality traits influence susceptibility to CSE victimisation.

The research follows a mixed methods sequential explanatory approach. Quantitative data have been gathered using questionnaires from a single case study. Qualitative data have been obtained via semi-structured interviews. The mixed methods approach aims to obtain a fuller understanding of the effects of personality characteristics, disposition to risk, risky habitual behaviour, motivations and demographics on susceptibility to CSE victimisation of employees (Saudi citizens and non-Saudis) in a public organisation in Saudi Arabia.

The quantitative data were collected and analysed in the first phase of the research (a survey questionnaire, N = 394). In the second stage, 15 semi-structured interviews were undertaken and analysed. This approach is especially useful in studies where the quantitative research phase produces unexpected findings, as it allows the researcher to examine these findings in greater detail during the qualitative phase. This sequential explanatory approach also provides further support for the research model and answers the research question.

The findings from this research in some cases confirm those found in other studies, and in a number of instances contradicts those found in previous work. The findings show that of the 16 hypothesised factors, one of which is divided into 3 sub-hypotheses, 7 factors (neuroticism, agreeableness, extraversion, openness to experience, risky information security habitual behaviour, professional advancement and gender) had positive associations with CSE susceptibility over LinkedIn, while 4 (conscientiousness, IT self-efficacy, age and structural power/level of work) had negative associations with susceptibility to CSE victimisation over LinkedIn. This study has also revealed significant differences within four demographic groups (age, gender, nationality, structural power/level of work). Gender, followed by age, had the most significant impact on employee susceptibility to CSE victimisation over LinkedIn. Notably, male employees were at greater risk of susceptibility to CSE victimisation than females were. These quantitative findings were supported by observations and insights gleaned from knowledgeable interviewees. Furthermore, this study has identified an emerging motivational factor that operates on CSNS. This factor, favouritism, has the potential to increase individuals' risk of susceptibility to CSE attacks.

To conclude, the main contributions of this study are:

1) A comprehensive Model of Susceptibility to CSE Victimisation on LinkedIn, applicable to any employee or organisation member accessing a career-oriented SNS.
2) Unlike previous frameworks, this model assesses employee weaknesses and strengths in the aforementioned five domains that impact their CSE vulnerability.
3) A new factor unearthed in the follow-up qualitative phase is favouritism as a motivating factor for professional advancement.
4) This study has found that two factors associated with the ubiquitous and indispensable nature of Internet-connected devices in the workplace influenced susceptibility: IT-self efficacy and risky information security habitual behaviour.
5) This study is the first to examine structural power as a factor contributing to CSE susceptibility.

Dedication

To Shaikha and Kenan

for providing me with comic relief when it was much needed.

ACKNOWLEDGEMENTS

It is with sincere gratitude with which I would like to acknowledge the following persons who have contributed to the realisation of my research.

Foremost, I would like to express my respect and appreciation for my advisor, Dr Aideen Keaney in the Department of Computer Science and Statistics of Trinity College, Dublin, Ireland for her patience, invaluable input, motivation and continuous support of my research and studies.

I extend my deepest gratitude to my mother Noura and my father, Ret. Navy Captain Khaled Alotaibi, who have provided endless encouragement and reassurance throughout my academic journey.

Additionally, I would like to thank my sisters Ghadeer and Abeer, and my brother, Dr Nasir Al-Otaibi, for their emotional support and selfless provisions to my well-being.

My deepest thanks and respectful appreciation to King Salman for providing me the opportunity to fulfil my goal in achieving this honourable distinction.

I would also like to acknowledge the Kingdom of Saudi Arabia's Ministry of Human Resources and Social Development staff for permitting access to and facilitation of the data collection process.

I greatly appreciate the generous time and consideration extended to me by Dr Abdullah Algarni of the K.S.A. Institute of Public Administration for his guidance and expertise in the investigative aspects of my research.

I would be ungrateful if I didn't acknowledge my friends as well. My kindest gratitude to Mohammed Alghuraisa and Dominique Winders, who have always been there when I needed them, regardless of the distance between us. My thanks to Rakan Algasabi, for always calling me long-distance to see how I was doing. And last, but not at all least, my thanks as well to Saleh Altoaimi, for his fruitful advice on investment matters.

RESEARCH OUTPUT

Papers published in conference proceedings

Alotaibi, M.K.N. 2019. A hypothesised model to examine susceptibility to cyber-social engineering through LinkedIn in the workplace. *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance*. HAISA 2019, pp. 203–214.

Alotaibi, M.K.N. 2020. Employees' interest in professional advancement on LinkedIn increases susceptibility to cyber-social engineering: An empirical test. In: Clarke N., Furnell S. (eds) *Human Aspects of Information Security and Assurance*. HAISA 2021. IFIP Advances in Information and Communication Technology, vol 593. Springer, Cham. https://doi.org/10.1007/978-3-030-57404- 8_7

Work-in-progress papers

Alotaibi, M.K.N. and Keaney, A 2021. 'The influence of personal characteristics and other factors on employee's susceptibility to cyber-social engineering over a career-oriented platform'.

Alotaibi, M.K.N. and Keaney, A 2021. 'Favouritism as an emerging motivational factor exploited by cyber-social engineers through the unity principle: A qualitative perspective'.

Papers presented at conferences

Alotaibi, M.K.N. 2019. A hypothesised model to examine susceptibility to cyber-social engineering through LinkedIn in the workplace. Paper presented at the International Symposium on Human Aspects of Information Security & Assurance (HAISA), 15 – 17 July, Nicosia, Cyprus.

Alotaibi, M.K.N. (2020). Employees' interest in professional advancement on LinkedIn increases susceptibility to cyber-social engineering: an empirical test. The 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece. July 8-10) – Online.

ABSTRACT

To date, career-oriented social networking sites (CSNS) have not received sufficient attention from cybersecurity researchers. In today's world of increased online professional networking and communication, this means an increase of cybercrime incidents. The phenomenon of user susceptibility to cyber-based attacks in the form of malicious persuasive messages is still not well understood, particularly when users access SNS/CSNS in public sector organisations. This study addresses this gap in the extant literature, and the research findings provide a theoretical contribution in the field of information system security (ISS). This research seeks to understand how and to what extent personal characteristics and other factors play a role in an employee's susceptibility to cyber-social engineering (CSE) victimisation when accessing professional SNS, such as LinkedIn, in the workplace. This study extends a validated model by Saridakis *et al.* (2016) by adding five personality traits (FFM), two motivational factors, two additional behavioural factors and two additional demographic factors. The study approach is pragmatic, combining aspects of both positivism and interpretivism. Thus, it employs a mixed methods sequential explanatory approach which combines quantitative and qualitative data in a single case study. In the first phase of the research the quantitative data were collected via a survey questionnaire (N = 394). The findings from the survey data were investigated in more detail in the qualitative phase, in which 15 semi-structured interviews were conducted. The findings from this research in some cases confirm those of other studies, and in others contradicts those reported in previous work. Study findings show 7 factors (neuroticism, agreeableness, extraversion, openness to experience, risky information security habitual behaviour, professional advancement and gender) had positive associations with CSE susceptibility over LinkedIn, while 4 factors (conscientiousness, IT self-efficacy, age and structural power/level of work) had negative associations with susceptibility to CSE victimisation over LinkedIn. This study also revealed significant differences with regard to 4 demographic variables (age, gender, nationality, structural power). Gender, followed by age, had the most significant impact on employee susceptibility to CSE victimisation over LinkedIn. Male employees were at greater risk of susceptibility to CSE victimisation. Main contributions include: Model of Susceptibility to CSE Victimisation on LinkedIn; Favouritism as a motivating factor for professional advancement; First study to examine structural power as a factor in CSE susceptibility. Implications for organisations include: Organisations should incorporate validated psychometric evaluations as part of their recruitment platform; Organisations should conduct IS awareness training that fosters an understanding of CSE and risks associated with CSNS.

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF FIGURES

LIST OF TABLES

LIST OF CHARTS

LIST OF ABBREVIATIONS

Abbreviation	Full Name or Term
4G	fourth generation mobile network technology
ANOVA	analysis of variance
BBC	British Broadcasting Corporation
CSE	cyber-social engineering
CSNS	career-oriented social networking site(s)
CTU	Counter Threat Unit
CWB	counterproductive workplace behaviour
FBI	Federal Bureau of Investigation (United States)
FFM	Five Factor Model
Gov.	government
InfoSec	information security
IS	information systems
ISA	information security awareness
ISS	information systems security
IT	information technology
LAT	lifestyle activity theory
LI	LinkedIn
LRAT	lifestyle/routine activity theory
MHRSD	Ministry of Human Resources and Social Development
NIC	National Information Center
ORGLS	Organisation – Labour Sector
ORGSD	Organisation – Social Development Sector
PBC	perceived behavioural control
PC	personal computer
PII	personally identifiable information
PT	personality traits
RAT	routine activity theory
REC	research ethics committee
RHB	risky habitual behaviour
RHBIS	risky habitual behaviour – information security
RHBLE	risky habitual behaviour – level of engagement
SA	Saudi Arabia
SE	social engineering
SNS	social networking site(s)
TPB	theory of planned behaviour
TRA	theory of reasoned action
UIT	unintentional insider threat
UK	United Kingdom
USB	universal serial bus

1. Introduction and Background to the Research

1.1 Introduction

Social networking sites have become a major repository for all types of personal and demographic data, including groups with which individuals are affiliated, other individuals with whom they are connected, their streaming updates and their personal credentials (Ellison and Boyd, 2013; Bagrow, Liu and Mitchell, 2019). Moreover, as a result of the increase in professional networking and sales activity conducted online, the use of social networking services or sites (SNS) within organisations is becoming more prevalent (Valos *et al.* 2016; Bretschneider and Parker, 2016). This has created a vulnerability which can allow criminals access to an organisation's data (Kirichenko, Radivilova and Carlsson, 2017) by using manipulative and persuasive techniques. In 2016, a US report revealed that 60% of enterprises had been affected specifically by cyber-social engineering (CSE) offences. The report stated that 65% of these attacks jeopardised the personal data of employees, while 17% successfully breached a company's financial accounts (Information Security Media Group [ISMG], 2016). The most commonly used professional SNS platform is LinkedIn (Clement, 2019a). Content sharing and user engagement numbers continue to grow, according to a Data Science Manager with LinkedIn Engineering:

> *more people are using the feed and giving feedback to their network's posts: our members generate tens of millions of viral actions (likes, comments, and re-shares), and the number is increasing more than 50% year-over-year* (Barrilleaux and Wang, 2018)

LinkedIn has been portrayed as a site on which users do not need to be concerned about who views their personal information or photos, since the activity on this SNS is geared towards business activities (Cooper and Naatus, 2014). However, a cyber-social engineer could elicit and appropriate available information from the company posted on its LinkedIn profile, such as its addresses, logos and affiliated groups. Then such an engineer could create a bogus profile, with which they could request a link to employees' SNS profiles, and such attempts are often successful (Silic and Back, 2016; Jagatic *et al.*, 2007).

One such profile has attracted the attention of the Counter Threat Unit (CTU) of Secureworks, a US-based global security firm. In early 2017, CTU uncovered phishing attacks via LinkedIn involving malware aimed at the Middle East and focussing on organisations in Saudi Arabia. CTU noticed what they deemed to be unsuccessful phishing campaigns, which were followed by "*highly targeted spear-phishing and social engineering attacks from a threat actor*" posing as a UK-based female photo editor, with an attractive LinkedIn profile photo ("borrowed" from a real person's profile) and plausible credentials (CTU Research Team, 2017, "Mia Ash" persona). CTU's investigation revealed that the persona named "Mia Ash" had

> *a well-established collection of fake social media profiles that appear intended to build trust and rapport with potential victims. The connections associated with these profiles indicate the threat actor began using the persona to target organizations […]*

The threat group thought to be behind these campaigns and the Mia Ash persona has targeted

> *telecommunications, government, defense, oil, and financial services organizations based in or affiliated with the MENA region, identifying individual victims through social media sites*. (CTU Research Team, 2017, Summary).

A recent counterintelligence study by the German Ministry of the Interior (BfV) has shown that LinkedIn was of interest to the Chinese intelligence services, which gathered employees' personal data. The BfV stated that "*the intent is to compromise individuals' computers and their corporate or government access to ultimately penetrate organisations of interest*" (TechCentral.ie, 2017, paragraph 3). By the end of 2020, there were more than738 million LinkedIn accounts (LinkedIn, 2020). LinkedIn has been the target of CSE attacks. More than 117 million LinkedIn accounts were hacked by a phishing email campaign in 2012: it is reported that the hack ultimately resulted in users' information and credentials being placed on the dark web in 2016 (BBC, 2012; Silic and Back, 2016; Dellinger, 2017).

LinkedIn is not, of course, the only SNS targeted by CSE attackers. Several recent studies note that the increased numbers of CSE attacks are the result of a lack of training offered to users (Junger, Montoya and Overink, 2017; Terlizzi, de Souza and Cortez da Cunha, 2017). Silic and Back (2016) found that although employees are periodically made aware

of security issues and given training programs to address potential threats in IS environments, the training does not include the online realities of threats involved when using SNS at work. Because it is difficult to regulate and control SNS usage in the workplace (Vaast and Kaganer, 2013), it is hard to mitigate cyberspace scam victimisation. This is increasingly the case, especially with the growth of the mobile ecosystem and the related increase of IS security threats due to unintentional insider attitudes to potential cyber risk. According to a 2017 report by the Castle Point Borough Council (UK),

> *…insiders or employees … accidentally cause cyber harm through inadvertent clicking on a phishing email, plugging an infected USB into a computer, or ignoring security procedures and downloading unsafe content from the Internet. Whilst they have no intention of deliberately harming the organisation, their privileged access to systems and data mean their actions can cause just as much damage as a malicious insider. These individuals are often the victims of social engineering – they can unwittingly provide access to the networks of their organisation or carry out instructions in good faith that benefit the fraudster.* (Mills, 2017, p. 2)

Many employees and other insiders (such as contractors) in professional fields will have a personal LinkedIn account. LinkedIn is a popular professional network platform that has not yet been extensively studied. It is important to examine LinkedIn, the most commonly used career-oriented SNS, since users' motivations for engaging on this particular platform differ from those on other platforms, such as Facebook, and this difference might affect employee behaviour and susceptibility.

1.2 Aims and Significance of Research

The overall aim of this research is to expand the existing literature by identifying the underlying causes of employee susceptibility to CSE victimisation on LinkedIn in the workplace. This research will examine whether, and by what mechanisms, the personality traits of employees accessing LinkedIn can make their organisations susceptible to the risks of CSE. In order to achieve this aim, the study will also examine how, and to what extent, employee susceptibility to risk of CSE attack on professional SNS is correlated with the following dimensions in five domains:

a) personality characteristics

b) disposition to risk: risk perception, risk propensity (willingness to assume risk), perceived control of information (privacy risk), IT self-efficacy

c) risky habitual behaviour: frequency of SNS use, level of engagement, information security habitual behaviour

d) demographics: age, gender, nationality, role in organisation (structural power)

e) motivational factors: self-presentation and professional advancement

In other words, what specific personal characteristics and other factors identified above can increase an employee's risk of CSE attack on LinkedIn? This research explores the vulnerability of employees in Saudi Arabia's public sector organisations to CSE victimisation. This is an important issue, as public sector organisations hold large amounts of personally identifiable information (PII) on Saudi citizens and residents that can be exploited if attackers gain access to it.

This study uses a mixed-method sequential research methodology to gain a deeper understanding of employees' personality characteristics and other factors and how these could contribute to their susceptibility to cyber-victimisation or deception on LinkedIn.

1.3 Problem Statement

There are benefits to using SNS, but also many risks. SNS can hold a plethora of personal information, which is viewable to all because the majority of users are on default privacy settings (Furnell, 2008; Wong *et al.*, 2014). Few studies to date have looked at LinkedIn as a platform that can be a potential launching ground for CSE attacks (Silic and Back, 2016). The "*number of victims is higher on LinkedIn if a job is offered on that network, because many people use that platform for career enhancement*" (Vishwanath, 2017, p. 78). Users of job-related social networking platforms are motivated by self-presentation and professional advancement (Kim and Cha, 2017). Self-presentation is a form of information disclosure (Bronstein, 2013). As such, individuals who are driven by self-presentation are keen to initiate interactions and build relationships (Schwämmlein and Wodzicki, 2012). These motives of career advancement can be seen as an element that could be exploited by scammers posing as hiring recruiters. LinkedIn members are found to be significantly more likely than Facebook users are, to allow public access to their professional and educational data (Zhitomirsky-Geffet and Bratspiess 2015, Silic and Back, 2016).

Skeels and Grudin (2009) and Silic and Back (2016), when studying workplace users of Facebook and LinkedIn, found that employees often have difficulty controlling the content

they post when switching between SNS platforms; in fact, this raises questions as to the adequacy of individuals' ability to control their information and/or their IT self-efficacy. The information contained on LinkedIn, in particular, can pose a risk for organisations, considering that LinkedIn offers "Company Profiles" (Samuelson, 2008), a feature that enables organisations to have their own independent profile after a pre-authentication process. As of October 2020, there were over 20 million company profiles on LinkedIn (Broadband Search, 2020). "*social engineers can gather a vast amount of employee information a lot faster*" (Scheelen *et al.*, 2012, p. 44) from these profiles, such as job titles, names, email addresses, partnering organisations and upcoming projects. This information can be exploited easily to identify "*different staff in different buildings and different departments…the easiest way to build a target list is the business social network, LinkedIn*" (Allsopp, 2017, p. 68).

Recently, a cyber security firm uncovered cyber-attacks, aimed at military and aeronautics companies in the Middle East and Europe, that used LinkedIn messaging as an entry point (Knowles, 2020). "*In order to appear credible, the attackers posed as representatives of well-known, existing companies in the aerospace and defense industry*" (Breitenbacher and Osis, 2020, p. 2). The attackers would send a LinkedIn message describing a job offer. According to the research team that discovered it,

> *the LinkedIn profile was fake, and the files sent within the communication were malicious. Once the recipient opened the file, a seemingly innocent PDF document with salary information related to the fake job offer was displayed. Meanwhile, malware was silently deployed on the victim's computer.* (Knowles, 2020, paragraph 6)

Research into the examination of the susceptibility of users to CSE attacks in SNS platforms is at an early stage (Algarni, 2013, 2016; Albladi and Weir, 2018). A number of factors have been examined in the literature that could pose CSE risks to users on social media platforms. These factors included competence, motivation and past experience with CSE influencing individual ability to identify cyberattacks over SNS (Albladi and Weir, 2017). Additional examined factors were habitual behaviours, such as frequency of SNS use (Vishwanath, 2014) and users' understanding of SNS privacy settings (Halevi, Lewis and Memon, 2013b). Other relationships examined were social media behaviour and risk

of cybercrime victimisation and their relationships to disposition to risk and SNS usage (Saridakis *et al.*, 2016).

Personality traits have been highlighted as predictors of susceptibility to phishing victimisation (Halevi, Lewis and Memon, 2013a; Halevi, Memon and Nov, 2015; Albladi and Weir, 2018). A limited number of studies have examined the influence of personality traits on susceptibility to cybercrime over SNS platforms (Algarni, Xu, and Chan, 2017; Albladi and Weir, 2017; Frauenstein and Flowerday, 2020). These studies have integrated the Big Five personality traits (see Chapter 2) as influencing factors on mediators that can consequently determine the level of impact on user susceptibility to CSE vectors on social media platforms, such as in Frauenstein and Flowerday (2020) and Albladi and Weir (2017). In other studies the Big Five have been used as auxiliary information in creating profiles of susceptible users, such as in Algarni *et al.* (2017). However, in those studies personality characteristics were not examined as direct influencing factors.

One framework (Uebelacker and Quiel, 2014) presents personality traits as being directly affected by the principles of influence used generally by social engineers. However, to the best of this researcher's knowledge this framework has never been empirically tested. Van de Weijer and Leukfeldt (2017) employed the Five Factor Model (FFM) in a study to compare susceptibility to traditional crimes with susceptibility to cyber deception. They contended that personality traits were associated with cybercrime victimisation but that personality traits alone explained little about cybercrime victimisation. Other variables examined in the literature are behavioural and perceptual factors, such as users' risk perceptions and behavioural engagement. These have been proven to play crucial roles in susceptibility to CSE (Vishwanath, 2014; Silic and Back, 2016; Moody, Galletta and Dunn, 2017).

Saridakis *et al.* (2016) considered a broader range of factors, both dispositional/perceptual (risk perception, risk propensity, IT self-efficacy and perceived control over information) and behavioural (SNS usage). However, their study did not consider personality traits. Moreover, they did not investigate further to explain their quantified findings, and in discussing their study's limitations they suggested the need for a qualitative phase to dig deeper into the causation and level of impact on susceptibility.

To the best of this author's knowledge, there is no study which has addressed susceptibility to CSE victimisation on SNSs by combining personal characteristics with other factors

such as personal dispositions, habitual behaviours, and demographic variables such as age, gender, level of work and nationality. A study of the relationships between such factors and the perception of cyber risks can provide further explanation of users' vulnerability to cybercrime.

A further gap in the literature that needs to be addressed in investigating susceptibility to CSE over SNS is the relationship between culture and risky human behaviours. Internet-connected technologies are increasingly integrated into the infrastructure and day-to-day work of organisations. When using SNS technologies inside these organisations, susceptible employees could endanger sensitive organisational data. In business-oriented SNS, users are incentivised to present themselves to other professionals and to advance their careers by actively engaging with others (Kim and Cha, 2017). These types of motivations can be perceived by a CSE perpetrator as ripe for exploitation. In their systematic review of user-focussed studies on phishing, Das *et al.* (2019) highlighted the imperative of "*focusing on future research and the courses of action that are still needed to better understand the user and their motivations and behaviors as they respond to phishing efforts, including a call for researchers to better report on the user component of any future work*" (Das *et al.*, 2019, p. 1). Generally, computer-based behaviour that entails information security has not been the focus of research on CSE over SNS. Determining the level of InfoSec habitual behaviour needed to mitigate the success of CSE attacks, especially against organisations, is lacking. Algarni (2019) asserted that "*behavioral compliance of individuals in response to attacks is a key element in information security*" (p. 22). Koochaksaraee (2019) argued that "*most security-related behaviour is habitual behaviour, which can be improved though an awareness training program and effective educational methods*" (p.18). Assuming that these two statements are true, they point to a need for a deeper understanding of the relationship between human behaviour and user susceptibility to cyber-social engineering.

And finally, much of the research to date has been primarily conducted in relation to the general public (Junger *et al.*, 2017) or to students and faculty (Greavu-Servan and Serband, 2014) in studies of CSE via SNS (Albladi and Weir. 2017, 2018; Halevi *et al.*, 2013b; Vishwanath, 2014, 2015a) or of online users in general (Saridakis *et al.*, 2016), as opposed to employees (Terlizzi, de Souza and Cortez da Cunha, 2017). Ford (2016) explicitly cautions against using student samples in research, since this does not replicate real-world situations relevant to organisations.

1.4 Research Question

The main aims of this study are to identify which personality traits of employees and other factors can increase their susceptibility to CSE tactics carried out via SNS, and particularly over career-oriented SNS. The research question of this study is:

Q1: How, and to what extent, do personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering (CSE) victimisation when accessing professional SNS, such as LinkedIn, in government organisations in Saudi Arabia?

1.4.1 Conceptual framework and research methods

This research is an extension of a model proposed by Saridakis *et al.* (2016) which examines user behaviour and the risk of cybercrime victimisation over social media. The Saridakis *et al.* (2016) model encompasses five factors: social media usage, perceived control over information, computer self-efficacy, risk perception and risk propensity. They also partially controlled for other individual characteristics such as educational background, age and gender. Their model is grounded in the Theory of Planned Behaviour, Theory of Reasoned Action and Lifestyle/Routine Activity Theory (LRAT; Cohen and Felson, 1979) and its application in online environment (Saridakis *et al.,* 2016).

The model proposed in this thesis expands on that model to include other factors that have emerged from the literature. Four additional factors are added to the model. These are personality characteristics, power position within an organisation, nationality and risky habitual behaviour, which consists of three subfactors: information security habitual behaviour, level of engagement and frequency of SNS use. This extended model examines employees' susceptibility to CSE victimisation over career-oriented SNS in public sector organisations in Saudi Arabia.

The new extended model adds specific factors that allow for a more holistic understanding of CSE susceptibility from various aspects of user characteristics and dispositions: behavioural, perceptual, demographic, motivational and personality. These additional factors and subfactors may play a role in employee susceptibility to influential messages relevant to cybercrimes, hence, jeopardizing the personal data of others as well as proprietary information belonging to the organisation.

To answer the research question, an extensive literature review was carried out, examining and assessing previous relevant studies and highlighting any gaps. An extended model was proposed. This model was tested using a survey and semi-structured interviews. The research takes a pragmatic philosophical stance, using a mixed method sequential explanatory design. A detailed description and discussion of the research methods can be found in Chapter Four.

The quantitative data were collected from employees and analysed in the first phase of the research (a survey of 394 participants). In the second phase, 15 semi-structured interviews were conducted and subsequently analysed. This strategy is especially beneficial when unexpected findings emerge from the first phase (quantitative research), as the researcher can then investigate these findings in more detail during the qualitative phase. The data were gathered from a single government organisation in Saudi Arabia, namely, the Ministry of Human Resources and Social Development. This organisation has access to the National Information Center (NIC; see Section 1.7.2.1), a government hub of information on citizens and expatriate residents.

1.5 Research Objectives

The aim of this research is to identify potential factors responsible for employee/users' susceptibility to CSE on LinkedIn. To achieve this goal, the study examines a number of factors including personal characteristics and other personal dispositions that have the potential to make users susceptible on SNS and in particular on career-oriented SNS (CSNS). The knowledge obtained through this process helps in developing a model that can aid in designing appropriate preventative strategies within the domain of cybersecurity. Thus this study will improve cybersecurity measures for organisations and assist them by:

- Investigating the relationships between employee personal characteristics and their vulnerability to cyber-social engineering
- Defining the most significant demographic dimensions that contribute to employee susceptibility to CSE: this includes gender, age, nationality and role/power level within the organisation
- Developing a model that incorporates the factors that influence CSE victimisation
- Identifying vulnerabilities of examined factors in this current study's extended framework (see Chapter 3), supplemented by qualitative explanations of why these relationships exist

- Presenting implications and recommendations for individuals and organisations

This research provides an in-depth study of various personal and perceptual aspects, controlling for gender, nationality and age groups within the organisational domain with respect to susceptibility to cybercrime.

1.6 Scope of This Study

There are four main entities that can be addressed in scientific research when investigating cyber social engineering; these are the offender, the victim, the means of influencing the victim and the context in which the event takes place (see Chapter Two). The main focus of this study is on the victim. More specifically, the scope stays within the boundaries of receiver personality characteristics (the victim), which for the purposes of this research is limited to employees, categorised by gender, age group, role in the organisation, nationality, and dispositional and perceptual factors consisting of perceived control over privacy risk, risky habitual behaviour, risk perception, IT self-efficacy, self-presentation and career advancement. These last two constructs are pertinent because LinkedIn specialises in providing a platform suitable for both job hunters and head-hunters (employment recruiters). The context in which the CSE phenomenon takes place will be confined to the Saudi public sector, with particular attention to LinkedIn as the dominant career-oriented social networking site.

1.7 An Overview of the Kingdom of Saudi Arabia

The Kingdom of Saudi Arabia (KSA or Saudi Arabia) was selected as the case study country because it is the home country of the author of this thesis. Saudi Arabia is the birthplace of Islam, and its monarch is called "*the Custodian of the Two Holy Places*", meaning Makkah and Madinah, the two most sacred sites for Muslims. Islamic mores and laws are the de facto societal values and national laws of the Kingdom of Saudi Arabia. Saudi culture is thus intertwined with Islamic/Muslim culture.

The majority of employed Saudi citizens work in the nation's public sector (Harvard Kennedy School, 2019): estimates vary regarding the exact proportion, but according to recent reports, it is as high as 72% (Assaad and Barsoum, 2019). Although women account for only 22% of the Saudi workforce overall, more than 70% of employed females work in the public sector (Harvard Kennedy, 2019); thus, a study sample drawn from the government sector can be assumed to be generally more representative of the nation's population than a sample taken from the private sector, which is highly skewed toward non-

Saudi (expatriate) and male employees (Harvard Kennedy, 2019). The following subsections provide brief but relevant context regarding the demographic characteristics of Saudi Arabia, the organisation of its public sector and the use of SNS — and of LinkedIn particularly — in Saudi Arabia.

1.7.1 Population

The population of Saudi Arabia was over 34 million as of the end of 2019, with approximately 30% of the population under the age of 25 years (General Authority for Statistics, 2019). Average life expectancy is 75 years (World Bank, 2018). Arabic is the official language and is the language of government and business, but English is taught as a second language in schools and is also used in some professional fields, including in education, which is a major employer in the public sector. Digital and internet penetration is relatively high: over 93% of the population has internet access, and there are 123 mobile phones for every 100 people (World Bank, 2018).

1.7.2 The Public Sector in Saudi Arabia (KSA)

The Kingdom of Saudi Arabia is an absolute monarchy; its executive branch consists of the Diwan (Prime Minister's Office) and 25 ministries. These ministries each have departments and sections, and many of these are located in the administrative regions. The judicial branch also has regional offices, as does the legislative branch in the form of the Shura Council (the parliament). In addition, each region and each municipality within those regions is served by administrative departments at the level of the governor, city hall, and so on. Under the auspices of ministries and departments there are numerous civil service agencies, such as the Saudi Post (postal service) and the General Authority of Zakat and Tax (Gov.SA, 2020). As mentioned in the overview above, the majority of Saudi Arabia's citizens work in this large public sector, and although the government wants to reduce this proportion to 20% by 2030, it is likely that the government will continue to be the largest employer in the country for decades to come (Harvard Kennedy, 2019).

1.7.2.1 National Information Center

Under the auspices of the Ministry of Information, the National Computer Center was established in 1979, in order to provide information technology (IT) services to the MOI and to the Kingdom's Presidency of State Security. Renamed the National Information Center (NIC) two years later, the NIC has since grown in scope and size. It now provides

the state security with secured computer and telecommunications systems; current research in IT; e-services in security, public services and administration; data storage and retrieval; IT training programs; and strategic plans for continued development of IT services to the Saudi government. The NIC is integrated into and provides IT services and support for regional levels of government as well (National Information Center, 2020).

1.7.2.2 Ministry of Human Resources and Social Development

The backstory to the establishment of the Ministry of Human Resources and Social Development (MHRSD) reflects Saudi Arabia's own development as a modern, independent state and its subsequent transformations throughout the twentieth and into the 21st century as an emerging economy with a large and complex civil service bureaucracy. What follows is a timeline of the main changes to the organisation and its mandate, as translated and summarised from its official Arabic-language website:

1929 – For the first time in Saudi Arabia, a central unit was created to maintain records on and provide services to state employees. This was later expanded to include the centralisation of public employment records, which was the first organisation for civil service affairs in the country.

1939 – A central administration for personnel affairs, the Bureau of Civil Servants and Retirees, was set up under the auspices of the Ministry of Finance.

1945 – The first administrative system for government employees was established: the Bureau of Civil Servants and Retirees became the Personnel and Retirement Office.

1953 – The Council of Ministers was established, and the Council designated the General Civil Service Bureau as the authority responsible for administering personnel affairs and monitoring the enforcement of personnel-related regulations. The General Civil Service Bureau was transferred from the oversight of the Ministry of Finance to that of the Council of Ministers.

1961 – The Ministry of Labor and Social Affairs was established and given the mandate that is essentially the same as that of the MHRSD today.

1965 – The Council of Ministers transferred the responsibility of supervising public institutions to the Bureau.

1977 – The Civil Service Council was established as an independent legislative body headed by the prime minister and charged with drafting policy, setting up plans and

programs to implement policies, and issuing executive regulations pertaining to civil service employees.

1999 – The General Civil Service Bureau was replaced by the Ministry of Civil Service, which continued the work of the Bureau.

2004 – The Ministry of Labor and Social Affairs was split into two separate and independent entities: the Ministry of Labor and the Ministry of Social Affairs.

2015 – These two Ministries were once again merged, this time under a slightly different name: the Ministry of Labor and Social Development.

2020 – In February, the Civil Service Ministry was merged with the Ministry of Labor and Social Development to become the current Ministry of Human Resources and Social Development. (*Asharq Al-Awsat*, 2020; MHRSD, 2020a, *About Ministry*)

Thus, by the time this study was conducted the current MHRSD had become the amalgamation of three previously separate ministries.

According to its mission statement, the Ministry of Human Resources and Social Development focusses on empowering the individual, society and institutions, promoting social responsibility, strengthening the labour market by developing policies and legislation, and enabling the Ministry's employees to provide a distinct experience to the beneficiaries (MHRSD, 2020a, *About Ministry*). MHRSD has three stated objectives:

1. To formulate the overall policy for national labour and social affairs within a framework commensurate with the values, principles and systems of Saudi Arabia;
2. Project planning and implementation; and
3. Contributing to the balanced direction of social development in Saudi Arabia "*aimed at raising the awareness of citizens, improving their standard of living and preparing the foundations for a decent life for them*" while "*preserving and supporting spiritual and moral values to build an integrated, resilient society*" (MHRSD, 2020b, About Ministry).

1.7.3 Social Networking Sites

A social networking site (SNS) is an online platform via which users maintain a public-facing profile and interact with other users on the same site. Users "post" or upload text messages, digitised media (photos, images, audio-video, etc.) to share publicly or with

specific individual users or groups with whom they share a connection. A user profile usually contains all or some of the following PII: legal name, date of birth, physical address, email address(es), phone number(s), and visual personal identification such as a profile photo (Boyd and Ellison, 2007).

1.7.3.1 Types of social networking sites

Saridakis *et al.* (2016) distinguish between categories of SNS according to the purpose and nature of content sharing on the site. Although many of the largest SNS (e.g., Facebook, YouTube, and WhatsApp) are multi-purpose, it is reasonable and practical for the purposes of this study to identify two main purpose types: personal/leisure and academic/career. Personal/leisure oriented SNS are those whose primary purpose is to allow users to connect online with friends, family, and their wider social network. Academic/career-oriented SNS belong to what Saridakis *et al.* (2016) identify as having a "*knowledge-exchange purpose…allow[ing] users to share ideas and content*" (p. 322). LinkedIn is a knowledge-exchange, career-oriented SNS.

1.7.3.2 SNS use in Saudi Arabia

As mentioned in Section 1.7.1 above, more than 93% of the population in Saudi Arabia has internet access. According to Global Media Insight (2019), around 23 million (68% of the population) are active social media users, with YouTube, Facebook, Instagram, Twitter, and LinkedIn being the five most popular SNS in the Kingdom. Nine out of ten SNS users in Saudi are under the age of 35 (Kemp, 2020).

1.7.3.3 LinkedIn

Launched in 2003 and based in the United States, LinkedIn is the world's largest career-oriented network. It boasts over 706 million users worldwide, "*in more than 200 countries and territories*". Its stated mission is to "*connect the world's professionals to make them more productive and successful*" (LinkedIn, 2020, About). According to a survey of LinkedIn users in the United States, 84% of respondents stated that they used LinkedIn to strengthen their professional network (Clement, 2019b). In addition to its primary function as a social networking site for professionals, LinkedIn offers business-to-business (B2B) services, including personnel recruiting, advertising, and online learning (LinkedIn, 2020,

Business Solutions). The company was acquired by Microsoft in 2016 (LinkedIn, 2020, About).

1.7.3.4 LinkedIn Use in Saudi Arabia

Roughly 8.12 million people in Saudi Arabia (around 24% of the population) have LinkedIn accounts (Global Media Insight, 2019); over 4 million of them are active LinkedIn users (LinkedIn, 2020). By comparison, LinkedIn has over 30 million users in Great Britain (LinkedIn, 2020), which is about 44% of the population in Britain. Only 18.6% of LinkedIn users in Saudi Arabia are female (Kemp, 2020), which is not surprising, considering that women make up only 22% of the workforce, as mentioned at the beginning of this section (1.7). The number of MHRSD employees who are "on LinkedIn" – that is, who have active, publicly accessible LinkedIn accounts – was around 700 in October 2019. Interestingly, by the end of September 2020 that number had doubled to over 1400, and by March 2021 there were more than 2200 MHRSD employees on LinkedIn (MHRSD LinkedIn profile page, see Figure 1-1).

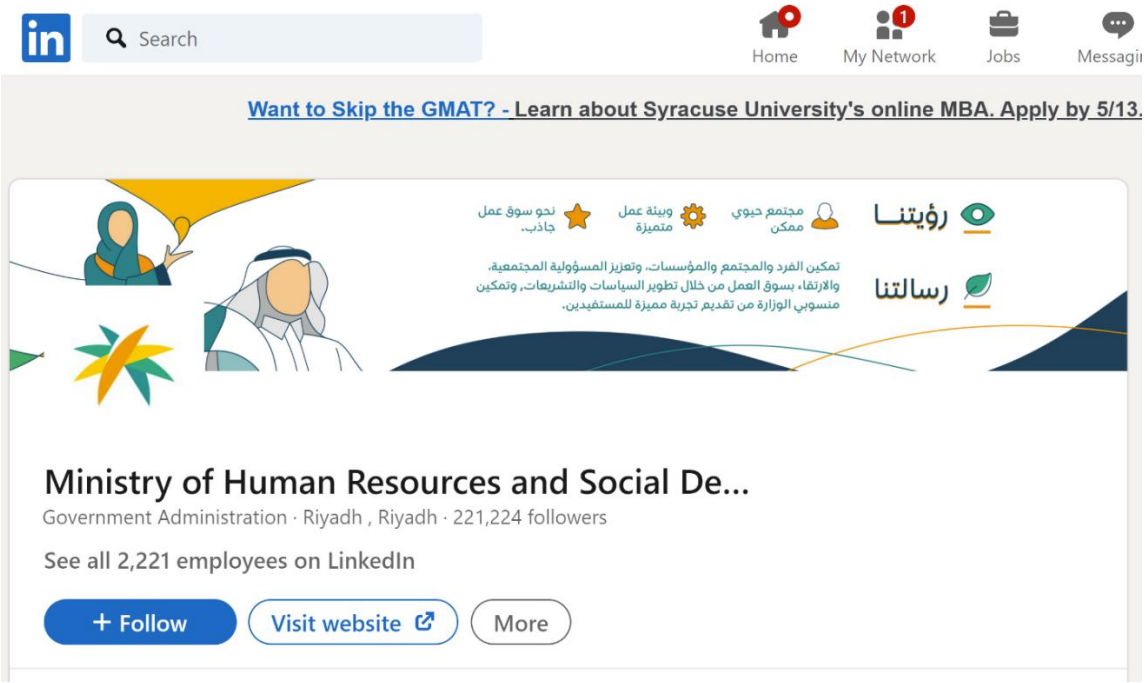


Figure 1-1 Ministry of Human Resources and Social Development's LinkedIn Page, 24 Mar 2021

1.7.4 Cybersecurity in Saudi Arabia

Due to Saudi Arabia's accelerated pace of IT adoption and transition to digital information management (including cloud storage), it is increasingly becoming a target for cyber threats

(Malek, 2019). The Kingdom enacted the Anti-Cyber Crime Law in 2007, and in 2017 it set up the National CyberSecurity Authority (NCA) with the aim of centralising cybersecurity monitoring and prevention (NCA, 2020, About NCA). The National Cyber Security Center (NCSC) "*operates around the clock to monitor and proactively detect any potential cyber breaches against governmental and other critical national infrastructure systems*" (NCA, 2020, National Cyber Security Center).

Despite these 24/7 efforts, in early 2020 the U.S.–Saudi Business Council reported a prediction that 50-60% of Saudi Arabian organisations would fall victim to a cyberattack within the year. The public sector is a frequent and favourite target of cyber criminals, with phishing being the weapon of choice (U.S.–Saudi Business Council, 2020). In 2020, a new variety of CSE threat emerged: COVID-19 related phishing scams. A report by the Mimecast Threat Intelligence Centre found that between January and March 2020, global monthly volumes of spam and opportunistic cybercrime detections increased by 26.3%, while impersonation fraud detections increased by 30.3%. In the Middle East specifically, the Mimecast found increases in malware (22%) and spam (36%) during February and March, corresponding to the first appearance of the virus in the region. They reported a seven-and-a-half-fold "*increase in unsafe clicks during the first three months of year — likely as a result of a rise in human error caused by stress, unusual working environments and our desire to stay informed*" (Gevers, 2020). The Saudi government is trying to address this ongoing concern by modernizing its information security governance, increasing spending on cybersecurity, and encouraging the participation of private cybersecurity firms. If organisations were able to understand and identify the factors that make their employees susceptible to such threats, this would go some way towards mitigating the risks.

1.8 Literature Review Process

The literature review for this thesis started with a broad approach. The intent was to scan databases of existing recent academic and industry literature in order to unearth books, articles and reports pertaining to the topic of "*social engineering via email or SNS*". The reason for including "*email*" as a key term is because, like SNS, email applications require registration, engagement and communication. Most major email providers have – retroactively in some cases – followed the pattern set by SNS apps by encouraging or even requiring users to create public-facing profiles and to display a photo of themselves in their profile. The search used key terms such as *social engineering, deception, influence over the internet, cyber-attacks* and *vulnerability/susceptibility*. The search aimed for research

published in journals, conference proceedings and PhD theses, as well as industry reports. In particular, it focussed on research that presented models (some were tested, others only proposed) positing explanations for relationships between certain factors. From there the search branched out to include research and theories involving those factors. The literature review then funnelled down to models and attacks carried out on SNS and emails, and whatever variables these models encompassed.

1.9 Thesis Outline

This thesis consists of six chapters, summarised as follows:

Chapter One is the present chapter; it introduces the research topic, states the aims and significance of the study, states the problem and poses the question to be investigated, defines the scope of the study, and provides an overview of the Saudi Arabian context. This outline of the thesis is also presented.

Chapter Two presents a review of the literature. It introduces the general background and key concepts of the field of Information System Security (ISS), including definitions. It also provides brief context in order to help the reader understand the concepts from which the topic of social engineering is derived. A presentation of the thesis study-focus follows and will include definitions and the core concept of susceptibility to cyber-social engineering (CSE). The literature review then discusses relevant studies that have investigated user susceptibility to CSE. The various factors, frameworks and models developed in these studies are presented and their constructs are identified. A number of research strands emerge from the literature review and are categorised into studies that examine CSE susceptibility or risk vulnerabilities related to personality, cognitive psychology, users' personal dispositions, and contextual and demographical aspects.

Chapter Three is the theoretical conceptualisation. It presents a justification for the research model and provides an explanation of how the hypotheses of this research are formulated and are presented in a conceptual framework.

Chapter Four presents the research methodology. It proceeds to discuss the philosophical assumptions and research strategies underpinning this study. The predominant philosophical assumptions are looked at and presented; the epistemological stance adopted for this research project is the pragmatic approach, which combines fundamentals of both positivism and interpretivism. The chapter describes the adopted research methodologies

and research design, instruments, data collection and sampling techniques, and modes of analysis that are used in this research. This chapter also describes the research method used to collect the required data, which involves mixed methods, consisting of a quantitative study (questionnaire) followed by a qualitative study (semi-structured interviews) as well as the single case study and sampling techniques used in this research. Data preparation practices and an introduction to the data analysis procedures are also described.

Chapter Five presents the statistical analysis of the data and the study findings. It begins with descriptive statistics of the demographic profile of the sample. It proceeds to the inferential phase, in which both the quantitative and qualitative data, collected via the survey questionnaire and semi-structured interviews, respectively, are analysed.

Chapter Six discusses the findings of the study with respect to the research question and hypotheses. At the end of this chapter a framework is presented that is an extension of the model put forth by Saridakis *et al.* (2016). This extension consists of factors mostly responsible for employee susceptibility to CSE on LinkedIn, and is the main contribution of this thesis. This chapter reviews the contribution of its findings, which include the extended theoretical model. The contribution of the research to theory and practice is asserted.

Chapter Seven presents the implications of this study. The chapter also discusses the limitations of the study and provides some suggestions for future research. Finally, the chapter proposes some recommendations for practice that emerged from this study.

2. Literature Review

This chapter begins by describing the literature review process for this thesis. It then introduces the general background and key concepts of the field of Information System Security (ISS), including definitions. It also discusses the context from which the concept of social engineering is derived. A presentation of the study-focus of this thesis follows, and includes definitions and the core concept of susceptibility to cyber-social engineering (CSE). Cialdini's seven principles of influence (Cialdini, 2016) are introduced and described in detail in this chapter. These principles are useful in describing user susceptibility to CSE and thus facilitate an understanding of the approaches taken by CSE attackers. The review then discusses relevant studies that have investigated user susceptibility to CSE. The various factors, frameworks and models developed in these studies are presented and their constructs are identified. A number of research strands emerge from the literature review and have been categorised into studies that examine CSE susceptibility or risk vulnerabilities as they relate to personality psychology, users' personal disposition, and contextual and demographical aspects.

2.1 Literature Review Process

Bryman (2012) advised that the next step after formulating the research question(s) is to conduct a review of the literature. Neuman (2014) asserted that the premise of the literature review process is "*the idea that knowledge accumulates and that we can learn from and build on what others have done*" (p. 126). The purpose of the literature review is to identify (1) what is already known about the topic of interest, (2) relevant concepts and theories, (3) research methods and strategies previously employed in studying this area, (4) any important controversies and (5) any substantive inconsistencies in findings (Bryman, 2012, p. 98).

The literature review for this study began with a broad approach. The intent was to scan databases of recent academic and industry literature in order to unearth books, articles and reports pertaining to the topic of "social engineering via email or SNS". The reason for including "email" as a key term is because, like SNS, email applications require

registration, engagement and communication. Most major email providers have – retrospectively in some cases – followed the pattern set by SNS apps by encouraging or even requiring users to create public-facing profiles and to display a photo of themselves in their profile. The search used key terms such as *social engineering*, *deception*, *influence over the internet*, *cyber-attacks* and *vulnerability/susceptibility*. The search preference was for peer-reviewed articles published in journals, conference proceedings and PhD theses, as well as industry reports. In particular, the search focused on research that presented models (some were tested, others only proposed) positing explanations for relationships between certain factors that influence susceptibility to online social engineering fraud. From there the search branched out to include further research and theories involving those factors. The literature review then narrowed down to models and attacks carried out on SNS and emails, and whatever variables these models encompassed. Research that addressed user susceptibility generally was included, but the review focused on user susceptibility in email and SNS contexts, with a particular interest in the SNS context. Works excluded from this review comprised research focussed on the following: the perspective of the social engineer, the semantic detection of attacks, countermeasures that prevent social engineering attacks, and social engineering awareness frameworks, as well as highly technically-orientated studies, such as algorithms that identify phishing emails.

The following databases were searched: Scopus, Web of Science, IET Inspec, dblp computer science bibliography, Google Scholar, Saudi Digital Library, Saudi Open Data, and the Mendeley community crowd-sourced research database. The time period included in the search was from 2000 to the current date. More recent literature (2010 and later) was preferred for the literature presenting or evaluating frameworks relating to susceptibility to social engineering in cyberspace.. However, literature published prior to 2010 was considered if it presented theoretical foundations or extensions (e.g., Fishbein and Ajzen, 1975; Goldberg, 1990; Trumbo, 2002; Parrish, Bailey and Courtney, 2009), or is considered seminal work (e.g., Straub, 1990; Cialdini, 2001) and/or written by key authors in their fields (e.g., Mitnick and Simon, 2001; Workman, 2008).

The literature review process was iterative, and generally followed the steps described by Algarni (2016, p. 27). Figure 2-1 illustrates the cycle.

Figure 2-1 The Literature Review Process (adapted from Algarni, 2016)

2.2 Information System Security

Information system security (ISS) is a blended term consisting of two computer science terms: information systems and the security of information systems. The first part (IS) was defined by Cherdantseva and Hilton (2013) as

> "*a socio-technical system, which delivers information and communication services required by an organization in order to achieve business objectives. In general an IS encompasses six components: (1) information and data, (2) people. (3) business processes, and information communication technologies (ICT), which include (4) hardware, (5) software, and (6) networks*" (p. 547).

The field of interest in this thesis is information systems security; it is commonly mentioned synonymously in the literature as two terms: information system security (ISS) and information security, which is often shortened to InfoSec. There is a great variety in terms of how information system security has been defined by authors within the literature. The international organisation of standardisation (ISO) defined information system security

(ISS) as "*the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investment and business opportunity*" (ISO/IEC 27002:2013). The United States Code 44, Section 3552(b)(3) defined information security as:

> *"protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: A. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; B. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information, and C. Availability, which means ensuring timely and reliable access to and use of information"* (US Code, 2014, 3552(b)[3]).

According to Rao and Nayak (2014), information security (InfoSec) is a set of methodologies and processes which involve three indispensable components: people, organisation (policies and processes) and technology (Figure 2-2).

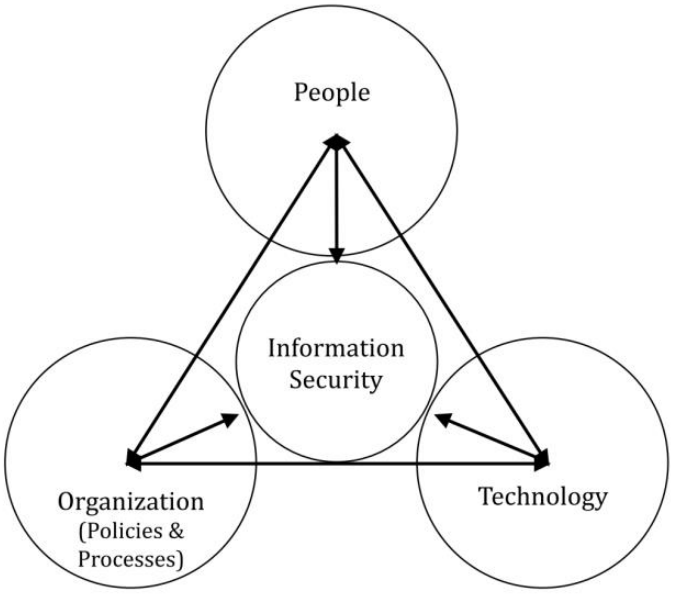


Figure 2-2 People, processes and technology triad for information security

Source: Rao and Nayak (2014, p. 43.)

Good cybersecurity is essential for all, but particularly for businesses and organisations that store sensitive data, from financial information to the personal details of clients, patients or

civilian records. Cybersecurity breaches can happen because of insufficient protection that lets in attackers or because users unintentionally give them access (Mundie, 2014). Major organisations and businesses typically have high levels of cybersecurity, but if the employees using their systems are susceptible to attack, even when away from work using their own social media platforms, cyber breaches can then become more likely. The Ponemon Institute (2012, p. 7) reported that 39% of organisations' security breaches are the result of "human error". For example, Yokoyama (2016) argued that if "*employees use external SNS to discuss internal problems, there is a risk of information leakage. One message containing secret data, as well as photos or videos containing training confidential data can bring problems of information leakage*" (p. 5*)*. This leaked information could potentially be used by cyber attackers to create a large, sophisticated attack campaign on the entire company (Symantec, 2013; ISMG, 2016). LinkedIn is an attractive SNS platform for cyber-social engineering attacks (term defined below, in Section 2.3) because it hosts the professional profiles of employees, which sometimes include their official company email addresses and display other credentials that can be exploited through a number of cyber-social engineering methods (Wilcox, Bhattacharya and Islam, 2014; Silic and Back, 2016).

People are an essential element of the three classified components of the of ISS triangle (see Figure 2-2). Specifically of interest is how they would act, react and behave as users within an organisation when exchanging content in the context of cyberspace. Naturally, the human factor in ISS/Information Security has been the subject of research for almost as long as ISS has been in existence (e.g., Martin, 1973; Madnick, 1978). Early research, however, was not grounded in theory and/or did not investigate causality (Straub, 1990; Pahnila, Siponen and Mahmood, 2007). Straub (1990) sought to fill this gap with his Security Impact model. Straub's model was based on general deterrence theory, which posits that "*the practice of instilling fear in people […] will prevent them from committing crimes in the future*" (Legal Dictionary, 2017, general deterrence). Thus, the focus was on the perpetrator, not on the user who would be the potential victim. More recent research on the human element in ISS has emphasised the role of the user (Qin and Burgoon, 2007; Herath and Rao, 2009a, 2009b; Safianu, Twum and Hayfron-Acquah, 2016; Hadlington, 2017) and examined aspects such as individual differences, personality traits and cognitive abilities (Parsons *et al.*, 2010). These factors are discussed in further detail in Sections 2.7 and 2.8 of this chapter.

In this research context, users' actions and interactions on social networking sites (SNS), and specifically career-oriented social networking sites (COSNS), are of interest. In particular, this research delves into the role(s) played by an individual's personal characteristics and other factors of employee susceptibility to cyber-social engineering (CSE) victimisation when accessing professional SNS. Researchers have begun to pay more attention to users' online behaviour and surrounding environments, and the impact of these on cybercrime, phishing victimisation and susceptibility (Lacey, Salmon and Glancy, 2015; Saeed *et al.*, 2019). Indeed, it has been frequently declared that human nature remains an insider threat to any organisation – the weakest link in the organisation or company's InfoSec defence (Hu, West and Smarandescu, 2015; Vishwanath, Harrison and Ng, 2016) because we are "*not as careful as we know we should be*" (Mueller, 2009, 00:05:60). Rao and Nayak (2014) contended that 80% of security incidents originate from insiders/employees; in *The InfoSec Handbook*, they defined a security threat as "*anyone or anything that poses danger to the information, the computing resources, users, or data. The threat can be from 'insiders' who are within the organization, or from outsiders who are outside the organization*" (p. 31).

Possibly one of the most successful technical ploys to encourage users into divulging their social media profile usernames and passwords is through "*prompting victims to input user and password information in pop-up windows*" (Conteh and Schmick, 2016, p. 34). Other common and effective tactics involve phishing links (Das *et al.*, 2019) or impersonated profiles of acquaintances on SNS such as LinkedIn (McBride, Carter and Warkentin, 2012; see also Section 2.3). People tend to be socially influenced (Wei, Zhao and Zheng, 2019) and can, due to either good intentions or a trusting nature, at times be willing to expose and share a password or personal private information. They do this as a result of a trick or simple persuasion, without realising that they are unlocking a secured gate when responding to malicious cyber-social engineering tactics. Attacks by exploiting human inattentiveness can lead to serious consequences when personal or organisational private data is compromised.

Safianu *et al.* (2016) posited that "*humans are important factors that affect information securities effectiveness […] security is not solely a technical problem*". Users have to use their experience and control their behaviour along with using their perceptual and cognitive skills to detect the intentions of others (Vishwanath *et al.*, 2011). This can be very challenging in a hectic modern-day environment. Table 2-1 provides some examples of

risks that could occur in an organisation. As can be seen from this table, bad actors may be either internal or external to the organisation. Fraudsters can bypass organisational systems by taking advantage of people who are unwary or have other personal weaknesses that are then seized upon by the perpetrator. Means of exploiting human weaknesses via the Internet are referred to collectively as *cyber-social engineering*, and this phenomenon is described and explained in further detail in Section 2.3.2.

Table 2-1 Examples of Internal and External Threats to Information Security

Internal Threats	External Threats
- Fraud, misuse of assets or information - Errors or mistakes by employees - Espionage, shoulder surfing - Social engineering by employees - Exploitation of lack of knowledge or ignorance of fellow employees - Use of weak administrator passwords or passwords of others and gaining unauthorized access - Theft - Policies not executed or followed - Improper segregation of duties, leading to fraud or misuse - Malware infection threats due to infected media usage or unauthorized software downloads	- Social engineering - Attack by hackers/man in the middle - Blackmail, extortion - Espionage

Source: Rao and Nayak (2014, pp. 34-35)

2.3 Definitions of Key Terminology

This section defines some important terms that are used throughout the thesis.

2.3.1 Social Engineering (SE)

Mitnick and Simon (2001) defined social engineering as a practice in which a person:

> *uses influence and persuasion to deceive people by convincing them that the social engineer is someone he [or she] is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.* (p. iv)

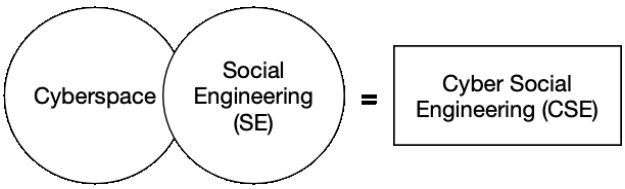
Mouton *et al.* (2014) defined SE as "*the exploitation of humans in order to gain unauthorized access to sensitive information*" (p. 266). The process of such exploitation

encompasses both psychological persuasion and technical tactical knowledge. SE was described by Gragg (2003, p. 4) as a "*method or technique that can be complex and diverse*". He suggested that its complexity lay in attackers having a deep understanding of various illicit technical tactics, alongside the skills of persuasion (see Section 2.7).

These definitions of SE give the impression that it is wholly negative and always used for nefarious purposes, and indeed, this study examines only the negative effects of social engineering. However, SE may also be used for benign and even positive purposes. Social engineering can be a useful tool for governments, NGOs and other organisations to effect positive behavioural changes in individuals' health, financial and social habits, using tactics applied within social marketing. SE interventions can be applied by legislators to shape and change citizens' behaviours, and consequently the society, for the better. SE can be employed to create an effective social reaction, such as warning labels on cigarette packets, or fake speed cameras on highways (Kennedy and Parsons, 2012).

2.3.2 Cyber-social Engineering (CSE)

Cyber-social engineering (CSE) consists of scams leading to the victimisation of individuals who have the propensity to be deceived and manipulated via the various means of communication on the Internet. The International Police (Interpol.int) consider social engineering scams to be crime and have broadly described them as "*fraud*". Such attacks "*are carried out online – for example, by email or through social networking sites*" (Interpol, 2015, p. 1). These occur when criminals seek to exploit the trust of individuals in order to retrieve their "*bank details, passwords or other personal data*" (Interpol, 2017). Therefore, social engineering is a crime in both the real world and cyberspace. For the purpose of this research, the blended term *cyber-social engineering* (CSE) is used in order to distinguish the cyberspace version from social engineering (SE).. In this thesis, the term *cyber-social engineering* and its abbreviation, *CSE*, are used whenever the specific phenomenon of *social engineering in cyberspace* is discussed, whether by other researchers or by this researcher.



CERT-UK (acronym for the UK government's Computer Emergency Response Team) described social engineering in the context of cyber-security as a tactic with the main purpose of deploying a network attack to deliver malware or persuade gullible, curious, acquiescent, greedy or otherwise vulnerable individuals to give out personal information. This is achieved by using techniques such as phishing emails or online impersonation (CERT-UK, 2015, p. 3).

2.3.3 Susceptibility

The *Oxford English Dictionary* defines *susceptibility* as the likelihood of an individual "*to be influenced or harmed by a particular thing*" (*OED*, 2020a, susceptibility). *Susceptibility* is a term used interchangeably in the CSE literature with *vulnerability*. In the domain of InfoSec research, a susceptible individual is more likely to be gullible (CERT-UK, 2015) and will have an increased chance of being fooled, often by a persuasive scheme and sometimes without reasonable proof (Greenspan, 2009; Bullée *et al.*, 2018). Albladi and Weir (2018) defined susceptibility with regard to CSE as "*a set of user attributes that incline […] a user to be a victim of social engineering attacks*" (p. 4). A number of researchers (Dalal and Gorab, 2016; Dreibelbis *et al.*, 2018) have mentioned CSE susceptibility in connection with counterproductive workplace behaviour. (CWB) is behaviour by a member of an organisation that results in harm to the organisation or to its members (Martinko, Gundlach and Douglas, 2002; see Chapter Three, Section 3.4.1). In discussing CSE susceptibility, it is useful to borrow some terminology from Martinko *et al.*'s (2002) work on CWB. The attributes that can influence the success of victimisation can be internal to the individual: *individual differences*, such as human factors in the shape of personality traits, or external: *situational variables*, such as culture and organisation (Martinko *et al.*, 2002, p. 38).

2.4 Social Engineering Approaches

While social interaction has evolved from the physical to cyberspace settings in many respects, so also has social engineering. According to Seidenberger (2016), social engineering can take place in four different ways (see Fig. 2): First, there is *offline* SE, such

as the cases of Frank Abagnale[1] and James Hogue[2]. The second type is *offline-to-online*, such as baiting, which involves the attacker deliberately leaving an attractively labelled flash drive containing malware in a designated place, awaiting an inquisitive victim. A third social engineering approach is fully *online*, taking the form of social media imposters, profile cloning, clickjacking (McBride *et al.*, 2012), phishing/spear phishing and farcing (Vishwanath, 2015a). The fourth approach is *online-to-offline*, and involves acquiring personal information through a method such as cyber-humint[3] (cyber human intelligence), a term first used by Alcantara (2010).

Some approaches involve physical social engineering, such as pretexting; however, as the emphasis of this thesis is on cyber-social engineering, the emphasis will be on cyberattacks. The most common types of CSE attacks are described in further detail in Section 2.5. Figure 2-3 shows how these approaches have evolved, starting from offline SE to CSE, to offline SE and then back. The arrow (→) shows how the approaches have evolved.

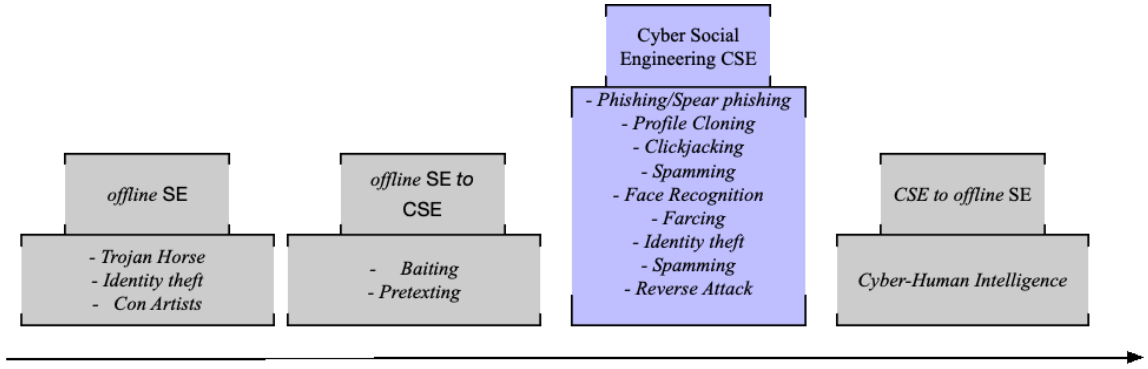


Figure 2-3 Social Engineering Approaches. Adapted from Seidenberger (2016, p. 6)

CSE attacks are typically launched over four phases, as presented in the next section.

[1] A popular US con artist and impersonator known to have defrauded authorities with crimes associated with bad cheques via the use of social engineering. He was subsequently hired by the US Federal Bureau of Investigation (FBI) for his expertise gained from his fraudulent criminal past. Abagnale's life was partially depicted in the film *Catch Me If You Can* (Biography.com, 2014).

[2] An infamous con man listed among the top 10 imposters by *TIME* magazine, most notably for deceiving his admissions committee to Princeton Univ. and making it through to the dean's list. He was later charged with forgery, falsifying records, and wrongful impersonation (Schmidt, 2017).

[3] Cyber-humint is defined as an advanced social engineering trajectory, where an offender combines espionage operations and persuasion skills in cyberspace to collect data about an unsuspecting target's digital footprint of their online activities, such as livestreaming, posted on their social networking account. It can also be used to supplement other real life espionage collecting methods (Forrester and den Hollander, 2016; Seidenberger, 2016). It is a social engineering approach that utilises the cyber network to collect information on particular physical targets.

2.5 Phases and Types of CSE Attack

According to Mitnick and Simon (2001), there are four phases to a social engineering attack. The initial phase, research, refers to the process of data collection from the target. The second phase is focused on trust-building through persuasion between the attacker and the target. In the third phase, various techniques are employed to seduce the intended victim, including misinformation, misrepresentation, and the use of language familiar to the target; these actions demonstrate empathy, provide a sense of validation, or satisfy a need for attention. Once trust is gained, the attacker can finally exploit this virtual bond and use the information gleaned in the final phase to attack the unsuspecting victim (Mitnick and Simon, 2001). In the context of CSE, the process is as follows:

- Phase 1: Collection of factual information about the potential victim being exploited, studying individuals and businesses associated with the target to unveil potential vulnerabilities (Muniz and Lakhani, 2013).
- Phase 2: Entrustment; process of communication, forming a trusting relationship with the unsuspecting victim via persuasion.
- Phase 3: Exploring and analysing the unsuspecting victim via relationships aimed at manipulation in order to compromise the system (Patel, 2013; Samani and McFarland, 2015)
- Phase 4: Finalisation of interaction with the potential victim, without arousing suspicion, through the execution of CSE attacks (Samani, 2010).

Descriptions of commonly used CSE methods are presented in Table 2-2.

Table 2-2 Examples of CSE methods

Types of attacks by Social Engineers on SNS	Description
Phishing/ Spear Phishing	The most common attack using email (Microsoft Report, 2018); increasing in SNS environments (Nagy and Pecho, 2009). Can be launched in the form of a malicious link sent via a LinkedIn InMail or private message feature (Muncaster, 2017). Phishing relies on elements of manipulation and exploitation of trust (Junger *et al.*, 2017) and aims to collect sensitive personal data such as passwords (Kontaxis *et al.*, 2011). According to the annual "State of the Phish" report (Proofpoint, 2018), in 2018 76% of organisations were deemed susceptible to phishing schemes.
Profile Cloning (Impersonation)	Typically launched via SNS. It is carried out by using publicly viewable credentials, personal information, posts, shared content, likes, etc., to create new forged profiles that are identical to original existing profiles. These fake profiles are used to deceive others (Bilge *et al.*, 2009).
Clickjacking	This is a serious CSE threat on social networks, as it can cause damage to the stolen credentials of unsuspected users. It consists of two types, as detailed by Rehman *et al.* (2013): - *Cursorjacking*: Hijacking the pointer movement. This uses a page or profile embedded code, which runs by fooling the user into thinking that the pointer appears to be clicking on a seemingly harmless button that has another function (Goodey, 2015). - *Likejacking:* A SNS enabled technique, sometimes in the form of a flashing ad that attracts the user to click the concealed malicious hyperlinked "like" button. It can appear as a Facebook, Twitter, or LinkedIn likes.
Face Recognition	Some online users, aware of lurking danger on cyberspace, make their SNS profile viewable only to known connections, although their profile picture is still publicly visible. Cyber-social engineers can download a profile photo and use face recognition software to identify the user from other websites that provide more PII about the target, such as their profile on a company website (Fire et al., 2013). This is not hypothetical: Millions of people uploaded photos to what they thought was a cloud storage app; the company used those photos to develop facial recognition tools, which they sold to third parties (Solon and Farivar, 2019).
Spamming	By exploiting public posts, attackers can lure more connected users to view and accept a message, never suspecting the threat (Wasson-Blader, 2009; Zhu *et al.*, 2012).
Farcing	A form of cyber espionage via SNS. It consists of two stages. Stage 1: the attacker creates a phoney SNS profile; Stage 2: attacker sends a friend request. This method is often used by attackers wishing to access a particular unsuspecting victim whose profile is not public (Vishwanath, 2014; Palmer, 2017).
Reverse Attack	Requires an influential scenario wherein the social engineer attacker waits for the unsuspecting target to initiate the first communication request. In the SNS context, the potential victim assumes the fake profile is someone familiar and then initiates contact with the attacker (Irani *et al.*, 2011).

As can be seen in Table 2-2, cyber-social engineering relies on the element of manipulation (Mouton *et al.*, 2014) until trust is formed with an unsuspecting victim (Hadnagy, 2011). When trust has been established, the attacker uses an orchestrated scenario to deceive the targeted victim. Attacks often follow Cialdini's (2001; 2016) principles of influence: these principles are discussed in more detail in Section 2.7. This type of internet crime has a financial impact on organisations that are infiltrated through an unsuspecting employee; in early 2016, the Internet Crime Complaint Center at the US Federal Bureau of Investigation (FBI) reported that social engineering and associated cybercrimes cost companies of all sizes across 108 countries more than USD 2bn between October 2013 and February 2016 (Scannell, 2016).

2.6 CSE Attacks on Social Networking Sites

SNS have continued to grow in popularity as a means of person-to-person communication. As early as 2016, it was reported that 25% of the total time spent on the internet was on SNS (GlobalWebIndex, 2016; Warner-Søderholm *et al.*, 2018). see Section 2.8.4.1). In 2012, people spent an average 90 minutes per day on SNS; by 2017, that had increased to 2 hours and 15 minutes (Metev, 2020). It is estimated that in 2020, people spent an average of 2 hours and 24 minutes per day on SNS (Broadband Search, 2020). Moreover, compared to email, SNS communications reveal a great deal more of a user's character, as well as personal information and interactions in terms of posts, shares and private messaging. Phishing attacks or online scams, a common CSE technique, have become easier to launch, since personal information can at times be publicly accessed from SNS (Choo, Smith and McCusker, 2007). Thus, it is easy to see how SNS are an attractive medium for CSE attacks, such as phishing links and impersonation (Nagy and Pecho, 2009; Chitrey, Singh and Singh, 2012; Algarni, 2016). Account login credentials, credit card or bank account details and general PII are among the sorts of data harvested by cyber-social engineers via SNS; such information becomes the basis for further CSE attacks (Trend Micro, 2020).

In the email environment, several studies have investigated the roles played by user characteristics and message characteristics on users' susceptibility. Halevi *et al.* (2015) performed a spear-phishing experiment on 40 employees of a large company in India. They found that people who were more conscientious were more likely to respond to a targeted phishing email that appealed to their sense of order and efficiency. The authors found that women in general had a higher susceptibility to phishing emails. Interestingly, Halevi *et al.*

(2015) reported that "*people who underestimate their [own] susceptibility may be more likely to be attacked*" (p. 7). In this same study, Halevi *et al.* (2015) also investigated the effect of "*computer-mediated communication competence*" (p. 2) on susceptibility and found no correlation. In contrast, Kleitman, Law and Kay's (2018) results showed little effect from personality and gender, but "intelligence" (participants took an intelligence test as part of the study) and "*knowledge of computers and phishing*" were significantly correlated with lower susceptibility. Goel, Williams and Dincelli (2017) reported that messages designed "*to appeal to recipients' psychological weaknesses [specifically, the] fear of losing or anticipation of gaining something valuable increased susceptibility*" (p. 22). Regarding message characteristics, Blythe, Petrie and Clark (2011) reported that successful phishing emails used convincing-looking logos, as well as formatting and images that approximated those found in actual official communications.

2.6.1 CSE Attacks on Organisations via SNS

CSE presents a serious threat to information and personal security due to the growing tendency for fraudsters to exploit and misuse social networks and virtual communities (Scott, 2017). According to Mills (2009), social networking sites are considered the new "*battleground*" for cyberattacks, since personal, employment, and other geographic and demographic information are exposed. He stressed that such sites "*can be used as a means of social engineering against not only that person but any organization's information security with which this individual is affiliated*" (Mills, 2009, p. 139). Susceptible users on SNS platforms are perceived as being unaware of potential threats; they do not suspect communication from an unknown origin, or even believe that they are susceptible to manipulative CSE (Sanders, 2016). This vulnerability leaves organisations open to attack (Wilcox *et al.*, 2014).

For businesses that increasingly rely on remote collaboration, online channels of communication, and online platforms and tools for virtual communication, CSE poses a serious threat to the security of the organisation's data centres. This corresponds with the growing trend towards BYOD, or "*bring your own device*", which is linked by Krombholz *et al.* (2015) to "*policies and the use of online communities, communication and collaboration tools in private and business environments*". Combining online tools in both private and business environments provides cyber attackers with many new opportunities for malicious activities.

This threat has become even stronger in the time of the COVID-19 pandemic, during which, according to a survey by business research firm Gartner, 88% of businesses and organisations worldwide have "*mandated or encouraged all their employees to work from home*" (Marinova, 2020, Item 2). In a recent survey by IT security firm Tessian of 250 IT decision-makers in the US and the UK, 82% of IT leaders believed their companies to be at greater risk of phishing attacks due to employees working from home (Tessian, 2020). The primary causes of concern were increased incidence of phishing attacks, BYOD risks, employees connecting to public Wi-Fi, and increased use of email and messaging apps (Williams, 2020a). Their fears are apparently justified: NORDVPN reported that according to the US FBI, the average number of daily cyberattacks had increased 400% compared to pre-pandemic levels (Williams, 2020b). Furthermore, the annual Secureworks Incident Response report highlighted that "*cybercriminals are targeting vulnerabilities created by the pandemic-driven worldwide transition to remote work*" and that "*[t]hreat actors including nation-states and financially-motivated cyber criminals are exploiting these vulnerabilities with malware, phishing, and other social engineering tactics*" (Williams, 2020c, paragraphs 3 and 7).

A case in point: in November 2020, Microsoft warned its office software subscribers that organisations were being specifically targeted by cybercriminals aiming to harvest login credentials. They described attacks that "*leverage social engineering attempts and a range of sophisticated means to evade detection. The phishing emails use timely lures to impress urgency and are tied to remote work, password updates, conference call information, helpdesk tickets, and other pressing matters*" (Davis, 2020, paragraphs 2-3). Also in response to the remote working boom, the time-honoured "Account Suspended" phishing scam has been directed at users of videoconferencing apps like Zoom, Google Meet and Microsoft Teams. Such messages are sent out via SNS, email or text message, and they contain authentic-looking URLs and logos. They typically urge the recipient to immediately click on the provided link in order to "reactivate" their account (Meyer, 2020). Variants of this tactic are messages stating that "you missed a meeting" or that "you're invited" to join a meeting. The links in these messages either download malware or direct the victim to a fake login page where their login credentials are harvested (Meyer, 2020).

2.6.2 CSE Attacks on LinkedIn

According to *Business Insider* magazine, LinkedIn is the most trusted of all the major social media platforms and has maintained this number one spot in trustworthiness every year from 2017 to 2020 (Schomer, 2019; Insider Intelligence, 2020). As of the last quarter of 2020, LinkedIn had over 200 million monthly active users; this CSNS platform had 546 million total accounts and was adding 5.26 million new accounts each month (Broadband Search, 2020). In their comparison of Facebook, LinkedIn, and Twitter, Kim and Cha (2017) found that the motivations for using these SNS differ. They identified five motivations for people to use LinkedIn:

1. *Expressive information networking*
2. *Boredom relief through entertainment*
3. *Escape through companionship*
4. *Professional advancement*
5. *Self-presentation* (Kim and Cha, 2017, p. 11).

Kim and Cha (2017) used the term "*expressive information sharing*" to refer to the informal, often emoticon-laced messages and images shared and exchanged on SNS, and they noted that this was a primary motivation for users across all SNS. In the LinkedIn context the authors called this "expressive information networking". According to Kim and Cha (2017), there are two motivations that are "*the most salient*" to LinkedIn (p. 15). These are *professional advancement* (helpful for career advancement, sharing work-related curriculum vitae posts, networking with other professional contacts, obtaining peer support from others) and *self-presentation* (providing personal credentials, introducing or telling others about oneself; Kim and Cha, 2017).

These motivations can be misused by a social engineer masquerading as an employer (Misra and Goswami, 2017), a job seeker, or indeed a colleague. Typical vectors of attack include connection requests, private messaging and InMail, and notification emails purportedly from LinkedIn (Gray, 2018). One such case involved an Irish engineer working for a company in Belgium. He was contacted on LinkedIn by someone posing as a recruiter; the impersonator used a cloned profile of an actual recruiter's authentic LinkedIn profile. The communication eventually moved from LinkedIn to email messaging, and the authentic-seeming fraudster presented him with a "firm offer" of an attractive position in Ireland. Convinced he had been hired, the victim quit his job, only to find out that the new

position did not exist. The duped engineer eventually found another job, but had lost several months' pay in the interim (Cleary and Kelly, 2017).

In accordance with the phases of social engineering attack (Mitnick and Simon, 2001), it is likely that CSE attackers will cultivate skilful influential messages to respond to these motivations based on the context. "*LinkedIn is a goldmine for cyber criminals and hackers, who can easily trawl through profiles to identify known vulnerabilities and details of organisational security infrastructure*" (Talent, 2016, paragraph 3). Most recently, researchers at ESET discovered cyber-attacks targeting military and aerospace companies in the Middle East and Europe that used LinkedIn messaging as a point of entry (Knowles, 2020). "*In order to appear credible, the attackers posed as representatives of well-known, existing companies in the aerospace and defense industry*" (Breitenbacher and Osis, 2020, p. 2). The attackers would send a LinkedIn message describing a job offer (Figure 2-4).

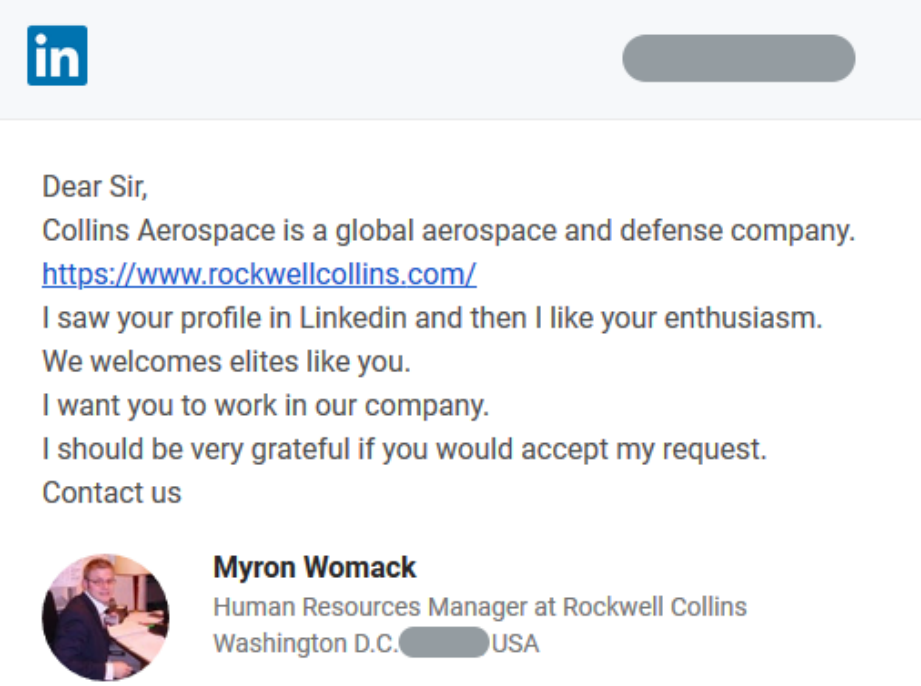


Figure 2-4 A "job offer" sent via LinkedIn to employees at a targeted company

Source: Breitenbacher and Osis (2020, p. 3)

As reported by *SecurityBrief* from the principal investigator,

> *the LinkedIn profile was fake, and the files sent within the communication were malicious. Once the recipient opened the file, a seemingly innocent PDF document with salary information related to the fake job offer was displayed. Meanwhile, malware was silently deployed on the victim's computer. In this way, the attackers*

> *established an initial foothold […]. Following this, the attackers performed a series of steps. Among the tools the attackers utilised was custom multistage malware that often came disguised as legitimate software, and modified versions of open-source tools. In addition, they leveraged 'living off the land' tactics, including abusing preinstalled Windows utilities to perform various malicious operations. The attacks we investigated showed all the signs of espionage…* (Knowles, 2020, paras. 6-11)

From the foregoing description, it is apparent that the perpetrators implemented all four phases of CSE attack (Section 2.5). Such attacks are becoming more frequent and sophisticated in cyberspace throughout the world (Das *et al.*, 2019), and Saudi Arabian organisations are increasingly vulnerable, as detailed in the next section.

2.6.3 CSE Attacks Targeting Saudi Arabia via SNS

According to Elnaim and Al-Lami (2017) and Sawahel (2015), the Kingdom of Saudi Arabia was listed amongst the top ten countries most vulnerable to cyber-attacks in the Middle East. Saudi Arabia is becoming an attractive location for investors due to its solid economy, status as host of major organisations in the region, strategic location, and high consumer spending. Hadi Jaafarawi of the California-based IT security firm Qualys stated that "*hackers are increasingly targeting data warehouses and social networking sites that contain valuable information, which they can then either hold for ransom or exploit for blackmail, extortion, coercion and other purposes*" (Hamid, 2017, paragraph 20).

According to a 2017 report by social media security firm ZeroFOX, the overall number of impersonation occurrences on social networking sites saw an 11-fold increase between December 2014 and December 2016. In Saudi Arabia, it is difficult to give an exact figure for the number of SNS attacks that took place, considering that it is estimated that 30% of phishing attacks that caused data breaches in the country were never reported (FraudWatch International, 2017). One series of connected CSE attacks that was discovered by a California-based cybersecurity firm, and reported in 2017 by the Saudi National Cyber Security Center (NCSC), was a cyber espionage campaign aimed at mining data from computers via email phishing techniques seeking the PII of targeted users (Auchard and Paul, 2017). Another was the campaign targeting Saudi LinkedIn users via the fake profile of a female named "Mia Ash", as detailed in Chapter One.

Financial loss due to cyber-attacks is an ongoing concern. More than USD 1bn in Saudi bank losses were recorded over a period of two years (Alarishi, 2012) due to data breaches

from various cybercrimes, including CSE. Citing an IBM report, the U.S.–Saudi Business Council highlighted that in 2019 the average cost to Saudi Arabia of each data breach was US $5.97 million, and the average number of compromised records per incident was 38,800, the highest in the world — in comparison, the global average was 25,500 records per incident (U.S.–Saudi Business Council, 2020).

This continuing problem could be the ramification of failures on the part of employees and managers to accurately assess the importance of the safe use of computer networks within an organisation. To this point, Alzamil (2012) found that managers and subordinates in Saudi Arabia require frequent training in security risk perception due to their misconceptions about the influence of humans within an organisation. According to Alzamil (2012):

> *Most organizations focus on the technologies aspect in information security rather than human aspect to protect their information assets from any vulnerability that may lead to possible attacks. Such results required very urgent actions from the top management of many Saudi organizations.* (p. 51)

Again, this is an ongoing problem for Saudi organisations, and the public sector is a clear target of cybercriminals. According to the first summary report issued by the newly established NCSC, in the third quarter of 2017 more than half of the cyber-attacks were on government entities, and of these, "*intrusion attempts represented most of these threat alerts with 59%*" (Ministry of Communications and Information Technology [MCIT], 2018a, 99093). In their next quarterly report for the fourth quarter of 2017,

> *the number of the Threat Alerts was slightly higher (7%) as compared to the third quarter of 2017. 'Malicious Code', 'Unauthorized Access' and 'Information Leakage' showed an increase, which indicates that the threat actors were successful in gaining access to affected systems. Moreover, it* reflects the threat actors' current objective in harvesting credential and identity information. (MCIT, 2018b, 99558; emphasis added)

NCSC's next report, for the first quarter of 2018, noted an increase in the number of attacks and cyber-threats compared to the previous quarter, and that "*malware and hacking attempts represented most of the cyber-threats. This indicates that attackers wanted to stay within the affected networks for as long as possible*"; moreover, there was "*a significant increase in the use of malware, indicating that the hackers were using new tools and*

methods to access and damage sensitive information" (Taher, 2019, item 1). "*During the same period, government agencies were the most targeted, followed by institutions within the education sector and the telecommunications sector*" (Taher, 2019, item 2). Thus, the NCSC reports showed a clear upward trend in the number of cyber-attacks on government institutions aimed at accessing sensitive data.

An industry report by Tenable in August 2020 showed that a lack of knowledge and understanding of cybersecurity on the part of companies in Saudi Arabia was a likely factor in the high number of successful cyber-attacks (Kelly, 2020). This brings the discussion back around to the human element in the ISS triangle, and the CSE tactics used by perpetrators to gain entry to their target sites.

2.7 Principles of Influence in Cyber-social Engineering: Understanding Offender Psychological Tactics

Persuasion is the process of using communication to induce someone to change their attitude (Lumen, 2020). Persuasion theory is an area of research in social psychology and is generally concerned with the relationship between attitudes and behaviours (Ajzen and Fishbein, 1980). According to Gardikiotis and Crano (2015), a number of prominent theories of persuasion are grounded in broader approaches such as learning/conditioning (e.g., Hovland, Janis and Kelley, 1953) and consistency/cognitive dissonance (e.g., Festinger, 1957). Two influential theories of persuasion that consider how attitudes predict behaviour are the theory of reasoned action (TRA; Fishbein and Ajzen, 1975), and theory of planned behaviour (TPB; Ajzen, 1985). These theories are discussed in further detail in Chapter Three, Sections 3.1.2 and 3.1.3, respectively.

In an experiment carried out on passers-by in a shopping district, Junger *et al.* (2017) showed how personal information (such as email address, partial bank account number, and details of recent online purchases, including name of webstore) could be accessed relatively easily through manipulative and persuasive tactics via an in-person "survey". Montañez, Golob and Xu (2020) noted that persuasion was a central concept in cognition-based theories of the psychology of cybersecurity. Cognition is commonly defined as "*the mental action or process of acquiring knowledge and understanding through thought, experience, and the senses*" (OED, 2020b, cognition). A prominent theory that takes a cognitive approach (i.e., how cognitive processes enable or inhibit persuasion) is the elaboration likelihood model (ELM; Petty and Cacioppo, 1986). Robert Cialdini's

principles of influence (2001, 2016) resulted from his collaboration with Petty and Cacioppo (Cialdini, Petty and Cacioppo, 1981); his principles are based on ELM (Stoltenberg and McNeill, 1984; de Jong, 2018).

Cialdini's principles are commonly used in marketing, as they have been shown to be effective in enticing people to purchase a product and thus promote sales (Cialdini, 2001, 2016; Shrum *et al.*, 2013). These principles include offering prizes and "warning" potential purchasers that the item is scarce and they risk missing out if they do not act quickly. However, these principles can also be used by cyber-social engineers to manipulate and entice unsuspecting victims to respond to CSE attacks (Ferreira, Coventry and Lenzini, 2015). Manipulation is considered to have a central role in persuading potential CSE targets (Alexander, 2016; Bullée *et al.*, 2018; Kee, 2008); the power of persuasion in influencing social behaviour was highlighted in the work of Simons (1976). Cialdini (2001, 2016), currently a leading expert in influence and persuasion, advanced Simons' research and developed a framework of influence tactics. This framework originally consisted of six universal principles of influence: *reciprocity*, *scarcity*, *authority*, *consistency and commitment*, *liking* and *social proof* (later renamed "*consensus*"). Cialdini (2016) later added a seventh principle: *unity* (Table 2-3). As he explained, this seventh principle emerged from his research over time (Cialdini, 2016).

Table 2-3 The Seven Universal Principles of Influence

Principle	**Explanation**
Reciprocity	People feel obliged to provide some service or material good to someone in return for what they have received from that person/entity.
Scarcity	People want more of those things they can have less of.
Authority	People follow the lead of credible, knowledgeable experts.
Consistency and commitment	People like to be consistent with the things they have previously said or done. Consistency is activated by seeking and requesting small initial commitments.
Liking	People prefer to say "yes" to people/entities that they like.
Consensus/Social proof	Especially when they are uncertain, people will look to the actions and behaviours of others to determine their own.
Unity	If people feel a shared identity with someone (as part of "us"), this leads to acceptance, trust, cooperation, liking, help and assent.

Source: Adapted from Cialdini (2016, 2020) https://www.influenceatwork.com/principles-of-persuasion.

Importantly, Cialdini (2016) stressed that timing is critical in effective persuasion; specifically, the influencer needs to lay the groundwork for the persuasive effort. In fact, Cialdini called it "pre-suasion – *the process of arranging for recipients to be receptive to a message before they encounter it.*" (2016, p. 4). This concept aligns with the four phases of CSE attack (Section 2.5), in which "*pre-suasion*" would happen during phases 1 and 2. Of the seven principles, unity and reciprocation, conjointly with consistency and commitment, are techniques commonly used by cyber-social engineers. As Ferreira *et al.* (2015) explain, these tactics often take the form of emails to launch malware.

These three principles are typically deployed in phases 2 and 3 of a CSE attack. In a CSE attack via LinkedIn, unity is often the first principle put to work, such as when the cyber-social engineer initially contacts the targeted individual, posing as someone in their industry or profession, a colleague (Section 2.6.2). However, it should be noted that the unity principle has not yet been empirically examined in social engineering research (Montañez *et al.*, 2020). Using reciprocity as a CSE tactic in the context of LinkedIn, the attacker has several options depending on the degree of connectedness s/he shares with the targeted individual. For example, if the attacker is only a second- or third-degree connection, they can "Like" or comment positively on their target's post. If the attacker has (by deception or otherwise) become a first-degree connection, he/she can perform more valuable favours, such as endorsing the target's professional skills, or even writing a spurious recommendation. Consistency can add a personal and informal feel over time (Ferreira *et al.*, 2015), and this can entice a vulnerable individual on SNS to provide valuable information (Algarni, 2016).

Quiel (2013) discussed the ways in which cyber-social engineers use these principles. The scarcity principle was used, for instance, in an incident reported by Independent.ie (2017) in which a cyber-social engineer posted a bogus job vacancy on LinkedIn with a link to apply. The job vacancy stressed that applicants must apply within a limited timeframe. Quiel (2013) explains that the social proof principle is used when a cyber attacker acts as a self-proclaimed expert in cybersecurity, purposely to connect with actual IT experts. This method enhances the trustworthiness of their profile, as the more people with whom the attacker is connected, the greater the social proof or consensus that the fake account is real. This also allows the attacker to benefit from the "liking" principle, which states that people tend to say "yes" to others whom they like. This principle helps users to feel comfortable,

making it more probable that they may link to a fake account because it shares familiar credentials or has an attractive profile picture (Wani and Jabin, 2018).

Similarly, the "authority principle" is used by social engineers to create profiles impersonating someone with high organisational status (Figure 2-5), which can also influence users (Frumento *et al.*, 2016; Khanna, 2016). Finally, reciprocity is a strong social norm that compels people to "repay" others for what they have received from them. This principle is used by cyber-social engineers in SNS when they offer a favour in advance of the attack in order to increase compliance (Algarni, 2016). In the context of LinkedIn, depending on the degree of connectedness the attacker shares with the targeted individual, the CSE attacker could endorse the skills of the intended target or simply "like" or comment favourably on something posted by the targeted user. According to the rules of reciprocity, the unsuspecting victim would then feel obliged to return the favour in some way. This form of persuasion can encourage a user to click on a malicious link (Quiel, 2013).

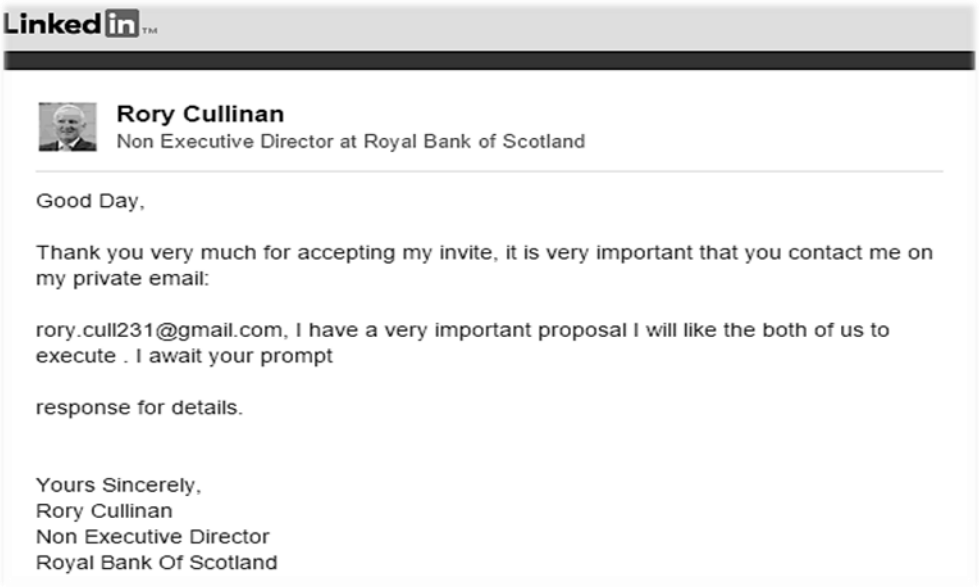


Figure 2-5 Nigerian Prince Scheme (or 419) via LinkedIn. Source: Solano (2015)

Studies have used these principles to identify the psychological concepts that explain a situation of influence, such as to raise sales in the marketing domain (Cialdini, 2001; Lystig Fritchie and Johnson, 2003; Gneezy, 2017) or as persuasion for various social behavioural changes (Seethaler and Rose, 2003; Jacob, Guéguen and Boulbry, 2018). Uebelacker and Quiel (2014) used Cialdini's principles of persuasion (there were only six in his framework at that time) to build a model attempting to explain how the Big Five personality traits (see

Section 2.8.1) may correlate variously with higher or lower susceptibility to CSE tactics in individuals. Their model is described in Section 2.9.1.3.

2.8 Susceptibility to Social Engineering in Cyberspace

A body of research has studied the human aspect and vulnerability/susceptibility to possible cyberattacks. A wide range of factors have been presented in the literature explaining why some users may be more susceptible to CSE. In their systematic review of the psychological factors of internet fraud victimisation, Norris, Brookes and Dowell (2019) found that these fell into three broad categories: dispositional, experiential and "message". The first two relate to the victim and the third category refers to the tactics of the attacker (p. 4). Norris *et al.* (2019) noted that there is some degree of interplay between these categories. In the literature on this subject carried out for this thesis, the prominent dispositional factors include personality traits (Parrish *et al.*, 2009; Bansal, Zahedi and Gefen, 2010; Darwish, El Zarka and Aloul, 2012; McBride *et al.*, 2012; Alseadoon, Othman and Chan, 2015; Albladi and Weir, 2017), (propensity to) trust (Hadnagy, 2011; Junger *et al.*, 2017), perceived control over information (Malhotra, Kim and Agarwal, 2004; Krasnova *et al.*, 2010), risk perception (Halevi *et al.*, 2016; Das *et al.*, 2019), risk propensity (Cases, 2002; Nguyen and Kim, 2017) and motivation (Workman, 2008; Williams, Beardmore and Joinson, 2017a). Less commonly mentioned factors include self-awareness and other perceptual factors, self-deception and emotion (Williams *et al.*, 2017a). Dispositional factors are often discussed in connection with cognitive processing such as heuristics (Vishwanath *et al.*, 2011, 2016; Benenson, Gassmann and Landwirth, 2017). Behavioural and experiential factors discussed in the literature on susceptibility to CSE include habitual behaviour, level of online experience/IT self-efficacy, previous experience with CSE victimisation, and culture (both national and organisational).

2.8.1 Personality Traits – The Five Factor Model (FFM)

A number of studies have examined the Five Factor Model (FFM) as it applies to cybersecurity, also referred to as the Big Five Theory (e.g., Junglas and Spitzmüller, 2006; Korzaan and Boswell, 2008; Parrish *et al.*, 2009; Bansal *et al.*, 2010; Darwish *et al.*, 2012; McBride *et al.*, 2012; Alseadoon *et al.*, 2015). The FFM personality traits are seen to be a predictor of an individual's attitude towards risks and susceptibility in relation to cybersecurity (Hadlington, 2017; King *et al.*, 2018). There are tools available to measure personality traits. These can be used to examine how an individual's behaviour may be

influenced and shaped according to their personality type. Each trait can be scored, and the scores used to show which user personality types are more susceptible to CSE than others. These Big Five personality traits are sometimes presented according to the mnemonic OCEAN: *openness to experience*, *conscientiousness*, *extraversion*, *agreeableness*, and *neuroticism/emotional stability* (Goldberg, 1990). These characteristics are also associated with sub-traits, as described in the following subsections.

2.8.1.1 Openness to Experience

The *openness to experience* trait indicates a willingness to try new things without worrying or hesitation, to be enthusiastic and not easily alarmed (Mundie, 2014). Junglas and Spitzmüller (2006) suggest that highly open individuals have no privacy-sharing issues when asked to enable their mobile location services. This suggests that open people may not consider the possibility of social engineering threats, creating a fertile ground for CSE attacks. Alseadoon *et al.* (2015) and Halevi *et al.* (2013a) found that individuals who score high on this trait are more likely to accept phishing emails. In the SNS context, however, Albladi and Weir (2017) found no direct or mediated link between this trait and CSE victimisation.

2.8.1.2 Conscientiousness

This trait includes individuals who are disciplined, trustworthy and tend to follow rules and policies (Frauenstein and Flowerday, 2020), Conscientious people have been described as compulsive in their behaviour (Carter *et al.*, 2016) but not impulsive (Williams *et al.*, 2017a). They are punctual and, in their careers they seek self-efficacy (Bandura, 1989) and career information (Reed, Bruch and Hasse, 2004). It has been argued that people with moderate to high levels of self-discipline (a sub-trait of *conscientiousness*) tend to overwhelm their perception and thinking process due to continuous attention to information, and this can consequently increase their risk of falling victim to CSE, such as a phishing attack (Williams *et al.*, 2017a). Studies on personality and individual differences have shown that excessively high levels of conscientiousness can lead individuals to unrealistic expectations of their abilities (Sherry *et al.*, 2007; Stoeber, Otto and Dalbert, 2009), and "*the more extreme these expectations are, the less likely they are to be met*" (Carter *et al.*, 2016, p. 519). Other studies, however, have found opposing evidence. For example, a study published by Darwish *et al.* (2012) found that mature individuals who are characterised as being highly cautious (high conscientiousness) are less likely to be at risk

of becoming victims of phishing emails. Parrish *et al.* (2009) also found that highly conscientious individuals are less likely to be susceptible to phishing emails due to their tendency to follow policies.

2.8.1.3 Extraversion

This construct, proposed by Eysenck (1990), represents an individual who is social, assertive, active and talkative. In the context of cybersecurity, Darwish, El Zarka and Aloul (2012) and McBride *et al.* (2012) posited that individuals with high levels of *extraversion* may be more likely than less extroverted people to bypass IT security policies. For example, disobeying computer security rules and regulations may result in individuals accepting malicious requests, as they may be more vulnerable to persuasive and deceptive messages. Workman (2008) suggested three types of attitudinal commitment significantly related to extraversion: normative commitment (degree of emotional attachment), affective commitment (extent of fear of loss), and continuance commitment (sense of responsibility). A high level of these traits can result in a user being vulnerable to many forms of persuasive and deceptive messages. This is in line with an SE susceptibility study carried out in the context of organisations by Erdheim, Wang and Zickar (2006). This finding is backed up by studies carried out by Parrish *et al.* (2009) and Alseadoon *et al.* (2015), who also suggested that highly extroverted people were more likely to share sensitive information, and were thus more gullible when faced with phishing emails. In the SNS context, Albladi and Weir (2017) found that high extraversion can increase Facebook users' susceptibility to CSE attacks. Conversely, it has been suggested that employees who are strict about not sharing passwords – and who are therefore less likely to become victims of CSE – may be viewed by their co-workers as "*unsociable*" (Weirich and Sasse, 2001, p. 142).

2.8.1.4 Agreeableness

According to Parrish *et al.* (2009), people with higher levels of *agreeableness* are described as "*compassionate and cooperative rather than antagonistic and suspicious*" (p. 289). Costa and McCrae (1992) asserted that this trait was also associated with *dependent personality disorder*. This disorder, as described by Saß (2001) is characterised by an obsequious personality, in which the individual pays particular attention to others and consequently is equipped to spot a lie or deceit. Nevertheless, when related to studies in the IS security context, this trait, when scored high, has frequently been found to have a positive link to falling for phishing emails and potentially increases the possibility of

victimisation even by other means of CSE attacks. Parrish *et al.* (2009) and Alseadoon *et al.* (2015) found a significant positive relationship between high levels of agreeableness and accepting phishing emails. In their taxonomy of the Big Five traits, John and Srivastava (1999; Section 2.9.1.4) listed *trust* (meaning propensity to trust, see Section 2.8.2.1) as a sub-trait of agreeableness. In their exploratory study investigating why some employees comply with security protocols and others do not, Weirich and Sasse (2001) reported that sharing passwords among co-workers was viewed as a sign that they trusted each other, and conversely, refusing to share one's password with a colleague was perceived negatively, as an indication of a lack of trust in that person. Workman (2008), echoing Mitnick and Simon (2001; see Section 2.5) found that establishing trust with a potential victim was an important strategy of successful cyber-social engineers.

It is important to note, however, that a recent study by Albladi and Weir (2017) found that high levels of agreeableness had a significant negative effect on users' susceptibility to cyberattacks on Facebook. Erdheim *et al.* (2006) asserted that *compliance* was a sub-trait of agreeableness and thus could lower an individual's susceptibility in general. Another possible explanation for this negative association was posited by Enos *et al.* (2006), who found that individuals who scored high on this trait seemed to be equipped with better skills to detect deception. As Uebelacker and Quiel (2014) suggested, these contradictory findings indicate that more investigation of this characteristic is needed.

2.8.1.5 Neuroticism (Emotional stability)

The characteristic of neuroticism (often referred to by its opposite on the dimension: emotional stability) has also been shown to influence susceptibility to cyber-attacks. Albladi and Weir (2017) found that neurotics are less trusting and more careful, thus decreasing their susceptibility. However, Halevi *et al.* (2013b) reported a high correlation between neuroticism and falling victim to phishing attacks, contending that people with this trait are prone to believe what they are told and unable to detect a lie, making them vulnerable to cyber victimisation. In yet other studies, neuroticism correlated negatively with IT self-efficacy (Halevi *et al.*, 2016; see Section 2.9 and Chapter Three, Section 3.4.4), but positively with security and privacy concerns (Cofrin, 2011). Shappie, Dawson and Debb (2020) reported that the inverse of neuroticism, emotional stability, was "*positively associated with information security awareness (defined as the extent to which someone*

understands the information security rules and guidelines of their workplace and behaves accordingly)" (p. 2).

2.8.1.6 Personality Traits and CSE – A Summary

The research on the relationships between each of the Big Five traits to CSE susceptibility has revealed mixed findings. Some studies suggest that individuals with high levels of *openness*, *agreeableness* and *extraversion* are more susceptible to CSE victimisation (Parrish et al., 2009; Uebelacker and Quiel, 2014; Alseadoon *et al.*, 2015). Other research showed that scoring high on *openness*, *conscientiousness* and *agreeableness* is associated with reduced propensity for risk (see Section 2.8) and higher levels of information security awareness (ISA; McCormac *et al.*, 2017b; Butavicius *et al.*, 2017; Hadlington, 2017). As discussed in Section 2.8.1.5, the research on the association between neuroticism/emotional stability and CSE is similarly inconclusive. Further examination of these relationships is needed in order to reach an understanding from a wider perspective.

2.8.2 Attitudes to Risk/Susceptibility (Personal Dispositions)

Albladi and Weir (2016) argued that it was crucial to examine the perceptions as well as the behaviour of individual users in order to identify "*the weak points in users' ability to detect and defeat these* [CSE] *attacks*" (p. 6). Human factors involving aspects of perception, cognition, and use of heuristics have been taken into consideration in a number of recent cyber-social engineering studies. An in-depth review of the literature for this thesis identified a number of personality dispositions as contributing factors to an individual's susceptibility to CSE. The following factors are some of the most commonly attributed in the literature, and have been selected for discussion because they work together to provide an understanding of the disposition of end-users to risk and their attitude towards cyber attackers. For example, as Malhotra *et al.* (2004) point out that in information privacy-related research, "*trust and risk are the two most salient beliefs*" and that a "*trust–risk model has been used to explain a variety of behaviors in an uncertain environment*" (p. 341).

2.8.2.1 Trust, Propensity to Trust, and Risk

Trust is the fundamental element of the second of the four stages of CSE attack: entrustment (see Section 2.5). Trust is also a key component in Cialdini's (2001, 2016) principles of influence (see Section 2.7). Trust is a concept (or a process; Alarcon et al., 2018) that is

acknowledged by scholars to be difficult to understand (Das and Teng, 2004). Trust had originally been studied by psychologists and behavioural economists as a feature of cooperative behaviour (Deutsch, 1958, 1960). Warren, Leitch and Rosewall (2011) contended that "*trust [was] a critical determinant of sharing information and developing new relationships*" (p. 232). Rousseau *et al*. (1998) synthesised the different explanations of trust across various disciplines into this generally accepted definition: "*Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another*" (p. 395). Defining trust in the context of SNS, Warren *et al.* (2011) described it as the willingness of an individual "*to be vulnerable to the actions of*" the trustee (p. 232).

Trust has been variously conceptualized (Deutsch, 1958, 1960; Rousseau *et al*., 1998; Das and Teng, 2004; Evans and Revelle, 2008), but often as comprising three components: beliefs (e.g., tendency/propensity to trust, trustworthiness, etc.), intentions (e.g., willingness to be vulnerable) and actions, which are behaviours performed by the trustor based on their trust beliefs and trust intentions (Alarcon *et al.*, 2018). This view of trust aligns with the theory of planned behaviour (TPB; Ajzen, 1985) that is the overarching theory for this thesis (see Chapter 3, esp. Section 3.1.3).

Different aspects of trust have been investigated: dispositional, perceptual, situational and behavioural (Das and Teng, 2004). These are illustrated briefly in this subsection. From the dispositional aspect, *propensity to trust* is a personality sub-trait (Rotter, 1967, 1980): a characteristic of personality in which the individual tends to trust other people (Rotter, 1967; Mayer, Davis and Schoorman, 1995; Alarcon *et al.*, 2018). Specifically, propensity to trust has been found to correlate positively with extraversion and negatively with neuroticism (Evans and Revelle, 2008). A user's personality – in particular, his/her propensity to trust – is suggested to play a role in susceptibility to cybercrime on SNS, as trust is leveraged to entice users of SNS to share information (Waldman, 2016). Rocha Flores (2016) inferred that trust was one significant factor that influenced employee resilience to SE. He posited that "*employees who exhibit a greater trust are easier to deceive, hence are less resilient to social engineering*" (p. 18). It is clear from Rocha Flores' (2016) statement that he is referring to *propensity to trust*, not trust generally.

From the perceptual aspect, trust was found to have a relationship with perceived risk (Freudenburg, 1993; Earle and Cvetkovich, 1995, 1997; Siegrist, Cvetkovich and Roth,

2000; on *perceived risk*, see Section 2.8.2.3). However, there is disagreement among scholars as to the nature of this relationship (Das and Teng, 2004). Trust has been posited to be a substitute for knowledge in the perception and evaluation of risk (e.g., when knowledge is lacking about risks of a particular course of action) (Seigrist, 2021/2019). Others have argued that the affect heuristic (see Section 2.8.2.4) influences both trust and perceived risk, possibly confounding the relationship (Slovic *et al*., 2005). In the SNS context, Albladi and Weir (2017) suggested that the likelihood of an individual trusting another person over the internet can vary depending on how online users perceive risk in social networking communication.

Behaviourally, trust is associated with risk-taking. Das and Teng (2004) contended that "*behavioral trust can be viewed as risk taking, so that the causal relationship between subjective trust and behavioral trust is similar to that of perceived risk and risk taking*" (p. 85). Seigrist (2021/2019) pointed out that trust involves actual, not just perceived, risk, as does the lack of trust. By default, people assume that information is true, so trust is a natural part of communication (Bond and DePaulo, 2006; Williams *et al.*, 2017a). Nevertheless, controlling information by deciding what should and should not be released or shared in cyberspace depends on an individual's perception of the risk involved and his/her willingness to trust strangers.

From the situational aspect, Corritore, Kracher and Wiedenbeck (2003), Wang and Emurian (2005), and Albladi and Weir (2017) highlighted that the level of trust can vary between individuals and depends on the context. Albladi and Weir (2016) examined trust as a factor in their research on susceptibility to social engineering in the SNS context, and Williams *et al.* (2017a) included trust in their theoretical review of factors influencing susceptibility to cybercrime victimisation in the workplace (see Section 2.9.2). Research on the relationships between trust, propensity to trust and risk perception has often included demographic factors such as age and gender (Evans and Revelle, 2008). These relationships are discussed further in Section 2.8.5.

2.8.2.2 Perceived Control over Information

Refraining from the risky behaviour of posting too much personal information online is an essential step to reduce CSE victimisation (CERT-UK, 2015). In an SNS context, privacy is determined on the basis of one's control over the flow of one's personal information, including the transfer and exchange of information (Dwyer, Hiltz and Passerini, 2007; Shin,

2010; boyd, 2008). A stronger belief in one's ability to control and restrict SNS privacy settings can decrease concerns of the risks associated with phishing attacks (van Schaik *et al.*, 2017). This could mean that individuals' perceptions of controlling their personal information, such as information shared by students (Lawler, Molluzo and Doshi, 2012) or by professionals (Snyder, Carpenter and Slauson, 2007), can be considered a contributing factor to information privacy on SNS.

In contrast, other authors have found that perceived control over information can increase the risk associated with cybercrime. Malhotra *et al.* (2004) and Krasnova *et al.* (2010) argued that having a high *perceived control of information* was likely to alleviate users' privacy concerns and, consequently, decreased their perceived risk of being victimised by CSE on SNS. This relationship can be more critical when an overlap exists (Figure 2-6) between a user's personal and professional life. The result is an intersect where rich information could be used by social engineers to craft various advanced schemes of spear-phishing attacks (Edwards *et al.*, 2017; Frumento *et al.*, 2016) tailored to fit the preferences of a specific employee. Skeels and Grudin (2009) and Silic and Back (2016), when studying workplace users of Facebook and LinkedIn, found that employees often had difficulties controlling the content they posted when switching between SNS platforms.

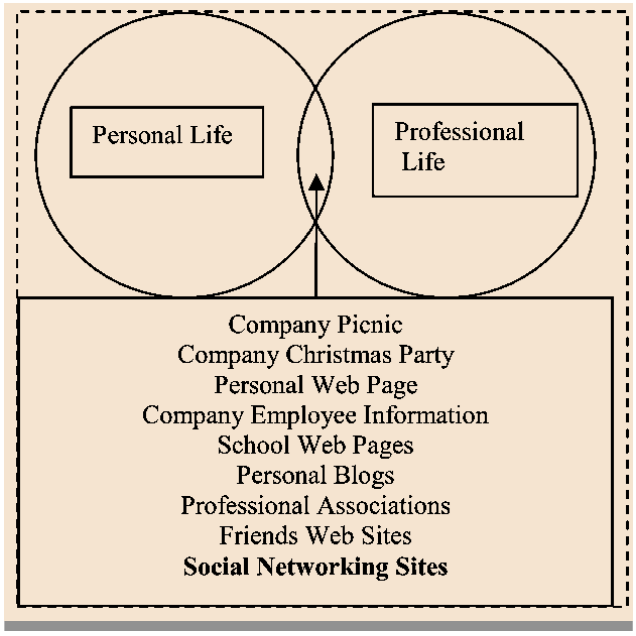


Figure 2-6 The Intersection of Personal and Professional Lives in the 21st Century

Source: Snyder et al. (2007, p. 5)

2.8.2.3 Risk Perception and Cyber-Risk Beliefs

Risk perception was mentioned earlier as it relates to trust and propensity to trust (Section 2.8.2.1). Risk perception has been defined as individuals' "*beliefs, attitudes, judgements and feelings as well as the wider cultural and social dispositions they adopt towards hazards and their benefits*" (Royal Society, 1992, p. 89). Risk perception in an online context is based on the individual's instinct towards a potential outcome of information processing (Trumbo, 2002), whereas cyber risk belief is influenced by previously experienced incidents online (Vishwanath *et al.*, 2016). It is unclear what causes a cautious individual, even when encountering a previously known threat, to still accept another scam email in spite of the potential risks. Such behaviour may possibly be due to their risk aversion level and an expectation of few benefits with known high risks (FINRA Investor Education Foundation, 2013). High levels of risk perception have been found to predict secure behaviour and security self-efficacy in cyberspace (Halevi *et al.*, 2016).

In an organisational context, individuals with high risk perception are more likely to comply with company rules and safeguards for online behaviour (Mearns, Matthiesen and Eid, 2011; Johnston, Warkentin and Siponen, 2015; Silic and Back, 2016). Conversely, Algarni (2016) posited that organisations that have not yet experienced serious cyber-attacks and have not trained their employees about social engineering threats might find that employees differ from one another in their cyber-risk beliefs. Algarni (2016) made his assertion in the context of his investigation of two different organisations. The first had suffered a serious cyber-attack a couple of years earlier and had subsequently implemented cybersecurity awareness training for its employees; this training included recognising social engineering threats. "*In contrast, the second organisation had not yet experienced a serious cyber-attack, and its employees had not been involved in professional training about social engineering*" (Algarni, 2016, p. 115). Algarni argued that it was to be expected that those employees who had not undergone training would have "*different risk beliefs and different levels of awareness*" with respect to cyber-social engineering (p. 115).

2.8.2.4 Heuristics, Judgement and Decision Making

Williams *et al.* (2017a) highlighted *heuristics* as cognitive processing factors pertaining to individuals' judgements and their likelihood of making them susceptible to social engineering in the workplace. Chaiken's (1980) heuristic–systematic model (HSM) describes two main ways in which humans process information. Systematic processing is

time-consuming and requires thorough and careful attention to detail, whereas heuristic processing is simple and quick, with less reliable means to judge the validity of a message (Chaiken, 1980). Heuristics are thus a mental shortcut that helps people to make decisions and judgements quickly without having to think heavily, research, or analyse a lot of information (Otuteye and Siddiquee, 2015). Vishwanath *et al.* (2016) posited that cognitive heuristics also involved drawing quick conclusions to judge a context (persuasive context) by connecting cues to judge a message. Blythe *et al.* (2011) observed that people tended to be "*more aware of technical security attacks, but less aware of threats posed by social engineering*", so they relied on heuristics to determine if an email was "suspicious" or not (p. 2). Indeed, heuristic techniques for decision making, (e.g., deciding on the legitimacy of a website or URL), have been thought to be effective in thwarting phishing attacks (Gastellier-Prevost, Granadillo and Laurent, 2011). However, a recent study carried out by Benenson *et al.* (2017) found that "*decisional heuristics are easy to misuse in a targeted attack, making defence especially challenging*" (p. 610). Heuristics can lead to errors in judgement, enabling even the most intelligent individuals to fall victim to CSE.

There are three types of heuristics that users commonly use to judge an influential message:

1. *Availability heuristic*: People who have readily available examples in their minds from either previous incidents or a lot of information exposure (e.g., from social media or TV) can make biased judgements. For example, when a user is continuously exposed to CSE techniques, such as trending hashtags or lottery reports on SNS (events, news, incidents, celebrities, promotions, etc.), the information may seem relevant and genuine when it is in fact a deceptive message tailed by a phishing link (Williams *et al.*, 2017a). In their SCAM framework construct of *cyber-risk belief* (Section 2.9.2.3), Vishwanath *et al.* (2016) disagreed and asserted that people were capable of making suitable judgements in response to a phishing email based on previous media exposure and past experience.

2. *Representativeness heuristic*: This type of heuristic is used when individuals base their judgements on pre-conceived stereotypes (Tversky and Kahneman, 1974). In other words, if a user sees a message featuring aspects that they consider trustworthy, they may open themselves to CSE. Williams *et al.* (2017a) suggested that CSE techniques could play on *representativeness heuristic* thinking by design; for example, "*online romance scammers may attempt to embody particular*

characteristics and communication styles that people typically associate with trustworthiness" (Williams *et al.* 2017a, p. 416).

3. *Affect heuristic*: This type of thinking occurs when individuals base their judgements on the triggering impact of an emotional influence (see Section 2.8.3.3). For example, when people are going through emotional distress, such as depression, anxiety or sadness, they are more likely to seek out short term ways to relieve their distress (Isen and Patrick, 1983). This may mean that an individual who is driven by an emotional need could be more likely to respond to a malicious message in cyberspace.

Williams *et al.* (2017a) highlighted two additional cognitive biases that can negatively affect judgement and thus have a link to users' susceptibility to online victimisation. Alongside Kahneman's heuristics types, these two cognitive biases are known as confirmatory bias and hindsight bias.

A) *Confirmatory bias:* This suggests that individuals tend to select information from the current environment that confirms or at least supports their present beliefs or goals. At the same time, people tend to overlook what disconfirms their beliefs or goals. For example, "*in online romance scams with individuals who are particularly lonely or strongly desire attachment, then they* [the targeted victims] *may be more likely to search for information that confirms this belief and dismiss information that contradicts it*" (Williams *et al.* 2017a, p. 416).

B) *Hindsight bias* is described by Williams *et al.* (2017a) as the situation in which the individual thinks that they could have predicted an outcome after it has happened, even though there had been no way of predicting it. In other words, "*once individuals have become the victim of a scam, findings of repeat victimisation in the future could also be linked to a hindsight bias, whereby previous scams are dismissed as being different and more predictable than the current proposition*" (Williams *et al.* 2017a, p. 416).

Vishwanath *et al.* (2016) and Vishwanath (2015a) state that the cognitive activity needed to make a decision to either accept or reject a suspicious persuasive message (e.g., a

phishing attack) employs *systematic processing.* Vishwanath *et al.* (2016) used the distinction between systematic and heuristic processing in their model to distinguish levels of susceptibility by assessing the degree of user suspicions towards all sorts of cyber deception threats. Specifically, their model posits that a "*higher level of heuristic processing is likely to decrease individuals' suspicion about the veracity of a phishing email*" whereas a "*higher level of systematic processing is likely to increase individuals' suspicion*" towards that phishing attempt (p. 6).

2.8.2.5 Risk Propensity/Approach to Risk

As mentioned at the beginning of this section (2.8.2), attitude to risk may be determined by personality traits. *Risk propensity* is often referred to as the willingness to assume or avoid risks (Sitkin and Pablo, 1992; see also Chapter Three, Section 3.4.3). Risky behaviours have been linked to human dispositions within IS security, such as impulsiveness (Hadlington, 2017) and attitudes towards cybersecurity (Vishwanath *et al.*, 2016. Other studies have found a positive relationship between risk perception and adoption of IS security practices (Halevi *et al.*, 2016; van Schaik *et al.*, 2017). An individual's level of risk propensity can vary based on the context, such as with a financial risk as opposed to a leisure one (Ermer, Cosmides and Toby, 2008; Weber, Blais and Betz, 2002). Thus, risk propensity depends on the source of the risk, and this is certainly the case in cyberspace as well (Cases, 2002).

A person's individual approach to risk could also have consequences for cybersecurity; this may be even truer in the context of SNS compared to email, due to SNS being a place of rich – and often instant – social communication and interaction (Collin *et al.*, 2011). In particular, LinkedIn, Twitter and Facebook have been classified as sources of such risk (Saridakis *et al.*, 2016), as discussed earlier in section 2.6. In addition, Byrnes, Miller and Schafer (1999) found that men have been shown to engage in more risky behaviours than women, implying that gender may have a link to willingness to take risks on the internet (Section 2.8.5.2). Hopes of attaining a perceived benefit can increase an individual's propensity to take risks in cyberspace (Nguyen and Kim, 2017), potentially causing users to fall victim to CSE tactics. On LinkedIn, for example, a user may be inclined to respond to a deceptive private/direct message from an apparently genuine source that seems to offer a lucrative employment position (Section 2.5; see also Chapter Four, Section 4.15.2.2).

2.8.2.6 Self-Awareness

This characteristic was presented as a potential factor by Williams *et al.* (2017a) but had not emerged in previous studies. The authors integrated *self-awareness* with Cialdini's principles of influence (Section 2.7) in a framework to examine susceptibility to phishing in the workplace. This factor, and how it may be associated with an individual's attitude to cyberspace risks, was justified by its use in previous studies on traditional crimes and on persuasion in general. The authors of one such study, Fenigstein, Scheier and Buss (1975), posit that self-awareness is related to resistance to influence. Following on from this, Williams *et al.* (2017a) asserted that self-affirmation theory, an adaptation to threatening information or experience (Sherman and Cohen, 2010), would shed some light on how self-awareness can either increase or decrease individuals' susceptibility to cyber-social influence. They explained that self-awareness increased susceptibility to such messaging when a targeted recipient believed that the sender (or in the case of CSE, the fabricated "person" of that sender) is in some way similar to him/herself. Conversely, this same trait or state decreases susceptibility if the intended recipient perceives the sender as different from her/himself. It seems that the mediating factor in the relationship is "*attentional bias*", especially if the messaging conveys a perceived threat (Williams *et al.*, 2017a, pp. 413-414). Such messages can increase susceptibility "*to online scams that use threat-based influence techniques, such as phishing e-mails focused on the potential suspension of an online account, particularly if they resonate with the individual's current behaviour, such as failing to monitor bank accounts for suspicious transactions*" (p. 414).

2.8.2.7 Other identified perceptual factors impacting CSE victimisation.

A study was conducted by Algarni, Xu and Chan (2014) on social engineering in SNS (Facebook). They used source credibility theory[4], which focuses on the notion of individuals assessing the source of an approaching message (which may come from a social engineer) to make judgements that can increase the likelihood of an unsuspecting victim interacting with that message. Algarni *et al.* (2014) identified factors influencing users' judgement on Facebook: *perceived competence*, *perceived attraction*, *perceived worthiness* and *perceived sincerity*. These factors were identified through the interpretation of

[4] The source credibility theory presented by Hovland *et al.* (1953) stated that individual receivers are more likely to be induced when the source presents itself as being trustworthy (Choo, 1964).

qualitative data collected from 24 employees; further empirical investigation is needed to confirm these findings.

2.8.2.8 Motivation

A user's online *motivations* can have an impact on their susceptibility to influence by a CSE message. Workman (2008) suggested three motivational factors that are likely to be linked to susceptibility to victimisation: fear of loss (affective commitment), feeling of obligation (continuance commitment), and emotional connection (normative commitment). Albladi and Weir (2018) found that motivation to use SNS "*causes the individual to engage more in social networks without conducting preventive measures*" (p. 23). In an earlier study (see Section 2.9.1.3), Albladi and Weir (2017) argued that user's various motivations (e.g., seeking to make professional or personal connections online) could explain their attitudes and thus behaviours regarding disclosing PII on SNS. In a scenario-based experiment, they found that indeed, motivation played a mediating role in increasing user susceptibility to cyberattack victimisation (Albladi and Weir, 2017). The literature indicates that users of career-related SNS such as LinkedIn generally engage on these platforms because of two motivations: self-presentation and professional advancement (Kim and Cha, 2017). These motivations are discussed in detail in Chapter Three, Section 3.4.8 and Chapter Four, Section 4.15.2.2.

2.8.3 Behavioural and Experiential Factors

As Young *et al.* (2018) observed, "*The perspective of human factors is largely missing from the wider cyber security dialogue and its scope is often limited*" (p. 244). This section considers aspects of individual experience and behaviour that the literature proposes may affect susceptibility to cyber-social engineering.

2.8.3.1 Habitual Level of Engagement

Young *et al.* (2018) contended that there are three types of behaviours: reflex, habitual and thoughtful. Reflex is basic cognition in response to signals from the senses, such as opening an email attachment without stopping to consider whether it is safe or not. Reflex is automatic processing. Habitual behaviour requires some level of cognitive assessment. An example of habitual behaviour would be agreeing to show one's location on SNS to boost visibility or downloading software from an unverified website believing that the firewall system of one's organisation will block it if it poses a threat. Habitual behaviour involves

heuristic processing. Thoughtful behaviour requires a higher level of cognitive assessment; it involves systematic processing. An example of thoughtful behaviour is implementing the training one has received related to risky cybersecurity practices, and mitigation toward threats. Considering that behaviour is usually accomplished through both thoughtful consideration of the situation and logical processing, Koochaksaraee (2019) inferred that "*most security-related behaviour is habitual behaviour, which can be improved through an awareness training program and effective educational methods*" (p. 18).

Researchers have given limited consideration to incorporating habitual variables in models that examine susceptibility to cybercrime (see Section 2.9 for a further discussion of the models). Some authors have examined email habits (Vishwanath *et al.*, 2016), level of involvement (Albladi and Weir, 2018, 2020), and social media habits and usage (Vishwanath, 2014; Saridakis *et al.*, 2016). The findings of these studies all agreed that a high level of activity on SNS and high frequency of checking messages, combined with low risk perception and/or IT self-efficacy, could increase cyber-attack victimisation in both email and SNS contexts (Vishwanath, 2015a; Saridakis *et al.*, 2016; Albladi and Weir, 2018). Moreover, time (in terms of frequency and duration) is a component of level of engagement. The rise in popularity of SNS as a multi-purpose communication tool (see Section 2.6) has meant increasing amounts of time are being spent on SNS (Metev, 2020).

In his investigation of susceptibility to victimisation on Facebook, Vishwanath (2014) distinguished between attempting to "*friend the target*" and to "*procure information from the target*", a "level 1" and "level 2" attack, respectively (p. 87). Vishwanath (2014) found that people who were "*habitual Facebook users*" (i.e., they used the SNS frequently and were active on the platform) were susceptible to level 2 attacks, whereas individuals who did not meet the criteria of *"habitual user"* were not susceptible to scamming via information request (p. 93). Vishwanath (2014) posited that the automaticity that comes from habitual use might cause such individuals to be less attentive to cues (i.e., to use heuristic processing) in the phishing message that would alert them to its deception (p. 93; see also Section 2.9.2.3; Vishwanath *et al.*, 2016).

In their study of factors that influence employees' non-malicious information security behaviour, Pattinson *et al.* (2015a) examined age, level education, personality, ability to control impulsivity, and IT self-efficacy. They recommended that future research should investigate how individual, organisational and interventional factors might influence an

employee's "*accidental-naive*" behaviour while using computers and how this impacted "*the protection of information at their place of work*" (p. 240). Specifically, they called for future research to "*empirically test a variety of management interventions to ascertain which are the most effective and cost-efficient*" (p. 240).

2.8.3.2 Expertise and Experience

Parrish *et al.* (2009) argued that experiential factors (e.g., general, technological and professional experiences) can influence personality traits; for instance, young professionals' experience in the workforce can help shape their consciousness into becoming experts. Jacoby *et al.* (1986) noted that individuals' experience and expertise differed; the authors defined experience as "*made skilful through observation and participation in a particular activity, while expertise is defined as skilful in a particular field*" (p. 469). Williams *et al.* (2017a) consider expertise as a potential factor in how an employee forms a judgement on an influential message (e.g., a phishing email), in that higher degrees of expertise lessen the likelihood of being deceived by the message. Similarly, Vishwanath (2015a) highlighted the fact that students tend to have more experience with social media than do older employees, which makes the former relatively less susceptible to victimisation by phishing. However, other researchers have noted that, as a demographic, undergraduate students are reportedly more susceptible to phishing attacks and thus have been a favourite target of CSE attackers (Sebescen and Vitak, 2017). In fact, a key study conducted by Sillence *et al.* (2006) did not support Vishwanath's (2015a) argument. They examined a proposed website trust framework to assess why online users' vigilance-through-practice differs. They determined that users perform fact-finding analyses to determine the trustworthiness, credibility and authenticity of websites. The researchers found that inexperienced users go through three stages of a trust-credibility framework consecutively: (1) heuristic evaluation of the website interface, (2) further website analysis of its content and (3) long-term engagement with and use of the site. Surprisingly, Sillence *et al.* (2006) concluded that some users with more expertise (~6 months) were more likely to skip stages 2 and 3, probably due to overconfidence, and this unsystematic evaluation of websites increased their susceptibility.

2.8.3.3 Previous Experience of Cybercrime

Previous experience of CSE victimisation was found to be a significant mediating factor between the personality trait of *agreeableness* and susceptibility to CSE attack (Albladi

and Weir, 2017). The study, however, does not explain why this is the case. Parrish *et al.* (2009) considered prior experience in general as a potential factor influencing users' attitudes towards cyber risks (e.g., phishing emails). This experiential factor in their model encompasses three types based on previous findings; *general* (whether positive, such as having children, or negative, such as being the victim of a scam or financial hardship), *technological* (past experience of CSE attacks or training against CSE attacks), and *professional* (career/academic).

Of particular interest, they reported that prior experience with CSE victimisation influenced users' attitudes towards cyber risks (e.g., phishing emails) by reducing their levels of agreeableness (Parrish *et al.*, 2009, p. 292). Bailey, Mitchell and Jensen (2008) reported that working students were less susceptible to phishing than their non-working counterparts, and students in different academic departments (i.e., fields of study) could differ in their levels of susceptibility to phishing (Jagatic *et al.*, 2007, cited in Bailey *et al.*, 2008). Albladi and Weir (2018) also highlighted that prior experience of CSE attacks (e.g., phishing) has rarely been considered in previous models.

2.8.4 Contextual Factors

This section discusses aspects of the contextual factors that may influence a user's susceptibility to cyber-social engineering attacks.

2.8.4.1 Culture

Sawaya *et al.* (2017) argued that culture is a complex term that is difficult to describe and quantify. Bellman *et al.* (2004) and Cho, Rivera-Sanchez and Lim (2009) used Hofstede's (1980) dimensions of culture, for instance, to approximate cultural differences in privacy risk. In the context of information systems, Hofstede's index was used by Krasnova and Veltri (2010) to study cultural variation with regard to information disclosure and privacy risk. The same method was also employed by Rocha Flores (2016) in a cross-cultural study of the degree of employees' resilience to SE. Previous literature has suggested that cultural differences may impact users' susceptibility to requests, such as those seeking donations for fake philanthropic fundraising[5] on SNS sites. Culture is a predictive factor of how an individual may respond to certain email requests (Williams *et al.*, 2017a; Airehrour, Nair and Madanian, 2018; Butavicius *et al.*, 2017). For example, as Williams *et al.* (2017a)

[5] https://www.scamwatch.gov.au/types-of-scams/fake-charities

reported, people in collectivist cultures exhibited "*a greater tendency to conform to social norms and to mimic the behaviours of those around them*" (p. 417), an aspect which may be exploited by cyber-social engineers.

Moreover, cross-cultural studies of IS security and privacy differences have revealed a significant impact of culture on individuals' attitudes in cyberspace (Cvrcek *et al.*, 2006; Almakrami, 2015; Rocha Flores *et al.*, 2015; Zhao, Street and Hinds, 2012). For instance, Almakrami (2015) ran a sequential explanatory research study and found that Australians refrained from disclosing information on Facebook, being more conservative online than offline, compared to Saudis who, due to relationship restrictions in offline settings, tended to compensate by being more open on Facebook. The examination as to whether culture in terms of the "nationality" of individuals (Albladi and Weir, 2018), as "language" (Alseadoon *et al.*, 2015), or as a society type (e.g., individualist, collectivist; Alseadoon *et al.*, 2015; Rocha Flores *et al.*, 2015) has, according to Albladi and Weir (2018), been given limited attention in IS security research. Following Hofstede's (1980; Hofstede, Hofstede and Minkov, 2010) framework linking national culture with organisational culture, other researchers have examined national and organisational culture (Rocha Flores, 2016), both of which have been defined as "*a pattern of basic assumptions that a group of individuals has developed in learning to cope with its problems of external adaptation and internal integration*" (Schein, 1984, p. 3).

Rocha Flores (2016) found that countries' social differences in terms of inherited culture, language, religion and customs, values, inclusiveness, and being collectivist or individualist, could impact employees' resilience to social engineering. He infers that "*culture influences the relationship between an employee's intention and his or her behavior* … [and how] *culture affects the behaviors and decision-making of their employees is especially important for organizations*" (p. 193).

Rocha Flores' (2016) study of American, Swedish and Indian users found that resistance to phishing was strongest for Americans and weakest for Indian participants, as shown by their responses to an information security awareness (ISA) assessment, cited in Butavicius *et al.* (2017). Thus, organisations should recognise the national characteristics of employees in establishing their organisational routines for online security. The same study recommended that a wider scope should be adopted to examine the impact of culture on SE by sampling other nations in respect to their collectivist or individualist tendencies.

A study carried out by Cialdini *et al.* (1999) on intended compliance to a request found significant differences between Polish and American (US) students. Other studies have addressed culture in terms of the "*nationality*" of the end-user (Alseadoon *et al.*, 2015; Albladi and Weir, 2018; Sawaya *et al.*, 2017). In particular, Alseadoon *et al.* (2015) referred to culture as "*language and nationality*" (p. 93).

Al-Hamar, Dawson and Guan (2010), in a study of email phishing, found that people's religious cultural values can make individuals apt to behave in a generous and trustworthy manner. Middle-Eastern culture, and Saudi Arabian culture in particular, is classified as tribal (Vennekens, 2015). A comparative cross-cultural study of personality traits in a real setting showed that tribal men are more "*agreeable*" than urban men (Varadwaj and Rath, 2018). As such, a cyber-social engineer could easily take advantage of such cultural vulnerabilities. However, it may be argued that this cultural landscape has changed, considering the extensive impact of globalisation and western cultures since the turn of the millennium.

2.8.4.2 Organisation

As Silic and Back (2016) highlighted, few studies have examined employees' reactions and behaviours when receiving influential phishing email attacks; therefore, little is known about "*how organizations are dealing with the associated threats*" (p. 36). In order for organisations to protect their information security, human behaviour must be considered (Connolly *et al.*, 2017; see Section 2.2), such as how employees operate their computers and how familiar they are with InfoSec practices. Li (2015) asserted that organisational culture could play a role in behaviour, stating that "*the phenomenon of culture associated with employee behaviour appears to be increasingly important in today's workplace*" (p. 16). The particular culture of the workplace may influence employee behaviour in ways that expose the company to online threats, like phishing emails (Sasse, Brostoff and Weirich, 2002), and leave workers vulnerable to online technological and communication threats. Some factors that can cause this include being unfamiliar with new technology, being pressed for time, heavy workload demands and information overload (Klein and Calderwood, 1991; Mack and Rock, 1998; Koumpis *et al.*, 2007).

Furthermore, it is estimated that 92% of the data breaches within the public sector were due to social breaches (Verizon, 2018) in which policies were bypassed by unwitting employees. D'Arcy, Hovav and Galletta (2009) and McBride *et al.* (2012) emphasised the

significant threat to organisations from employees' failure to observe good information security practices, combined with a lack of compliance regarding mitigation actions to limit exposure to cyber threats. They highlighted the importance of periodically informing and updating employees regarding new CSE methods to refresh and sharpen their ISA. This is vital since the success or failure of cyber-attacks depends to some extent on the "*behavior or an attitude of an organization and/or its members towards protecting the organization's information assets*" (Alzamil, 2012, p. 38).

Good cybersecurity practices may also be related to structural power in an organisation. A study by Pitesa and Thau (2013a) found that individuals in powerful positions, such as managers within an organisation, were generally more able to resist social influence techniques than were those in lower positions (employees/subordinates). They attributed this to the higher-powered individuals typically being more able to act independently, which makes them less likely to submit to persuasive and influential messages. Conversely, less powerful individuals tend to depend more on outsiders, making them more susceptible to scams. Alzamil (2012) carried out a comparative study of managers and employees in relation to the influence of InfoSec awareness on their daily business; he noted a lack of training and policy enforcement in Saudi organisations.

2.8.4.3 SNS context

Only a small number of studies in the existing literature have investigated end-user susceptibility to CSE victimisation in the context of SNS, such as Facebook (Algarni *et al.*, 2014; Albladi and Weir, 2017; Vishwanath, 2015b; Halevi *et al.*, 2013a, 2013b), while Saridakis *et al.* (2016) addressed cyberattack victimisation through the general use of SNS platforms. It is important to highlight that the studies of Albladi and Weir (2017), Vishwanath (2015b), and Halevi *et al.* (2013a, 2013b) used experimental scenarios in their study of phishing emails. A social networking-based phishing (SNP) attack was deployed in a study by Vishwanath (2017). This contradicts the ethical restrictions imposed by SNS providers. Other studies have deployed experimental phishing attacks in the context of SNS, but used participants' official email to assess susceptibility and then followed up with observation and analysis of participants' Facebook profile timelines and networks of "friends", using interview questions. As far as this author is aware, to date there has not been any study examining the threat of CSE on LinkedIn.

2.8.5 Demographics

Lupton (1999) argued that for studies of risk, demographics such as age, gender, education and nationality among others should be addressed. These factors could cluster in influencing an individual's perception and attitude towards risk. The age, gender and education level of participants received attention in previous studies pertaining to phishing susceptibility. In particular, age and gender were shown to have relevance in influencing individuals' ability to identify CSE attacks (e.g., phishing emails; Sheng *et al.*, 2010; Jagatic *et al.*, 2007; Kumaraguru *et al.*, 2010). However, the empirical findings as to how age and gender affected individuals' susceptibility to CSE have been contradictory.

2.8.5.1 Age

In a model developed by Saridakis *et al.* (2016) to examine the risks of cybercrime victimisation in the context of SNS, the researchers found older users to be less likely than younger users to become victims of cybercrimes. Similarly, Leukfeldt and Yar (2016) found that the younger the user, the higher the risk. This agreed with a previous study by Sheng *et al.* (2010), which discovered that the age group of 18-25 years was the most susceptible to phishing. However, this was found to be mediated by factors such as risk-taking behaviours, IT expertise and educational background. Moreover, age has been reported to be a mediating factor for other dispositional and perceptual factors, such as risk perception and risk propensity (Bonem, Ellsworth and Gonzalez, 2015). Grimes *et al.* (2010) reported that compared to young people, pensioners had lower awareness of cybersecurity risks, and this was mainly due to cohort differences in education and the divide between digital natives and non-natives.

2.8.5.2 Gender

The World Health Organisation (WHO) defines *gender* as "*the socially constructed characteristics of women and men – such as norms, roles and relationships of and between groups of women and men. It varies from society to society and can be changed*" (WHO, 2020). However, the term *gender* is often used loosely to include the biological and physiological characteristics that distinguish males and females. For the purposes of this thesis, it is assumed that the social science and IS literature in which *gender* has been included as a variable uses the WHO's definition.

Some IS research on the relationships between gender, risk perception and trust online has been conducted in the e-commerce environment (Garbarino and Strahilevitz, 2004; Awad and Ragowsky, 2008; Reidl, Hubert and Kenning, 2010). Using both a survey and an experiment, Garbarino and Strahilevitz (2004) investigated the effect of gender on risk perception for risks commonly associated with buying online. The researchers found that women's risk perception was higher than men's but that receiving a recommendation from a friend regarding an e-commerce site led to "*both a greater reduction in perceived risk and a stronger increase in willingness to buy online among women than among men*" (p. 768). Based on previous research suggesting that women tended to be more receptive than men were to advice from friends, Garbarino and Strahilevitz (2004) inferred a causal relationship from their research results. That is, for women, the friend's recommendation of a site reduced the participant's level of perceived risk associated with that site, which in turn led to an increase in the female participant's willingness to make an online purchase.

Citing Garbarino and Strahilevitz (2004) and other studies, Reidl *et al*. (2010) pointed out that although IS research was producing "*increasing evidence that women and men differ in their decisions to trust*", it had so far failed to provide a convincing explanation for "*these gender differences*" (p. 397). Reidl *et al.* (2010) therefore examined gender differences in decisions to trust in an online environment. They used functional magnetic resonance imaging (fMRI) to measure the brain activity of participants as those men and women were assessing the trustworthiness of online market offers. They reported a difference between men and women in the areas of the brain that assess trustworthiness. They also found that women activated more brain areas than did men, from which Reidl *et al.* (2010) concluded that there are differences between males and females in the way they processed trust and evaluated trustworthiness.

In cybersecurity research, much of the literature supports the contention that females are generally more susceptible to cyber-social engineering attacks than males are (Sheng *et al.*, 2010; Halevi *et al.*, 2013a, 2013b; Blythe *et al.* 2011; Goel *et al.*, 2017). However, the findings indicate some complexity in the relationship between gender and susceptibility to CSE. Research carried out by Carnegie Mellon University found that women had a higher propensity to fall victim to CSE (in the form of phishing scams) than men did, because women engaged more with social media advertisements and shopping offers (Greitzer *et al.*, 2014; Airehrour *et al.*, 2018). Anwar *et al.* (2017) found that female employees' IT self-efficacy was significantly lower than that of males and, thus, their cybersecurity

behaviour is risky, putting their cybersecurity at stake. It seems that women can be easily enticed by phishing attacks; however, Goel *et al.* (2017) argued that women may be more likely to open a phishing message, but not necessarily more likely to click on an embedded link. Leukfeldt and Yar (2016) found that women with higher education levels and in higher paid jobs were at higher risk of victimisation. This contradicts the general argument by Byrnes *et al.* (1999) that men were more prone to taking risks than women, and an interview with a social engineering expert, Christopher Hadnagy, who stated: "*women are more cautious by nature and that makes them less susceptible to social-engineering attacks*" (Mills, 2010).

Whether viewed as a dispositional social construct or a physiological individual difference, gender is a demographic variable that could be shaped by environmental influences such as culture. Previous studies (Costa, Terracciano and McCrae, 2001; Rolland, 2002; Srivastava, John, Gosling and Potter, 2003) found that age and culture can be moderating factors impacting on the development of personality in different genders. Thus, culture can be assumed to play an underlying role influencing how an individual (male/female) perceives and engages with persuasive messages or deception.

2.8.6 Summary of Factors Relating to Susceptibility to Cyber-Social Engineering

This section has introduced a number of prominent factors from the literature on susceptibility to social engineering in cyberspace. These include dispositional, behavioural, experiential, contextual, and demographic influences. The Big Five personality traits have been shown to be salient in influencing user susceptibility (Alseadoon *et al.*, 2015; Albladi and Weir, 2017; Goel *et al.*, 2017; van de Weijer and Leukfeldt, 2017). A plethora of personal dispositional factors influence attitudes to risk. These include but are not limited to: propensity to trust (Warren *et al.*, 2011); perceived control over information (Krasnova *et al.*, 2010); risk perception (Silic and Back, 2016) and cyber-risk beliefs (Algarni *et al.*, 2014); heuristics, judgement and decision making (Benenson *et al.*, 2017; Williams *et al.*, 2017a); risk propensity (Nguyen and Kim, 2017); self-awareness (Williams *et al.*, 2017a); and motivation (Kim and Cha, 2017). Then there are the behavioural and experiential influences, such as habitual level of engagement (Albladi and Weir, 2018), expertise (Sillence *et al.*, 2006), and previous experience of cybercrime (Parrish *et al.*, 2009). Contextual factors associated with susceptibility to CSE include national culture (Alseadoon *et al.*, 2015), organisational culture (Pitesa and Thau, 2013a, 2013b), and the

intersection of the two (Rocha Flores, 2016). The SNS environment is perhaps an obvious contextual aspect to investigate in a study on susceptibility to CSE on SNS (Albladi and Weir, 2020), but to date it has been scarcely considered in the literature. The findings of these studies are not always in agreement, which suggests the need for further research. Finally, two salient demographic factors associated with susceptibility to CSE are age (Saridakis *et al.*, 2016) and gender (Leukfeldt and Yar, 2016).

2.9 Previous Models and Frameworks

Having explored many of the concepts that are either essential or pertinent to susceptibility to cyber-social engineering in the SNS context, the next step is to search for an appropriate model through which to conceptualise the phenomenon. This section presents and reviews previous models that describe the interaction between user characteristics and susceptibility to cyber social engineering. The frameworks presented in the first half of this section (2.9.1) all make use of the Five Factor Model (FFM) of personality traits, whereas the frameworks described in the second half (Section 2.9.2) incorporate cognitive, and in some cases, behavioural factors. Two recent models were added, one each to Sections 2.9.1 (Frauenstein and Flowerday, 2020) and 2.9.2 (Montañez *et al.*, 2020). These studies had not been published at the time that this researcher was preparing the research question for this thesis. Thus, they were not considered as possible models for the study, but they have been included to ensure that the literature review is as up to date as possible.

2.9.1 Susceptibility Frameworks Incorporating the Five Factor Model

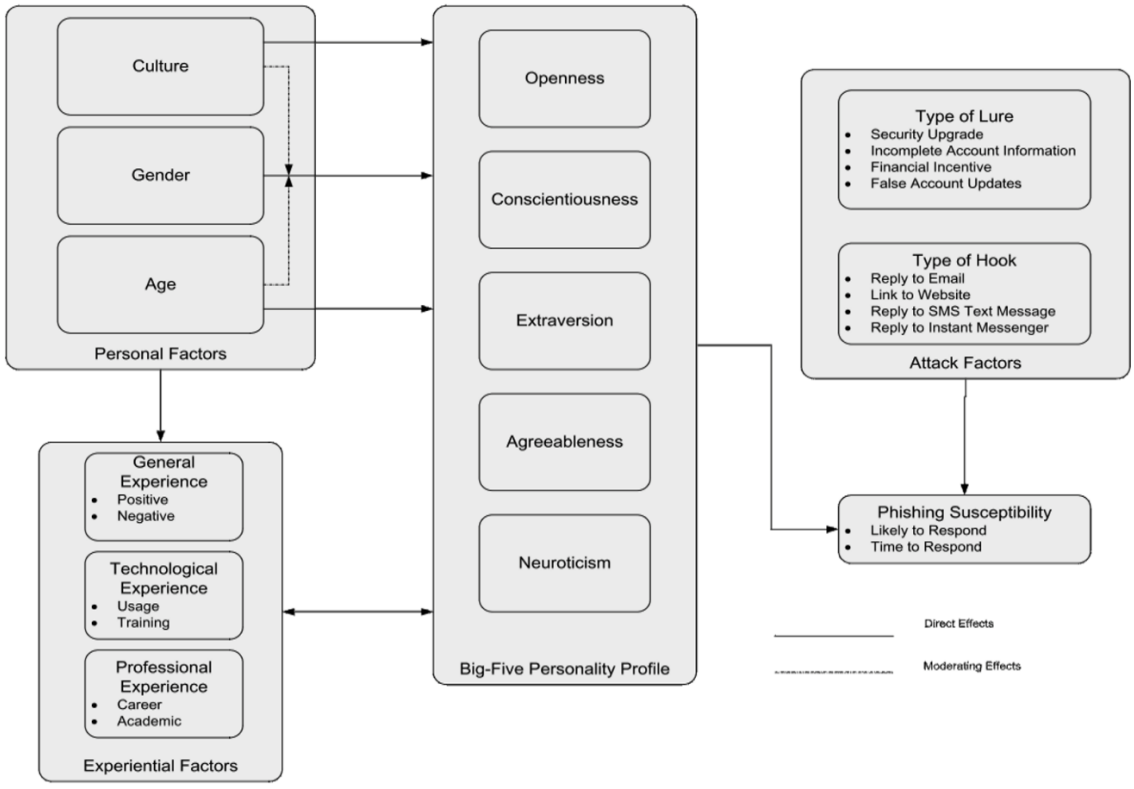
The personality factors discussed above are complex, and there is much interplay between users' basic personality types and the various contexts in which users operate. There have been a number of frameworks and models proposed that attempt to explain a user's susceptibility to CSE (e.g., phishing attacks). These models lay out more clearly the various contributing personality and contextual factors that can increase or decrease users' susceptibility to CSE. Appendix A presents 12 studies that investigated the relationship between personality traits and susceptibility to CSE in email and/or SNS contexts. The following sections (2.9.1.1 – 2.9.1.4) describe four of the CSE susceptibility frameworks that were developed, all of which integrate the Five Factor Model (FFM). The four frameworks are presented in chronological order according to their respective years of publication; they are then compared and contrasted in Section 2.9.1.5.

2.9.1.1 Phishing Susceptibility Framework – Parrish, Bailey, and Courtney (2009)

Many of the frameworks and models integrating FFM to examine CSE susceptibility were developed in the context of phishing emails. Parrish, Bailey and Courtney (2009) proposed a framework (Figure 2-7) that future researchers could use to find out more about why susceptibility to phishing attacks varies among users. Their model utilised the Big-Five framework to predict the human aspect of risky behaviours; it also integrated demographic factors (culture, age and gender) and experiential factors (general/life, technical, and professional experience; see Section 2.8.3.3) to understand the reasons for a user's inability to detect suspicious attacks. Previous studies (Costa *et al.*, 2001; Rolland, 2002; Srivastava *et al.*, 2003) found that age and culture could be moderating factors impacting on the development of personality, and that these effects also differed according to gender. Thus, Parrish *et al.* (2009) noted that it was important to add personal and experiential factors. They argued that these factors might influence the success and failure of phishing attacks and reveal user differences that required further exploration. For example, age, culture, and gender could have a direct influence on the degree of experience (whether general/life, technological or professional) amongst vulnerable users, and there could be an interplay among personal factors which might affect aspects of a user's Big Five personality profile. Parrish *et al.*'s (2009) framework for susceptibility to phishing was proposed for the email context in order to provide a structural support for further research in the realm of IS security. However, to this researcher's knowledge, their model has not been empirically tested.

Figure 2-7 Proposed Framework for Susceptibility to Phishing Email

Source: Parrish et al. (2009, p. 290)



2.9.1.2 Social Engineering Personality Framework (SEPF) – Uebelacker and Quiel (2014)

Uebelacker and Quiel (2014) developed a theory-based framework as a building block for their research, adopting FFM and Cialdini's (2001) six principles of persuasion (which these authors call "*principles of influence*") (Figure 2-8). This model was developed prior to Cialdini identifying the seventh principle, *unity* (Cialdini, 2016). Their framework was a theoretical tool that attempted to clarify individual differences in susceptibility to SE which, they asserted, would "*guide a researcher to provide a structural approach*" (Uebelacker and Quiel, 2014, p. 28). Using the findings of previous studies on the application of FFM, they inferred which personality types were associated with either a high or low susceptibility to the most impactful, influential techniques (6 principles). For instance, the framework was guided by the results presented by Cialdini, Trost and Newsom (1995) that highly extroverted people are less committed and consistent (shown in the dashed link in Figure 2-8 below) but are more likely to be attracted to *liking* and *social*

proof (shown with the solid link in Figure 2-8), while those who are highly agreeable are more driven to authority, reciprocation, liking and social proof, etc. They argued that women's tendency to be more agreeable was the reason behind their relatively greater vulnerability to risk.

However, Uebelacker and Quiel's (2014) model was based on a theoretical review, and although they referred to validated scales for the FFM constructs, they did not employ any validated measure for the constructs of the persuasion principles, such as the Susceptibility to Persuasion Scale (SPTS; Kaptein *et al.*, 2012). Researchers who subsequently investigated the relationship between personality traits and susceptibility to persuasion did refer to the SPTS. Alkiş and Temizel (2015) tested it on students in Turkey, Gkika *et al.* (2016) used Kaptein *et al.*'s (2012) methodology (but not their scale) on students in Greece, and Oyibo, Orji and Vassileva (2017) tested the SPTS in their research on Canadian participants (of whom 35.2% were students). Interestingly, none of these later studies cited Uebelacker and Quiel's (2014) framework, even though Oyibo *et al.* (2017) presented a model that was an exact mirror image of the SEPF. Thus, as of the date of this writing, it is unclear whether these later studies would constitute direct empirical evidence to support Uebelacker and Quiel's (2014) SEPF.

Moreover, the SEPF did not posit susceptibility as the dependent variable; therefore, findings of how each personality trait was influenced by each of the persuasion principles would not necessarily indicate vulnerability to social engineering That is, in the SEPF, the way in which each of the Big Five is influenced by authority, scarcity, reciprocity, social proof, liking, and commitment and consistency can only be retrieved from real-world data. It cannot be assumed that if, for example, agreeableness is positively influenced by authority, this relationship would always result in susceptibility. The level of influence between the Big Five personality traits and the six persuasion principles is expected to differ for each of these 30 potential relationships. For example, in order to demonstrate the extent to which agreeableness is positively influenced by authority and thus to establish the level of susceptibility, the model must include a *susceptibility to social engineering* construct. This added construct would allow a clear indication of whether or not these relationships are actually linked to this missing construct (susceptibility to social engineering). Perhaps this is one reason that later researchers who also investigated the relationship between personality traits and persuasion with susceptibility as a variable of interest or outcome did not make use of Uebelacker and Quiel's (2014) SEPF.

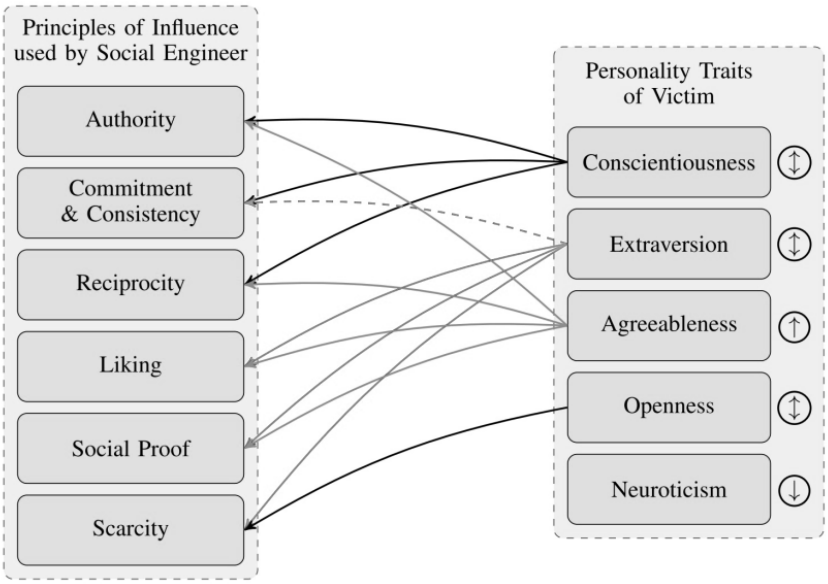


Figure 2-8 Framework of Social Engineering Personality Traits (SEPTF)

Source: Uebelacker and Quiel (2014, p. 27)

Note: Solid lines indicate positive influence, dashed line shows negative influence, and greyscale is applied so as to visually distinguish some lines from others. Arrows within circles indicate general personality assumptions about susceptibility (higher, lower, or both) for each trait.

2.9.1.3 Personality Traits-Mediator Susceptibility Model – Albladi and Weir (2017)

Albladi and Weir (2017) tested their Personality Traits-Mediator Susceptibility Model (see Figure 2-9) by conducting a study using a scenario-based system. The aim of the model was to gain insight into the role of the Big Five (OCEAN) personality characteristics in predicting a user's vulnerability to cyber-attack victimisation in the context of social media. The model examined each of the FFM traits and its relationship with four mediating factors (motivation to engage in the Facebook network, competence to deal with online threats, trust in other members and the platform service provider of the SNS, and previous experience with cybercrime), particularly in relation to Facebook. Their findings suggested that four of the personality types, excluding openness, have shown a significant indirect effect, that is, mediated by other factors (competence, trust, motivation, previous experience) on a user's susceptibility to cyber-attack. Surprisingly, as can be seen in Appendix A, unlike previous studies (Alseadoon *et al.* 2015; Parrish, *et al.*, 2009; Uebelacker and Quiel 2014), the agreeableness trait was shown to decrease susceptibility.

Their findings regarding the traits of vulnerable users in connection with the four mediating factors are as follows:

- *Conscientiousness*, with the mediating factor of competence, showed an indirect negative effect on susceptibility. There was no effect with motivation as the only mediating factor, but a joint negative effect was found when both motivation and trust were at play.
- *Neuroticism* was found to have an indirect negative effect only with the mediating factors of competence and trust (each on their own).
- *Agreeableness* was found to have an indirect positive effect only when past experience was a mediating factor.
- *Extraversion* had no effect with the mediating factor of motivation, but did have an indirect positive effect when both motivation and trust were present.

As discussed above, certain demographics have also been found to play a role in increasing or decreasing susceptibility (Sheng *et al.*, 2010; Halevi *et al.*, 2013a, 2013b; Blythe *et al.*, 2011; Goel *et al.*, 2017; Jagatic *et al.*, 2007; Saridakis *et al.*, 2016); however, no demographics were examined in Albladi and Weir's (2017) study. Because predicting human behaviour is a complex task, the authors suggested that further investigation of personality types in the context of SNS would be required. Table 2-4 shows the most important findings and areas for future research presented by Albladi and Weir (2017).

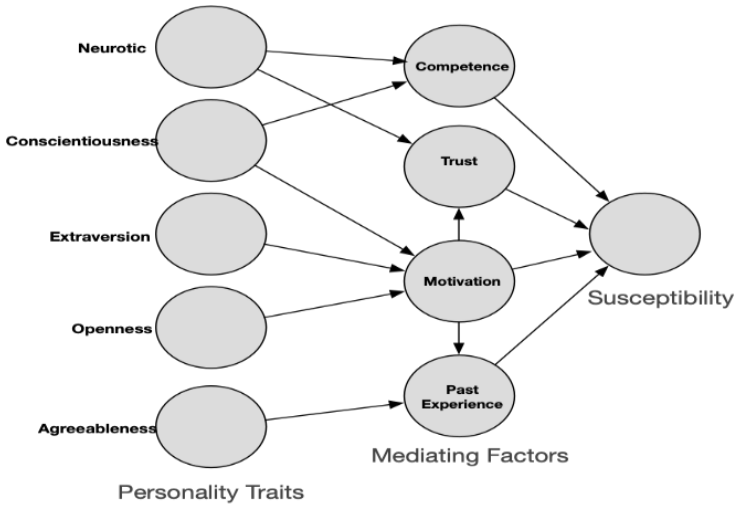


Figure 2-9 Mediating Model of SNS User's Susceptibility

Source: Albladi and Weir (2017, p. 2)

Table 2-4 Study Model Findings and Recommendation

Mediation Effects	Effects of Personality Traits	Future Research
Trust, motivation and previous experience with cybercrime as mediating variables positively and significantly influenced user susceptibility. Mediating factor of competence had negative effect on susceptibility to CSE.	Agreeableness had a significant negative effect on users' vulnerability to cyber-attacks. Extraversion was the trait with the most significant positive effect on user susceptibility.	More research on the impact of personality traits as antecedents of the other external factors is required, particularly to find how they impact behaviours and susceptibility to cyber-attacks on SNS.

Source: Albladi and Weir (2017).

2.9.1.4 Personality and Information Processing Model of Susceptibility to Phishing on SNS – Frauenstein and Flowerday (2020)

Like Uebelacker and Quiel (2014), Frauenstein and Flowerday (2020) considered Cialdini's principles of persuasion in conjunction with the Big Five personality traits as the theoretical basis for the effectiveness of CSE techniques such as phishing. However, unlike Uebelacker and Quiel's (2014) framework, Frauenstein and Flowerday (2020) did not incorporate the persuasion principles into their model, but instead added two mediating variables: systematic processing and heuristic processing (Figure 2-10). Frauenstein and Flowerday's (2020) examination of factors influencing user susceptibility to cyber-social engineering attacks focused in particular on the vector of phishing over SNS. The aim of their study was to quantitatively examine the association between SNS users' personality characteristics and their use of heuristic versus systematic cognitive information processing (see Section 2.8.2.4) in reacting to receipt of a phishing message. Frauenstein and Flowerday (2020) have claimed that theirs was the sole study to have tackled this particular relationship and how it might impact SNS users' susceptibility to phishing.

Frauenstein and Flowerday (2020) posited that heuristic processing would increase the likelihood of a user's susceptibility to phishing on SNS, whereas systematic processing would decrease the likelihood of such susceptibility. They further posited that personality type would influence whether an SNS user would employ systematic or heuristic processing in reacting to a phishing message. The authors hypothesized that each of the FFM traits has an association (either positive or negative based on the findings in the literature) with the use of heuristic and systematic processing, and that (as mentioned

above) this choice in turn would either increase or decrease susceptibility to SNS phishing attacks.

Using an online survey (a self-report questionnaire), Frauenstein and Flowerday (2020) collected data from a convenience sample of final year undergraduate students from three South African colleges (215 respondents: 53% male, 47% female). Their study looked at this particular population because students on the verge of graduation might bring security risks to those organisations that would subsequently hire them. Susceptibility was measured by presenting respondents with a screenshot of an actual phishing email that purported to be a notification from Facebook, and requesting the study participants to indicate their response to the following items: ("*reply to the email*", "*check the attachment*", "*ignore the email*", "*I do not trust this email*", or (the neutrally "*unsure*"). Frauenstein and Flowerday (2020) found that 40% would "*check the attachment*" (i.e., they were susceptible), nearly 10%% would delete the email and only 21% did not trust the phishing email. Their overall findings pertaining to the influence of personality traits on the type of information processing and the consequent outcome on susceptibility was illustrated in the structural model presented in Figure 2-10.

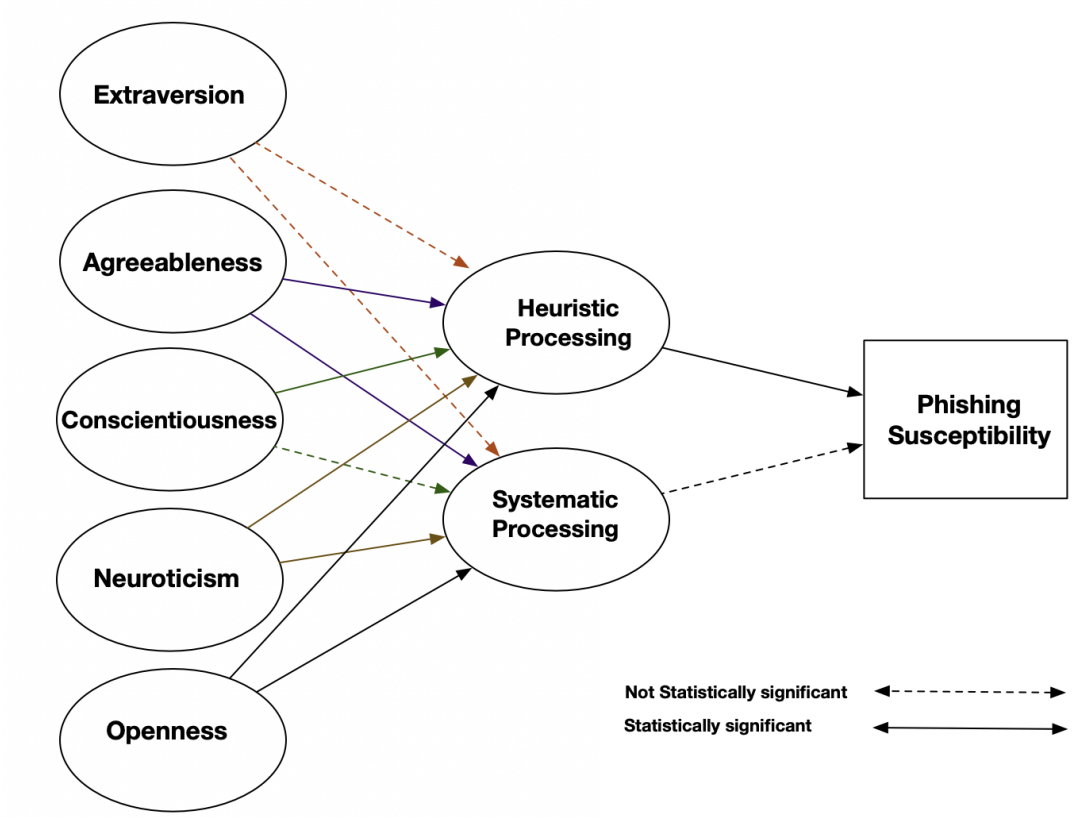


Figure 2-10 Personality Information Processing Model of Susceptibility to Phishing on SNS

Adapted from Frauenstein and Flowerday (2020, p. 8)

Frauenstein and Flowerday (2020) found that three of the five personality traits (openness, agreeableness, neuroticism) showed statistically significant relationships with both heuristic and systematic processing, in ways which may make students susceptible to phishing over SNS. Contrary to their expectations based on previous research findings, however, extraversion had no statistically significant relationship with either of the mediating variables. The authors surmised that this anomalous finding might be explained by the finding by Rolland (2002) that extraversion was "*sensitive to the cultural background of individuals*" (Frauenstein and Flowerday, 2020, p. 13). However, Rolland (2002) had also reported that agreeableness exhibited a similar sensitivity to culture, and yet Frauenstein and Flowerday's (2020) study found that agreeableness had a positive and significance influence on both mediating variables.

They further found that conscientiousness had a statistically significant negative relationship to heuristic processing, which they concluded was indicative of lower susceptibility to phishing attacks on SNS. Neuroticism had a statistically significant relationship with both mediating variables. The correlation of neuroticism with heuristic processing was contrary to expectation, whereas the strong positive relationship of this trait to systematic processing agreed with findings in the literature and indicated low susceptibility. Openness had a statistically significant positive association with heuristic processing, which was expected based on previous findings; this trait's statistically significant positive relationship with systematic processing was in contradiction with findings in the literature, however. Finally, Frauenstein and Flowerday (2020) found that heuristic processing had a significant positive influence on susceptibility to phishing.

2.9.1.5 Comparison/Contrast of Models Incorporating FFM

This section has presented four published frameworks of individual susceptibility to cybercrime victimisation. Two of these were proposed models (Parrish *et al.*, 2009; Uebelacker and Quiel, 2014), whereas the other two have been empirically examined (Albladi and Weir, 2017; Frauenstein and Flowerday, 2020). One investigated the general risk of cybercrime attacks (Albladi and Weir, 2017), while two others mainly focussed on the phishing vector of cyber-social engineering (Parrish *et al.*, 2009; Frauenstein and Flowerday, 2020). Uebelacker and Quiel's (2014) framework was a theoretical model

proposed in order to explain how people could be victimised by social engineering in general, through the mechanisms of the six principles of persuasion or influence.

Each of these models employed FFM differently. Parrish *et al.* (2009) applied the Big Five as mediating factors between demographic (age, gender, culture) and experiential (general, technical, professional) factors and phishing susceptibility. Albladi and Weir (2017) looked at personality traits as a predictor to susceptibility to being victimised by cyber-attack on SNS. They used multiple behavioural and experiential characteristics as mediators between FFM and susceptibility: user's motivation to engage on SNS, trust in other SNS members and the platform provider, competence (i.e., self-efficacy) in dealing with risks and previous experience with cyber-crimes. Frauenstein and Flowerday (2020) looked at cognitive information processing (i.e., heuristic and systematic processing), applying these as mediators between personality traits and phishing susceptibility on SNS. Unlike these three models, Uebelacker and Quiel's (2014) proposed exploratory model looked at the direct impact of personality traits on the six principles of influence. Their model was not concerned with phishing emails and SNS, but rather aimed to explore how susceptibility to social engineering could take place via employee interactions with ICT (specifically, computer and telephone networks) in the workplace. However, as explained in Section 2.9.1.2, because their SEPF model did not posit susceptibility as the dependent variable, findings of how each personality trait was influenced by each of the persuasion principles would not necessarily indicate vulnerability to social engineering had it been tested in a real-world study.

The two empirically tested models also differ from each other in terms of their population samples, data collection techniques and chosen FFM inventory. Frauenstein and Flowerday (2020) collected data from a convenience sample of 215 final year undergraduate students. Although it could be argued that a sample of students in the same year cohort can reflect the broader population in terms of some demographical, experiential and contextual aspects, it has long been understood that, "*compared with older adults, college students are likely to have less-crystallized attitudes, less-formulated senses of self, stronger cognitive skills, stronger tendencies to comply with authority, and more unstable peer group relationships*" (Sears, 1986, p. 515). Hence, such a sample would not be representative of the broader population. In contrast, Albladi and Weir (2017) collected data from both staff and students to test their model. Both of these models were examined through deploying an online self-report and convenience sampling approach. These methods can minimise

generalisability of the findings, because college students do not represent the general public in terms of age, experience, education and other characteristics.

Another limitation of the empirical examinations of these two models was that in order to measure susceptibility, participants were asked to respond to images of attack samples one at a time. In the real world SNS environment, users would likely be exposed to a much greater set of posts showing in their timeline, and how they engage with or avoid them can differ in a natural cognitive processing situation. Furthermore, their research involved the use of stimuli (sets of images) to prompt responses, which could result in a priming effect, meaning that it could inadvertently influence the participants' responses (Lavrakas, 2008). With regard to the two untested frameworks, their strengths and limitations would become clearer once they have been empirically examined, ideally in a real-world application.

2.9.2 Susceptibility Frameworks Incorporating Cognition and Behaviour

Researchers have identified other factors that explain CSE susceptibility in the context of SNS. Their constructs can be categorised under psychological aspects, such as *perceptual-related*, which involves perceived worthiness, perceived attraction, perceived competence, and perceived sincerity (Algarni *et al.*, 2014), as well as perceived risk and perceived control over information (Saridakis *et al.*, 2016). A number of other studies have investigated an individual's susceptibility to CSE in an email environment (Vishwanath *et al.*, 2016; Junger *et al.*, 2017; Goel *et al.*, 2017; Halevi *et al.*, 2013a, 2013b). As explained in Section 2.7, the persuasion principles work in cyberspace as well as in the physical world, and this is the basis of the model proposed by Algarni *et al.* (2014). Similarly, these principles should be equally effective in SNS and email contexts. Thus, models of CSE susceptibility in email contexts may be applicable to SNS as well. For example, Williams *et al.* (2017a) conducted a holistic review of psychological and contextual factors to propose a framework to test hypothesised vulnerabilities of factors and their interactions. These studies identified factors that are *cognition-related* (e.g., cognition and suspicion: Vishwanath *et al.*, 2016; cognition and social engineering: Montañez *et al.*, 2020) and *behaviour-related* (e.g., email habits and self-control: Vishwanath *et al.*, 2016). Williams *et al.* (2017a) identified other psychological factors (self-awareness, self-deception, self-control, propensity to trust, decision making by heuristic techniques, expertise, motivation, approach to risk, emotion) and *contextual-related factors* (culture, organisation). These five models are presented in chronological order according to their respective years of

publication (Sections 2.9.2.1 – 2.9.2.5); they are then compared and contrasted in Section 2.9.1.6.

2.9.2.1 Model of Impact of Source Characteristics on Users' Susceptibility to SE Victimization – Algarni *et al.* (2014)

The model presented by Algarni *et al.* (2014; see Figure 2-11) is based on *source credibility theory*. This theory is extensively applied in the marketing and communication domains to examine how likely an audience (the recipient) is to believe and accept a message from a particular sender or *source* (Eisend, 2006). The use of this theory helped Algarni *et al.* (2014) to identify 13 factors that would impact credibility, which they aggregated under four dimensions:

1) Perceived sincerity
2) Perceived competence
3) Perceived attraction
4) Perceived worthiness

The first three characteristics (perceived sincerity, competence and attraction) have been identified in previous marketing and communication research, while the fourth, perceived worthiness, resulted from their initial research. Their exploratory qualitative study looked at how these factors might influence a Facebook user's judgements as to the credibility of the attacker (impersonator). The researchers stated that because the variables they were interested in had been developed and tested in a different field of research (marketing), they chose to use an inductive method to construct their model (see Chapter Four, Section 4.4.1). They thus applied a grounded theory method by decoding interviews and initially identifying *a priori* factors from that data to be explored further. They then qualitatively validated each perceptual factor (perceived sincerity, perceived competence, perceived attraction and perceived worthiness) that could lead to victimisation. In order to mitigate bias stemming from self-reported data, Algarni *et al.* (2014) also observed the Facebook profiles and timelines of the study participants. The sample comprised 24 employees (11 females, 13 males) from various international organisations.

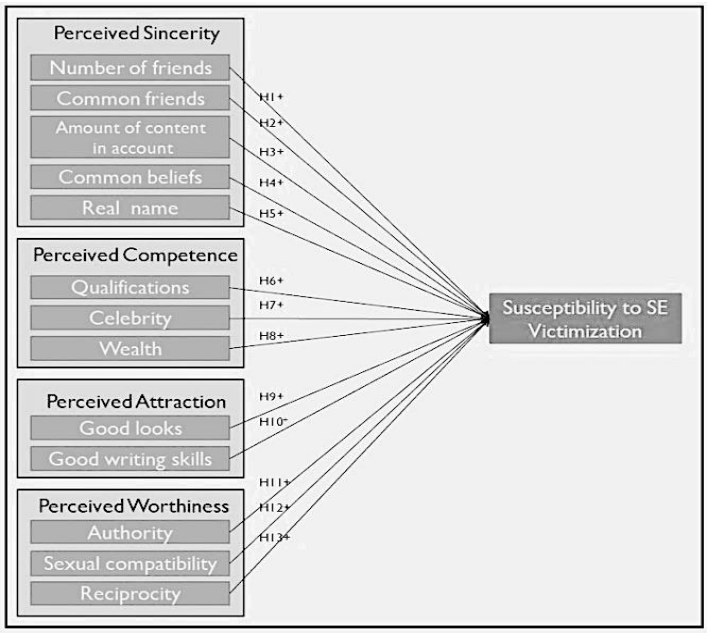


Figure 2-11 A Priori Model of the Impact of Source Characteristics on Users' Susceptibility to SE Victimization in Facebook. Source: Algarni et al. (2014)

The first dimension, perceived sincerity, was defined as including factors of honesty, trustworthiness and plausibility. The study revealed that users tended to feel comfortable with transparent profile information, a clear profile photo, and the use of first and surname rather than a nickname. With regard to perceived competence, the factors identified were qualifications, celebrity and wealth. When these factors were seen in the data many interviewees were inspired to follow, like or share the content of these profiles, some of which were found to be cloned profiles of existing users or impersonating figures who apparently did not have an SNS account. Factors in the dimension of perceived attraction were good looks and writing skills, as interviewees indicated that these factors reflected credibility.

The perceived worthiness dimension emerged from the interviewees' views that the friend requestor needed to be "worthy" of their friendship, through one of three factors: authority, sexual compatibility, or reciprocity — they would receive as much as they gave. Algarni *et al.* (2014) concluded that all 13 source characteristics identified in their model were "*critical in judging source credibility*" and thus they would impact the user's susceptibility to SE on SNS (p. 803). Personality type was also identified but was not examined in relation to susceptibility to CSE. As per the authors, these traits were added to ensure a diversified demographic of participants. They asserted that although further exploration would be needed to examine the validity of their findings, these results formed the basis for research

on deception and scams in SNS, data mining and privacy protection, among others (Algarni *et al.*, 2014).

2.9.2.2 Model of Social Media Behaviour and Risk of Cybercrime Victimisation – Saridakis *et al.* (2016)

Saridakis *et al.* (2016) developed a framework of victimisation risks for SNS platforms (Figure2.12). They used routine activity theory (RAT), theory of reasoned action (TRA) theory of planned behaviour (TPB) with this last theory's construct of perceived behavioural control (PBC) (Chapter Three, Section 3.1) to formulate a number of hypotheses. Saridakis *et al.* (2016) contended that the more actively users engaged on SNS, the more likely they were to become victims. They posited that people who perceived they had high control over their personal data on SNS platforms would be less likely to be exploited. They argued that users with high perceived control over their information would use the available SNS security safeguards and would thus be less likely to fall victim to cybercrime (for contrasting views, see Section 2.8.2.2). The authors also hypothesised that users with high IT self-efficacy (which they refer to variously as "ICT efficacy", "technical efficacy", "computer efficacy" and "computer self-efficacy") would be less likely to be victimised by cybercrime, whereas users with low risk perception and high risk propensity would be more susceptible to cyber-attack.

For their cross-sectional study, Saridakis *et al.* (2016) applied a self-selected, self-reported approach via an invitation to targeted SNS users to participate in an online survey. The researchers first examined users' habitual behaviours: specifically, how many SNS accounts an individual user had and how much time that individual spent on SNS platforms. They used these two elements together to measure "SNS usage". Saridakis *et al.* (2016) examined this variable by identifying types of SNS as per classifications employed by Hoffman and Fodor (2010), Kaplan and Haenlein (2010) and Xiang and Gretzel (2010). They asserted three categories of SNS (examples provided in round brackets below have been updated to reflect current trends):

1) Multipurpose dominant SNS (e.g., Facebook, Skype, WhatsApp, YouTube); users on these platforms share and access multimedia content and interact virtually.

2) Narrow-purpose SNS (e.g., World of Warcraft, Pinterest, Goodreads, TikTok); users of these niche sites tend to have specific interests, such as gaming, food/fashion, literature and micro-videos.

3) Knowledge-exchange purpose SNS (e.g., Twitter, LinkedIn, Medium) where users can exchange ideas and share and access information, whether via microblogging (Twitter) or longer form (Medium).

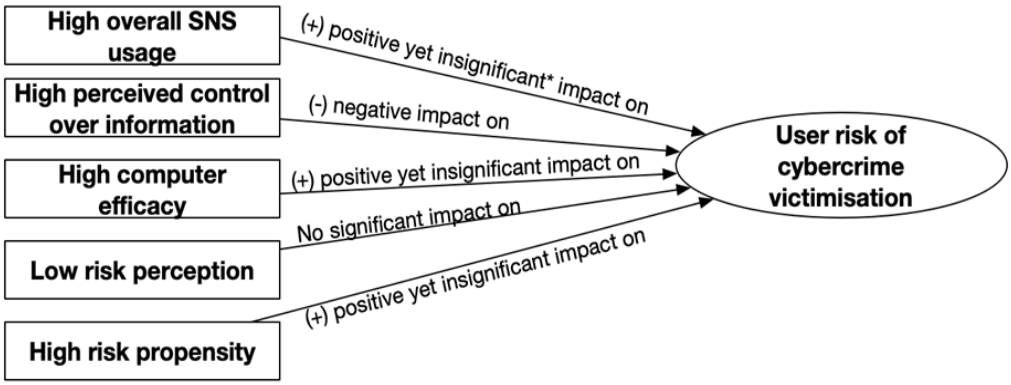


Figure 2-12 Final Model of Social Media Behaviour and Risk of Cyber Crime Victimisation Adapted from Saridakis et al. (2016, p. 323)

The above five hypotheses were examined via self-reported responses to the questionnaire; they had received usable questionnaires from 514 participants. Saridakis *et al.* (2016) found that, separately, the association with susceptibility to cybercrime victimisation differs for use of each of the three categories of SNS. These findings showed:

1) Multipurpose dominant SNS: a statistically significant negative association
2) Narrow-purpose SNS: no association
3) Knowledge-exchange purpose SNS: a statistically significant positive association

However, the authors noted that when these three categories were aggregated to generate an index of overall SNS usage, the resulting association was not significant. They interpreted the foregoing as partial support for their hypothesis that high frequency of SNS use had a direct positive impact on users' risk of cybercrime victimisation.

Saridakis *et al.* (2016) found that high perceived control over information was significantly negatively associated with risk of being victimised by cybercrime. Based on previous studies, Saridakis *et al.* (2016) had hypothesised that a low level of risk perception would have a positive effect on risk of victimisation. Surprisingly, however, they found no

significant impact on risk of cybercrime victimisation. In contrast, risk propensity was found to be positively associated with susceptibility to cyberattack. That is, when the risk propensity of an individual is high, victimisation is more likely to occur. The authors found no evidence to support the proposition that high IT efficacy might reduce the risk of cyberattack; in fact, it found a positive (but not significant) association between higher IT efficacy and risk of victimisation. The final results, showing the extent to which each of the examined factors had an effect on victimisation, are summarised in Figure 2-12.

Although gender, age and professional status were not considered as impacting factors in the study, they were examined statistically via collected demographic data. Saridakis *et al.* (2016) then looked specifically at whether the associations would maintain robustness if these individual characteristics were accounted for. Their study showed no gender effect on victimisation, contradicting previous findings in the literature (see section 2.8.5.2). They also reported that users aged 29-38 and 49-58 were less likely to be victims of cybercrime than those aged 18-28. Somewhat counterintuitively, especially considering the age-based findings, users with post-graduate, professional or technical status were more likely to be victimised than students and undergraduates.

Based on their findings, the authors proposed a model (see Figure 2-13) to help reduce susceptibility to various types of cyber victimisation when using Twitter and Facebook. This was based on the theory of planned behaviour (TPB; Ajzen, 1985; see Chapter Three, Section 3.1.3), which is used to predict behaviour in various contexts (Fleming *et al.*, 2017). When online users refrain from reporting their victimisation incidents and SNS services do not report cybercrimes that have taken place on their platforms, this is compounded by two human factors: high risk perception and low willingness to assume risk, which could both help in reducing cybercrime victimisation.

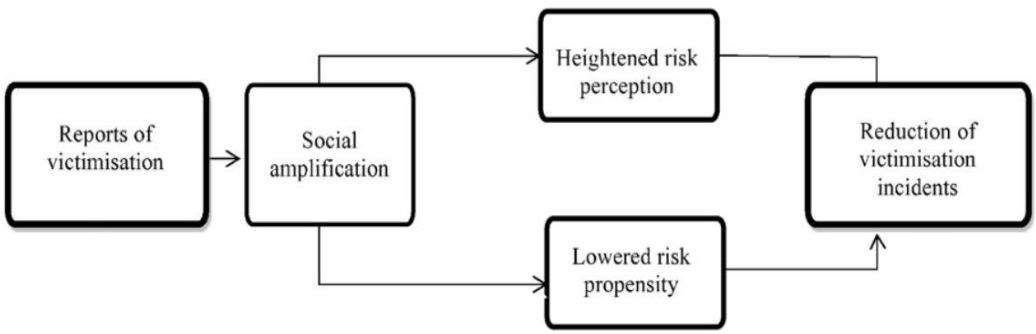


Figure 2-13 Proposed Mitigation of SNS Cybercrime Victimisation

Source: Saridakis et al. (2016)

2.9.2.3 SCAM (Suspicion, Cognition and Automaticity Model of Phishing Susceptibility) – Vishwanath *et al.* (2016)

Vishwanath, Harrison, and Ng (2016) developed their Suspicion, Cognition and Automaticity Model (SCAM; see Figure 2-14) by integrating an earlier model of information processing, suggesting that individuals make decisions about emails based on simple embedded cues (Vishwanath *et al.*, 2011). Their model was built on research in social psychology that suggests that ineffectual cognitive processing, such as ineffective reasoning through logic or making judgements using available information in an email, can be the key factors in phishing victimisation. The purpose of SCAM was to:

1) understand the functionality of how individuals are susceptible to victimisation by phishing attacks, and
2) understand the relative influence of cognition and habitual activities to explain victimisation risks.

The model encompasses multiple hypothesised "*core*" constructs: cognition, heuristic processing and systematic processing, cyber-risk beliefs, self-control and email habits; these are explained as follows:

Suspicion: Vishwanath *et al.* (2016) introduced this construct by explaining that although the construct *trust* had often been employed as a predictor of susceptibility, they found several drawbacks to this posited relationship. They argued that (1) *trust* comprised multiple dimensions, which would make it difficult to measure consistently; (2) "*conflicting interrelationships*" existed between different sorts of trust (for example, trust was "*orthogonal to*" rather than the opposite of distrust and "*trustworthiness*" was not the same as *trust*); and (3) trust was "*a rather poor predictor of deception-detection because the presence of trust desensitizes individuals to deception cues*" (p. 4). The authors posited that instead, *suspicion* (which they construe as "*the outcome of* [rather than a precursor to] *cognitive processes*", p. 18) should replace trust as a predictor of susceptibility. Of course, the relationship between suspicion and susceptibility would be the inverse of the association between trust and susceptibility, as the less suspicious a user was about a suspected phishing email, the greater their likelihood of susceptibility, and vice versa. Thus, SCAM used "*suspicion as the major endogenous predictor of individual susceptibility to email-based phishing*" (p. 5). That is, they posited that suspicion was a key predictor of susceptibility and that this relationship could not be attributed to external factors.

Cognition: This construct is linked to suspicion in that, when contextual factors point to contradictions between what is expected and what is perceived, a person's cognitive processes will spark suspicion (Lyons *et al.*, 2011). What is expected is the user's expectation of reality, and this is what the user believes is acceptable. What is perceived is when a user cognitively evaluates information within the same context, and the information in the context gives rise to suspicions about phishing emails. In other words, cognitive constructs encompass heuristics as well as systematic processing of persuasive messages, such as a suspected phishing email (see Section 2.8.2.4; Vishwanath *et al.*, 2016; Williams *et al.*, 2017a).

Cyber-risk beliefs: Cyber-risk beliefs (Section 2.8.2.3) are similar to other risk-related beliefs, but are specific to the online context (Vishwanath *et al.*, 2016). This factor is a core exogenous construct of SCAM that bridges the user's subjective knowledge of cyber risks with his/her experience and self-efficacy. Previous social psychology research has shown that an individual belief is formulated based upon external factors, such as previous experience and exposure to media, and internal factors, for example, personality and self-efficacy (Bandura, 1989; Vishwanath *et al.*, 2016).

Self-regulation (self-control): This is a susceptibility defence mechanism that works by setting self-limitations and boundaries with which the individual complies. It is in this context that users find they must be vigilant about their own actions when dealing with media-related channels (Vishwanath *et al.*, 2016). Moreover, people with deficient self-control can feel controlled by their own habits, which according to LaRose (2010) are "*automatic thought processes that are powerful predictors of media behavior*" (LaRose, 2010, p. 194). Thus, self-regulation is related to the next construct:

Email habit (habitual factor and level of engagement): Vishwanath *et al.* (2016) posited that since people were periodically engaged in checking emails during their daily routine, it had become a habit to do so. This behaviour may jeopardise their cyber-risk beliefs, as "*individuals under the influence of email habits are less likely to be suspicious of phishing emails and more likely to be deceived*" (p. 8). Email habit is therefore an emerging construct. Vishwanath *et al.* (2016) contended that email habit contributed to an individual's gullibility and predisposition to be taken in by deception as it led them to overlook details (decreased suspicion of risks; see also Section 2.8.2.4 on heuristics), particularly in phishing emails. Habit was also posited as a phishing susceptibility

predictor, alongside other identified susceptibility predictor factors that account for cognitive, preconscious and automatic processes.

The model was part of a large research programme on cyber users' susceptibility. It was tested by two experimental studies conducting two real email-based attacks; these attacks were used to examine students' susceptibility to phishing emails in responding to two types of experimental attacks: 1) hyperlinked email and 2) opening attached malicious files (see findings in Table 2-5). The experimental email addresses used were official university addresses to give a sense of credibility.

The effects that these constructs had on each other are illustrated in the following framework (Figure 2-14). It is important to remember that susceptibility in this case was measured as a lack of suspicion. Moreover, the study did not account for personality traits, other than as "*external factors…thought to indirectly influence deception by influencing the core constructs*" (p. 8). Vishwanath *et al.* (2016) noted this as a limitation of their model and suggested that the effects of personality traits should be examined in further work in order to understand what made some individuals more sceptical than others when it came to online deception. They cited an earlier study (Levine and McCornack, 1991) of how personality traits could differ in interpersonal deception. Levine and McCornack (1991) highlighted a trait called Generalized State Suspicion (GSS), which has been shown to be responsible for increasing suspicions that consequently increase the likelihood of detecting deception and being less susceptible. Vishwanath *et al.* (2016) noted that what remained unexplored was how GSS might impact susceptibility in a phishing email context. Another limitation of their study was its focus on a phishing email trajectory despite the existence of other appealing methods to entice victims. The use of a university email system is also viewed as a limitation. SCAM could potentially explain user gullibility in SNS, although other more convincing deception techniques than those found in email messages certainly exist on SNS, given the plethora of opportunities available via SNS to spread deception (Silic and Back, 2016).

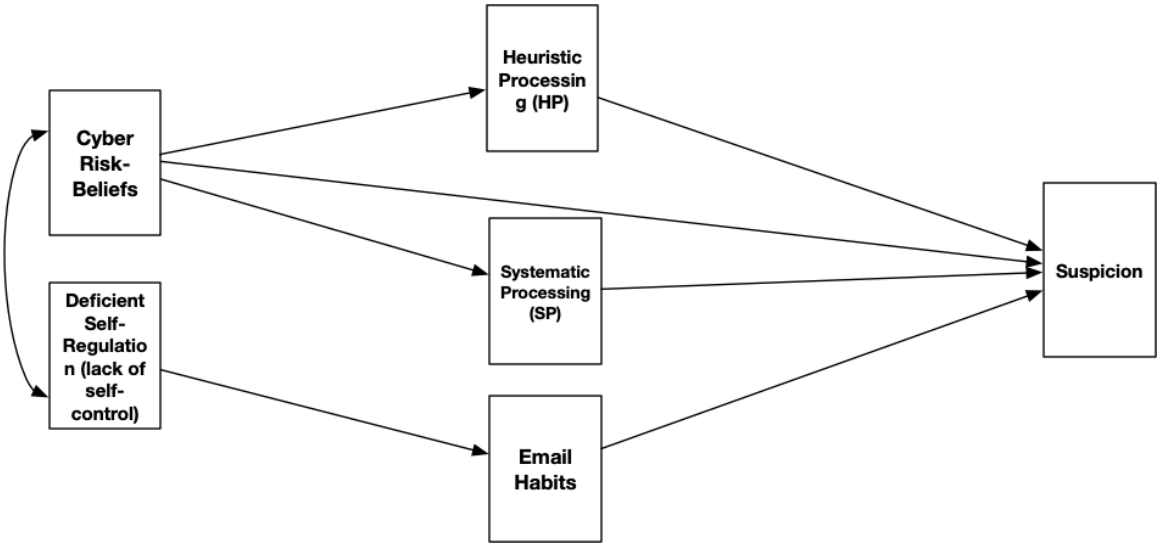


Figure 2-14 SCAM Model

Source: Vishwanath, Harrison and Ng (2016, p. 4)

Table 2-5 Relationship findings of phishing email experiment in 2 cases: clicking on links and opening attached file

Factors	Vishwanath *et al.*'s (2016) Research Findings	Type of Attack
Cyber risk-belief	This factor can impact users' cognitive analysis by decreasing heuristic processing in both experimental types; clicking on a link and opening an attached file.	Type 1) Phishing Link Type 2) Attachment
Heuristic processing	If increased, the authors argue that it will be less likely to lead to suspicion.	Phishing Link and Attachment
Systematic processing	If increased, will increase likelihood to be suspicious of potential attacks.	n/a
Deficient self-regulation (lack of self-control)	Lack of self-regulation influences high habituation to using emails.	Clicking on phishing links, opening attachments
Email habits	High habitual use of email can negatively influence levels of suspicion, similar to earlier study that habitual or frequent use of Facebook can lead to susceptibility to victimisation (Vishwanath, 2015).	Link and Attachment

2.9.2.4 Holistic Individual Susceptibility Model for Workplace Phishing – Williams *et al.* (2017a)

Williams, Beardmore and Joinson (2017a) proposed a theoretical foundation framework (see Figure 2-15) for future research on susceptibility to cybercrime victimisation in the workplace. The researchers started by naming eight "*influence techniques*" common to social engineering (Williams *et al.*, 2017a, p. 414), six of which are either exactly the same as or synonymous with the Cialdini's (2001) original persuasion principles. Williams *et al.* (2017a) added two techniques: *reward* (promise of monetary or psychological reward) and *loss* (threat of loss to recipients if they fail to respond; p. 414). Citing scant research on individual differences in susceptibility to scams in an online context, they conducted a review of the literature in the fields of consumer behaviour, decision making and persuasion. From that review they identified psychological and contextual factors that might affect a person's "*susceptibility to malicious influence online*" (p. 413). Seven individual differences emerged: *self-awareness, self-control, self-deception, (propensity to) trust, approach to risk, motivation* and *expertise*. The four contextual factors they identified were *heuristics, emotions, culture* and *organisation* (these factors are described in Sections 2.8.2 – 2.8.4).

The phishing susceptibility framework proposed by Williams *et al.* (2017a) attempts to show an individual's vulnerability factors as a whole. The authors grouped the "*risk factors*" into three levels: individual traits (T^{IND}, or *who*), cognitive and emotional states (St^{IND}, or *when*), and contextual factors (C^{IND}, or *where*). The fourth level depicted the influence mechanism (In^{MECH}, or *what*) used by the attacker (p. 417). This framework was developed to test interactions, as in the proposed equation (Figure 2-15):

Individual Susceptibility to Influence (S^{IND}) = *Individual Traits* (T^{IND}) + *Individual's Current State* (St^{IND}) + *Individual's Context* (C^{IND}) + *Mechanism of Influence* (In^{MECH})

$$\mathbf{(S^{IND})} = (T^{IND}) + (St^{IND}) + (C^{IND}) + (In^{MECH})$$

Figure 2-15 Holistic Individual Susceptibility Model (Williams et al., 2017a, p. 418)

Williams *et al.* (2017a) then proposed a framework based on this model, via which hypotheses about the interactions between these constructs might be tested. They posited that some of the 11 factors could have stronger effects on susceptibility than others, and in

their depiction of the framework the boxes containing those constructs are shaded (Figure 2-16).

T IND	High propensity to trust	Low self-control	Low self-awareness	High Risk-taking	High Self-deception	Expertise	High need for affiliation

St IND	Need for finance	Goal conflict	Desperation	Negative mood	Loneliness	Cognitive overload	Fatigue

C IND	Low power	Hierarchical Organisation Values	Individualistic Cultural Values	Relational Cultural Values

In MECH	Reciprocity	Scarcity	Commitment / Consistency	Conformity	Authority	Liking	Loss

Figure 2-16 Framework for testing hypotheses based on Holistic Individual Susceptibility Model (Williams et al., 2017a, p. 418)

The authors acknowledge that there is some overlap between factors listed in (T ^{IND}) and (St ^{IND}) levels (Williams, personal communication, 16/07/2018), such as need for affiliation, low power, and self-awareness, which would make it difficult to establish construct validity in an empirical study using their framework (see Chapter Four, Section 4.16). Additionally, and again prior to any empirical application, the complexity of the framework obscures a clear understanding as to how interactions among the various factors are interpreted as contributing to individual susceptibility. Indeed, Williams *et al.* (2017a) ponder this issue: "*…are these factors additive, in that each additional factor leads to a set increase in the degree of susceptibility, or are they multiplicative, in that certain combinations of factors lead to larger effects*?" (p. 418).

Further, some of the constructs mentioned in the model (see Figure 2-15) are either not explained thoroughly or not associated with any of the mentioned factors. For instance, fatigue, desperation and the need for finance are all grouped in the same category (St ^{IND}), although it can be argued that physical, mental and financial condition factors cannot be classified equally. Another weakness of the framework is that some factors are vague, such as the incomprehensible operationalisation of *self-deception*, and the complexity and generalisation of *emotions*.

Williams *et al.*'s (2017a) framework has not yet been empirically tested, although Williams, Morgan and Joinson (2017b) and Williams, Hind and Joinson (2018) conducted experiments examining susceptibility to authority and urgency (they differentiate urgency

from scarcity) in organisational/workplace settings. However, the model is useful in that some studies have examined the constructs of organisation and culture with regard to phishing emails and overall cyber victimisation risks; it has also been used to analyse employees' cybersecurity compliance (Williams *et al.*, 2018). These studies indicate that the assumptions of Williams *et al.* (2017a) with regard to culture are realistic, as they found that people from countries with individualistic national cultures, such as Australia and Sweden, were less likely to be susceptible to victimisation by CSE than those from nations that operated under collectivism, such as Saudi Arabia and India (Almakrami, 2015; Rocha Flores, 2016).

2.9.2.5 Cognition and Susceptibility to Social Engineering Cyberattack – Montañez *et al.* (2020)

Montañez, Golob and Xu (2020) have proposed a new sub-field of cybersecurity research that incorporated elements of cognitive theory, which they referred to as "*Cybersecurity Cognitive Psychology*" (p. 1). On the premise that social engineering cyberattacks (i.e., CSE attacks) are a specific type of psychological assault, they began by describing a framework of human cognitive function. Their framework adapted principles of cognitive psychology literature to account for factors that emerged from the cybersecurity domain. The authors used a broad definition of *cognition* (see Section 2.7) as being analogous to "*software*", supposing that the brain and its neurons were the "*hardware*" (Montañez *et al.*, 2020, p. 3). Thus, they assumed that cognition encompassed information processing – "*the basic function of the brain*" – and could also "*compute emotions*", but was not part of an individual's conscious awareness (p. 3).

This framework views human cognition as interaction between four cognitive domains (*perception*, *working memory*, *decision making*, and *action*) that Montañez *et al.* (2020) refer to as information processing components, analogous to software components for a computer's central processing unit. Briefly explained, *perception* takes information gathered via the senses and converts that information into neural codes to be employed in conscious behaviour. *Working memory* (analogous to random access memory in a computer) comprises both short-term memory and attention and shifts priority to different bits of information as needed. The *decision-making* component computes information from working memory and other sources such as long-term memory; decision making is then implemented as *action/behaviour* (p. 4).

The framework described by Montañez *et al.* (2020) included three short-term cognition factors (*workload*, *stress* and *vigilance*) and four long-term cognition factors (*personality*, *expertise*, *individual differences* and *culture*). They then extended this basic cognitive framework to account for social engineering cyberattacks (Figure 2-17).

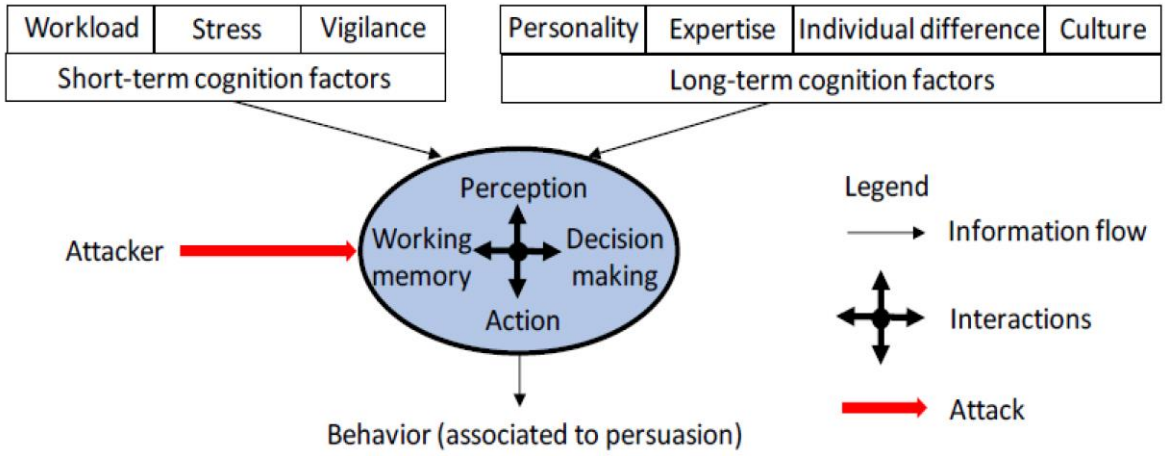


Figure 2-17 Schema of Human Cognition and SE Cyberattack (Montañez et al., 2020, p. 8)

Based on the existing literature, they posited the following:

Short-term Cognition Factors

Cognitive *workload* would likely reduce an individual's attentiveness (e.g., to phishing email cues; Vishwanath *et al.*, 2011), which could in turn lead to susceptibility to cyber-social engineering.

Stress may decrease an individual's ability to detect signs of malicious social engineering. In particular, stress may cause an individual to opt for heuristic rather than systematic processing when deciding how to react to a CSE attack. However, the authors highlighted that "*the direct effects of acute stress on cybersecurity social engineering have not been examined*" in the literature (Montañez *et al.*, 2020, p. 8).

Vigilance ought to help reduce susceptibility to online deception. However, vigilance deteriorates quickly over even a short period of time (Al-Shargie *et al.*, 2019), which could increase an individual's susceptibility to CSE attack.

Long-term Cognition Factors

Personality, particularly the FFM, and how it might influence susceptibility to phishing "*has been extensively studied*"; however, Montañez *et al.* (2020) argued that results from

the literature were inconclusive regarding the way in which personality influences susceptibility to CSE (p. 9).

Expertise, or rather three elements of expertise (*domain knowledge*, *awareness* and *experience*), emerged from their literature review as factors with potential to reduce susceptibility to CSE attack. Montañez *et al.* (2020) observed that these three components differed in their influence on an individual's susceptibility to CSE attack. They posited that expertise would have more impact than any other factor in reducing susceptibility to CSE, because this set of sub-factors equipped one to be able to detect CSE tactics.

Domain knowledge: is the term used by Montañez *et al.* (2020) to refer to IT self-efficacy. This element of expertise includes knowledge of how to surf the internet safely, such as the ability to detect and evaluate websites' certificates and other information indicating (lack of) authenticity. The authors posited that domain knowledge could aid in decreasing susceptibility to CSE attack.

Awareness: On its own, this factor was not likely to lower susceptibility to CSE attack, and even when combined with "*general technical knowledge*", awareness was deemed to have no effect on susceptibility, according to previous research (e.g., Halevi *et al.*, 2013a, 2013b; Junger *et al.*, 2017). Montañez *et al.* (2020) suggested that this could be because human cognition functions had not been considered in these relationships with regard to cybercrime (p. 10).

Experience, by which Montañez *et al.* (2020) mean one or more of the sub-factors "[*s*]*elf-efficacy*, *[IT] knowledge and previous encounters with cyberattacks*", should lower susceptibility to CSE victimisation, but only if these three elements were combined. Separately, these sub-factors of experience did not reduce susceptibility, according to the literature reviewed by these authors. They further posited that "*costly phishing experiences would greatly reduce one's susceptibility to social engineering cyberattacks, while non-costly experiences [would] not*" (p. 10).

Individual differences, for the purposes of Montañez *et al.*'s (2020) framework, referred only to *gender* and *age*. Based on conflicting results from previous studies that examined gender in relation to susceptibility to SE cyberattack (e.g., Sheng *et al.*, 2010; Halevi *et al.*, 2013a, 2013b, 2015, 2016; Saridakis *et al.*, 2016; Bullée *et al.*, 2017; Goel *et al.*, 2017; see Section 2.8.5.2), the authors speculated that gender would not have much influence on an individual's susceptibility to CSE attacks. Montañez *et al.* (2020) noted that studies

examining *age* in connection with susceptibility to SE cyberattack tended to focus on young adults (18-24) or rather older ones (45+), effectively ignoring the middle-aged demographic. According to what they gleaned from that literature, they posited that "*old people with higher education, higher awareness and higher exposure to social engineering cyberattacks*" would be less susceptible to CSE attacks (p. 11).

Culture as a factor in cybersecurity had been studied from various cognitive aspects: bias, decision making, risk perception, suspicion and attitudes to privacy (Hofstede *et al.*, 2010; Sheng *et al.*, 2010; Halevi *et al.*, 2016; Bullée *et al.*, 2017). Based on their review of the literature, Montañez *et al.* (2020) suggested that culture would influence attitudes towards privacy and trust, which would in turn impact susceptibility to CSE attacks.

Attack Effort

All the factors from this framework presented so far have described the target of the CSE attack. The final factor describes the attacker, or rather, the attacker's effort, including tactics and actions. These include *frequency of attacks, message appeal* (Cialdini's [2016] 7 principles of persuasion: Section 2.7) and *message quality*. From their review of the literature on the role of cognition in susceptibility to CSE attacks, Montañez *et al.* (2020) have suggested an inverse relationship between frequency of CSE attacks and the success of those attacks. With regard to message appeal, they noted two common CSE tactics that studies showed to be successful: contextualisation (pretexting) and personalisation: "*highly contextualized messages that target issues relevant to the victim are more successful*" (p. 15). While message appeal refers to a message's content, message quality refers to its form: well written, visually appealing and authentic looking. Montañez *et al.* (2020) asserted that these two factors "*which reflect attacker effort (e.g., using contextualization and personalization), have a significant impact on the attacker's success*" (p. 16). It should be noted that although they used the term "significant", they were not reporting any study results.

Montañez *et al.* (2020) further posited that, given the evidence in the literature that systematic processing is more successful than heuristic processing at thwarting CSE attacks (see Section 2.8.2.4), "*Training methods that ask people to consciously think about social engineering cyberattacks are unlikely to be very successful unless the learning reaches the point where it is a habit that, largely unconsciously, guides safer computer use behavior*" (p. 12).

The authors represented the essence of their framework via a "*mathematical function*" (p. 13):

behaviour = *f*(short_term_factors; long_term_factors; long_memory; attacker_effort)

They conceptualised the relative impact of each factor as positions on a spectrum that ranged from substantially reducing susceptibility to CSE attack to substantially increasing it (Figure 2-18).

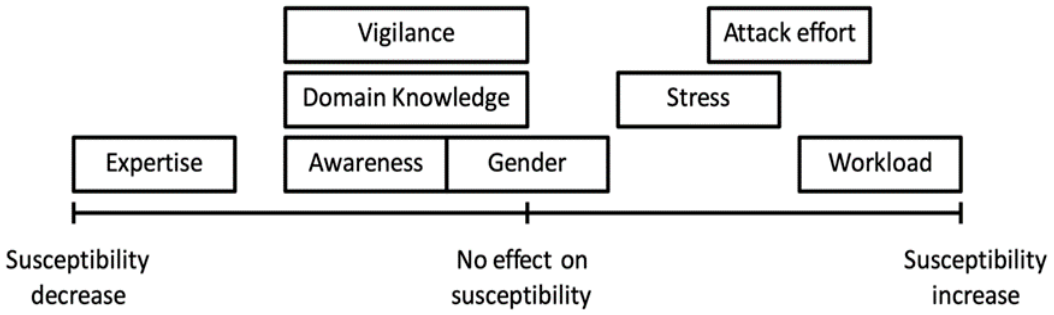


Figure 2-18 Speculation of relative impact of factors on susceptibility to social engineering cyberattack (Montañez et al., 2020, p. 18)

The authors suggested that users should be trained, not simply to be aware of SE attacks in cyberspace, but rather the training should focus on helping them to form unconscious cybersecurity habits to cope with these attacks. They also proposed that the above framework could be expanded to include physiological factors such as brain activity measurement and autonomic nervous system activity.

Montañez *et al.* (2020) claimed that their study was the first to systematically explore the psychological foundations of susceptibility to social engineering in cyberspace. Indeed, their model incorporates a range of factors prominent in the literature on "*cybersecurity cognitive psychology*". However, there appear to be weaknesses in their framework and in their presentation of the previous research. In their discussion of the role of experience as a factor, for instance, the authors appeared to conflate professionally grounded knowledge with past experience of cyberattack victimisation. In their summary of previous research on the effect of gender on susceptibility to CSE attack, they claimed that those studies indicating an association between these two constructs were "*initial studies*", while studies that had found no relationship between gender and CSE susceptibility were "*later studies*" (p. 11). This is questionable, considering that the dates of the studies in their "*initial*" group ranged from 2010 to 2016, while the dates in their "*later*" group were from 2014 to 2018.

To date, the model proposed by Montañez *et al.* (2020) has not yet been empirically validated.

2.9.2.6 Comparison/Contrast of Models Incorporating Cognition and Behaviour

The models discussed previously (Section 2.9.1) all incorporated the FFM. They considered individual differences, including personal disposition, and how they would influence a user's reaction to a CSE attack such as a malicious message. Some of those FFM-based frameworks also postulated how individual characteristics and dispositions could impact the cognitive state of the individual reacting to a CSE attack through mental processing, experiential factors, self-efficacy and goal-oriented behaviour. However, they mainly focused on personality traits, which are relatively stable characteristics (Uebelacker and Quiel, 2014). In contrast, the five models/frameworks discussed in this section (2.9.2) were designed to examine users' individual differences from various cognitive aspects, including perception, attitude, attitude to risk, trust/suspicion, habitual behaviour, IT self-efficacy and heuristic–systematic processing, when faced with a CSE attack. Two of the models were developed and tested in the SNS context (Algarni *et al.*, 2014; Saridakis *et al.*, 2016), one was developed and tested in the email context (Vishwanath *et al.*, 2016), one was proposed for workplace-related online interactions (Williams *et al.*, 2017a), while the fifth was not specific to a particular cyberspace environment (Montañez *et al.*, 2020).

Algarni *et al.*'s (2014) model of the Impact of Source Characteristics on User Susceptibility presented four perceptual factors which describe how an individual would judge the source of a message (i.e., the perceived sincerity, competence, attraction and/or worthiness of the persona assumed by the CSE perpetrator). As explained in Section 2.9.2.1, source characteristics is a concept applied frequently in marketing: what attracts viewers/users to a message or site while in an online context? While the model focussed on the user's perceptions of the presumed sender, it did not look into other individual differences (characteristics of the user) which could provide a better understanding of the influence of the message on the user.

Users do not only view; they engage, behave and operate on several levels, as when one operates a machine. How people browse the net, their usage patterns, how they behave and what degree of self-efficacy they possess while engaging in cyberspace generally, could give a more nuanced understanding of susceptibility. Examining other individual differences could help to account for such phenomena. This can be seen in the SCAM

(Vishwanath *et al.*, 2016). The SCAM model posited that the most important social-psychological cue affecting individual susceptibility to victimisation to phishing was suspicion, or the lack of it. Another key factor that would increase or decrease susceptibility was whether cognitive processing was heuristic or systematic. The SCAM also predicted that "email habits" as a behaviour would increase susceptibility to CSE attack, precisely because habitual behaviour favoured heuristic over systematic processing when checking emails, which in turn diminished suspicion.

A similar association was suggested regarding users' level of usage in the SNS context in Saridakis *et al.*'s (2016) model of Social Media Behaviour and Risk of Cyber Crime Victimisation. However, Vishwanath *et al.*'s (2016) and Saridakis *et al.*'s (2016) models differed in terms of the direction and type of influence of constructs in how they predicted susceptibility to cybercrime victimisation. The former posited that individual cyber-risk beliefs (i.e., risk perception) both indirectly (mediated by the choice between heuristic and systematic processing) and directly influenced whether or not a person might be suspicious of a malicious message. SCAM also placed email habits as the mediator between self-regulation online and suspicion. In contrast, Saridakis *et al.*'s (2016) model posited three perceptual factors (perceived control over information, IT self-efficacy and risk perception) along with two constructs representing behavioural patterns (risk propensity and SNS usage), all directly impacting susceptibility to cybercrime victimisation. Based on their findings, Saridakis *et al.* (2016) proposed a related model of "*Mitigation of SNS Cybercrime Victimisation*" (p. 22) that incorporated two mediating constructs: risk perception and risk propensity (Figure 2-13). Vishwanath (2016) focussed on two mediating elements: cognitive processing of the individual brain and habitual usage, and to what degree they could be influenced by self-regulation (behaviour) and cyber-risk belief (perception).

The two other models reviewed (Williams *et al.*, 2017a; Montañez *et al.*, 2020) were only proposed and not empirically examined. However, in a subsequent paper, Williams *et al.* (2017b) partially tested the Holistic Individual Susceptibility Model for Workplace Phishing via experiments involving two of its factors. In order for Williams *et al.*'s (2017a) complex hypothesis-based framework to be applied in the real world, it would require a clearer differentiation of some of its factors. For instance, the authors added "loss" as a persuasion principle to Cialdini's original six principles, whereas the existing principle of scarcity already entails loss: "*Loss is the ultimate form of scarcity*" (R. Cialdini, as quoted

in Carey, 2007, paragraph 15). Moreover, as stated by Williams, "*we acknowledge that there is likely to be a degree of overlap between these factors/levels*" in the Holistic Individual Susceptibility Model for Workplace Phishing (E. Williams, personal communication via email, 6 July 2018).

The fifth model (Montañez *et al.*, 2020) had not been tested as of the date of this writing. Based on an in-depth review of research in cybersecurity and cognitive psychology, the authors created the framework advocating for a sub-field of cybersecurity research, or rather an interdisciplinary field, called "Cybersecurity Cognitive Psychology". Their proposed Schema of Human Cognition and SE Cyberattack (Figure 2-17) would account for long-term cognition factors including individual differences such as personality and expertise, and short-term cognition factors like stress, vigilance and cognitive workload. Unlike the previous four models, the framework proposed by Montañez *et al.* (2020) placed an emphasis on the role of "attack effort", meaning the CSE attacker's tactics, including message appeal (persuasion) and frequency of attacks. The authors recommended that future extensions and testing of their model should account for physiological factors such as measurement of brain and nervous system activity. It might be difficult for a novice researcher to ascertain the validity of Montañez *et al.*'s (2020) model as a whole, although many of the underlying factors and hypotheses could be tested individually or in pairs (e.g., workload and vigilance, or stress and expertise) to assess their impact on susceptibility to CSE victimisation.

This section has presented and reviewed previous and recent models exploring or attempting to explain the relationships between various user characteristics and susceptibility to CSE victimisation. The resulting list of factors that are deemed to be highly relevant to the development of the hypotheses for this present thesis will be discussed in Chapter Three.

2.10 Summary of Literature Review and Research Gaps

It is evident that the research on information systems security must take into account the human element in that environment (Rao and Nayak, 2014). Scholars have agreed that human aspects of cybersecurity awareness are complex and should be given further attention (Gcaza *et al.*, 2015; Hadlington, 2017). Social engineering is a key component of cyberattacks that target individuals, or that target organisations via their employees. CSE, as a form of social engineering, employs the principles of persuasion to dupe and

manipulate gullible individuals (Ferreira *et al.*, 2015). Research has indicated that people still perform poorly in identifying lies and deception (Qin and Burgoon, 2007; Wright and Marett, 2010), let alone cyber-social engineering attacks (Algarni, 2016), particularly in the realm of susceptibility to CSE attacks carried out on SNS platforms (Algarni, 2019).

Much of the CSE research carried out in the context of SNS is still in its infancy. Very few studies have investigated influencing factors and attributes in the context of SNS, whereas there is a body of research on cyberattacks carried out via email is However, some studies have begun to examine CSE on SNS from the perspective of vulnerable end-users (Algarni *et al.*, 2014; Vishwanath, 2015a; Silic and Back, 2016; Albladi and Weir, 2017, 2018; Algarni, 2019). There is a body of research that considers how personality traits play a role in user susceptibility to CSE (Albladi and Weir, 2018; van de Weijer and Leukfeldt, 2017; Alseadoon *et al.*, 2015; Parrish *et al.*, 2009; Halevi *et al.*, 2013a, 2013b; Uebelacker and Quiel, 2014). The table in Appendix A, summarises the existing empirical and theoretical research focusing on personality traits in relation to user vulnerability/susceptibility to CSE attacks. However, these studies are mostly based on phishing emails and few have examined susceptibility to CSE carried out on SNS. This is primarily because phishing emails have been considered a more common CSE attack (Halevi *et al.*, 2013a, 2013b; Alseadoon *et al.*, 2015; van de Weijer and Leukfeldt, 2017).

Using the Five Factor Model (FFM), studies have quantitatively examined individual susceptibility in regard to phishing emails (see Appendix A), although there are disagreements in the findings as to how these traits are considered to predict user susceptibility. For instance, Halevi *et al.* (2013b) reported that neuroticism was the user trait associated with the highest risk of being victimised by malicious CSE such as phishing messages. On the other hand, Alseadoon *et al.*'s (2015) findings revealed four other traits (extraversion, agreeableness, conscientiousness and openness) that suggested users were the most gullible and, therefore, most susceptible to phishing emails. Uebelacker and Quiel (2014) suggested high levels of other traits may be influential: high levels of neuroticism for heightening individuals' susceptibility, and high levels of conscientiousness for minimising susceptibility.

Some studies have examined whether personal dispositions affect susceptibility to CSE. For example, trust/propensity to trust have been found to increase the threat of victimisation on Facebook, albeit in conjunction with other factors such as previous experience of attack. However, context is important, and one Facebook user will differ from another in their

level of trust (Albladi and Weir, 2017). Other personal dispositions, such as self-discipline and the tendency to comply with rules (Frauenstein and Flowerday, 2020), have been found to be associated with conscientiousness (Parrish *et al.*, 2009). In contrast, impulsiveness is associated with openness to experience and thus with less control over personal information (Halevi *et al.*, 2013a, 2013b; Alseadoon *et al.*, 2015). In addition, high extraversion is found to reduce willingness to obey security policies and rules, leading them to disclose more information on SNS (Darwish *et al.*, 2012). To date, the findings with regard to how dispositions are associated with personality traits are contradictory.

Although the research on CSE has considered personality traits as a potential susceptibility factor, further investigation is required to explain the impact of users' personality traits and how they may relate to a range of other factors, such as users' personal disposition, habitual behaviours and contextual factors including nationality (Albladi and Weir, 2018) and structural power (manager/employee) within an organisation (Williams *et al.*, 2017a). The role of traits such as neuroticism and conscientiousness in influencing susceptibility to various types of CSE threats, especially when associated with personal dispositions such as willingness to take risks and ability to control information, would also benefit from more exploration in different contexts.

Culture has also been found to have an impact on personality characteristics, especially in settings where traditional gender roles were minimised (Costa *et al.*, 2001). However, since it has been claimed that culture is hard to either quantify or criticise due to its complexity and generality (McSweeney, 2002; Sawaya *et al.*, 2017), nationality was used as a proxy in previous studies, e.g., Albladi and Weir (2018) and Alseadoon (2014). There is, however, a lack of understanding of nationality as an aspect of culture and its impact on personal dispositions (Section 2.8.4) toward cyber risks that rely on persuasion. CSE resistance is mediated by cultural dimensions such as individualism/collectivism (Hofstede 1980; Hofstede *et al.*, 2010), as found in a study by Rocha Flores (2016), particularly within organisations with participants of different nationalities (Sawaya *et al.*, 2017; Alseadoon, 2014; Albladi and Weir, 2018).

Research findings also suggest that susceptibility/vulnerability could differ with demographic factors, such as age and gender (Sheng *et al.*, 2010; Jagatic *et al.*, 2007; Kumaraguru *et al.*, 2010). For instance, Byrnes *et al.* (1999) found that men take more risks than women, implying that gender could have a link to willingness to take risks on the internet. However, this and earlier studies, such as Goel *et al.* (2017) and Mills (2010), have

revealed some inconsistencies in their findings as to whether men or women are more susceptible to phishing attacks. Age, rather than being a determinant by itself, can be a contributor to other dispositional and perceptual factors, such as risk propensity, risk perception (Bonem *et al.*, 2015) and IT self-efficacy (Grimes *et al.*, 2010).

The literature review conducted for this study revealed four important gaps in the research:

First, research on how personality traits and other factors can predict susceptibility to CSE in the workplace has tended to concentrate on email contexts and has largely ignored the SNS environment. Even fewer studies involving SNS have looked at how employees engage on career-oriented SNS. The literature reveals that people differ in their motivations for using SNS platforms (Kim and Cha, 2017; Hallikainen, 2015), and that SNS as a communication service also have different characteristics and communication avenues (Baruah, 2012) from those common to email, which can make them more attractive as targets for cybercriminals (Terrill, 2017; Symantec, 2015; Vishwanath, 2015a). According to *The Telegraph*, "*...people have grown wise to email spam. They recognise all the warning signs now. But a lot more people are tricked by spam messages sent by their 'friends' on sites like Facebook*" (Barnett, 2011). This may also be the case on other dominant SNS that are professionally oriented, such as LinkedIn, so that users on these sites are preyed upon by their own "connections".

A second gap in the extant literature is in relation to employees' susceptibility to cyber deception while using SNS in the workplace and the roles played by individuals within their organisation. Research highlights possible differences between the attitudes of employees and managers and the ways they interact in relation to persuasion within the organisation (Pitesa and Thau, 2013b), and specifically towards their perceptions of IS security risk and cyber social engineering in the workplace (Alzamil 2012; Williams, *et al.*, 2017a). With CSE via SNS becoming more prevalent, it is even more important to look into employees' personality characteristics, their behaviour online and demographics, as these could predict their levels of Information Security Awareness (ISA) (Cho and Kim, 2017; Gratian *et al.*, 2018).

The third gap found was that, as far as the author is aware, there has been no research to date that incorporates personality traits FFM with perceptual and behavioural variables to the risks of cyberattacks over SNS. This includes risk propensity and perception, habitual behaviour, such as level of involvement in SNS, and experiential factors, such as IT self-

efficacy. Such studies would enhance the understanding of employee vulnerability to CSE in the workplace.

The fourth and final gap is regarding the cultural dimension of collectivism/individualism (Hofstede, 1980). The importance of culture as an influence on virtual world is supported in the literature, and it has been recognised that culture has scarcely been studied in cybersecurity (Henshel *et al.*, 2016). Few studies have examined susceptibility to CSE victimisation within a national workforce. In fact, studies regarding CSE victimisation in Saudi Arabia have, to this researcher's knowledge, only been carried out using students in Saudi universities (e.g., Alseadoon *et al.*, 2012; Albladi and Weir, 2017). Given that employees are the frontline against any risk potentially arising in today's complex CSE warfare, the susceptibility of workers in large Saudi organisations could pose a much greater risk.

These four gaps will be addressed by the present study. As described in Section 2.9.3, the model (Saridakis *et al.*, 2016) that will serve as the basis for the study model of this thesis has been selected. In the next chapter (Chapter Three), the conceptual model and its underlying theories will be explained. The model will be extended with proposed additional factors, and justification for each factor presented. The hypotheses regarding the relationships between these factors will be developed and explained.

3. Conceptual Model and Development of Hypotheses

This chapter presents an explanation of how the hypotheses of this research are formulated and are presented in a conceptual model. This is the hypothetical model that will be examined and tested in this thesis. The chapter starts by presenting a number of theories that are often employed in information system security research in the domain of behavioural cybercrime research, including in studies on susceptibility to cyber-social engineering. The criteria and considerations for selection of an appropriate model for this thesis are then explained. Subsequently, the selected model on which the present research model is to be based is presented, along with the theories and concepts that underpin that original model, and, consequently, the proposed extension. Justification is provided for the design of the study model, and the proposed extension is explained. The conceptual model for the study is presented along with the proposed hypotheses. This is followed by a description and explanation of each hypothesis.

3.1 Theories Commonly Applied in CSE Susceptibility Research

The review of recent models of susceptibility to CSE carried out in Chapter Two (Section 2.9) highlighted a number of theories that are frequently found to underpin or at least inform those frameworks. Three such theories are lifestyle/routine activity theory (LRAT), theory of reasoned action (TRA) and theory of planned behaviour (TPB). This section discusses how LRAT has been employed to explain cybercrime susceptibility. TRA and TPB are two influential and related theories that explain perceptual behaviour. A fourth theory, counterproductive workplace behaviour (CWB), with its derived concept of counterproductive computer security behaviour (CCSB), was not employed in the models reviewed, but it is included in this section due to its emerging prominence in user-centred IS research (e.g., Hadlington, Binder and Stanulewicz, 2021).

3.1.1 Lifestyle/Routine Activity Theory (LRAT)

In 1979, Cohen and Felson proposed routine activity theory (RAT), which is an approach for analysing crime rate trends and cycles. Instead of focusing on the characteristics of offenders, Cohen and Felson (1979) focused on the circumstances in which offenders act. Cohen and Felson (1979) based their theory on crime rate trends in the United States

between 1947 and 1974. From this data, the researchers determined that crime rates are not necessarily linked to social causes (e.g., poverty, inequality or unemployment), but are instead linked to the opportunity for an offender to commit a crime. Furthermore, as the opportunity for crime increases, so does the rate of crime. Cohen and Felson (1979) proposed that, in order for a direct-contact predatory crime to be successful, three elements need to converge in time and space. These elements are: 1) motivated offenders, 2) suitable targets, and 3) the absence of capable guardians. Figure 3-1 provides a visualisation of RAT.

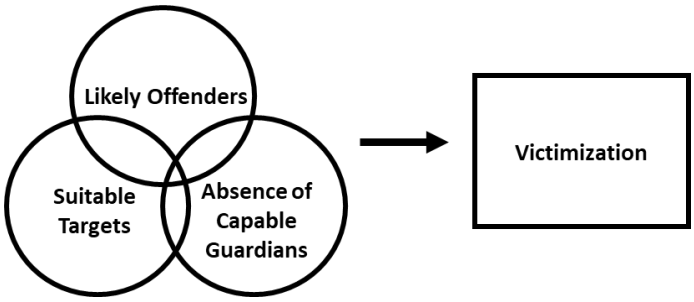


Figure 3-1 Visualisation of Routine Activity Theory (RAT). Source: Cohen and Felson (1979, p. 589)

Cohen and Felson (1979) define direct-contact predatory violations as *"illegal acts in which someone definitely and intentionally takes or damages the person or property of another"* (p. 589). Direct-contact predatory violations involve a physical encounter between a victim and an offender in a physical environment, Grabosky (2001) argued, that the RAT model *"is equally applicable to crime in cyberspace"* (Grabosky, 2001, p. 248, as cited in Leukfeldt and Yar, 2016, p. 264). An online setting without appropriate safeguards can provide the perfect setting for the three elements of RAT (motivated offenders, suitable targets, the absence of capable guardians), which leads to cyberattacks (Saridakis *et al.*, 2016). In describing their Model of Social Media Behaviour and Risk of Cyber Crime Victimisation, Saridakis *et al.* (2016) explained that the motivated offender is the cyber-attacker, the suitable target is the SNS user and, because the object of value is the user's personal information, the element of *guardianship* in RAT is the user's perceived control of that information.

Reyns (2013) found that individuals' routine activities in cyberspace can increase their susceptibility to identity theft victimisation. Thus, online social media timeline activity, blogs, email/instant messaging and downloading various types of digital materials can pose significant risk of victimisation (Reyns Henson, and Fisher, 2011). In their review of 11 empirical studies (N = 9,161), Leukfeldt and Yar (2016) found that engaging in online

communities, forums and social networking platforms can increase hacking victimisation. In addition, time spent using the internet (e.g., online shopping, downloading and gaming) was associated with phishing and malware victimisation (Leukfeldt and Yar, 2016). It should be noted that RAT is not designed to predict victimisation, but rather *"to describe the victimization event after it has already happened*" (Pratt and Turanovic, 2016, p. 348).

Around the same time that RAT was proposed, the lifestyle activity theory (LAT) was introduced by Hindelang, Gottfredson, and Garofalo (1978). Like RAT, LAT proposes the same triad as leading to victimisation (a motivated offender, an attractive target/victim, and the absence of capable guardianship). However, LAT goes beyond RAT's descriptive capability and *"conceives of risk in probabilistic terms"* in considering that some people's lifestyles, or more specifically, some of their habitual or routine behaviours, can *"elevate one's odds of being victimized"* (Pratt and Turanovic, 2016, p. 335). Thus, LAT differs from RAT in that whereas RAT is binary (either the conditions exist for victimisation or they do not), LAT incorporates the element of degree: the extent to which the conditions pose a risk for victimisation.

RAT and LAT are often used interchangeably or are combined, due to their similar foundations (Pratt and Turanovic, 2016). LAT can account for demographic differences and how these impact individual vulnerability (Bunch, Clay-Warner and Lei, 2015). The two theories are different, yet they share some key components; therefore, studies (e.g., Holt and Bossler, 2009; Reyns *et al.*, 2011; Bunch *et al.*, 2015; Leukfeldt and Yar, 2016; Choi and Lee, 2017) often combine them as lifestyle/routine activity theory, hereinafter referred to as LRAT (Figure 3-2). Sampson and Wooldredge (1987) argued that such a hybrid model (Figure 3-2), "*which incorporates lifestyles and routine activities with a more explicit focus on ecological proximity* [i.e., accessibility of the target victim and their property] *and macro sociological processes* [the "right" social/systemic conditions for the crime to be committed] ... *provides the most promising path for future multilevel victimization research*" (p. 391). Consequently, LRAT has been applied in a number of empirical analyses of vulnerability to victimisation in order to establish which measures may be necessary to prevent crime (Reyns *et al.*, 2011; Leukfeldt and Yar, 2016; Vakhitova, Reynald and Townsley, 2016).

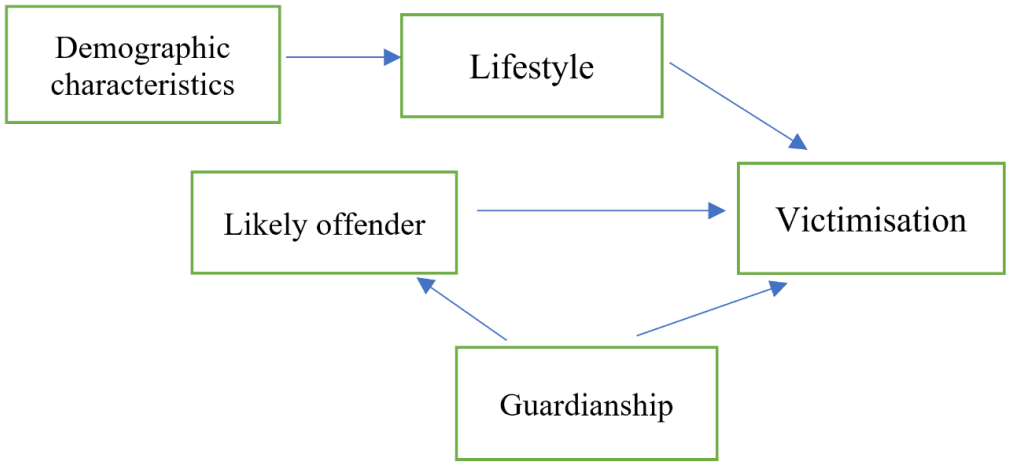


Figure 3-2 This author's visualisation of the Lifestyle/Routine Activity Theory (LRAT)

Another advantage of LRAT is that it can be used to explain different types of victimisation, including online victimisation (Reyns *et al.*, 2011; Saridakis *et al.*, 2016; Vakhitova *et al.*, 2016). Furthermore, criminologists suggest that people who use SNSs continuously (lifestyle) and compulsively (lack of guardianship) are at greater risk of becoming the victims of cyberattacks due to their increased exposure to willing offenders, also known as cybercriminals (Reyns *et al.*, 2011; Reyns, 2013; Saridakis *et al.*, 2016), or cyber-social engineers. Individuals' activity in cyberspace is reflected by their habitual behaviour and, therefore, the model examines individual compulsiveness. Previous studies have concluded that there is a relation between routine activity behaviours and cybercrime (Pratt, Holtfreter, and Reisig, 2010; Reyns, 2013). Importantly, a significant correlation has been found between routine activity that is unstructured, such as spending more time online and impulsive online shopping (Holtfreter *et al.*, 2015).

In their critique of LRAT, Pratt and Turanovic (2016) stated that the two models from the late 1970s (RAT and LAT) on which the hybrid was based, had been developed using what are now "*outdated measures of risky lifestyles*" (p. 10). Pratt and Turanovic (2016) contended that that while this was not an inherent limitation (measures could and should be updated), it was a limitation of LRAT that had not been addressed by 21st century researchers. Nevertheless LRAT remains highly influential and predominantly pivotal in the realm of criminological theories (Leukfeldt and Yar, 2016), and can be used to explain online users' vulnerability (Holt and Bossler, 2009; Reyns *et al.*, 2011; Leukfeldt and Yar, 2016).

Two theories that explain perceptual behaviour are TRA and TPB. Saridakis *et al.* (2016) stated that their model was based on the theory of reasoned action (TRA) and the theory of planned behaviour (TPB); thus, in order to establish the conceptual foundations of this thesis, it is important to introduce these two fundamental and related theories.

3.1.2 Theory of Reasoned Action (TRA)

Fishbein and Ajzen (1975) proposed the theory of reasoned action (TRA; see Figure 3-3) to explain the relationship between beliefs/attitudes and behaviour in an individual. The model has been used in various fields, including workplace organisational behaviour, to predict behavioural intention and even the behaviour itself (Pinder, 2014). According to TRA, behavioural intention is "*a function of salient information or beliefs about the likelihood that performing a particular behavior will lead to a specific outcome"* (Madden, Ellen and Ajzen, 1992, p. 3).

In TRA, beliefs that predict behaviour are of two types: behavioural and normative; behavioural beliefs influence a person's attitude towards performing a particular behaviour, whereas normative beliefs are what affect the individual's "*subjective norm*" regarding performing that behaviour (Fishbein and Ajzen, 1975). Fishbein and Ajzen (1975) use the term *subjective norms* to mean a "*person's perception that most people who are important to him* [sic] *think he should or should not perform the behaviour in question*" (p. 302). TRA has been used in ISS research to predict employee compliance with ISS policies (Pahnila *et al*., 2007; Siponen et al., 2014).

Importantly, as Madden *et al.* (1992) noted, TRA assumes that behaviours predicted by the model are "*under full volitional control*" (p. 4). Ajzen explains that behaviours are under "*volitional control*" when "*people can easily perform these behaviors if they are inclined to do so*" (Ajzen, 1985, p. 12). Indeed, the assumption of the presence of volitional control is one of the main criticisms of TRA (Pinder, 2014). Another important critique is that because it is a theory of "reasoned" action, intention is posited as the mediator between attitudes/beliefs and behaviours, and thus the model fails to account for "*categories of behaviors that require little or no thought*" (Pinder, 2014, p. 263), such as habits (habitual behaviour). Despite these limitations, TRA is a useful theory for the study of employee susceptibility to CSE, because its constructs of beliefs/attitudes and subjective norms (Figure 3-4) as motivational factors encapsulate internal perceptual constructs and external organisational cultural dimensions, respectively.

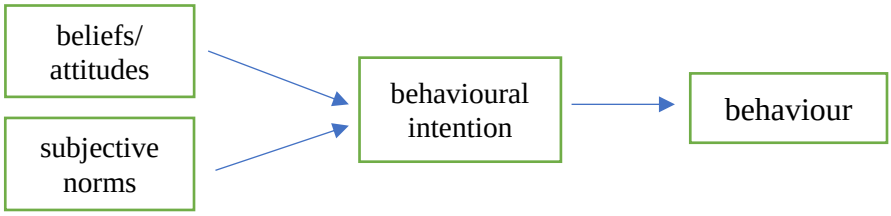


Figure 3-3 Theory of Reasoned Action (TRA). Adapted from Madden et al. (1992)

3.1.3 Theory of Planned Behaviour (TPB)

Ajzen later (1985) developed the theory of planned behaviour (TPB; Figure 3-4) to address one of the limitations of TRA (Fishbein and Ajzen, 1975), discussed in Section 3.1.2 above, by including the construct of "*perceived control*" (Ajzen, 1985, p. 12). According to TPB, intention can only be translated into actual behaviour if that behaviour is under an individual's perceived control (Madden *et al.*, 1992). "*Perceived behavioural control*" (PBC) refers to a person's perception of his/her ability to perform a given behaviour. "*To the extent that perceived control is likely to be realistic, it can serve as an estimate of actual control*" (Ajzen, 1985, p. 34).

PBC has often been used interchangeably with *self-efficacy* (Bandura, 1989) in the literature on behavioural influences, whereas some research in that same domain has treated them as separate but closely related constructs (Parkinson, David and Rundle-Thiele, 2017). According to Wallston (2001), these two constructs are operationalised slightly differently. PBC is evaluated by how easy or difficult the behaviour is perceived to be (e.g., "*I find it difficult to exercise three times a week*"), whereas self-efficacy is operationalised by how confident a person is in their ability to perform the behaviour under "*extenuating circumstances (e.g., 'I am confident that I can exercise three times a week even when I am away on vacation')*" (p. 2725). In Saridakis *et al.*'s (2016) model, PBC is present in the form of "*computer self-efficacy*".

TPB is meant to predict, or at least explain, behaviours in which individuals have "incomplete" volitional control (p. 28); as Ajzen stated, "*personal deficiencies and external obstacles can interfere with the performance of any behavior*" (p. 29). Ajzen (1985) further explained an individual's disposition towards any particular behaviour as the extent to which they positively or negatively appraise that behaviour. Thus, TPB takes into account beliefs, attitudes, subjective norms, and perceived behavioural control, in order to predict

deliberate, planned behaviour (Ajzen, 1985, p. 11). Moreover, TPB considers internal factors (e.g., personality, motivation, beliefs, attitudes, etc.) as well as external ones (e.g., culture, organisation, skills, resources, etc.). As Baker and White (2010) explained, "*The TPB posits that individuals' intentions are the proximal determinants of their behaviour, with intention conceptualised to capture individuals' motivation to perform a given behaviour*" (p. 1592). Thus, motivation is integral to TBP (Rhodes and Courneya, 2004).

Despite the fact that TPB was developed prior to the digital age, it has remained a (some have said *the*) predominant theory in ISS research (Lebek *et al.*, 2014; Pattinson *et al.*, 2015; Safa *et al.*, 2015; Jalali *et al.*, 2020). In his work on predicting cyberbullying behaviour, Barlett (2019) noted that TPB was more widely used than TRA in cyberbullying research, and that this was likely due to that addition of PBC as a construct. He asserted that the fact that TPB is not specific to online contexts is a limitation of the theory; nevertheless, he argued that TPB and other pre-Internet theories are potentially valid and useful in online contexts, as long as "*the lack of incremental validity*[6] *in applying these theories is acknowledged and applied*" (Barlett, 2019, p. 47). Given the above considerations, this author believes that TPB is useful and appropriate to serve as the overarching theory for the present study.

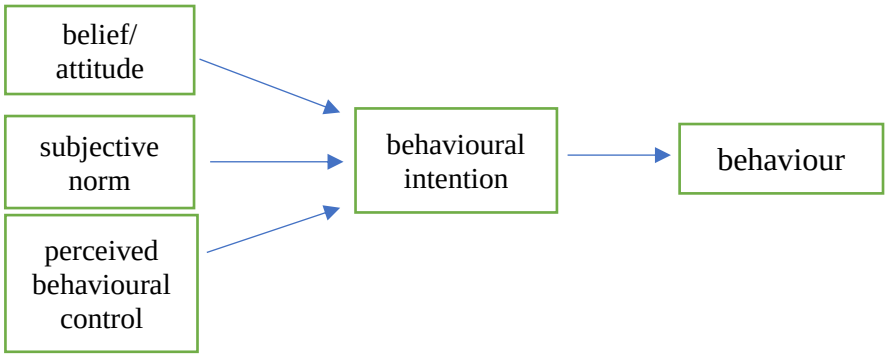


Figure 3-4 Theory of Planned Behaviour (TPB). Adapted from Madden et al. (1992)

3.1.4 Counterproductive Computer Security Behaviour (CCSB)

In addition to the three well-known theories described in Sections 3.1.1 – 3.1.3 above, counterproductive workplace behaviour (CWB) is a fairly new theory (Martinko, Gundlach and Douglas, 2002) that has more recently been applied to ISS research (Mercado, 2017; Ifinedo, 2019; Hadlington *et al.*, 2021). In their respective meta-analyses of studies

[6] Incremental validity is used to determine whether any improvement is achieved "*by adding a particular procedure or technique to an existing combination of assessment methods*" – APA Dictionary of Psychology. https://dictionary.apa.org/incremental-validity

investigating the relationships between personality traits and workplace behaviour, Salgado (2002) and Salgado, Moscoso and Anderson (2013) found that specific personality traits correlate with—and in some cases can predict—certain workplace behaviours, including counterproductive workplace behaviour (CWB). Martinko *et al.* (2002) define CWB as "*behavior by an organizational member that results in harming the organization or its members*" (p. 37). They integrated 19 major theoretical perspectives or frameworks regarding CWB to come up with a paradigm, the integrative theory of counterproductive work behaviour, that explains CWB as "*the result of a complex interaction between the person and the environment in which the individual's causal reasoning about the environment and expected outcomes drive the individual's behavior*" (Martinko *et al.*, 2002, p. 41). According to this paradigm, individual differences (i.e., internal factors), such as gender, self-efficacy, and personality traits, interact with external or "*environmental/situational*" factors (e.g., organisational culture, leadership style, adverse working conditions, rules and procedures) to influence an employee's causal reasoning, which in turn produces CWB. The integrative theory of counterproductive workplace behaviour incorporates concepts found in TRA (causal reasoning = reasoned action) and TPB (self-efficacy = perceived behavioural control).

CWB was initially conceptualised as "*deviant workplace behavior*" (Robinson and Bennett, 1995, p. 555). However, Mercado (2017) argued that when conceptualising CWB in the cybersecurity context, it "*need not be* normatively *deviant*", and in fact may include behaviours that are "*considered 'normal' based on prevalent performance norms and thus not qualify as deviant,* [e.g., checking personal emails, but] *they are still counterproductive*" (p. 6, emphasis in original). Furthermore, many of the items in CWB scales encapsulated malicious behaviour (Spector *et al.*, 2006), but Ifinedo (2019) noted that as CWB was updated to account for IS-related factors, the concept was expanded to include non-malicious cybersecurity behaviours, such as "*IS resource misuse and IS security carelessness*" (paragraphs 7-8). For example, Ifinedo's (2019) validated scale of Counterproductive Computer Security Behaviours (CCSB) includes items such as "*Pasting or sticking computer passwords on office desks*", "*Not updating anti-virus and/or anti-spyware software at work*" and "*Visiting nonrelated websites at work*" (see Figure 3-5).

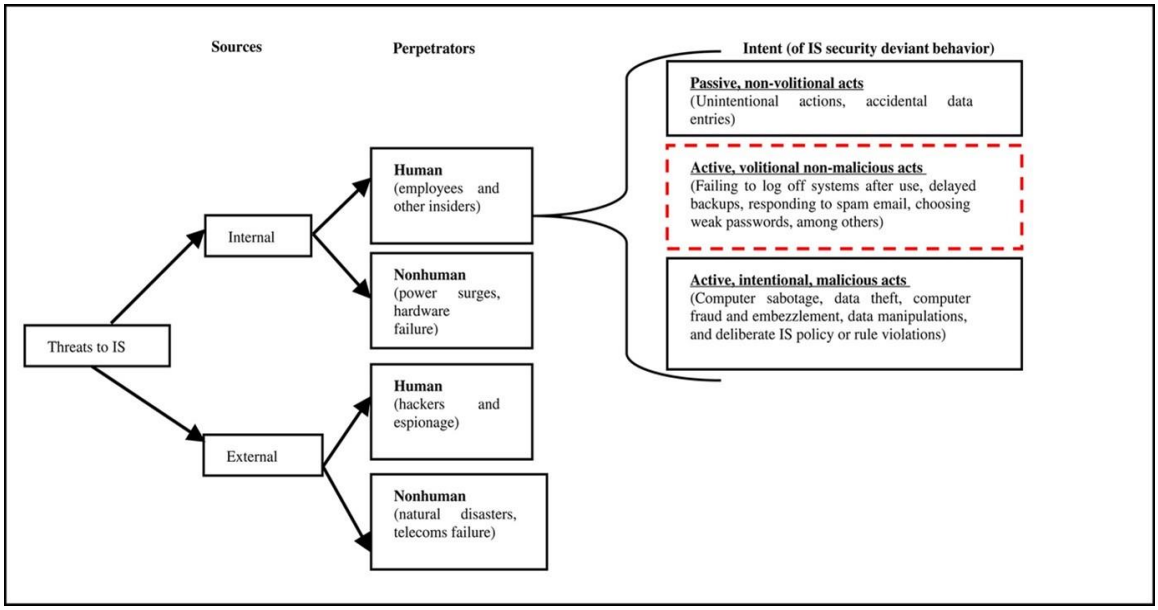


Figure 3-5 End user non-malicious, counterproductive computer security behaviours (Ifinedo, 2019)

3.2 Considerations for Selection of Appropriate Model for This Thesis

The seven frameworks originally reviewed in preparation for this study were Parrish *et al.* (2009), Algarni *et al.* (2014), Uebelacker and Quiel (2014), Albladi and Weir (2017), Saridakis *et al.* (2016), Vishwanath *et al.* (2016) and Williams *et al.* (2017a). Each of these models incorporated concepts worthy of consideration in deciding upon the model for this thesis (see Table 3-1). Three models (Parrish *et al.*, 2009; Uebelacker and Quiel, 2014; Albladi and Weir, 2017) employed the five-factor model of personality traits. The other studies (Algarni *et al.*, 2014, 2017; Saridakis *et al.*, 2016; Vishwanath *et al.*, 2016) focused on cognitive or socio-psychological (Williams *et al.*, 2017a, 2018) factors.

It was helpful to this research to start with a framework that had already been validated and tested. Of the seven models, only four (Algarni *et al.*, 2014; Saridakis *et al.*, 2016; Vishwanath *et al.*, 2016; Albladi and Weir, 2017) had been empirically examined. Due to the growing dominance of SNS as the main medium for online communication (Chapter Two, Section 2.6), an important criterion was that the model should have been tested in an SNS context. That described three of the last four (Algarni *et al.*, 2014; Saridakis *et al.*, 2016; Albladi and Weir, 2017). The next consideration was the salience of the psychological factors accounted for in the model. As mentioned in Chapter Two (Section 2.9.2), Albladi and Weir (2017) had considered no behavioural cognitive factors, whereas Algarni *et al.* (2014) and Saridakis *et al.* (2016) included a behavioural factor in addition

to perceptual ones. Algarni *et al.* (2014) and Saridakis *et al.* (2016) also considered two demographic factors, age and gender, which Albladi and Weir (2017) did not. The Model of Social Media Behaviour and Risk of Cyber Crime Victimisation (Saridakis *et al.*, 2016), which included risk propensity in addition to perceived risk and perceived control over information (see Chapter Two, Section 2.8.2), was deemed to be a suitable model upon which to base the present research model. That model is discussed in further detail in the next section (3.3).

Table 3-1 Factors in extended model.

	Existing models (proposed & empirically examined) from 2009-2018							
	Models Incorporating FFM			Models not incorporating FFM				
Model (year) / Factors	Parrish et al. (2009)	Uebelacker et al. (2014)	Albladi & Weir (2017)	Algarni et al. (2014, 2017)	Saridakis et al. (2016)	Vishwanath et al. (2016)	Williams et al. (2017)	Williams et al. (2018)
Demographic Factors								
Age	✓			✓	✓			
Gender	✓			✓	✓			
Socio-psychological Factors								
Personality traits (FFM)	✓	✓	✓					
Structural power (position)							✓	✓
Nationality/culture	✓							
Perceptual Factors (cognitive)								
Risk perception				✓	✓	✓		
Risk propensity (willingness to assume risk)					✓			✓
Perceived control of information					✓			
Self-efficacy/perceived competence			✓	✓	✓			
Habitual behaviour Factors								
Information security habitual practices/ self-control						✓	✓	
Level of engagement/involvement				✓	✓			
Frequency of use (time spent)								
Motivation								
Self-presentation			✓					
Professional-advancement/ enjoyment-seeking			✓					
Context								
Social Networking Sites			✓	✓	✓			
Email	✓					✓	✓	✓
ICT		✓						
Has model been examined?	No	No	Yes	Yes	Yes	Yes	No	Yes

✓ means this factor is found in both the study model and the existing model reviewed (See Ch. 2)

3.3 Model of Social Media Behaviour and Risk of Cybercrime Victimisation

Saridakis *et al.*'s (2016) Model of Social Media Behaviour and Risk of Cyber Crime Victimisation is based on three of the theories described in Section 3.1 above: routine activity theory (RAT), theory of reasoned action (TRA) and theory of planned behaviour (TPB). To overcome TRA's limitation of presumed volitional control (Section 3.1.2), Saridakis *et al.* (2016) added elements from TPB (Section 3.1.3) to their model. Nevertheless, TRA's constructs of beliefs/attitudes and subjective norms (Figure 3-3) as motivational factors are key components in the model (Figure 3-6), as they encapsulate the internal perceptual constructs and the external organisational cultural dimensions, respectively. As detailed in Chapter Two, the model (Figure 3-6) developed by Saridakis *et al.* (2016) represents the influence of social media behaviour and perceptual factors on the risk of cybercrime victimisation.

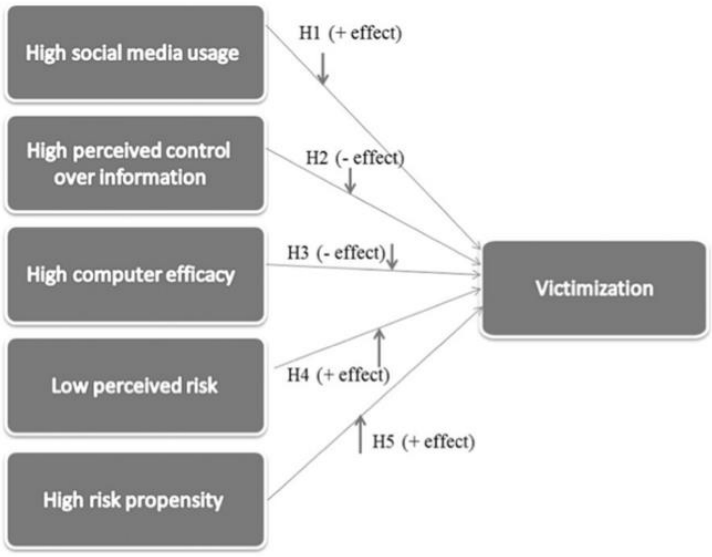


Figure 3-6 Model of Social Media Behaviour and Risk of Cyber Crime Victimisation

Source: Saridakis et al. (2016, p. 323)

Their supposition was that the more active on SNS people were, the more likely they were to become victims of cybercrime. Saridakis *et al.* (2016) describe this victimisation as encompassing *"personal and security sensitive information losses resulting from cybercrime, including online identity theft or usurpation, financial fraud, stalking and blackmail"* (Saridakis *et al.*, 2016, p. 4). This phenomenon of using deception and manipulation leading to the victimisation of susceptible individuals via the Internet is what is referred to in the present research as CSE (see Chapter Two, Section 2.3.2).

As described in Chapter Two (Section 2.9.2.2), the model put forth by Saridakis *et al.* (2016) encapsulates five different factors influencing the risk to a user of being victimised by CSE (Figure 3-6). The five constructs in Saridakis *et al.*'s (2016) model are: degree of SNS use (level of engagement), perceived control over personal information, computer efficacy, perceived risk and risk propensity (willingness to assume risk). These constructs were introduced in Chapter Two and are explained in further detail in Section 3.6 of this chapter. Beyond describing the three main theories underpinning their model, Saridakis *et al.* (2016) did not elaborate much on the theoretical basis for each independent variable in their model. However, they did identify the theoretical bases for their constructs as follows:

- *SNS usage* is based on RAT, as both the "*suitable target*" element and the concept of "*exposure to offenders*" in that model (Saridakis *et al.*, 2016, p. 9).
- *Perceived control over information* represents the element of guardianship in the RAT triangle (p. 10).
- *Computer/technical efficacy* (IT self-efficacy) is based on perceived behavioural control (PBC) as well as "*locus of control*" (p. 10).
- *Risk perception* and *risk propensity* are based on theories of risk taking and decision-making behaviour from organisational psychology (p. 11; they cite Trimpop [1994]).
- *Victimisation*, as explained in Chapter Two, is based on RAT, as the outcome of the convergence of the three elements of that model.

Saridakis *et al.* (2016) also partially controlled for other individual characteristics such as educational background, age and gender, but did not include them in the illustration of their model. Three of these factors (high SNS use, high risk propensity and high computer efficacy) were found to be positively related to users' risk of—or susceptibility to—being victimised by CSE. The remaining two factors (high perceived control over personal data and low risk perception) were found by Saridakis *et al.* (2016) to have a negative relationship to users' susceptibility to being victimised by CSE.

Saridakis *et al.* (2016) acknowledge several limitations of their research model, such as its exclusion of national/international legal, economic and technology contexts, and its capability to "*only measure victimisation that is known to users*" (i.e., its reliance on self-reported data, p. 24). They also mentioned that the model could benefit from interpretive/qualitative research in order to attain a fuller understanding of user motivations and behaviours.

The literature has highlighted a number of additional factors that have not been addressed in Saridakis *et al.*'s (2016) model. Whereas the five factors posited to influence risk of cybercrime victimisation in Saridakis et al's (2016) model are appropriate constructs for such an investigation, they are insufficient to explain a user's susceptibility to such victimisation. As mentioned in Chapter Two, Saridakis *et al.* (2016) collected data on age, gender and professional status, but they did not include them in their model. These and other stable characteristics of individuals, such as personality and culture/nationality, are so prominent in the literature on cyber-social engineering that a model of susceptibility to CSE victimisation should include them.

Further justification for the selection and extension of the study model provided in Section 3.4 below.

3.4 Conceptualisation: Design of the Research Model

This section explains how the research model was conceptualised and developed. As described in detail in the preceding chapters, this study aims to expand the existing literature by identifying underlying causes of employees' susceptibility to CSE victimisation in the workplace. Specifically, this thesis attempts to answer the following research question:

Q1. How, and to what extent, do personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering (CSE) victimisation when accessing professional SNS, such as LinkedIn, in government organisations in Saudi Arabia?

3.4.1 Justification for the Design of the Research Model

The literature review (see Chapter Two) has identified that personality traits, behavioural and other personal dispositions or user attributes (i.e., demographic characteristics) all potentially influence users' susceptibility to online risks. As explained in Section 3.2, after a review of several potentially useful models (see Table 3-1), Saridakis *et al.*'s (2016) Model of Social Media Behaviour and Risk of Cyber Crime Victimisation was selected as the basis for the present research model for the following reasons:

1) Their model was validated and tested empirically.

2) It was carried out in the context of SNS, and specifically, it distinguished knowledge-exchange SNS (such as LinkedIn) from multipurpose SNS (such as Facebook).
3) The number and length of items for each of the constructs were short enough that adding a few more for this present study would not become daunting for participants to complete.
4) Whereas other models had been based on susceptibility investigations using phishing experiments, Saridakis *et al.* (2016) used self-reporting to gather data on victimisation. This was an important feature, because both LinkedIn and MHRSD – the organisation which approved distributing this study's surveys to their employees – had denied the request of this researcher to launch a scenario-based experiment of CSE tactics on participants.
5) The model is suitable for application in an organisational setting because it consists of habitual behaviour, perceived control of behaviour, risk perception, risk propensity and self-efficacy – constructs that account for individual aspects of human cognition and behaviour (see Table 3-1).
6) Among the findings reported by Saridakis *et al.* (2016) was that for knowledge-exchange purpose SNS, there was a statistically significant positive association between high SNS use and susceptibility to cybercrime. This was a finding that seemed important to investigate further.

3.4.2 Proposed Extension to Model of Social Media Behaviour and Risk of Cybercrime Victimisation

The research question for this thesis focuses on the roles played by individual characteristics and other factors including perceptions, habits and motivations, in an employee's likelihood of being susceptible to CSE victimisation when accessing career-oriented SNS. The following diagram (Figure 3-7) presents the factors that have been investigated in this study. Additional factors were revealed in the literature and provide an extension of Saridakis *et al.*'s (2016) existing model of SNS behaviour and risk of victimisation (see Figure 3-6). It was decided to incorporate these additional factors in order to account for individual differences. FFM and motivational factors would be added to the basic model, similar to features found in Albladi and Weir's (2017) Personality Traits-Mediator Susceptibility Model. The justification for the inclusion of these additional

factors is presented in Section 3.6. The thesis model is based on the lifestyle/routine activity theory (LRAT; Cohen and Felson, 1979) and the five-factor model (FFM) of personality traits, together with theories of *risk perception* and theories underpinning *information security habitual behaviour*. These theories and hypotheses are discussed in further detail in Section 3.6.

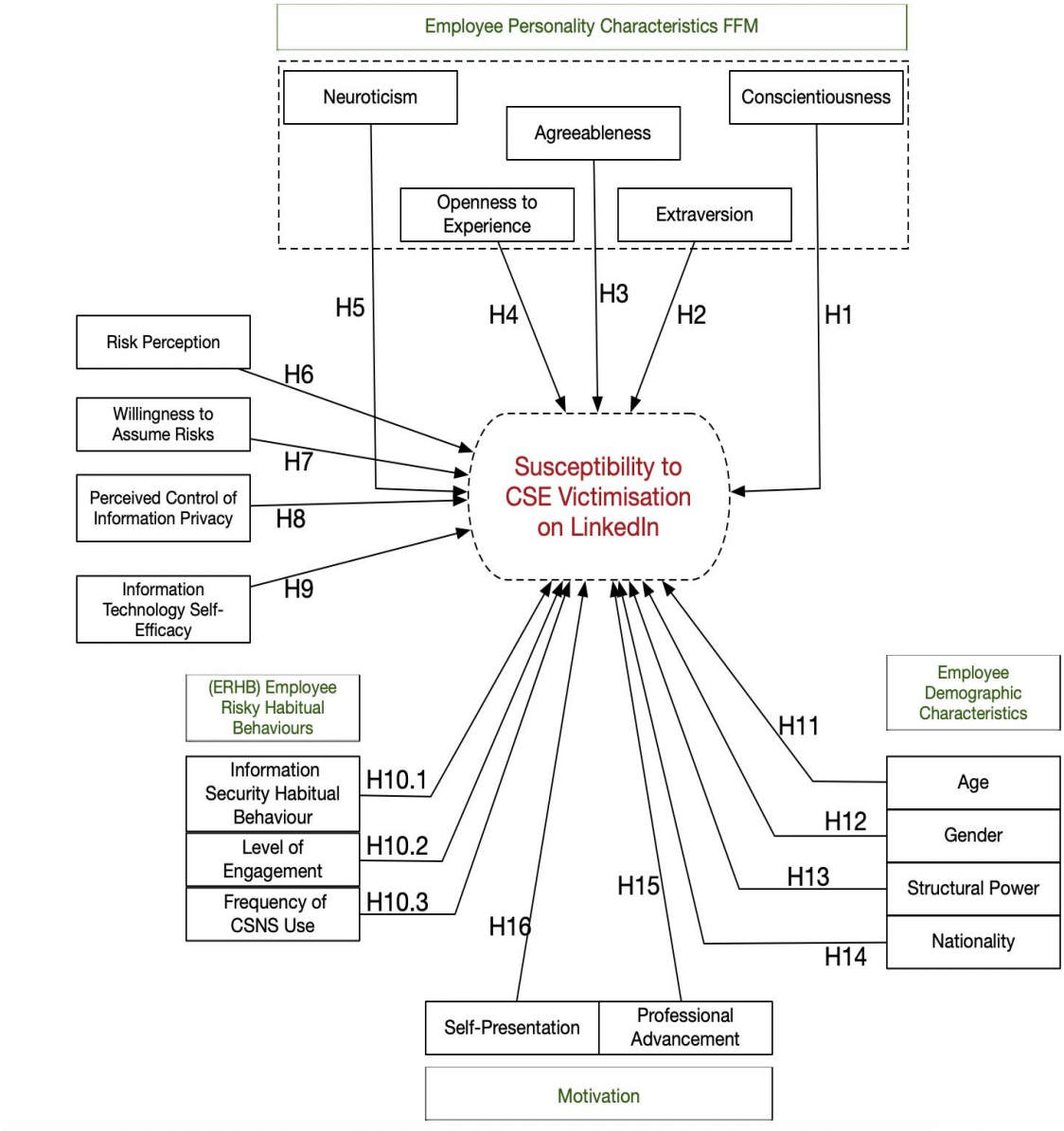


Figure 3-7 Hypothesised Model of Susceptibility to CSE Victimisation on LinkedIn

As can be seen in Figure 3-7, the study model (the hypothesised Model of Susceptibility to CSE Victimisation on LinkedIn) includes the five original factors from Saridakis *et al.*'s

(2016) model, but their single construct of "*SNS usage*" has been extended in this study as *employee risky habitual behaviours*, which has been split into three sub-factors: *information security habitual behaviour*, *level of engagement* and *frequency of CSNS use.* These factors have been included because social media usage involves habitual and temporal patterns that as per the literature can increase vulnerability to CSE. Furthermore, the Big Five personality trait constructs, two motivation constructs, and four demographic constructs (age, gender, structural/power role and nationality/culture) have been added.

The theoretical bases for the original constructs have been explained in the previous section. The theory of planned behaviour (TPB) is the overarching theory. The constructs are recapped below:.

- *Risk perception* and *risk propensity* (Chapter Two, Section 2.8.2 and this chapter, Section 3.6.2)
- *Perceived control over information privacy* (Chapter Two, Section 2.8.2 and this chapter, Section 3.6.3)
- *Computer/technical efficacy* (IT self-efficacy) (Chapter Two, Section 2.8.2 and this chapter, Section 3.1.3 and 3.6.3)
- *Employee risky habitual behaviours* (Chapter Two, Section 2.8.2 and this chapter, Sections 3.1, 3.1.4, 3.4, 3.4.2 and 3.6.1).
- *Personality characteristics* as a set of constructs are based on the five-factor model (FFM) of personality traits (Chapter Two, Section 2.8.1 and this chapter, Section 3.6.1)
- *Motivation* (Chapter Two, Sections 2.7 and 2.8; this chapter, Section 3.1.3)
- *Structural role/power* and *nationality/culture* are two of Hofstede's (1980, 2010) dimensions (Chapter Two, Section 2.8.4 and this chapter, Section 3.6.6).
- *Victimisation* is based on Cialdini's (2001, 2016) principles of influence (Chapter Two, Section 2.7), as well as on RAT (this chapter, Section 3.1.1), being the result of the convergence of the three elements of that model.

3.5 Hypothesis Development

As shown in Figure 3-7, the Model of Susceptibility to CSE Victimisation on LinkedIn proposed for this study consists of nine independent variables, three of which are multiple-factor constructs consisting of three, four, and five sub-constructs respectively, and one dependent variable (susceptibility to CSE victimisation on LinkedIn). The hypotheses proposed are as follows:

H1: Employees who express *high levels of conscientiousness are less susceptible* to CSE victimisation on LinkedIn than are those who express low levels of conscientiousness.

H2: Employees who express *high levels of extraversion are more susceptible* to CSE victimisation on LinkedIn than are those who express low levels of extraversion.

H3: Employees who express *high levels of agreeableness are more susceptible* to CSE victimisation on LinkedIn than are those who express low levels of agreeableness.

H4: Employees who express *high levels of openness to experience are more susceptible* to CSE victimisation on LinkedIn than are those who express low levels of openness to experience.

H5: Employees who express *high levels of neuroticism are less susceptible* to CSE victimisation on LinkedIn than are those who express low levels of neuroticism.

H6: Employees who express *high levels of risk perception are less susceptible* to CSE victimisation on LinkedIn than are employees with low levels of risk perception.

H7: Employees who express *high levels of willingness to assume risk are more susceptible* to CSE victimisation on LinkedIn than are employees with low levels of willingness to assume risk.

H8: Employees who *perceive they have control over information on LinkedIn* (privacy risk) *are less susceptible* to CSE victimisation on LinkedIn than are employees who perceive they have little control over their information.

H9: Employees who express *high levels of IT self-efficacy are less susceptible* to CSE victimisation on LinkedIn than are employees who express low levels of IT self-efficacy.

H10: Employees with *risky habitual behaviour* on LinkedIn *are more susceptible* to CSE victimisation than are those with lower levels of engagement on LinkedIn.

Hypothesis 10 comprises three sub hypotheses:

H10.1 Employees with *low levels of information security habitual behaviour* on LinkedIn *are more susceptible* to CSE victimisation than are those with higher levels of information security habitual behaviour on LinkedIn.

H10.2 Employees with *high levels of engagement* on LinkedIn *are more susceptible* to CSE victimisation than are those with lower levels of engagement on LinkedIn.

H10.3 Employees with *high frequency of SNS use* on LinkedIn *are more susceptible* to CSE victimisation than are those with lower frequency of SNS use on LinkedIn.

H11: *Older employees are less susceptible* to CSE victimisation on LinkedIn than are younger employees

H12: *Female employees are less susceptible* to CSE victimisation on LinkedIn than are male employees

H13: *Employees in senior positions* in the organisation *are less susceptible* to CSE victimisation on LinkedIn than are employees in a junior position

H14: The *nationality* of an employee *can increase their susceptibility* to CSE victimisation.

H15: Users who are *motivated by career advancement* on LinkedIn *are more susceptible* to CSE victimisation than are those who are less motivated in this way.

H16: Users who are *more inclined* than others *to present themselves and their credentials* on LinkedIn *are more susceptible* to CSE victimisation.

The development of these hypotheses is discussed in detail below.

3.6 Additional Factors for the Designed Model

The model proposed in this thesis expands on that of Saridakis *et al.* (2016) to include factors that have emerged from the literature. The additional factors are (1) personality

characteristics, which consist of the "big five"—openness to experience, conscientiousness, extraversion, agreeableness and neuroticism; (2) risky habitual behaviour, which consists of three subfactors: information security habitual behaviour, level of engagement and frequency of SNS use; (3) demographic variables, which consist of the four sub-factors of age, gender, nationality, and power position within an organisation; and (4) two motivational factors related to participating on LinkedIn, which are self-presentation and professional advancement. These factors capture the personal, dispositional, demographic and perceptual dimensions influencing employees' susceptibility to CSE risks of victimisation over career-oriented SNS in public sector organisations in Saudi Arabia.

The diagram (see Figure 3-7 above) presents the factors investigated in this study. The factors that can influence the success of victimisation may be internal, such as personality traits, or external, in the form of culture and organisation. A key element of the proposed research model includes personality characteristics, or personality traits. The purpose of this section is to define these factors and how they play a role in the proposed Model of Susceptibility to CSE Victimisation on LinkedIn. The relevant hypotheses are also presented.

3.6.1 Individual Personality Characteristics

There is an extensive literature (see Chapter 2, Section 2.9.1) that examines how FFM can affect susceptibility. Therefore, the first proposed extension to the Saridakis model is to include the "big five" personality characteristics from FFM. The big five personality traits (McCrae and Costa, 1987; Digman, 1990) were conceptualised before the average person had access to the internet; however, as mentioned in Chapter Two, Section 2.8.1, recent research (Parrish *et al.*, 2009; Darwish, El Zarka and Aloul, 2012; McBride, Carter and Warkentin, 2012; Uebelacker and Quiel, 2014; Albladi and Weir, 2017) has suggested that these traits may also determine a person's susceptibility to cybercrime. These five characteristics of a personality are often referred to by the mnemonic OCEAN: openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism (Goldberg, 1990, 1992). The proposed Model of Susceptibility to CSE Victimisation on LinkedIn defines and examines these traits based on the definitions given by Goldberg (1990, 1992).

Openness to experience: high levels of this trait indicate a willingness to try new things without worrying or hesitation, to be enthusiastic and not easily alarmed (Mundie, 2014).

Conscientiousness: individuals with high levels of this characteristic feel a sense of duty or responsibility towards others (McCrae and Costa, 1987), are not compulsive or spontaneous in their behaviour (Carter *et al.*, 2016), punctual and, in their careers, seek self-efficacy and career information (Reed *et al.*, 2004). **Extraversion:** a person with high levels of this trait has high energy and positive emotions, and is assertive, sociable and talkative (Eysenck, 1990). **Agreeableness:** an individual who has high levels of this characteristic is friendly, compassionate, cooperative and trusting in others (Costa and McCrae, 1992; Parrish *et al.*, 2009). **Neuroticism:** a neurotic person lacks emotional stability, self-confidence and impulse control. Figure 3-8 shows the Big Five personality traits.

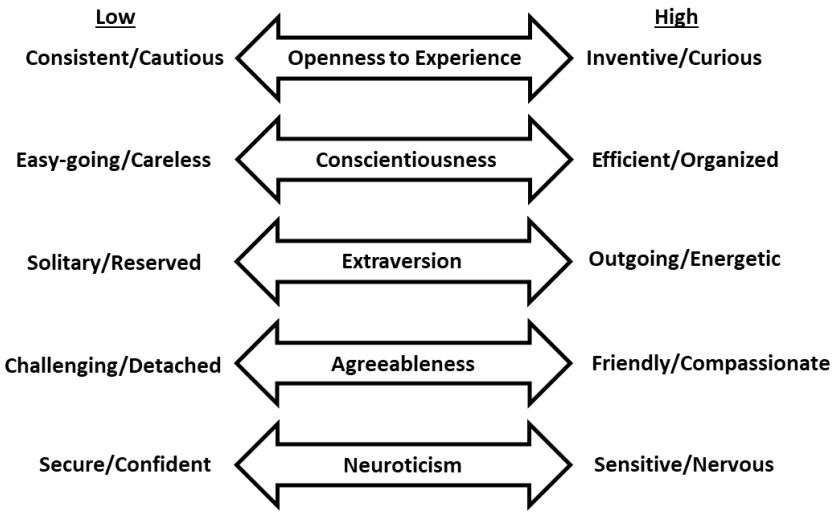


Figure 3-8 The Big Five personality characteristics on a continuum. Adapted from Goldberg (1990)

3.6.1.1 Personality Characteristics and CSE Susceptibility

The traits of *conscientiousness, extraversion, agreeableness, openness to experience,* and *neuroticism* are predicted to have a direct relationship to CSE susceptibility. The literature suggests that individuals with high levels of agreeableness, conscientiousness, openness and extraversion are more susceptible to CSE victimisation (Parrish *et al.*, 2009; Uebelacker and Quiel, 2014; Alseadoon *et al.*, 2015). However, the findings of the studies are not consistent; other researchers have found that these traits, except extraversion, were associated with reduced propensity to take risks and higher levels of information security awareness (ISA) (McCormac *et al.*, 2017b; Hadlington, 2017; Butavicius *et al.*, 2017). In addition, as mentioned in Section 3.1.4, personality traits correlate with and in some cases can predict workplace behaviours. The first five hypotheses of this thesis have been

developed based on specific suggestions from earlier research on employee behaviour that relates to the big five personality traits, as follows:

Previous research has indicated that highly conscientious individuals are less likely to be susceptible to phishing emails due to their tendency to follow policies (Parrish *et al.*, 2009; Darwish *et al.*, 2012).

H1: Employees who express *high levels of conscientiousness are less susceptible* to CSE victimisation on LinkedIn than are those who express low levels of conscientiousness.

There is an abundance of research demonstrating that employees with high levels of extraversion may be more likely than their less extroverted colleagues are to flout IT security policies (Darwish, El Zarka, and Aloul, 2012; McBride *et al.*, 2012; Albladi and Weir, 2017), including sharing sensitive information (Parrish *et al.*, 2009; Alseadoon *et al.*, 2015). Weirich and Sasse (2001) note that employees who are strict about not sharing passwords are seen by their co-workers as loners and tend to be more introverted and therefore less likely to become victims of CSE. Moreover, in the SNS context, Albladi and Weir (2017) found that high levels of extraversion can increase Facebook users' susceptibility to CSE attacks. Hence,

H2: Employees who express *high levels of extraversion are more susceptible* to CSE victimisation on LinkedIn than are those who express low levels of extraversion.

Most studies reviewed for this thesis have found that, in the information security context, agreeableness correlates positively to CSE victimisation. Parrish *et al.* (2009) and Alseadoon *et al.* (2015) found a significant positive relationship between agreeableness and accepting phishing emails: scoring high in this trait increases victimisation. Some research has shown that people who score high on trust, a sub-trait of agreeableness, tend to be willing to cooperate, making them more susceptible to CSE attacks (Weirich and Sasse, 2001; Workman, 2008). Conversely, Albladi and Weir (2017) reported that agreeableness had a significant negative influence on users' susceptibility to cyberattacks on Facebook. This could be explained by Erdheim *et al.*'s (2006) assertion that compliance (as in following company policy) is a sub-trait of agreeableness; thus this form of agreeableness could reduce susceptibility to CSE victimisation. Nevertheless, most of the literature points to the opposite effect. Therefore,

H3: Employees who express *high levels of agreeableness are more susceptible* to CSE victimisation on LinkedIn than are those who express low levels of agreeableness.

People who are open to experience are unhesitant about exploring unfamiliar territory. Research has shown that such individuals have no qualms about their data privacy and willingly enable their mobile location services (Junglas and Spitzmüller, 2006), and are more likely to open phishing emails (Halevi *et al.*, 2013a, 2013b; Alseadoon *et al.*, 2015). Thus, employees who score highly on this trait may not consider the possibility of CSE attacks, leaving them susceptible to CSE victimisation. In their research on users of SNS, however, Albladi and Weir (2017) reported no correlation between openness to experience and CSE victimisation. In this thesis it is hypothesised that,

H4: Employees who express *high levels of openness to experience are more susceptible* to CSE victimisation on LinkedIn than are those who express low levels of openness to experience.

Halevi *et al.* (2013a, 2013b) reported that neuroticism or emotional instability is strongly correlated to victimisation from phishing attacks; to explain this relationship, they posit that emotionally unstable individuals tend to believe what they are told and are not good at distinguishing between fact and falsehood. A conflicting view is that of Albladi and Weir (2017), who found that emotionally unstable people are less trusting and more cautious, thus reducing their susceptibility to CSE. This seems to corroborate the findings of Weirich and Sasse (2001), that emotionally unstable people fear punishment and therefore are more likely to comply with IT security policies.

H5: Employees who express *high levels of neuroticism are less susceptible* to CSE victimisation on LinkedIn than are those who express low levels of neuroticism.

3.6.2 Risk Perception and Risk Propensity

Risk perception is the "*subjective judgment that people make about the characteristics and severity of a risk*"; such judgements are based on a person's "*beliefs about potential harm or the possibility of a loss*" (Darker, 2013, p. 110). Risk perception can include cognitive and affective components. The cognitive component involves the use of intellectual skills (weighing the evidence, using reasoning and logic to reach conclusions), whereas the affective component consists of emotional appraisals (intuition, instinct or imagination; Slovic *et al.*, 2005). Ropeik (2002) has identified 14 specific factors that influence risk

perception. Four of these factors are of particular relevance to the theories underpinning the present research, and are explained as follows:

- *Trust vs. lack of trust*: When people trust the person or source they are receiving information from, they are less likely to be afraid, and therefore feel no need to behave cautiously; if the person or source providing the information is not trusted, the person receiving the information is more likely to be afraid and to act with caution. Trust has a relationship with perceived risk and risk-taking (Das and Teng, 2004). In the SNS context, the extent to which an individual trusts another "person" over the internet can depend on how the former perceives risk in SNS communication (Albladi and Weir, 2017). Williams *et al.* (2017) observed that "*propensity to trust is likely to vary according to the beliefs that people hold regarding the potential risks of online communications and technology in general*" (p. 415).
- *Origin (imposed vs. voluntary)*: People are more concerned about the risk others pose than the risk they themselves may pose (e.g., refusing to wear a face mask to protect others from COVID-19, talking on the phone while driving). In the context of SNS, by not following the company's cybersecurity policies, the employee may believe that s/he is simply taking a personal risk, and may not consider that s/he is putting colleagues, or indeed the entire company/organisation, at risk.
- *Control vs. lack of control*: This refers to one's perceived control over outcomes. This helps explain why someone is not afraid of driving a car—even though automobile crashes kill thousands of people each year—but may be afraid of flying in an airplane. This concept is also known as perceived behavioural control (PBC; Section 3.1.3) and is discussed in relation to CSE in the next section (3.6.3).
- *Risk vs. benefit*: Weighing the risks (or costs) and benefits of actions is something that people do every day. Slovic *et al.* (2005) note that if people have a favourable view of a technology or a related activity, "*they are moved toward judging the risks as low and the benefits as high; if their feelings toward it are unfavorable, they tend to judge the opposite—high risk and low benefit…* [known as] *the affect heuristic*" (p. S36).

In an online setting, risk perception, in both its cognitive and affective aspects, influences online users' individual susceptibility to CSE victimisation (van Schaik *et al.* 2018; Albladi and Weir, 2020), as expressed in this hypothesis:

H6: Employees who express *high levels of risk perception are less susceptible* to CSE victimisation on LinkedIn than are employees with low levels of risk perception.

Risk perception in this research refers to the likelihood an employee can recognise themselves to be at risk of deception. Workman (2008) argued, "*when people perceive that risk has diminished, they will behave in a less cautious manner*" (p. 317). A salient factor that is related to risk perception is risk propensity, or the willingness to take risks. Saridakis *et al.* (2016) explain the difference between the two concepts this way: "*While risk perception is a psychological status, risk propensity is an action state that determines the amount of risk an individual is willing to take*" (p. 6). However, the term "action state" may be misleading: Arend *et al.* (2020) note, "*In many real-life situations, risk derives from not implementing a particular action*" (p. 2). This is known as "*passive risk-taking: risk brought on or magnified by inaction*" (Keinan and Bereby-Meyer, 2017, p. 999). While the literature suggests that employees' motivations for subscribing to and participating on the LinkedIn platform are career advancement and self-presentation (Kim and Cha, 2017; Vishwanath, 2017), the desire to achieve a goal in cyberspace can increase the propensity to take risks (Nguyen and Kim, 2017), potentially causing users to fall victim to employment fraud (Cleary and Kelly, 2017; Krehel, 2016) through CSE tactics.

H7: Employees who express *high levels of willingness to assume risk are more susceptible* to CSE victimisation on LinkedIn than are employees with low levels of willingness to assume risk.

3.6.3 Perceived Behavioural Control and IT Self-Efficacy

As mentioned in Chapter Two (Section 2.8), a broad variety of factors can influence an individual's disposition to CSE victimisation. Perceived behavioural control (PBC), a construct in TPB (Section 3.1.3) was highlighted as a factor in the general theory of risk perception, and it has been examined in connection with risk perception in recent CSE literature (e.g., Rhee, Ryu and Kim, 2012; Beldad, 2015, 2016; van Schaik *et al.* 2017, 2018; Albladi and Weir, 2020). In particular, studies have found an inverse relationship between PBC and perceived risk: the more control people perceive themselves to have in a given sphere of operation, the less risk they perceive to be present (Rhee, Ryu and Kim, 2012; Vishwanath *et al.*, 2016; van Schaik *et al.*, 2017).

Additionally, risky behaviours can be due to users' low self-efficacy to protect their online information (Milne, Labrecque and Cromer, 2009; Di Giunta *et al.*, 2013). In Saridakis *et al.*'s (2016) model, PBC took the form of "computer self-efficacy". Saridakis *et al.* (2016) found that, in the SNS context, self-confidence in one's own ability and skills in computer

use was linked to reduced susceptibility to cybercrime victimisation. For this reason, IT self-efficacy, and its above-mentioned association with concerns of control over the privacy of users' information, is another dimension where further research is needed. Based on the foregoing, the following two hypotheses are to be tested:

H8: Employees who *perceive they have control over information on LinkedIn* (privacy risk) *are less susceptible* to CSE victimisation on LinkedIn than are employees who perceive they have little control over their information.

H9: Employees who express *high levels of IT self-efficacy are less susceptible* to CSE victimisation on LinkedIn than are employees who express low levels of IT self-efficacy.

3.6.4 Risky Habitual Behaviour and Information Security

As discussed in Section 3.1.1, LRAT accounts for risk in terms of probability, in that certain habitual or routine behaviours, can increase a person's chances of being victimised (Pratt and Turanovic, 2016). Pattinson *et al.* (2015) include risk as an integral part of their definition of information security behaviour. They define it as "*the full spectrum of behaviours by people who make significant use of computers as part of their job…these behaviours range from deliberate risk-averse behaviours to deliberate risk-inclined behaviours*" (p. 61). Therefore, some studies have recommended incorporating variables relating to users' habitual patterns in models of CSE victimisation risk in the context of SNSs. These variables include, for example, email habits (Vishwanath, 2015b; Vishwanath *et al.*, 2016); level of involvement (Albladi and Weir, 2018, 2020); and SNS usage (Vishwanath, 2015a; Saridakis *et al.*, 2016). The findings of these studies all suggest that a high level of engagement on SNS and constant checking of emails, combined with low levels of information security habitual behaviour, can increase the risk of cyberattack victimisation in both email and SNS contexts (Vishwanath, 2014, 2015b; Saridakis *et al.*, 2016; Albladi and Weir, 2018).

With regard to risky habitual behaviours involving company/organisation information security, a study involving 245 employees of a company in Finland found that employees' habits have "*a significant effect on intention to comply with IS security policies*", and this was the case even though employees were aware that non-compliance would result in punishment from their employer (Pahnila *et al.*, 2007, p. 156b). In contrast, a study carried out on employees in an organisation in Hong Kong found that the threat of punishment for

risky IS behaviour was a stronger deterrent for such behaviour than was the organisation's IS awareness program (Chu and So, 2020). These conflicting findings suggest that employees' nationality/culture may influence IS risky habitual behaviours and susceptibility to CSE attacks (see Section 3.6.6). Several authors have examined users' online engagement based on the premise of lifestyle/routine activity theory (Leukfeldt, 2015; Leukfeldt and Yar, 2016; Choi and Lee, 2017). Thus, users' online lifestyle and time spent in online communities and other various situations of online activity that expose an individual to malware (Holt, van Wilsem, van de Weijer, and Leukfeldt, 2018) can make them a visible target to cyber-social engineering offenders. Moreover, Halevi *et al.* (2013a) and Hadlington (2017) found that internet addiction increases an individual's vulnerability to cyberattacks. This implies that high usage and online presence increase the likelihood of CSE victimisation.

H10: Employees with *risky habitual behaviour* on LinkedIn *are more susceptible* to CSE victimisation than are those with lower levels of engagement on LinkedIn.

Hypothesis 10 encompasses three sub-hypotheses:

H10.1 Employees with *low levels of information security habitual behaviour* on LinkedIn *are more susceptible* to CSE victimisation than are those with higher levels of information security habitual behaviour on LinkedIn.

H10.2 Employees with *high levels of engagement* on LinkedIn *are more susceptible* to CSE victimisation than are those with lower levels of engagement on LinkedIn.

H10.3 Employees with *high frequency of SNS use* on LinkedIn *are more susceptible* to CSE victimisation than are those with lower frequency of SNS use on LinkedIn.

3.6.5 Demographic Factors

The literature has shown that age and gender have relevance in influencing individuals' ability to identify CSE attacks such as phishing emails, for instance (Sheng *et al.*, 2010; Jagatic *et al.*, 2007; Kumaraguru *et al.*, 2010). However, the empirical findings on how age and gender affect individuals' susceptibility to CSE are contradictory. With regard to age, Grimes *et al.* (2010) reported that elderly people had lower awareness of cybersecurity risks than did young people, and this was mainly due to cohort differences in education and the

divide between digital natives and non-natives. Based on similar premises, Whitty *et al.* (2015) hypothesised that older adults would be more likely than younger people to share passwords; in fact, the researchers found that the elderly were less likely to share passwords.

On gender differences, Anwar *et al.* (2017) found that female employees' computer self-efficacy was significantly lower than that of males, while Arend *et al.* (2020) reported that males had better adherence to cybersecurity practices than females did. From these and similar findings it has been inferred that females are generally more susceptible than males are to CSE attacks (Sheng *et al.*, 2010; Halevi *et al.*, 2013a; Blythe *et al.* 2011; Goel *et al.*, 2017). On the other hand, others have argued that men have higher risk propensity than women do, and that women tend to be "more cautious" than men, and that these gender-based differences should hold in online environments (Byrne, 1999; Mills, 2010).

Based on the foregoing, the following hypotheses are proposed:

H11: *Older employees are less susceptible* to CSE victimisation on LinkedIn than are younger employees [because the former are more likely than the latter to have a cautious attitude towards CSE risks].

H12: *Female employees are less susceptible* to CSE victimisation on LinkedIn than are male employees [because females are more likely than their male colleagues to have a cautious attitude towards CSE risks].

3.6.6 Cultural Factors: Organisation and Nationality

Rocha Flores (2016), Al-Hamar *et al.* (2010) and Albladi and Weir (2018) found that social differences between countries in terms of inherited culture, language, religion and custom, especially their collectivist/individualist character, could impact individuals' susceptibility to CSE attacks. Also, Williams *et al.* (2017) posited that employees in a "*position of relatively low power or status within the organisation, may* [be] *particularly susceptible to influence attempts*" (p. 418). As discussed in Chapter Two (Section 2.8.4), two of the dimensions from Hofstede's (1980) original model of cultural dimensions have particular relevance to the focus of this research: power distance and individualism/collectivism. "Power distance" refers to the extent to which members of a society or culture "*accept that power is distributed unequally and are prepared to take instruction or give it without concern for people's feelings. Those without power respect those who have it, and those*

with power expect those without it to follow instructions" (Alshehri, 2015, p. 16). According to Hofstede, Saudi Arabia scores high on these two dimensions of power distance and collectivism.

According to Furnell and Rajendran (2012), the nature of an employee's role in an organisation influences that individual's information security behaviour. In their study on information security compliance behaviour and behavioural intention, Aurigemma and Mattson (2017) reported that employees in relatively senior positions (meaning that they were in positions of authority over many others in the organisation) had greater PBC over behaviours entailing CSE risks than did employees in relatively junior positions. However, the researchers noted that had their study been conducted in a different cultural setting (whether geographically or organisationally), they may have found different results. For instance, in a phishing email experiment, Bullée *et al.* (2017) found that employees from cultures that scored high on Hofstede's (1980) dimension of power distance were more likely to provide their PII than employees from cultures scoring low on power distance. As Williams *et al.* (2017) have noted, "*The norms, habits and values inherent within a workplace are also known to guide behaviour and influence the assumptions that people hold when operating in the workplace*" (p. 417). It should be recalled from Section 3.1.2 that the constructs from TRA/TPB of beliefs/attitudes and subjective norms encapsulate the internal perceptual constructs and the external organisational cultural dimensions, respectively. Therefore, these are key components in the study model (Figure 3-7).

Therefore, the next two hypotheses are incorporated into the research model:

H13: Employees in *senior positions* in the organisation *are less susceptible* to CSE victimisation on LinkedIn than are employees in a junior position [because the former are more likely than the latter to have a cautious attitude towards CSE risks].

H14: The *nationality* of an employee *can increase their susceptibility* to CSE victimisation.

3.6.7 Self-Presentation and Professional Advancement

The literature has shown that the use of career-related SNS platforms usually has two basic motivations: self-presentation and professional advancement (Kim and Cha, 2017). Self-presentation is a form of information disclosure (Bronstein, 2013); consequently,

individuals who are driven by self-presentation are more inclined to develop relationships (Schwämmlein and Wodzicki, 2012). These motives of career advancement can be seen as an element that could be exploited by fake recruiter scams. LinkedIn members have been found to be significantly more likely than Facebook users to allow public access to their professional and educational data (Zhitomirsky-Geffet and Bratspiess, 2015), but there is little research specifically addressing these users' attitudes and dispositions toward potential CSE risk in the context of SNS generally, and specifically in relation to career-oriented SNS.

Subscribers to LinkedIn use the site primarily for professional advancement (for developing a professional future, sharing work-related career history posts, networking with professional contacts, obtaining peer support from others) and secondarily for self-presentation (providing personal credentials, introducing or telling others about themselves) (Kim and Cha, 2017), where the user portrays his/her professional identities. These motivations can be taken advantage of by a social engineer masquerading as an employer (Misra and Goswami, 2017) or job seeker, or using a cloned profile of a colleague. As stated by Dekay (2009, "*job candidates are increasingly presenting themselves in online communities to impress employers*" (p. 516). Therefore, any active individual who engages in a high degree of professional development activity and self-presentation behaviour exposes herself or himself to CSE.

These considerations lead to two further hypotheses:

H15: Users who are *motivated by career advancement* on LinkedIn *are more susceptible* to CSE victimisation than are those who are less motivated in this way.

H16: Users who are *more inclined* than others *to present themselves and their credentials* on LinkedIn *are more susceptible* to CSE victimisation.

3.7 Summary of the Chapter

In this chapter the theoretical foundations of the model upon which the study model is based were presented. Justification is provided regarding the selection of the Model of Social Media Behaviour and Risk of Cyber Crime Victimisation (Saridakis *et al.*, 2016). The conceptual model for this thesis, an extension of the model by Saridakis *et al.* (2016), was presented, and the hypotheses were developed. The additional theoretical bases for this study's conceptual model (Model of Susceptibility to CSE Victimisation on LinkedIn) were

presented and explained in order to achieve the research objective of identifying underlying causes of employees' susceptibility to CSE victimisation in the workplace. The research model is intended to account for human factors in susceptibility to CSE attacks, and thus has incorporated theories from behavioural psychology. In the next chapter, the research methodology is presented.

4. Research Methodology

This chapter consists of two main parts. The first part presents the philosophical assumptions underpinning this study, which guide the research strategies. The epistemological stance adopted for this research project is the pragmatic approach, which combines fundamentals of both positivism and interpretivism. The second part of the chapter presents a thorough discussion of the research methodology, research design, instruments, data collection and sampling techniques, and modes of analysis that are used in this research. In addition, the chapter discusses the reliability and validity of the research.

4.1 Research Philosophy and Philosophical Assumptions

This section discusses the philosophical assumptions and research strategies underpinning this study. The predominant philosophical assumptions are looked at and presented. Scientific research ought to be based upon underlying philosophical assumptions to establish the validity of the research after evaluation (Myers and Avison, 2002).

Saunders, Lewis and Thornhill (2015) highlight that research philosophies/approaches are about "*the development of knowledge and the nature of that knowledge*" (p. 107). The differences between such philosophies as positivism, realism, post-positivism, objectivism, interpretivism, holism and pragmatism impact the researcher's way of thinking while processing data collection and analysis., Moreover, the consideration of practical constraints, such as insufficient time, money and other resources can lead a researcher to decide to adopt a particular philosophy, and its associated approach(es), over another. The choice of research philosophy and approach in turn shapes the knowledge being developed (Saunders *et al.*, 2015).

4.1.1 Paradigm of Inquiry

This section introduces the foremost philosophical assumptions that influence IS research. Empirical research can be motivated and impacted by the researcher's beliefs and value preferences; therefore, from the outset it is essential to decide on the philosophical framework or paradigm for the study, which will lead the research process and to determine how the research should be carried out. The chosen research philosophy of a scientific

researcher can function as a means to fill the gap between their assumptions and the way the world is perceived. Saunders *et al.* (2015) highlight that research strategies and the methods deployed are based upon such philosophical assumptions, or *worldviews* (Bryman, 2012). In this section, three categories of essential assumptions are presented prior to introducing the research philosophy chosen for this thesis; these philosophical assumptions are dominant in social science research (Bryman, 2012):

- The nature of reality (ontology)
- The nature of knowledge and the relationship between the inquirer and that which is inquired into (epistemology)
- Methodology

Ontology is the study of being, which is concerned with the nature of existence and reality (Saunders *et al.*, 2015). Different perceptions of the characteristics of existence result in contrasting positions (Willis, Jost and Nilakanta, 2007). The prime focus of social ontology is the question of whether the social world can or should be regarded as a representation of the activities and perceptions of social acting individuals (*social constructions*), or whether they are *objective entities* based on reality outside of social acting individuals (Hussey and Hussey, 1997; Bryman, 2012). These ontological stances of social science research are respectively named *constructivism* and *objectivism*. Constructivism stresses that people's perceptions generate the existence of reality, which emerges from concepts, names and labels already existing in one's mind, to make sense of how people build reality. In contrast, objectivism regards the social world, such as the physical world we live in, as touchable and objective reality, and outside of people's perception.

Epistemology is a philosophical stance that pertains to the nature of knowledge; it assesses the appropriate method to study the world. Epistemology derives from the Greek term *episteme*, which means knowledge and reason (Stroll and Martinich, 2020). According to Stanton (2010), epistemology is generated from a unique individual experience. The epistemological stance identified for this study is the pragmatic approach, which combines aspects of both positivism and interpretivism (Saunders *et al.*, 2015). All three are relevant to IS research (Dhillon and Backhouse, 2001); they are explained below.

Positivism is a set of philosophical approaches suggesting that universal laws are perceived through a lens to explain how humans behave (Neuman, 2014). It advocates dealing with the social reality that is being observed (Saunders *et al.*, 2015). In order to explain an

experienced phenomenon, positivism is deployed, using observation and measurement, as this approach involves the elimination of subjective data (Neuman, 2014). This approach is guided by existing principles and methods to build hypotheses in order to test them (Bryman, 2012). Using this epistemology, social science researchers are likely to consider collected data in an objective way, with minimal bias, and in the same manner as a natural scientist (Hussey and Hussey, 1997; Stanton, 2010; Scotland, 2012). Positivism takes an objectivist ontological stance, and as such is grounded in the assumption that social reality is singular, objective and not altered by being examined. In this approach, explanatory theories are deployed to understand a particular social phenomenon, using the deductive process. Positivism views the researcher as an external observer to what is contained in a study (Cohen, Manion and Morrison, 2007). Positivism is largely associated with quantitative, rather than qualitative, research. Creswell and Plano Clark (2007) explain that studies which are carried out using quantitative methods emphasise objective measurements, by identifying and testing the validity of relationships between constructs to confirm or reject their prior formulation of hypotheses.

Interpretivism is an approach which is generally seen as an alternative to positivism (Bryman, 2012). It is an epistemology that a researcher adopts to understand and interpret the differences between people as social actors, according to meanings assigned to their social roles. Consequently, interpretivists believe that social reality is subjective and is influenced by the manner in which it is investigated in order to develop meaningful knowledge. Thus, different people may develop contrasting meanings and opinions (Saunders *et al.*, 2015); therefore, any emerging knowledge varies due to its characteristics of being culturally derived and historically situated (Scotland, 2012). The adoption of interpretivism is broadly associated with a qualitative research approach, in order to attain insightful meaning and reasoning from participants (Orlikowski and Baroudi, 1991; Bryman, 2012). The interpretivist paradigm is used to explain multiple realities through individuals' views and behaviours (Cohen *et al.*, 2007). Interpretivism is adopted, rather than the rigid structural model used in positivism, due to its flexibility and to identify meanings in human interactions (Bryman, 2012). Therefore, the goal of adopting interpretivism is to help understand and interpret what human behaviours mean, rather than just predicting causes and effects (Neuman, 2014). The interpretive explanatory goal is "*for others to mentally grasp how some area of the social world operates and to place what we want to explain within that world*" (Neuman, 2014, p. 84). Walsham (1993) explains that

the interpretive perspective allows for "*producing an understanding of the context of the information system, and the process whereby the information systems influence and are influenced by the context*" (Walsham, 1993, pp. 4-5).

Philosophical assumptions in IS research. According to Walsham (1993), interpretivism has been demonstrated to provide a valuable contribution to IS research. Orlikowski and Baroudi (1991) argued that whereas behavioural IS research had until that point in time drawn almost exclusively on the positivist natural science tradition in their philosophical assumptions, such assumptions "*may not always be appropriate for inquiry into the relationships between information technology and people or organizations*" (p. 2). The authors asserted that these relationships are contextually situated, and that "information processing is a social practice that impacts on a social world"; hence, it would be more appropriate to view social processes as "central to information systems phenomena" and to adopt additional research perspectives that come from the philosophical paradigms of social science research (Orlikowski and Baroudi, 1991, p. 24). In particular, one of the alternative epistemologies they recommend is interpretivism.

Pragmatism. The central idea of pragmatism is to focus solely on practical issues, in other words, to a pragmatist, knowledge as useful only if it is practical. According to this philosophy, there are numerous methods of viewing how the world operates, and not necessarily one single view that can describe the whole picture (Saunders *et al.*, 2015). Neuman (2014) describes this approach as a "pragmatic orientation toward social knowledge in which people apply knowledge in their daily lives; the value of knowledge is the ability to be integrated with a person's practical everyday understandings and choices" (p. 109).

Pragmatism is one of three different research epistemological approaches operating in information systems (IS). Several papers have acknowledged pragmatism in various domains, such as in accounting (Chua, 1986) and organisational studies (Wicks and Freeman, 1998), while others have highlighted the significance of the pragmatic approach in IS research, such as in Baskerville and Myers (2004), Myers and Avison (2002), and Goldkuhl (2004, 2008). According to Dudovskiy (2018, p. 45), pragmatics can combine both positivist and interpretivist positions within the scope of a single study, according to the nature of the research question. In addition, Creswell and Plano Clark (2007, p. 173) observed that "*pragmatism is the overarching paradigm for mixed methods research*". Burke Johnson, Onwuegbuzie and Turner (2004) referred to pragmatism as "*an attractive*

philosophical partner for mixed methods research" (p. 14). They also recommend that, "*research approaches should be mixed in ways that offer the best opportunities for answering important research questions*" (p. 16). Bryman (2012) agrees, and notes that in combining quantitative with qualitative research, this can "*allow the various strengths to be capitalized upon and the weaknesses offset somewhat*" (p. 628). Bryman expounds on this with an example of an actual study in the UK on public trust (or lack thereof) in government information regarding foot and mouth disease (FMD). In that study, a self-completion questionnaire administered to hundreds of participants was followed by three focus groups comprised of some of those same participants. While the questionnaire data revealed variation in the variables of interest, the focus groups provided:

> *valuable additional information, especially on the reasons, rationalizations and arguments behind people's understanding of the FMD issue. [...] As a result, the researchers were able to arrive at a more complete account of the FMD crisis than could have been obtained by either a quantitative or a qualitative research approach alone*. (p. 37)

Methodology – This term comprises two nouns: method and *ology*, and is defined as a branch of knowledge that pertains to the rationale and philosophical assumption underlying studies in natural, social or human science to form knowledge (McGregor and Murnane, 2010). Methodology is an approach to systematic inquiry; it is a combination of principles, rules and methods that are the product of the reasoning behind the researcher's choice of a particular method or set of methods (Kawulich, 2012). A single research methodology often employs a number of research methods. Furthermore, the choice of methodology is not simply a selection of methods, because any and all methods selected must be appropriate for the methodology. In order for this to happen, it will require the appropriate method(s) to be identified, which is a technical procedure while conducting research to achieve the best possible answers. Identifying the research method relies on the individual perspective of the researcher's philosophy, in parallel with the research problem to be addressed (See Chapter 1).

4.2 Research Approach of This Study

This study adopts the pragmatic approach, which mixes both quantitative and qualitative methods. According to Creswell and Plano Clark (2007), the value of using the pragmatic

paradigm is to focus on the research problem, followed by increasing knowledge about the problem using appropriate approaches. The research problem under investigation is:

> Q1. How, and to what extent, do personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering (CSE) victimisation when accessing professional SNS, such as LinkedIn, in government organisations in Saudi Arabia?

The question can be restated as follows:

> Do personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering (CSE) victimisation when accessing professional SNS, such as LinkedIn, in government organisations in Saudi Arabia? If so, how, and to what extent, does this occur?

This research examines whether personal characteristics and other factors play a role in an employee's likelihood being susceptible to CSE victimisation. To answer this question a positivist stance is adopted. A questionnaire is used to gather information from the employees of one government organisation and its affiliates in the Kingdom of Saudi Arabia. This organisation is linked to the country's main technology infrastructure hub, and it is a major repository for all Saudi citizens' and foreign residents' sensitive and private data.

A number of hypotheses have been formulated based on the existing literature. These hypotheses will be tested using quantitative methods. The research also examines how, and to what extent, personal characteristics and other factors play a role in CSE victimisation. To answer this question an interpretivist stance is adopted. The output of the quantitative research carried out in the survey is used to inform the input for qualitative research, in the form of interviews with participating employees, academics and experts in the field. This pragmatic approach has been chosen to gain a deeper understanding of employees' susceptibility to CSE on LinkedIn.

4.3 Research Methodology

Research methodology, defined earlier in Section 4.1.1, is an essential element in every research; as such, the determination of a suitable method is a crucial part of the study. The methodology of any given research is helpful in establishing its components alongside the research structure, such as its approach, design, strategy and research philosophy. The

following sections will discuss the choice and suitability of the methodology for the purposes of the research question at hand (see Sections 4.1 and 4.2). This study examines an essential component in InfoSec for organisations: the human component, which could either help to protect, or lead to the compromising of, sensitive data. Thus the research design and strategy focus on how to effectively investigate the impact of personal characteristics and other factors, identified from the literature review, on employees' susceptibility CSE risk over career-oriented social networking sites. This section also considers the limitations and advantages of the design and methods used.

4.3.1 Research Design

When deciding on a study design, or as Bryman (2012) describes it, "*a general orientation to the conduct of social research*" (p. 35), a researcher may choose among three options: quantitative, qualitative, and mixed methods (Bryman, 2012). With a quantitative design, the researcher follows established procedures and provides relevant documentation of the study sample, the data collection methods and procedures, and any statistical operations. Qualitative research is similar to quantitative in that it also aims to ensure that the findings accurately reflect the data. Qualitative research is primarily inductive, interpretivist rather than positivist, and "*embodies a view of social reality as a constantly shifting emergent property of individuals' creation*" (Bryman, 2012, p. 36). Description of data in a qualitative design often includes quotes from participants and other qualitatively rich data meant to strengthen the validity of the findings (Kawulich, 2012). The third research design option, mixed methods, is discussed in the next section.

4.3.2 Mixed Methods Approach

The adoption of the pragmatist approach, as in mixed methods, overcomes some of the issues linked with using single methods (Saunders *et al.*, 2015). As discussed in Section 4.1.1 above, pragmatism has been described as the "*overarching paradigm*" of mixed methods research (Creswell and Plano Clark, 2007, p. 173). While there is a broad array of methodological techniques in the domain of IS research, using mixed methods research can serve to enhance and sustain various IS phenomena being examined, as well as to ensure the formation of a comprehensive and collective body of knowledge (Lee and Hubona, 2009; Mingers, 2001; Venkatesh, Brown and Bala, 2013; Weber, 2004).

A mixed-method approach requires a wider range of abilities while administering the research data collection and the later analysis in both quantitative and qualitative forms (Bryman, 2012). Nonetheless, the utilisation of both quantitative and qualitative techniques when addressing a research problem can combine the strengths of these two methodologies.; The main advantage to mixed methods as a methodology is that the combination of quantitative and qualitative findings result in further insights that would not be apparent from the quantitative or qualitative findings on their own (Creswell and Plano Clark, 2007). In this thesis, the application of a mixed method approach can help in attaining a better understanding of employees' personal characteristics and the connection between their risky behaviours and their susceptibility to CSE over career-oriented SNS.

Creswell and Plano Clark (2007) stress that researchers should determine and reference the type of mixed methods design that will be used in their study. They highlight four main designs that can be adopted: triangulation, exploratory, explanatory and convergence. For the purposes of this study, a sequential explanatory design has been selected. The advantages and suitability of this design choice are described in the following section.

4.3.3 Sequential Explanatory Design

The primary data collection is quantitative. In this phase, the researcher statistically analyses the data to produce key findings, which later lead to further questions. Answers to those new questions are collected in the second phase in a qualitative manner, using various techniques such as focus groups, semi-structured interviews or a Delphi technique (Creswell and Plano Clark, 2007). The underlying rationale for an explanatory design process is to qualitatively dig deeper into the observed quantitative results to enrich, elaborate and provide a better understanding of the research questions. This can be achieved by exploring participants' opinions in more detail (Kawulich, 2012). The usefulness of this approach is determined when unpredicted findings can emerge from the first statistical analysis, as the researcher will consequently dig deeper in more detail by deploying a second, qualitative stage (Bryman, 2012). The primary reason for selecting a sequential explanatory design rather than an exploratory design for the present study is that the phenomenon (susceptibility to social engineering in cyberspace) has already been identified and defined in the literature. Thus, the first phase is focussed on quantifying the phenomenon in the context of the study. The explanatory part of this design is needed during the second phase of the study, in order to gain insights into the quantitative findings.

Sequential explanatory mixed methods design is well suited to case study research that involves both quantitative and qualitative data collection. (Bryman 2012; Lalor *et al.*, 2013). This type of design is illustrated in Figure 4-1 below.

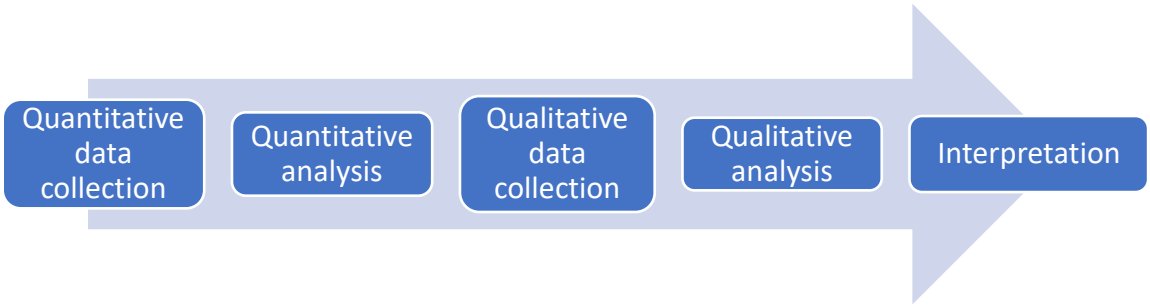


Figure 4-1 Sequential explanatory mixed methods design
Adapted from Steinmetz-Wood et al. (2019)

4.4 Suitability of Methodology and Methods

For this research study, the combined findings of an integrated analyses from both quantitative and qualitative data will identify the factors which are linked to employees' exposure to CSE on CSNS. From this a preventive set of recommendations will be developed. Initially, the researcher had planned to include in the study design an experiment on targeted participants involving a purported phishing attack. LinkedIn was contacted in writing to seek guidance on how to execute such an experiment according to the guidelines and rules of the platform. The company replied with a clear request to refrain from launching any type of cyber-social engineering scenario (see Figure 4-5 in Section 4.13). Consequently, using an experiment intended to assess user susceptibility was withdrawn from consideration.

4.4.1 Quantitative Method: Survey Questionnaire

Quantitative methods are often found to be a suitable part of explanatory research, where the aim is to test a conceptualised model of designed hypotheses (as is the case with the present study, which extends the model of Saridakis *et al.*, 2016). There are a number of quantitative methods for gathering social science data, such as survey questionnaires, interviews, observation, literature/database/document review, and experiments. Some of these methods, such as interviews and observation, are also employed in qualitative research (Bryman, 2012). Due to the constraints posed by time, bureaucracy, cost and

ethical considerations (see Sections 4.11 and 4.14), the survey questionnaire was determined to be the most efficient and suitable method for the purposes of this study.

4.4.2 Qualitative Method: Interview

The qualitative stage of this research is meant to address the "how", and to add insight to the "to what extent" part of the research question. Qualitative methods of data collection typically employed in social science research include interviews, textual or discourse analysis, observation and focus groups (Bryman, 2012). As mentioned above, a survey questionnaire was the instrument for the quantitative part of the mixed methods study design. For the qualitative/interpretive phase of this research design it was decided to employ interviews with experts from a variety of disciplines related to the focus of the study, as well as with public sector employees in similar positions to some of the survey respondents. This follow-up stage is carried out to seek clarifications with regard to issues raised by the quantitative data collected.

Kvale (1996) highlighted that via the interview, the researcher tries to understand a phenomenon from the point of view of the interviewee. The interviewer attempts to obtain from the interviewee "*subjective information about a particular topic or experience*" (Kvale, 1996, p. 1). Thus, it should be noted that interview data is often messy and "*cumbersome*" to record, transcribe, and – in the case of this study's interview data – to translate with accuracy (Bryman, 2012, p. 565). This study uses semi-structured interviews. With the semi-structured interview, the questions are usually more general than those in a structured interview; the interviewer can vary the order of the questions and may even "*ask further questions in response to what are seen as significant replies*" (Bryman, 2012, p. 716).

The rationale behind using semi-structured interviews is that it is a feasible, powerful tool to give room for participants to express their opinions and for questions to evolve and be reworded during the process (DeJonckheere and Vaughn, 2019). Data collection gaps can be present when interviewing, which must be filled for the data to be valid and reliable, and this is not possible when sticking to the exact questions; rather, the ability to probe further is valuable (Cohen *et al.*, 2007). Thus, it was determined that the semi-structured interview was the most flexible and appropriate data collection method for the qualitative phase of this study.

The objective of applying mixed methods is to gain a rich data set surrounding specific research issues. As mentioned in Section 4.3.2, the rationale for using such a method is to bridge the gap between the quantitative and qualitative approaches, when the information obtained from just one methodology is inadequate. By employing mixed methods, the researcher is able to cross-check or "*triangulate*" the findings from the quantitative part of a study with those from the qualitative part (Bryman, 2012, p. 392). Using mixed methods also ensures variation in data collection methods and this allows for greater validity. Also, mixed methods can answer questions from a number of perspectives (Venkatesh, Brown and Sullivan, 2016).

4.5 Research Strategy

A research strategy is an integral part of the research methodology. The research strategy provides a comprehensive guide and direction for the research process by which the research is conducted (Saunders *et al.*, 2015). The strategy of the research is chosen based on the nature of the research problem (Bryman, 2012). According to Saunders *et al.* (2015), a research strategy can include surveys, case studies, grounded theory or action research, and that a "*case study strategy can be a very worthwhile way of exploring existing theory…and also provide a source of new research questions*" (p. 140).

Case study methods have been criticised for their lack of external validity in that their findings often are not representative of any population beyond the actual study sample and thus are not generalisable (Bryman, 2012, pp. 69-70). However, Yin (2009) argued that case study research was useful to study a phenomenon in its natural context, and Zainal (2007) observed that "*they are widely recognised in many social science studies, especially when in-depth explanations of a social behaviour are sought after*" (p. 1). Moreover, as Bryman (2012) notes, "*case studies are frequently sites for the employment of both quantitative and qualitative research*" (p. 68), which suits the mixed method research design of the current study. However, he cautions that it is sometimes difficult to distinguish whether a study is actually a case study as opposed to a different research design, such as a cross-sectional design study (p. 68). Bryman (2012) contended that for a research design to be considered a case study, the case should be "*an object of interest in its own right, and the researcher aims to provide an in-depth elucidation of it*" (p. 69). Complex areas of any given study can adopt the case study method. Case study methodology has been applied in a number of studies in related domains such as in IT

education (Gülseçen and Kubat, 2006), cybersecurity risk (Rowe *et al.*, 2012), individuals resisting spear phishing attacks (Thomas, 2018) and risks on social networking sites (Kim and Joukov, 2016).

4.5.1 Holistic Single-Case Study

A holistic single-case study design (see Figure 4-2) of employees working at a large government administration at the Ministry of Human Resources and Social Development (MHRSD) in Saudi Arabia has been chosen for this study. Yin (2009) and Saunders *et al.* (2015) agree that single-case studies can be used as a representation of a critical or unique case, and Saunders *et al.* (2015) argued that the sole crucial criterion for choosing a single case is that it has to lead in "*defining the actual case*" (p. 140). As explained in Chapter One, Section 1.7, it was decided to draw the study sample from the government sector because, due to demographic and policy factors, the public sector in Saudi Arabia is assumed to be generally more representative of the nation's population than a sample taken from the private sector would be. The organisation of interest is MHRSD, which was selected because it has access to and is the primary repository for the personally identifying information of all Saudi citizens and resident expatriates. A cyber-attack on this organisation could impact the privacy and security of hundreds of thousands, if not millions, of people. In this study, the focus is on the employees of this organisation (MHRSD), and in particular, their susceptibility to CSE over professional SNS (CSNS), because these workers are the frontline that can unwittingly provide intruders with unauthorised access to what should be secured data within the organisation. Thus, the case under investigation in this study is a clear representation of a critical case.

Yin (2009) explains that a single case study is classified as *holistic* when the research is only concerned with an organisation as a whole and there is only one unit of analysis (see Section 4.6). That is to say, "*when no logical subunits can be identified or when the relevant theory underlying the case study is itself of a holistic nature*" (p. 50). In this study, the data collection is carried out in the Ministry of Human Resources and Social Development which, as its name implies, consists of two divisions, known as the Human Resources Sector and the Social Development Sector. However, although each division has its own responsibilities, in the end these responsibilities and services are combined. For example, when a citizen requests a service, whether that is related to finding a job, understanding their labour rights, access to a support programme for their family, or any or all of these,

s/he would simply go to one of the forward-facing employees, who would then guide the citizen and perform all of these tasks under one roof. Therefore, for the purposes of the present research the data collected from these two divisions is combined and analysed together. The only time a distinction is made between these two sectors of MHRSD is for demographic description of the participants, so that along with their gender and nationality, the division of the ministry in which they are employed is also specified. Thus, according to Yin's (2009) definition this is a holistic single-case study.

Single case studies often have their limitations, most commonly with concerns to issues of methodological rigour, researchers' subjectivity and/or validity. Nevertheless, Saunders *et al.* (2015) assert that these weaknesses "*can potentially be offset by situating them within a broader, pluralistic mixed-method research strategy. Whether or not single case studies are used in this fashion, they clearly have a great deal to offer*" (p. 5). Moreover, Zainal (2007) notes that concerns regarding validity can be addressed "*by triangulating the study with other methods*" (p. 2).

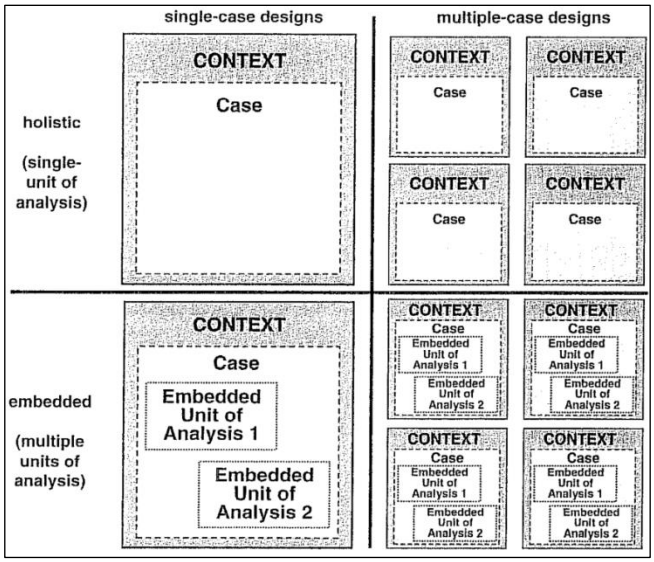


Figure 4-2 Basic Types of Designs for Case Studies (Yin, 2009, p. 46)

4.6 Unit of Analysis

In this holistic single-case study design, the case is the set of employees of the organisation (MHRSD) in either of its two divisions (the Human Resources Sector and the Social Development Sector). The unit of analysis is the subset of MHRSD employees who use CO-SNS. It is important to define the unit of analysis with reference to the *target population* and the *sampling frame* in the sampling procedure; these are discussed in Sections 4.7 and 4.8, respectively.

4.7 Target Population

The first stage in the sampling process involves targeting a population that suits the research objectives. Therefore, when identifying a target population, the researcher must have specific inclusion and exclusion criteria. Neuman (2014) defines a target population as "*The concretely specified large group of many cases from which a researcher draws a sample and to which results from the sample are generalized*" (p. 252). Accuracy in identifying the sample is a necessity so as to be able to draw appropriate conclusions from a sample that is relevant to the research question.

In order to identify an appropriate sample, one must consider the unit of analysis in the research. In this research, the unit of analysis is the subset of employees of MHRSD who use career-oriented SNS (see Section 4.6). Both males and females were targeted and included in the sample (see Chapter Five, Table 5-1). Anyone under 18 years of age would be excluded for ethical and legal reasons (see Section 4.13); however, it can be assumed that few, if any, employees in the specific Saudi public sector organisation under investigation would be below the age of 18.

4.8 Sampling Strategy

Identifying an appropriate sampling strategy is an important part of the research process. A sampling strategy generally involves identifying the target population (Section 4.7 above), the qualifying characteristics of that population relevant to the research problem, the sample size and the method of selection. Sampling strategies are of two main types: probability sampling and non-probability sampling (Neuman, 2014). Purposive sampling is a form of non-probability sampling which involves the selection of units of analysis that have specific reference to the research problem and questions (Bryman, 2012). In purposive sampling, the researcher employs various methods in an attempt "*to locate all possible cases of a highly specific and difficult-to-reach population*" (Neuman, 2014, p. 273). For this reason, and due also to time limitations and financial constraints, a purposive sampling technique was used in the current study. Figure 4-3 illustrates the strategy used in the current research.

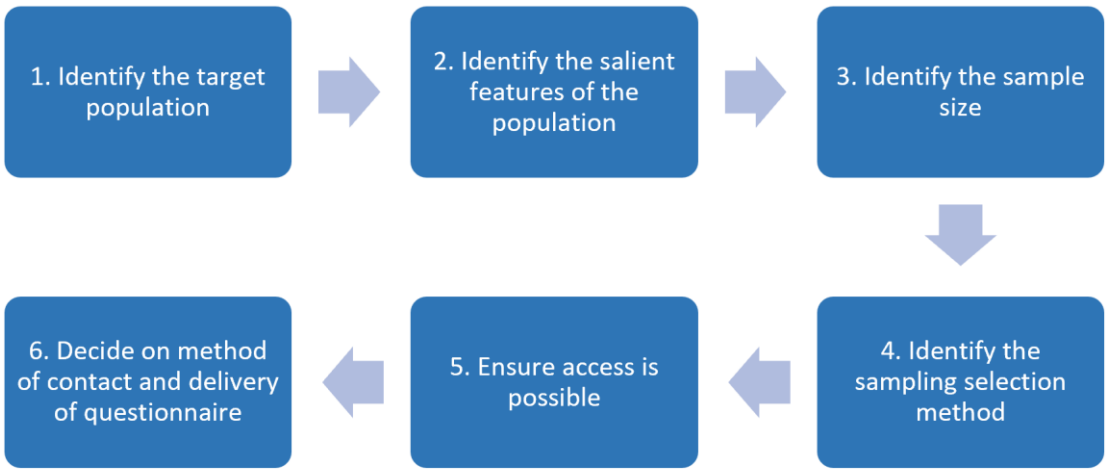


Figure 4-3 Sampling Strategy (adapted from Cohen et al., 2007, p. 117)

4.8.1 Sampling in a Case Study

As with other research designs, sampling issues are of concern in case study research. However, sampling in case study research has requirements specific to this type of design. With case study research designs, "*the researcher must first select the case or cases; subsequently, the researcher must sample units within the case*" (Bryman, 2012, p. 417). Yin (2009) points out that "*cases are not 'sampling units' and should not be chosen for this reason*" (p. 38). As Bryman (2012) notes, "*those individuals who are members of the case study context have to be sampled according to criteria too*" (p. 12). The organisation that is the context for this study is MHRSD. The strategy is based on purposeful sampling of those who use a professional SNS. This involves seeking out employees of this major government organisation who use LinkedIn. Data has been collected from employees at MHRSD, because it is an organisation which has access to data provided from the Saudi National Information Center (NIC). As explained in Chapter One, Section 1.7.2.1, the NIC is the main e-government network hub in the Kingdom of Saudi Arabia; the centre stores sensitive data of both citizens and expatriates, which portrays the magnitude of the organisation's sensitivity in terms of state security.

4.8.2 Sampling Frame

The sampling frame is a list of all those within a population who can be sampled. That list should be "*empirically concrete*", "*specific*" and "*closely approximate all population elements*" (Neuman, 2014, p. 252). The sampling frame delineates the individuals who are to be the sample of the target population: those who are eligible and meet the inclusion

employees of MHRSD to whom the researcher was granted access by the ministry, and who use CSNS.

4.8.3 Ministry of Human Resources and Social Development

The size of the workforce employed directly by MHRSD is not mentioned on the organisation's official website, and despite repeated attempts by the researcher, no administrator or representative of the Ministry would provide that information – not even a rough an estimate. However, according to the organisation's official profile page on LinkedIn, the size of MHRSD is in the range of 5,000 to 10,000 employees (LinkedIn.com, 2020, MHRSD Overview). Unfortunately, and somewhat ironically, LinkedIn has proved to be the only possible source to obtain this information.

It is relevant to note that, according to that same LinkedIn page, the number of MHRSD employees who are "on LinkedIn" – that is, who have active, publicly accessible LinkedIn accounts – was around 700 in October 2019. Interestingly, by the end of September 2020 that number had doubled to over 1400, and by March 2021 there were more than 2200 MHRSD employees on LinkedIn (MHRSD LinkedIn profile page, see Figure 4-4). However, despite the marked increase, this figure may be an underrepresentation of the actual number of MHRSD employees who have LinkedIn accounts. This is because many Saudi LinkedIn users tend to type their company affiliation in manually, whether in English or in Arabic, instead of selecting the pre-stored LinkedIn groups and pages of their organisation; as a result, they may not be included in LinkedIn's automated tally of employees of that company regardless of the actual number, the fact that the number of MHRSD employees who have active LinkedIn accounts is rising is important, because employees are the "*weakest link*" in an organisation's information security and are "*the root cause of information security breaches*" (Chu and So, 2020, p. 1). Thus, it can be argued that the greater the number of users, the greater the chances for a CSE attack to be perpetrated on the organisation.

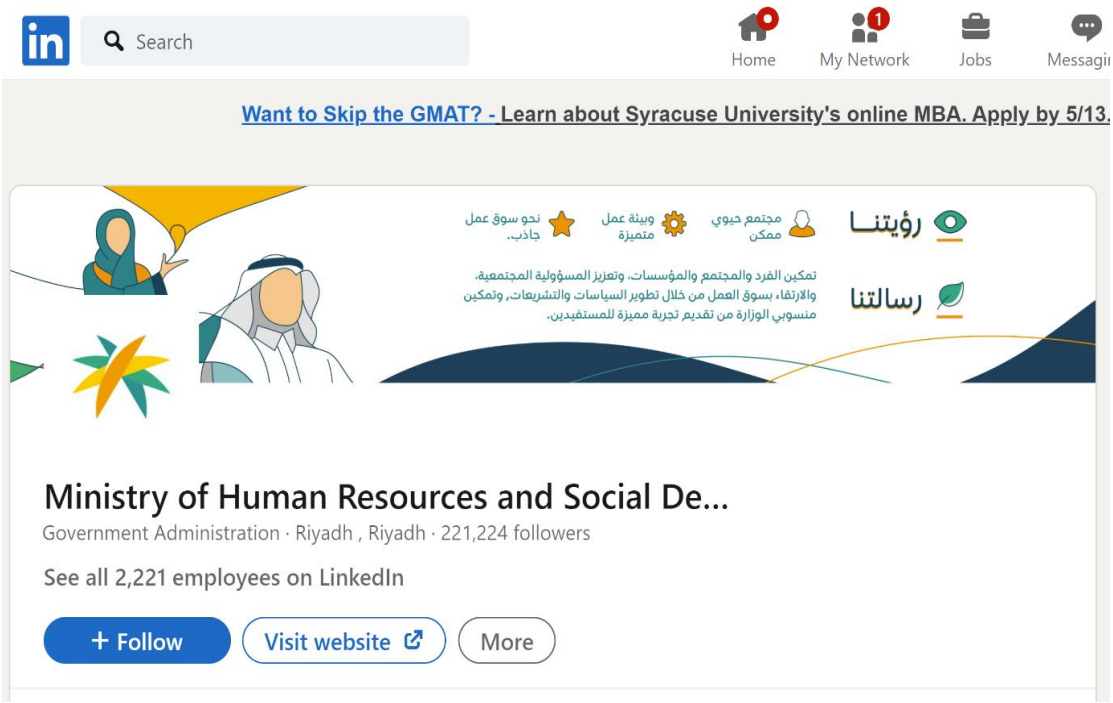


Figure 4-4 Ministry of Human Resources and Social Development's LinkedIn Page, 24 Mar 2021

4.8.4 Sample Size

Neuman (2014) argued that "*the size of a sample is less important than how accurately it represents the population*" (p. 253). Nevertheless, determining the size of the sample necessary for the research is a crucial step in the overall sampling strategy, particularly since an inappropriate sample size can result in data that is of poor quality and inadmissible in terms of achieving the stated research objectives. Bryman (2012) notes that using small sample sizes might prevent researchers being able to carry out important statistical tests and establishing certain relationships among the proposed variables. Saunders *et al.* (2015) comment that sample size is governed by: the degree of accuracy necessary, including the level of certainty that data characteristics are representative of the target population and the margin of error which is tolerable in statistical analyses; the chosen statistical techniques to be utilised in analysing the data; the size of the target population; and, to a lesser extent, any time restrictions that may apply to the research. Therefore, Saunders *et al.* (2015) argued, it could be said that sample size is a matter of both researcher judgement and mathematical calculation. One way of determining sample size is to rely on researcher judgement based on the comprehensive investigations that are necessary when conducting research, as this results in the researcher's in-depth familiarity with the subject at hand

(Saunders *et al.*, 2015). Nonetheless, it is also asserted that defining sample size should be well justified and grounded in academic standards and/or previous theoretical propositions (Bryman, 2012). Hence, this study shall rely upon the precedent established by previous similar research.

Certain types of analyses tend to require minimum sample size numbers in order to generate data that is sufficient. This mixed-methods research design has both quantitative and qualitative components. In quantitative research, according to Cohen *et al.* (2007), a useful "*rule of thumb*" is at least 30 cases per variable in one's research model; however, they note, "*of course, the thirty cases for variable one could also be the same thirty as for variable two*" (p. 101). Chu and So (2020) followed this rule in their study of unethical IS behaviour by employees: they examined seven variables in their model and relied on a sample of 210 participants. The number of variables in the present proposed Model of Susceptibility to CSE Victimisation on LinkedIn is 18, including demographic variables and sub-constructs. Using the above-mentioned rule of thumb, this would require a minimum sample size of 540 for the survey questionnaire. This sample size was the target; however, impediments to data collection (see Section 4.10) imposed practical constraints on the number of surveys that could be distributed, so that the total delivered to respondents was 467, and the number of usable questionnaires was 394 (Table 4-1).

Sample size can be calculated via a number of different statistical analyses. However, the majority of these require the size of the target population in their formulae. Saridakis *et al.* (2016), on whose model this present research model is based, used purposive sampling, as does this study. Their target population was much larger than that of the current study, as they were investigating "*online social media users*" in general. "*Over 700 individuals*" responded to their survey, which resulted in 514 "*usable*" questionnaires (Saridakis *et al.*, 2016, p. 323). For his study on human factors in cybersecurity Hadlington (2017) drew a sample of 538 participants from what was ostensibly the population of adult employed Internet users in the United Kingdom (p. 6) – again, a much larger population than that of the present study.

The size of the target population in this research can only be estimated roughly (at between 5000 and 10,000 employees, as stated in Section 4.8.3). Assuming that 10,000 is the upper limit of the population of MHRSD employees and based on the precedent established by these previous similar studies, this researcher, while aiming for the optimal rule-of-thumb sample size of 540, recognised that it would be difficult to obtain this many willing and

available participants. The Ministry of Education provided this researcher with a letter of permission (Appendix B) to disseminate paper survey questionnaires and conduct the survey. This author made the rounds of the MHRSD offices in Riyadh and Jeddah, visiting each section in person to explain the research to employees and ask them if they would be willing to take the survey. They were invited to have a look at the first page to read and accept. No questionnaires were sent by email as the researcher did not have permission for this. The researcher followed this routine for 4 to 5 hours every weekday for three months, the aim was to distribute and receive completed questionnaires from as many willing participants as possible – optimally, 40 to 50 a week. To enlist female participants, the researcher was not permitted access to the women's sections of the organisation. Instead, he had to request a female employee to hand them the questionnaires, waiting while these were filled in. The organisation offered no assistance, other than managers providing contact details of those who were on leave or who otherwise could not be reached in person. In some cases, arrangements were made to meet with employees in conference rooms. Sometimes this researcher approached employees in the organisation's car park to ask them to complete the survey; some questionnaires were completed by filling it in on the hood of their cars.

Given the constraints above-mentioned, a more attainable and flexible range of 300 to 500 participants was proposed for this research project (see Appendix C). In the researcher's judgement, based on previous studies of a similar nature, a sample size in this range is sufficient to fulfil the research objectives.

4.9 Timescale

Cross-sectional designs involve collecting data at a single point in time. The present research employs a cross-sectional approach, which is preferred because it enables a large amount of data to be collected in a short space of time. Quantitative data collection was conducted between 7 October 2019 and 7 January 2020. Quantitative analysis was carried out between 25 February 2020 and 20 June 2020. This was interrupted twice: from 13 March to 1 April 2020 whilst the college was shut down due to the COVID-19 pandemic and again after this researcher's repatriation from Dublin to Riyadh, for three weeks' quarantine beginning 24 May 2020. Qualitative analysis was also cross-sectional; it was carried out from 10 November 2020 until 1 December 2020. However, the researcher

received permission from the interviewees to contact them at a later date (during the analysis phase) if any clarification was needed regarding their statements.

4.10 Study Constraints

"*All research is constrained by time and resources*" (Bryman, 2012, p. 82). Four types of constraints affected the conduct of this research: time, bureaucracy, financial cost and a pandemic. Three of these constraints were anticipated, the fourth was not. At times, these constraints often seemed to converge (see, e.g., Section 4.12.4). Rules and regulations governing research by Saudi students stipulate that official approval should be obtained from the Ministry of Education, which finances this research and oversees the nature of the study. Furthermore, one of the rules was that the maximum duration allowed to a PhD candidate for data collection outside Ireland was three months.

As Bryman (2012) explains, "*Access is usually mediated by gatekeepers, who are concerned about the researcher's motives: what the organization can gain from the investigation, what it will lose by participating in the research in terms of staff time and other costs, and potential risks to its image*" (p. 151). Following the approval by the School of Computer Science and Statistics, TCD Research Ethics Committee (REC) to conduct data collection, it took over five months to obtain official approval from MHRSD, and only one out of seven attempts to gain data collection permission was successful (see Section 4.11.1).

Due to the country's customs and conservative Islamic culture, strict segregation is maintained between males and females in the workplace, and MHRSD is no exception. This male researcher was not allowed to contact any female employees directly. This was a predicament faced in the early stages of data collection, but after suitable arrangements were made, permission was granted to have women participate (see Section 4.11.1).

For the present study, the financial costs were not burdensome. These included printing 550 copies of the questionnaire (although the Ministry assisted by printing most of the questionnaires and absorbing the cost), and transport to and from the two sites where the survey was distributed, namely the MHRSD head office in Riyadh and its branch in Jeddah.

The constraint that has had the greatest impact on this study has been the COVID-19 pandemic. This event disrupted the timely execution of the qualitative phase of the research, for which the semi-structured interviews were planned to be conducted face to face in Saudi Arabia. Due to international travel restrictions and local lockdowns (including

TCD being shut down from mid-March until August 2020), the researcher was unable to travel from Dublin to Riyadh in June 2020 as planned. Instead, a repatriation flight was arranged via the Saudi Ministry of Foreign Affairs. In the end, the interviews were conducted via videoconferencing and telephone, as per TCD's new Corona Guidelines 2020 for conducting research during the pandemic. As a result of these disruptions and changes, the time frame for completion of the qualitative phase had to be extended.

4.11 Data Collection: Survey Questionnaire (Quantitative)

As explained in Section 4.3.3, in the sequential explanatory design used in this study the quantitative data is collected first, so that it may be analysed statistically; this analysis produces some findings and perhaps additional questions. The sample is drawn from the sampling frame. The quantitative survey instrument, a questionnaire, is designed. Prior to administration, the survey questionnaire is tested via the use of a pilot study. The quantitative data collection process is detailed in the following subsections.

4.11.1 Sample Selection (Participants)

As discussed in Section 4.8.4, the targeted sample size of 540 for the survey corresponds to previous studies in similar subject areas to this one that carried out data collection within a short time frame (see Appendix C). An invitation letter was sent to directors of IT and/or research departments in seven different ministries of the Saudi government to ask permission for employees to participate in this study; only one ministry granted permission: MHRSD. More than 540 employees were approached (see description of this process in Section 4.8.4), of which 467 agreed to participate. Time slots were arranged for these employees to meet either individually or in groups in the organisation's conference halls to participate in answering the paper-based questionnaire.

As mentioned in Section 4.10, special arrangements had to be made for female participants. After being notified of the study by MHRSD's IT department, any women who were willing to participate could do so if they were accompanied by female security personnel. Those security personnel would take the place of the researcher in administering the survey, and they were instructed as to how to guide female participants through completing the questionnaire. In case of queries, the security personnel could contact the researcher.

4.11.2 Survey Design

The collection of data for this research was undertaken in Saudi Arabia and focussed on professionals who use LinkedIn. The susceptibility of these employees to CSE attacks is being examined based on the proposed Model of Susceptibility to CSE Victimisation on LinkedIn (Figure 3-7). The variables of interest are summarised here:

1) Personality traits (openness, conscientiousness, extraversion, agreeableness, neuroticism)
2) Employees' demographics (age, gender, structural power, nationality)
3) Personal disposition/attitude to susceptibility/risk on LinkedIn, specifically:
    a. willingness to take risks
    b. risk perception
    c. level of engagement on LinkedIn
    d. IT (digital or computer) self-efficacy: confidence level with operating information technologies
    e. perceived control over information (privacy risk)
    f. self-presentation and professional advancement

In line with the positivist approach of the quantitative phase of this study, the survey consisted mostly of close ended questions, in which a fixed set of answers was possible for each. Data from responses to close ended questions are easier to compare, code, and analyse (Bryman, 2012; Neuman, 2014). Where possible existing empirically tested scales are used. Many of these scales were measured using Likert scales. The advantages and limitations of Likert scales are discussed in Section 4.14.1.

The questionnaire consisted of 98 questions (Appendix D). The first two questions were about respondents' use of SNS and CSNS; these questions allowed the researcher to double-check that participants fit the criteria for inclusion in the study sample. Questions 3 – 7 elicited responses regarding the demographic variables. The overall breakdown of the focus of the questions is presented in Table 4-1.

Table 4-1 Questionnaire Structure

Items	Constructs Being Measured
1 & 2	Use of SNS and CSNS
3 to 7	Demographics and contextual factors
8 to 27	Personality traits
28 to 47	Risky habitual behaviour – Information security (Hadlington [2017] Risky cybersecurity behaviour scale)
48 to 52	Risky habitual behaviour – Level of engagement & Frequency of use
53	Risky habitual behaviour – Frequency of LinkedIn usage at work
54 to 57	Risk perception
58 to 61	Willingness to assume risk on LinkedIn
62 to 69	Perceived control of information – Privacy risk
70 to 82	Susceptibility to CSE victimisation on LinkedIn - Self-presentation
84 to 92	Susceptibility to CSE victimisation on LinkedIn - Professional advancement
93 to 95	CSE awareness (contextual factors)
96 & 97	Victim of CSE attack

4.11.3 Translation of Questionnaire

It is important to ensure a valid method is used to translate the original version of the research instrument, making sure the content of the translation is equivalent to the original language. In this study, the target population within the public organisation spoke Arabic and English, Arabic being the official language in Saudi Arabia, followed by English. The survey translation underwent a translation guided by Brislin's (1970) back-translation method to ensure the accuracy of the final version. This method encompasses three steps:

1) A certified translation firm translated the questionnaire from English to Arabic.
2) A different certified translation firm conducted a reverse translation of the already translated questionnaire, from Arabic back into English, its source language.
3) Lastly, two bilingual assistant professors from a Saudi university performed a comparative review of the two versions, for assurance of validity and to avoid any alterations impacting the meaning of survey items. This process was carried out in consultation with the researcher in cases where clarification was needed regarding the cybersecurity items addressed in the survey.

As a result of the foregoing process, a few phrases of the Arabic version had to either be elaborated upon or amended to ensure the correct meaning. After the pilot study, a few additional items were highlighted and reviewed with another expert to ensure accuracy (see Table 4-2).

4.11.4 Piloting and Testing of Questionnaire

Bryman (2012) defines a pilot study as a trial phase prior to the actual data collection, targeting a smaller number of participants. Neuman (2014) highlights the importance of conducting such a small-scale trial run to identify any cognitive or technical issues that may arise which require amendments to the designed questionnaire, its wording or sequence. In addition, a pilot study provides for assessments of the validity and reliability of the data being collected (Saunders *et al.*, 2015). With reference to piloting sampling, according to Connelly (2008), the extant literature proposes sampling for a pilot study should be 10% of the projected sample for the larger parent study. As mentioned in Section 4.8.4, the targeted optimal sample size for this study was determined to be 540; hence, 10% of the maximum total amounts to 54 participants.

A group of government employees, academics and doctoral researchers (male and females, Saudi nationals and expatriates) totalling 51 participants were purposefully selected for a pilot study administered over Google Hangouts[7]. An expert in the field of IS strongly recommended conducting a cognitive evaluation or testing of survey questions to ensure that the questionnaire captured the scientific intent of each item and most importantly that it made sense to respondents and to identify places of ambiguity, if any (Neuman, 2014). Indeed, such an assessment was carried out as part of the pilot study. This cognitive testing ensured that the survey items were clear and understandable to respondents. Any identified weaknesses or ambiguities in the items were then rectified (see Table 4-2).

The pilot survey was conducted over eight weeks, from 12 June to 7 August 2019. The draft survey was submitted on 8 May 2019 to the REC Required amendments were submitted by 12 June 2019, and ethical approval was received on 8 August 2019. The researcher conducted the pilot study until approval was received. While waiting for any of the Saudi public sector organisations contacted to agree to participate in the study, this author could only approach participants online for piloting. Moreover, the researcher would

[7] Google+ Hangouts is a one-to-one or group communication that enables a conference meeting (Hangouts, 2019).

not be able to initiate data collection until approval was received from the Saudi Cultural Attaché to leave Ireland. These overlapping processes took five months.

Notes were taken to record any questions or concerns voiced by participants, and to observe how they reacted to the questions. Suggestions and feedback were recorded and once again presented to experts in comparative linguistics, as well as to experts in the Arabic language, to ensure that the Arabic version of the survey conveyed exactly the same meaning as the adopted English instruments. During the pilot study, a few items required minor alterations, such as splitting long sentences. In both language versions, a few of the items had to be rephrased and simplified to match the intended meaning of the item being addressed. The topic and/or wording of some of these items were perceived as unacceptable or raised a flag amongst participants. This was highlighted with the personality characteristics scale, given the nature of the sensitivity of some of the questions, such as being "*fascinated with the theory of evolution*". A few of the items that were modified are listed in Table 4-2, as examples. The full list of modified items is found in Appendix E.

Table 4-2 Items Changed in Questionnaire, Retaining Intended Meaning.

Variable	Statement	Changed to	Rationale
Openness (Personality traits) Item 18	I have thought a lot about the origins of the universe.	I thought about how the universe, and life on earth, was first created.	Acceptability for participants (Arabic version)
Openness (Personality traits) Item 19	I am fascinated with the theory of evolution.	I am fascinated about what others have to say about how life on earth was created, including the theory of evolution.	Acceptability for participants (Arabic version)
Extroversion (Personality traits) Item 24	I would enjoy being a theoretical scientist.	I would like to work on developing new scientific theories.	Clarity for participants (both language versions)
Susceptibility to CSE (binary dependent variable)	Have you ever encountered a situation over professional social networking site that compelled you to provide personal information or money when later you found you were a victim of a scam?	In all the time since you have been using LinkedIn, have you ever had something bad happen (at your work or in your personal life) to you that you can trace back to your usage of LinkedIn?	Clarity for participants (recommended by experts – both language versions). For Arabic version, after the phrase meaning "something bad", the phrase: "(i.e., deception through phishing and fake recruitment)" was added .

Prior to administering the survey and after the piloting process, further evaluation was undertaken of the overall content. Four expert reviews of the survey were carried out, involving two researchers in Computer Science from the School of Computer Science and Statistics, Trinity College Dublin; an academic expert in the field of Industrial and Organisational Psychology, University of South Africa (UNISA); and an expert in the field of Human Factors Psychology from Embry-Riddle Aeronautical University in Daytona Beach, Florida, USA. All assisted in providing feedback and suggestions (see Appendix F) to improve the questionnaire design as a whole. The experts also provided feedback on the issue of how to determine the susceptibility of an individual using a self-reported response to an indirect question, which is a crucial concern of this study.

The expert reviewers advised the replacement of "Daily" with "Always" in the (1 = Never/7 = Daily) 7-point scale in the variable "Risky habitual behaviour: information security habitual behaviour and level of engagement", on the grounds that the items "shared your password with a friend or a colleague", "used or created a password that is only based on your family name or date of birth", "downloaded free anti-virus software from an unknown

source", "shared your current location on social media", "talked about private company information on any of your social media sites", and the like cannot realistically be considered as actions that are performed on a daily basis. A better word would be "always", as something done routinely and repetitively, but not every single day. This change removes any confusion that could face participants when answering these items in the survey.

One scale which experts suggested should be replaced was the 10-item personality trait psychometric; it was considered to be too short and consequently was replaced by a 20-item scale. Additional feedback suggested eliminating certain items, as well as generating others In accordance with the feedback, cognitive testing was carried out as part of the pilot study described above.

4.11.5 Administration of Questionnaire

When deciding on the method of administering the survey for the quantitative phase, the advantages and disadvantages of paper-based versus web-based questionnaires were considered. Web-based surveys are less expensive and easier to administer (Bryman, 2012; Hohwü *et al.*, 2013), but paper-based surveys generally have higher response rates (Cohen *et al.*, 2008), substantially so if administered on site (in person) rather than via postal mail (Kongsved *et al.*, 2007; Hohwü *et al.*, 2013). When questionnaires are administered in person, the administrator (usually, the researcher) is able to oversee the process and explain the procedure to participants; this encourages completion of the questionnaire by respondents and minimises the temptation for them to randomly select items (Christmas treeing; Cohen *et al.*, 2007). The main disadvantage to in-person administration is the artifact threat of experimenter expectancy, which means that the researcher's expectations about the results of their research are inadvertently conveyed to participants and influence their responses (Cohen *et al.*, 2007). After weighing the advantages and disadvantages, the researcher determined that paper-based questionnaires were more suitable for this study.

Prior to the overall process, a detailed meeting schedule had been requested, uploaded and approved by the Ministry of Education as a third-party facilitator between the researcher and MHRSD, since it oversees the research process. Administering the questionnaires ran from 7 October 2019 until 7 January 2020.On the first day (and any other days during that period if requested), the researcher presented the official letter of approval from MHRSD and the Ministry of Education. On the last day of the survey administration period, the

researcher presented the closure letter indicating that this data collection process had ended (Appendix G). Upon approval from the appropriate authorities, participant information leaflets and consent forms (Appendixes C3, C5 & C1), along with the paper-based questionnaires were distributed in either of two language versions (English or Arabic), accompanied by machine-readable answer sheets (for Scantron software[8]), to targeted individual employees in selected affiliated MHRSD offices. As described in Section 4.11.3, these surveys had been prepared in English and translated into Arabic, undergoing linguistic scrutiny in order to avoid mistakes in meaning.

Response Rate

Data collection started in Saudi Arabia on 7 October 2019. The Ministry of Education gave this researcher a maximum time frame of three months in which to complete this process. Paper survey questionnaires were distributed in person to 467 employees in the MHRSD, in the head office in Riyadh and a branch office in Jeddah. Collection of the data ended on 7 January 2020, and thus took exactly three months. Table 4-3 summarises the number of questionnaires distributed and received back.

Table 4-3 Survey Administration

Delivered questionnaires	Returns	Response rate (%)
467	402 (394 usable)	84.37%

As shown in Table 4-3, the number of completed questionnaires was 402 (of which 394 were usable) out of 467 delivered; thus, the response rate is over 84%, which is considered a "*very good*" rate of response (Bryman, 2012, p. 235). The relevance of the questionnaire to the participants was clearly indicated in the instructions and inside the questionnaire itself.

[8] Scantron software converts paper tests and survey responses into machine readable data: https://www.scantron.com/scanners-forms/remark-classic-omr-software/

4.12 Data Collection: Semi-Structured Interviews (Qualitative)

In a sequential explanatory design, answers to new questions that arise from the data gathered in the quantitative phase are sought in the qualitative second phase of data collection: in this case, via semi-structured interviews. The structure and advantages of semi-structured interviews were discussed in Section 4.4.2. The sample for the interviews is drawn, not from the sampling frame, but from industry experts and academics. Two interviewees were from the sample of participants who took part in the survey. The qualitative instrument, a semi-structured interview, is designed. As with the questionnaire, prior to administration the qualitative instrument (the interview) is "calibrated" via the use of a pilot study. This process is described in the following subsections.

4.12.1 Sample Selection (Participants)

The targeted interviewees for this study were academics, IT/cybersecurity experts and employees of MHRSD. The researcher contacted potential participants via university website faculty pages, and via LinkedIn and Twitter, by searching using keywords in both Arabic and English. Keywords included *cybersecurity, cyber psychology, computer science PhD, IT expert* and the like. The research also reached out to a number of frequently hosted speakers on these subjects who also post awareness and educational infographics and tweets about computer science topics and who have profiles in the mentioned platforms.

In total, 15 individuals participated in the interview: 7 female and 8 males. This number is within the "*organization and workplace research norm of 15−60 participants*" for interview samples, according to Saunders and Townsend (2016, p. 836). Two of the male participants were non-Saudi nationals (expatriates working and residing in Saudi Arabia); all other participants were Saudi citizens. Only two participants (a female HR specialist and a male IT centre manager) were from the actual sample of MHRSD employees who had taken part in the survey. As a condition for its approval of the survey being administered to its employees, the organisation required that the section requesting contact details of survey participants be removed. The researcher searched for MHRSD employees on LinkedIn and requested them to participate in the interview. These were the only two who had responded that they were willing to participate. The other 13 participants were industry experts/professionals and/or academics in IT, cybersecurity, psychology, sociology and related fields.

4.12.2 Interview Design

As with the quantitative data, the collection of qualitative data for this research was undertaken in Saudi Arabia and focussed on professionals who use LinkedIn. In drafting the interview questions, this researcher drew on the quantitative findings, especially any findings that were unexpected or not easily explained. The proposed interview script was submitted as part of the ethics review application (Appendix H). A draft of the interview script was sent to an expert in industrial and organisational psychology. Upon his recommendation, questions were reworded slightly, and the order rearranged, in order to minimise ambiguity, improve flow and increase relevance for the participant.

As mentioned in Section 4.4.2, in a semi-structured interview, the interviewer is free to vary the order of the questions and may even pose additional questions as a follow-up to responses that are deemed significant. The content of the interview consisted of 40 questions designed to elicit data that corresponds to each of the 18 variables of the study model, summarised here:

1) Personality traits (openness, conscientiousness, extraversion, agreeableness, neuroticism)
2) Employees' demographics (age, gender, structural power, nationality)
3) Personal disposition/attitude to susceptibility/risk on LinkedIn, specifically:
    a. willingness to take risks
    b. risk perception
    c. level of engagement on LinkedIn
    d. IT (digital or computer) self-efficacy: confidence level with operating information technologies
    e. perceived control over information (privacy risk)
    f. self-presentation and professional advancement

The interview questions (Appendix H) were presented roughly in the same order as the research hypotheses (see Chapter 3).

4.12.3 Translation of Semi-Structured Interview

The translation process for the interview script differed from that of the survey questionnaire. As most of the interview questions were based on the items in the survey, and the latter had undergone the rigorous back-translation process (see Section 4.11.3), The

researcher relied on the lexical/semantic elements in the English and Arabic versions of the questionnaire in preparing the English and Arabic versions of the interview questions. A bilingual assistant professor from a Saudi university reviewed and compared the two versions, for assurance of validity and to avoid any discrepancies in meaning, ensuring that the Arabic translation accurately reflected the English meaning. The linguist made a few minor corrections to the Arabic text, and there was no back-translation done. As the researcher would be present at the interviews, the researcher could clarify any misunderstandings.

4.12.4 Pilot Study for Semi-Structured Interview

As with survey questionnaires, semi-structured interviews (explained in Section 4.4.2) also benefit from being tested via piloting. The semi-structured interview was piloted by conducting the interview using the exact same questions in length and content as the study interview, with five participants. For this purpose, a convenience sample was deemed practical and suitable. Participants were acquaintances of the researcher and were not selected from the target population of MHRSD employees, nor were they selected for their occupational speciality or position such as IT/cybersecurity experts.

Initially, REC approval had been obtained to conduct the interviews face to face. However, just as the interviewing phase began, the COVID-19 pandemic struck, and due to travel restrictions, lockdowns and associated precautionary measures, the researcher had to change the proposed interview method. As per the Corona Guidelines 2020, the ethics approval had to be re-submitted to request to conduct all interviews online and/or via telephone. Hence, only the first three pilot interviews were carried out in person (face to face), whereas the last two were conducted via telephone. The participant information leaflet and consent form were provided to the three in-person interviewees; these documents were read out loud to the other two participants and sent to them for signature via email.

The pilot interviews were conducted on 27 August 2020. The five participants in the pilot study included four university graduates and one with a high school diploma. Two females and three males participated; all were in their late 20s and early 30s. The interviewer (this researcher) read the questions aloud in Arabic. Two of the participants responded to the questions in English, because although they were native speakers of Arabic, they felt more comfortable expressing themselves in English. As a result of this test run, and with the

previous recommendations of the expert reviewer (Section 4.12.2) in mind, a few minor revisions were made to the order and wording of the final interview questions. In addition, a number of questions were added based on the findings (see Appendix I). The pilot interviews were also an opportunity for the researcher to test the software and device (voice recording app on a smartphone) used in recording the interviews.

4.12.5 Administration of Interviews

Due to COVID-19, the ethics application had to be resubmitted to seek approval for conducting the interviews online and/or via telephone instead of face to face (see Appendix C, p. 7). After approval was granted, the participants were contacted individually to set up suitable times for the interviews. Seven female and 8 male participants were interviewed via Skype, Google Hangouts, Zoom or over the phone. All the participants were provided with participant information leaflets and consent forms to sign (Appendix C4, C6 & C2), prior to digitally recording the interviews. Some of these were distributed via their preferred messaging app such as Twitter or LinkedIn. The forms were emailed to the participants who were in academia. All participants agreed to permit the interview to be audio recorded. At the beginning of each interview, participants were provided with a brief summary of the topic being investigated and the approximate expected length of the interview. The researcher conducted the interviews in English and/or Arabic and took notes in Arabic and English as appropriate. In addition to interviewee responses, these notes included relevant demographic details such as age, gender, job title/position, place of work, as well as contact information should any follow-up be required. The open-ended structure and content of the interview questions allowed participants to describe their knowledge of and experiences, if any, with CSE attacks, and to express their views on the factors related to susceptibility to CSE.

4.13 Ethical Considerations

Given the requirement for strict observance of cultural and religious values in Saudi Arabia, the researcher conformed to certain modes of behaviour and socio-political concerns. Indeed, there was a concern that some of these sociocultural norms might incline participants to refrain from freely expressing their point of view, whether during the survey or the recorded session in the interview phase. Most of these concerns revolved around privacy and ensuring compliance with strict requests by MHRSD. For example, MHRSD requested removal of respondents' contact details from the survey, which had been elicited

in cases where participants were willing to be contacted for a follow-up interview (the qualitative phase of this research).

Bryman (2012) highlights that a researcher should guarantee the rights, privacy and welfare of participants in the study. To ensure that this research is compliant with the principles of ethical research, an application for approval of ethical research was submitted to Trinity College Dublin (TCD) and handled by the REC through the School of Computer Science and Statistics. This application was approved. The ethical application considered seven fundamentals to guarantee appropriateness with regard to collection of data in an ethical and legal manner; these fundamentals are as follows:

Access and acceptance: Obtaining approval and access from a suitable organisation (e.g., Ministry of Human Resources and Social Development – MHRSD) with employees engaged in career-oriented social networking sites, to collect data from and about the targeted sample of the study. This was acquired before conducting data collection, on the condition that a copy of the completed thesis would be provided to the organisation.

Informed consent: Ensuring correct content and format of informed consent of Saudi and expatriate employees within the ethical and voluntary boundaries to accept or reject participation (Cohen *et al.*, 2007). Each participant was given an informed consent sheet to be read and signed prior to starting the questionnaires and interviews.

Anonymity of participating employees: Completed answers by participants were given full anonymity, unless they were willing to participate in the semi-structured interview phase, in which case they gave only their email address as a means of contact. However, as mentioned earlier, at the end of data collection MHRSD requested removal of that survey section, but was willing to provide means of contacting volunteers for a follow-up interview (qualitative phase) after the quantitative analysis.

Obviating harm: Data collection should be handled with respect to the participant during the process with minimum harm "beneficence & the absence of maleficence (research should have the maximum benefit with minimal harm)" *(*p. 4) as per the TCD Policy on Good Research Practice/Article 2.2. This principle was observed by ensuring that data collected from participants should not be used in any way that might affect their careers, positions or relations between them and their colleagues.

Confidentiality and General Data Protection Regulation (GDPR): Data was collected in Saudi Arabia, but the analysis was planned to be carried out within the boundaries of the

European Union (EU); therefore, the data collected has to comply with the GDPR. Data was encrypted and stored in a secure password-protected cloud device which would remain offline at all times until names and organisations were replaced with distinctive code to ensure anonymity. Data was only kept for the duration of the study.

Ethical approval was requested and granted by the Research Ethics Committee of the Computer Science and Statistics Department, Trinity College Dublin. Appendix C includes relevant documents pertaining to research ethics guidelines following the first round of reviews by the committee. It also describes how the study of personal characteristics and other factors influencing susceptibility CSE on CSNS is addressed. Another consideration that was addressed was the request by LinkedIn to refrain from launching any type of CSE tactics as an experiment on targeted participants; consequently, a case study based on experiments to assess user susceptibility was withdrawn from consideration in this study (see Figure 4-5).

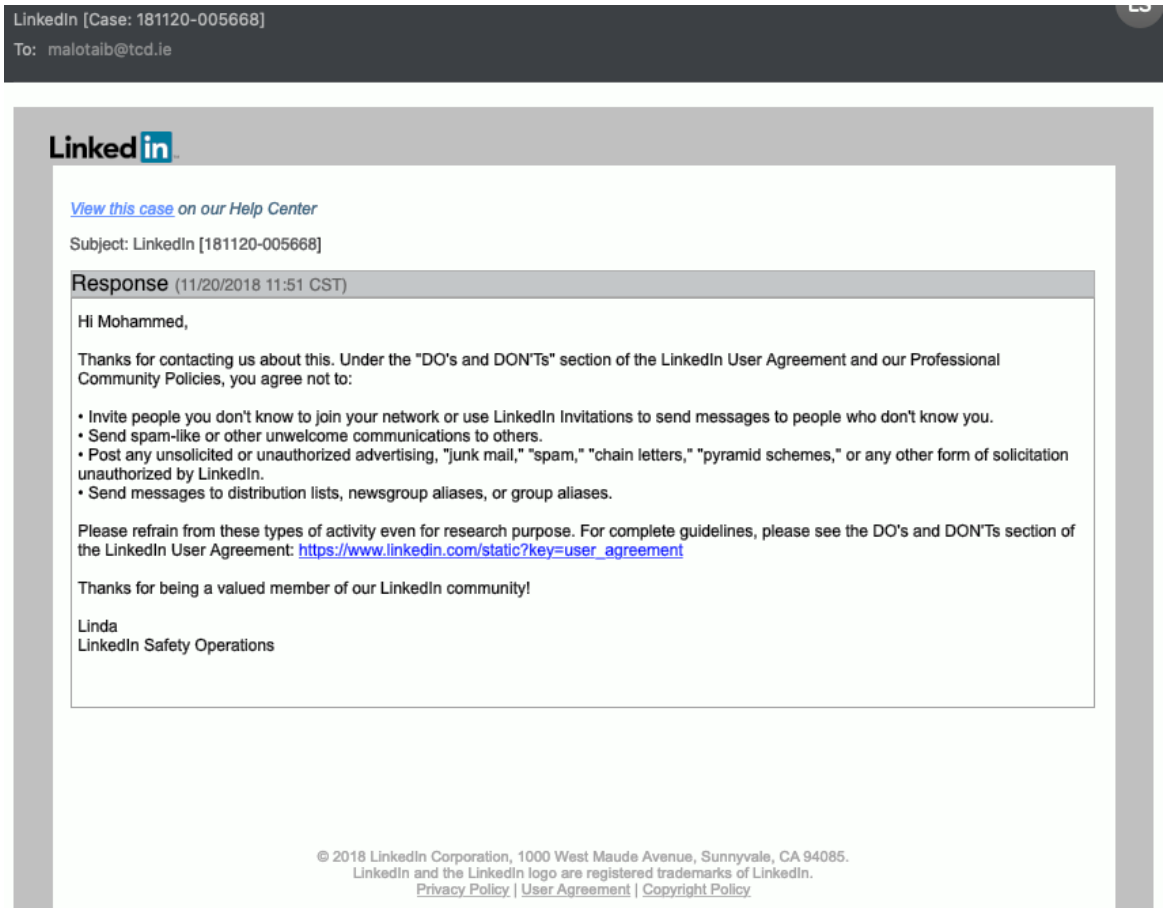


Figure 4-5 Official email from LinkedIn denying permission to launch vulnerability experiments

4.14 Scaling

A ranking or rating scale is a measurement instrument for quantitative data; often used in survey research, it "*captures the intensity, direction, level, or potency of a variable construct along a continuum*" (Neuman, 2014, p. 230). Self-report scales typically ask the respondent to either rank or rate the presented responses in association with the question asked. Likert scales, a version of which is employed in the questionnaire for this study, were developed by Rensis Likert (1932; Neuman, 2014) and are commonly employed in survey-based research in the social sciences (Cohen *et al.*, 2007; Bryman, 2012). A Likert scale consists of a single dimension with the semantic indicators at two ends of the scale being polar opposites (e.g., "hot" and "cold"). Respondents are presented with a statement and instructed to indicate on the ordered numerical or categorical scale the extent to which they agree or disagree with that proposition (Neuman, 2014). Cohen *et al.* (2007) note that "*the assumption of unidimensionality*", meaning that the scale should measure "*only one thing at a time*" is a key strength of Likert scales (p. 326; emphasis in original).

There are a couple of options to consider regarding the number of points to use in a Likert scale. The first is to decide whether to include a mid-point, that is, exactly halfway between the two diametrically opposed ends of the scale. This would allow for a neutral response (e.g., "neither agree nor disagree"). This would be achieved via an odd-numbered scale such as five, seven or nine points. Cohen *et al.* (2007) note that a scale without a mid-point (i.e., with an even number of points) would eliminate central tendency bias, in which participants habitually select the neutral option (p. 327), thus forcing the respondent to choose a side, so to speak. After deciding on an even or odd number of points, the next consideration is how many points to include. The most commonly used are 5-point and 7-point scales (Cohen *et al.*, 2007). The reliability of the scale increases with the number of points up to seven, after which there is very little increase in reliability (Neuman, 2014, p. 232).

4.15 Constructs and their measurement instruments

The survey has used previously validated survey instruments where possible. The construct measurements used in the survey are presented below, in the order of the hypotheses to which they correspond. This is followed by tables with the items and Likert scale used (strongly agree – strongly disagree) and (Yes/No).

4.15.1 Dependent Variable: Susceptibility to CSE on LinkedIn

To measure users' susceptibility to CSE attacks (e.g., phishing links), most previous studies have deployed real attack scenarios (Vishwanath *et al.* 2016; van de Weijer and Leukfeldt, 2017; Albladi and Weir, 2017). As explained in Sections 4.5 and 4.14, the researcher originally had planned to conduct such an experiment, but had to abandon this plan after being informed by a LinkedIn Safety Operations team member that the platform explicitly prohibits such tactics, even for research purposes (Figure 4-5 in Section 4.13). Saridakis *et al.* (2016) measured susceptibility to CSE on SNS by conducting a survey, they asked participants directly if they had been at risk of SNS victimisation (see Chapter Three, Section 3.3.4); they did not conduct any experiments in conjunction with their survey.

Other research has involved observation and analysis of users' behaviour in their SNS profiles and timelines (Algarni *et al.*, 2014). A cognitive reflection test (CRT; Kumaraguru *et al.*, 2010; Butavicius *et al.*, 2017) and susceptibility to persuasion test (Modic, Anderson and Palomäki, 2018) have been developed by the universities of Helsinki and Cambridge, respectively. The three questionnaires for CRT can only be executed in a lab, paired with experimental scenario sessions or showing images of emails and asking participants their likelihood to click or not on a link. CRT, however, originally was intended to test people's ability to make a decision either rationally or intuitively by solving three sets of mathematical problems, after which the researcher would determine in a comparison if there had been any relationship between their impulsiveness score and their judgement responses in the experimental lab session. Parsons *et al.* (2013) and Parsons *et al.* (2016) found that low scores in CRT indicate high susceptibility to attacks, based on their judgements in phishing experiment sessions, whereas Kumaraguru *et al.* (2010) found the reverse; that high CRT scores in impulsiveness indicate high susceptibility by making wrong judgements.

To test employees' proneness to CSE in the workplace, Mitnick and Simon (2001) suggest using a security awareness assessment. Since this study is designed to be carried out in the workplace, IT security management begins with users' IS security awareness (Armstrong *et al.*, 2018). One can surmise that the higher the scores obtained by employees' practices in terms of information security and awareness, the less susceptible they are, as found in a study by Schaeken (2018). The Human Aspects of Information Security Questionnaire (HAIS-Q) by Parsons *et al.* (2017), which is validated in studies such as Butavicius *et al.*

(2016) and McCormac *et al.* (2017a) can be used to assess employees' level of IT security awareness. It has been used frequently in studies of data breaches through phishing, where low scores indicate vulnerability. Based on Butavicius *et al.* (2017), de Vries (2017) highlights that the "*HAIS-Q method notes cybersecurity is constantly evolving, which means it is possible the model has to be revised due to new emerging threats and technological improvements*" (p. 34). Also, Parsons *et al.* (2017) found that "*participants who had higher scores on the HAIS-Q also had better phishing performance*"(p. 43), meaning that they were better able to resist such attacks.

However, HAIS-Q does not entirely cover the element of influence and deception. Other studies have used a survey paired with a phishing email experiment (scored as 1 if they clicked on the link, 0 if they did not; Moody *et al.*, 2017). Alseadoon *et al.* (2013), investigating the factors related to detecting deception, measured susceptibility by asking participants to scale their likelihood of responding to five phishing emails, without knowing that they were all phishing emails. They used a 7-point Likert scale, where 1 indicated "definitely will ignore" and 7, "definitely will respond".

In their investigation of users' susceptibility to CSE victimisation, Albladi and Weir (2020) employed an online survey that incorporated a scenario-based experiment. Participants reviewed a set of information in the form of text and images and were asked to react to the information. Each of the six images of Facebook posts represented a different genre of cyber-attack commonly found on SNS (p. 6). Participants were asked to suppose that they had encountered each post on Facebook, and on a 5-point Likert scale, to indicate their level of agreement or disagreement with statements like "I would click on this button to read the file" (p 7). Other studies in the literature have measured susceptibility by inviting users to click on spear-phishing links. As mentioned in Sections 4.5 and 4.14, this study has refrained from using experimental scenarios on SNS for ethical reasons. Aburrous *et al.* (2010) found that, in a study carried out on bankers' susceptibility to phishing, "*Some of the employees called the experiment unethical, inappropriate, illegal and unprofessional*" (p. 251).

Therefore, due to the sensitivity of the phenomenon, *susceptibility* (the dependent variable), a pivotal element of this study, is measured by asking anonymous participants an indirect and non-invasive question, instead of using the terms "have you been victimised?" or "have you been scammed?" in accordance with Nuno and St. John (2015), who noted,

> *evidence suggests that data validity may be increased by applying methods specifically developed for investigating sensitive topics. Such methods […] ensure respondent anonymity, increase willingness to answer honestly, and critically, make it impossible to directly link incriminating data to an individual*. (p. 6)

As an example, in a study on scam compliance and the psychology of persuasion (Modic *et al*., 2018), a method of examining students' susceptibility to phishing (dependent variable) was developed and validated using a binary variable Yes/No question. Participants were asked to answer three questions encapsulating the criteria (plausibility, give info and lost money), indicating whether they thought people would likely respond favourably to a number of scenarios (e.g., fake cheque, phishing, "Nigerian" scam, lottery, loan, online relationships, pyramid scam, etc.). They were further asked if they had ever provided information requested via any of the listed scenarios, and if so, if they had lost any money to such scams (Modic *et al.*, 2018).

Measuring the dependent variable (susceptibility to CSE attacks over LinkedIn) was guided by the indirect method of formulating a question and using a binary variable of Yes/No answer. The choice of this method was based on reviews by academic experts in the fields of computer science, organisational psychology and human factors. Participants were asked a binary-type self-report question; *In all the time since you have been using LinkedIn, have you ever had something bad happen (at your work or in your personal life) to you that you can trace back to your usage of LinkedIn?* Answers were coded (0 = No, 1 = Yes), and sensitive or identifiable responses (e.g., PII) were omitted. Participants were also given the option to elaborate further, in an open-ended follow-up question, *If you have answered yes to the question, could you briefly explain what happened and how you knew what you did on LinkedIn was the reason?*

4.15.2 Independent Variables

As with the dependent variable, there are a number of validated scales in the literature that measure many of the dependent constructs in the study model. The variables and the relevant scales are presented in the order of the hypotheses to which they correspond.

4.15.2.1 Personality Characteristics

This key set of constructs was measured using the FFM personality trait model. These characteristics of personality are openness to experience, conscientiousness, extraversion,

agreeableness, and neuroticism (OCEAN; Goldberg, 1990, 1992). The proposed model defines and examines these traits based on the definitions given by Goldberg (1990, 1992; see Chapter Three, Section 3.4.2 and Figure 3-7).

Conscientiousness (H1) is measured on a continuum from *efficient/organised* to *easy-going/careless*. This construct measures the extent to which a person has the tendency to be organised and dependable, show self-discipline, act dutifully, and aim for achievement. It also assesses whether an individual prefers planned, rather than spontaneous, behaviour. **Extraversion** (H2) is measured on a continuum from *outgoing/energetic* to *solitary/reserved*. This construct measures the extent to which a person has energy, positive emotions, is assertive, sociable, and talkative. **Agreeableness** (H3) is measured on a continuum from *friendly/compassionate* or *believing in others* to *challenging/detached* or *suspicious of others*. This construct measures the extent to which a person has the tendency to be compassionate and cooperative. It is also a measure of one's trusting and helpful nature, along with temperament. **Openness to experience** (H4) is measured on a continuum from *inventive/curious* to *consistent/cautious*. This construct measures appreciation of art, emotion, adventure, unusual ideas, curiosity, and variety of experience. **Neuroticism** (H5) is measured on a continuum from *sensitive/nervous* to *secure/confident*. This construct measures a person's degree of emotional stability and impulse control.

There are numerous FFM scale assessments available. The most commonly used are presented here, in descending order according to the number of items they consist of. The Revised NEO Personality Inventory (NEO-PI-R; Costa and McCrae, 1992) contains 240 items. The NEO-FFI (NEO Five-Factor Inventory) is a shorter version of the NEO-PI-R, consisting of 60 items (Costa and McCrae, 1992). There is a 50-item IPIP (International Personality Item Pool) version of the Big Five markers (Goldberg, 1999). Yet another instrument is the 44-item Big-Five Inventory, BFI (John and Srivastava, 1999). Donnellan *et al.* (2006), developed a Mini-IPIP, a 20-item short version (5-point scale) of the longer 50-item test which is used in van de Weijer and Leukfeldt (2017). Each personality trait is measured with four items as per recommendations by Saucier and Goldberg (2002, pp. 43-44) who assert that four items are enough as "*a practical minimum*" for the psychometric length. Donnellan *et al.* (2006) reported that the Mini-IPIP was internally consistent across five studies (≥ .60) and approximated the 50-item scale in terms of reliability and validity. Thus, the authors assert, the Mini-IPIP scale is "*a psychometrically acceptable and*

practically useful short measure of the Big Five factors of personality" (Donnellan *et al.*, 2006, p. 192).

Several short FFM surveys have also been developed. The 10-item assessment of personality traits (FIPI) uses a 7-point scale developed by Gosling, Rentfrow and Swann (2003). Although the authors claim the scale is valid, Woods and Hampson (2005) note limitations (cited in Donnellan *et al.*, 2006). Gosling *et al.* (2003) posit that FIPI is "*less reliable, converges less strongly*" when compared with other FFM measures, yet their study findings suggest that the "*FIPI instrument can stand as a reasonable proxy for a longer Big-Five instrument, especially when research conditions dictate that a very short measure be used*" (p. 513). This measure was used in studies investigating the role of the big five personality traits in users' susceptibility to cyber-attack victimisation in the context of online social networks (Albladi and Weir, 2017), the impact of users' characteristics on their ability to detect phishing emails (Alseadoon *et al.*, 2015), and personality and behavioural factors in user susceptibility to phishing attacks (Alseadoon *et al.*, 2012).

Given the time limitation for completing the survey on site, and more importantly, that the FFM is a pivotal element of this research, for which an acceptable result must be unequivocally achieved, the 10-item (7-point) scale and 20-item (5-point) scales were considered as adequate measurements for these five constructs. Based on the expert review at the pilot stage of the questionnaire, the 20-item test on a 7-point scale was used for this research (Table 4-4) and was translated into Arabic.

Participants were asked the key overall question: *How likely would you be to agree or disagree with the following statements?*

1 = Strongly Disagree, 2 = Disagree, 3 = Slightly Disagree, 4 = Neither Agree nor Disagree, 5 = Slightly Agree, 6 = Agree, 7 = Strongly Agree

Table 4-4 (Mini-IPIP) 20-Item Personality Traits Measurement Applied (Donnellan et al., 2006).

Item	Construct measured
Q1. I have thought a lot about the origins of the universe (reworded in Arabic version)	Openness to experience
Q2. I like to keep all my belongings neat and organized	Conscientiousness
Q3. I am a very shy person	Extraversion
Q4. I am always generous when it comes to helping others	Agreeableness
Q5. I always treat other people with kindness	Agreeableness
Q6. Sometimes I get so upset I feel sick to my stomach	Neuroticism
Q7. I am highly interested in all fields of science	Openness to experience
Q8. I like to have a place for everything and everything in its place	Conscientiousness
Q9. I am kind	Agreeableness
Q10. When I am under great stress, I often feel like I am about to break down	Neuroticism
Q11. I am quiet	Extraversion
Q12. I am fascinated with the theory of evolution (reworded in Arabic version)	Openness to experience
Q13. I am neat	Conscientiousness
Q14. I am sympathetic	Agreeableness
Q15. I am withdrawn	Extraversion
Q16. My feelings are easily hurt	Neuroticism
Q17. I would enjoy being a theoretical scientist (reworded in Arabic version)	Openness to experience
Q18. I am organized	Conscientiousness
Q19. I am quiet	Extraversion
Q20. I often have headaches when things are not going well	Neuroticism

4.15.2.2 Perception of Risk of Possible CSE Attacks

Risk perception was found to have a link to both systematic and heuristic information processing (Trumbo, 1999, 2006). Algarni (2019) posits that, within the IS realm, social networking site users have doubts about whether these platforms can be considered a secure means of communication, due to various latent online attacks (e.g., loss or compromise of personal information, financial theft) (Lee and Rao, 2007). A perceptual element of a threat can be present and alarming, as the literature suggests. The degree to which the risk perception arises varies from one individual to another, especially when users of

professional-oriented SNS are motivated by professional advancement and self-presentation. In such cases, a well-tailored attack can succeed by compromising the victim's disclosed resume and/or other sensitive information.

Risk perception measurement instruments tend to be developed for specific domains and fields, such as health/safety, finance/commerce, tourism/recreation and so forth (Weber *et al.*, 2002; Wolff, Larsen and Øgaard, 2019). The measure for *risk perception with regard to SNS use* (H6) employed in the current study is the same used by Saridakis *et al.* (2016), and is based on an adapted measure from Malhotra, Kim and Agarwal (2004). The measurement scale in the original study is a 7-point Likert-scale. Employees were asked to assesses and rate their perception of the risk involved in providing personal information and credentials on LinkedIn (Table 4-5; IDCARE, 2018).

The scale was adapted for the context of this study. Participants were asked the key overall question: *How likely would you be to agree or disagree with the following statements?*

1 = Strongly Disagree, 2 = Disagree, 3 = Slightly Disagree, 4 = Neither Agree nor Disagree, 5 = Slightly Agree, 6 = Agree, 7 = Strongly Agree

Table 4-5 Items Measuring Risk Perception

Scale Item	**Original questions adapted by Saridakis *et al.* (2016) from Malhotra, Kim and Agarwal (2004)**	**Items adapted for this research setting**
Construct:	**Perception of risk of possible CSE attacks**	**7-point scale**
Risk_Perception1 (H6)	In general, it would be risky to give (information) to SNS.	In general, it would be risky to give information in response to requests on LinkedIn.
Risk_Perception2 (H6)	There would be high potential for loss associated with giving (information) to SNS.	There is a high potential for loss associated with giving information in response to requests on LinkedIn.
Risk_Perception3 (H6)	There would be too much uncertainty associated with giving (information) to SNS.	There would be too much uncertainty associated with giving information in response to requests made via LinkedIn.
Risk_Perception4 (H6)	Providing SNS with (information) would involve many unexpected problems	Providing professional SNS sites with information would involve many unexpected problems.

4.15.2.3 Willingness to Take Risks

The concept of willingness to assume risk or risk propensity falls into the category of personal disposition, a factor that influences users' general victimisation in cyberspace (Buchanan and Benson, 2019; Moody *et al.*, 2017; Saridakis *et al.*, 2016; Williams *et al.*, 2017). It is broadly defined as the likelihood of a person to accept uncertainty; scholars differ as to whether risk propensity varies with both personality and situations or is a "personal trait that is stable across situations" (Das and Teng, 2004, p. 108; see also Chapter Three, Section 3.4.3. Willingness to assume risk can be associated with propensity to trust (Das and Teng, 2004). Dispositional trust, which is the tendency to take risks and trust something due to the advantages that might arise from that trust, is described as crossing a broad spectrum of situations and is triggered by the assumption that something is trustworthy (McKnight, Choudhury and Kacmar, 2002). Workman (2008) notes:

> while people generally state they are concerned about information security and privacy—even claiming they are willing to pay a fee to protect their personal information—in many cases they are willing to trade-off privacy for convenience or even bargain the release of very personal information in exchange of relatively small rewards. (p. 316)

In a LinkedIn context, an individual may be inclined to engage or respond to a deceptive message that promises the potential reward of a highly paid work position. Online users who have a higher propensity to take risks are also predicted to engage in risky behaviours online, such as disclosing their ID number to a bogus job application or clicking on a phishing link in their private messages or mailbox.

As with the other constructs from Saridakis *et al.*'s (2016) Model of Social Media Behaviour and Risk of Cyber Crime Victimisation (Chapter Three, Figure 3-6), the current study makes use of the same scales, with the wording of the items revised to reflect the research questions of this thesis. The construct of *willingness to assume risk* (H7) was measured on five items describing their risk-taking likelihood level while on professional SNS platforms (Table 4-6) and in the present study is measured on a 7-point scale to assess to what degree a user is willing to take and accept risk. This measure was based on the one used by Saridakis *et al.* (2016), which in turn was adapted from Chang and Chen (2008).

Participants were asked the key overall question: *How likely would you be to agree or disagree with the following statements?*

1 = Strongly Disagree, 2 = Disagree, 3 = Slightly Disagree, 4 = Neither Agree nor Disagree, 5 = Slightly Agree, 6 = Agree, 7 = Strongly Agree

Table 4-6 Items Measuring Willingness to Assume Risk.

Scale item	Original questions adapted by Saridakis *et al.* (2016) from Chang and Chen (2008)	Items adapted for this research setting
Construct:	**Willingness to assume risk on LinkedIn**	**7-point scale**
Willingness_Assume_Risk1 (H7)	I am willing to take substantial risks to do online shopping.	I am willing to take substantial risks to actively engage with services and features provided on LinkedIn.
Willingness_Assume_Risk2 (H7)	I am willing to accept some risk of losing money if online shopping is likely to involve an insignificant amount of risk.	I am willing to accept some risk of losing money if a LinkedIn job offer involves an insignificant amount of risk.
Willingness_Assume_Risk3 (H7)	I am willing to accept some risk to my personal information if online shopping is likely to involve an insignificant amount of risk.	I am willing to accept some risk to my personal information if a LinkedIn career opportunity (e.g. job post offers, contracts, agreements) involves an insignificant amount of risk.
Willingness_Assume_Risk4 (H7)	I am more comfortable using familiar SNS than something I am not sure about.	I am NOT more comfortable using familiar professional SNS than something I am not sure about.
Willingness_Assume_Risk5 (H7)	I am cautious when trying new SNS.	I am NOT cautious when trying new career-based SNS platforms.

4.15.2.4 Perceived Control of Privacy Risk

This construct has been found to be a positive predictor in relation to risk perception in a study examining a set of online threats over the Facebook SNS; the more strongly that Facebook users felt they were in control over their information privacy overall, the less likely they would be to choose specific safer privacy settings (van Schaik *et al.*, 2017). Similarly, Saridakis *et al.* (2016) found that individuals tended to be less likely to fall victim to cybercrime on SNS when they perceived they had control over their personal information. Van Schaik *et al.* (2017) found that a substantial number of users on Facebook who never changed their default privacy setting did not believe that any other users could search for their profile; they also claimed to be confident about how they controlled their information and believed that they were able to control what to disclose.

Users can have various purposes for engaging on SNS. Using the default privacy settings often enables features provided by these services, giving users more reach and visibility on the platform. The trade-off is less privacy for increased benefits such as employment/business opportunities, connections and/or endorsements. Users are triggered

to operate this way because, as found in a study investigating Facebook privacy concerns carried out by Acquisti and Gross (2006), people trust their own ability to control the information they share. However, the longer that users stay on default settings when controlling their privacy for visibility on LinkedIn, for instance, the higher the chances of intrusion into their privacy Hoadley *et al.*, 2010, which can unknowingly be exploited by attackers in combination with SNS algorithms for promotion purposes.

This construct was measured by focusing on how users perceive their level of control over their information shared on SNSs. *Perceived control of privacy risk* (H8) was originally measured with four items on a 7-point scale, with questions adapted by Saridakis *et al.* (2016b) from Xu *et al.* (2008) and Krasnova *et al.* (2010). One item has been omitted to improve the validity of the scale, resulting in three items measured on a 7-point Likert scale. The scale was adapted to reflect the research questions of this thesis (Table 4-7).

Participants were asked the key overall question: *How likely would you be to agree or disagree with the following statements?*

1 = Strongly Disagree, 2 = Disagree, 3 = Slightly Disagree, 4 = Neither Agree nor Disagree, 5 = Slightly Agree, 6 = Agree, 7 = Strongly Agree

Table 4-7 Items Measuring Perceived Control of Privacy Risk

Scale Item	**Original questions adapted by Saridakis *et al.* (2016) from Xu *et al.* (2008)**	**Items adapted for this research setting**
Construct:	**Perceived control on privacy risks**	**Seven-point scale**
PCOPRISK1(H8)	I believe I have control over who can get access to my personal information collected by SNS.	I believe I have control over who can get access to my personal information collected by LinkedIn.
PCOPRISK2(H8)	I think I have control over what personal information is released by SNS.	I think I have control over what personal information is released by LinkedIn.
PCOPRISK3(H8)	I believe I have control over how personal information is used by SNS.	I believe I have control over how personal information is used by LinkedIn.

4.15.2.5 Information Technology Self-Efficacy

Information technology self-efficacy is the individual ability to perform effectively when using technologies (Albladi and Weir, 2016). Bandura (1989) highlighted that the scale of self-efficacy must be specifically made for a particular domain, rather than be assessed with general measures. A higher level of self-efficacy can lead to a higher level of awareness and, therefore, a higher level of successful and decent behaviour in a social networking site environment (Milne *et al.,* 2009). Users' overall knowledge and confidence when operating computer technologies could help decrease one's general level of susceptibility to phishing attacks.

SNS technology self-efficacy is defined as "*the personal confidence in one's ability to successfully understand, navigate, and evaluate content, which should alleviate doubts and suspicions when dealing with social networking sites*" (Romm-Livermore and Setzekorn, 2009, p. 6). In the context of SNS, self-efficacy implies that users are expected to be skilled and operate effectively when creating their profiles and/or navigating, to be aware of the terms and privacy policies, and able to distinguish between fake and authentic profiles, websites and associated products of the application they are using (Zubiaga and Ji, 2014). In a study measuring self-efficacy as a factor in people's ability to determine whether SNS accounts were authentic or fake, confidence in making judgements was linked to the "*ability of human beings to detect authenticity of online social media*" (Sandy, Rusconi and Li, 2017, p. 7). All reputable SNS applications provide written guidance for users. Most SNS platforms publish statements to the effect that it is incumbent upon users to familiarise themselves with the terms and conditions provided by the platform, as these educate users about how to behave in a safe and precautionary manner, such as not sharing passwords or identifying potential links and malwares or fabricated applications. The agreements also cover legal rights, "Do's and don'ts", such as forbidding users to disclose sensitive information to others, which breaks these agreements; in return, the service becomes safe and protects the user from negative repercussions. For example, LinkedIn has a page called "Professional community policies", where it states, among other things:

- Tell us if you see something unsafe, untrustworthy, or unprofessional.
- Do not create a fake profile or falsify information about yourself.
- Do not engage in spam or scams.
- Do not share false or misleading content

- Do not share junk mail, spam, chain letters, phishing schemes, or any other scams are also prohibited. (https://www.linkedin.com/legal/professional-community-policies).

The measure used in the current study for *information technology self-efficacy* (H9) in the context of SNS is the same used by Saridakis *et al.* (2016). It measures an individual's confidence level in their IT skills with particular reference to their use of SNS (Table 4-8). It is measured by four items on a 7-point scale as follows:

Participants were asked the key overall question: *How likely would you be to agree or disagree with the following statements?*

1 = Strongly Disagree, 2 = Disagree, 3 = Slightly Disagree, 4 = Neither Agree nor Disagree, 5 = Slightly Agree, 6 = Agree, 7 = Strongly Agree

Table 4-8 Items Measuring Information Technology Self-efficacy

Scale Item	**Original questions adapted by Saridakis *et al.* (2016b) from Sam *et al.* (2005).**	**Items adapted for this research setting**
Construct:	**Computer self-efficacy**	**Seven-point scale**
IT_Self_Efficacy (H9)	I feel confident operating a personal computer.	I feel confident operating a digital device.
IT_Self_Efficacy (H9)	I feel confident understanding terms/words relating to computer hardware.	I feel confident understanding terms/words relating to SNS policy agreements.
IT_Self_Efficacy (H9)	I feel confident troubleshooting computer software.	I feel confident navigating SNS applications and websites.
IT_Self_Efficacy (H9)	I feel confident troubleshooting computer problems.	I feel confident knowing/recognizing the authenticity of a LinkedIn website or smartphone app.

4.15.2.6 Employees' Risky Habitual Behaviour (ERHB)

Phishing attacks, a common tactic deployed by cyber-social engineers, may only be successful when they are less likely to happen, or are rare in a particular form of online communication (Linkov, Zámečník, Havlíčková and Pai, 2019). When social engineering attacks are more frequent and believed to be more likely to happen, individuals in turn will have less trust in emails, be more inclined to follow good information security practices, and consequently make fewer mistakes (Sawyer and Hancock, 2018). The literature shows that low perceived risk and low levels of information security habitual behaviour can

induce irresponsible cybersecurity activities. Since social engineering normally aims to take advantage of human behavioural weakness (Mitnick and Simon, 2001), this human weakness could lead to poor cybersecurity practices, such as failing to update anti-virus software, sharing location on SNS, downloading data from unknown sources or sharing passwords. Such irresponsible online security habits and fewer precautionary behaviours can make an individual more susceptible to various cyberattacks over social media platforms (Milne *et al.*, 2009).

A number of studies have found that a high level of engagement on SNS and constant checking of emails, combined with low levels of information security habitual behaviour, can increase the risk of cyber-attack victimisation in both email and SNS contexts (Vishwanath, 2015a; Saridakis *et al.*, 2016; Albladi and Weir, 2018). Therefore, the construct of risky habitual behaviour (H10) is measured by combining three aspects: information security habitual behaviour (H10a), level of engagement on SNS (H10b), and frequency of SNS use (H10c).

Information security habitual behaviour was measured by adopting the Hadlington (2017) test, which was originally developed by Egelman and Peer (2015). Hadlington (2017) adapted a few items from Egelman and Peer's (2015) assessment to fit the context of users engaged on SNS, such as *"accepting friend requests on social media because you recognize their photo"*. Such items indicate susceptibility to victimisation via CSE deception. Both scales (Hadlington, 2017; Egelman and Peer, 2015) were developed to examine habitual safe use of computer and cybersecurity practices. Both assessments achieved an acceptable reliability of Cronbach's alpha: 0.823 on a 7-point Likert scale and 0.801 on a 5-point Likert scale, respectively.

The scale was adapted to reflect a number of items that are relevant to risky practices that users might have engaged in during the previous six months in relation to CSE schemes launched on professional SNS. Participants rated the items on a scale of 1–7 (where 1 = Never and 7 = Always). Scores can range from 0-150 on the sum of 20 items. A higher mean score indicates that employees are engaging in more risky cybersecurity behaviours that make them more susceptible to CSE victimisation. The starred (*) items are the most relevant questions to the setting of this study. Studies have found that an individual's low information security habitual behaviour, which includes being irresponsible when assessing privacy and security risks while engaging online and on SNS, is associated with

increased susceptibility to cybercrime victimisation (Vishwanath, 2014; Saridakis *et al.*, 2016; Albladi and Weir, 2018). This scale was defined as RHBIS (Table 4-9).

Participants were asked the key overall question: *In the past 6 months, have you?*
1 = Never, 2 = Once, 3 = two or three times, 4 = a few times per month, 5 = once a week, 6 = a few times per week, 7 = Always

Table 4-9 Items Measuring Susceptibility to CSE Risks on Professional SNS (RHBIS – H10a).

Scale Item	Adopted Construct and Items	Adapted questions for this research setting (Susceptibility to CSE risks on professional SNS
RCSB	**Hadlington (2017) Risky Cybersecurity Behaviour Scale**	**Seven-point scale**
RHBIS1	Sharing passwords with friends and colleagues.	Sharing passwords with friends and colleagues.
RHBIS2	Using or creating passwords that are not very complicated (e.g. family name and date of birth).	Using or creating passwords that are not very complicated (e.g. family name and date of birth).
RHBIS3	Using the same password for multiple websites.	Using the same password for multiple professional SNS sites.
RHBIS4	Using online storage systems to exchange and keep personal or sensitive information.	Using online storage systems to exchange and keep personal or sensitive information.
*** RHBIS5**	Entering payment information on websites that have no clear security information/certification	Entering payment information on websites provided through LinkedIn that have no clear security information/certification
RHBIS6	Using free-to-access public Wi-Fi	Using free-to-access public Wi-Fi
RHBIS7	Relying on a trusted friend or colleague to advise you on aspects of online security.	Relying on a trusted friend or colleague to advise you on aspects of online security. (reverse coded)
RHBIS8	Downloading free anti-virus software from an unknown source.	Downloading free anti-virus software from an unknown source.
*** RHBIS9**	Disabling the anti-virus on my work computer so that I can download information from websites.	Disabling the anti-virus on my work computer so that I can download information/documents shared by users on LinkedIn.
RHBIS10	Bringing in my own USB to work in order to transfer data onto it.	Bringing in my own USB to work in order to transfer data onto it.
RHBIS11	Checking that software for your smartphone/tablet/laptop/PC is up to date.	Checking that applications on my smartphone/tablet/laptop/PC are up to date through the Organisation's network. (reverse coded)
RHBIS12	Downloading digital media (music, films, games) from unlicensed sources	Downloading digital material (Videos, Documents, Applications) from LinkedIn users regardless of its authenticity.
RHBIS13	Sharing my current location on social media.	Sharing/revealing my current location on LinkedIn.
*** RHBIS14**	Accepting friend requests on social media because you recognise the photo.	Accepting connection requests on LinkedIn because you recognise the photo.
*** RHBIS15**	Clicking on links contained in unsolicited emails from an unknown source	Clicking on links contained in unsolicited LinkedIn Inbox messages from an unknown source
*** RHBIS16**	Sending personal information to strangers over the Internet.	Sending personal information/ credentials to unknown employers over LinkedIn
*** RHBIS17**	Clicking on links contained in an email from a trusted friend or work colleague.	Clicking on links contained in a LinkedIn message from a trusted friend or work colleague.
RHBIS18	Checking for updates to any anti-virus software you have installed.	Checking for updates to any anti-virus software you have installed. (reverse coded)
*** RHBIS19**	Downloading data and material from websites on my work computer without checking its authenticity.	Downloading data and material from LinkedIn on my work computer/smartphone without checking its authenticity.
RHBIS20	Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)	Storing organisations information/materials on my personal electronic device (e.g. smartphone/tablet/laptop)

Level of Engagement was measured by asking participants about their disposition towards their activities while engaging on SNS with their peers, and about their security behaviour in relation to embedded features provided by the service. This helps to determine their precautionary habit level with particular focus on SNS/CSNS. A new scale has been developed to measure the level of engagement using Hadlington (2018) measurement. The following items were identified from the findings of past studies; these studies suggest that high level of engagement on SNS and constant checking of email can increase the risk of CSE victimisation in both email and SNS contexts (Vishwanath, 2105a, 2015b; Saridakis *et al.*, 2016; Albladi and Weir, 2018). These items were approved by experts in organisational psychology as a potential activity to increase risk of CSE on SNS. In the present study, internal consistency tests for these items have achieved a reliability score with Cronbach's alpha of 0.881. Participants were asked to rate their SNS habitual behaviours on a 7-point scale (where 1 = Never and 7 = Always) during the previous six months (Table 4-10).

Participants were asked the key overall question: *In the past 6 months, have you?*

Table 4-10 Items Measuring Risky Habitual Behaviour: Level of Engagement (H10b)

Scale name	Risky Habitual Behaviour: Level of Engagement
RHBLE1	Logged into social media sites from your electronic work device (e.g., smartphone/tablet/laptop)
RHBLE2	Checked your email notifications from social media sites
RHBLE3	Talked about private company information on any of your social media sites
RHBLE4	Sent messages to work colleagues through one of social media sites you belong to
RHBLE5	Shared photos or videos containing company Information on social media sites

Frequency of SNS use was measured by adapting Saridakis *et al.*'s (2016) instrument by asking participants about the number of times they normally use their professional SNS account while at work, measured on a 7-point scale. Participants were asked to address a specific question to measure their frequency of use in the workplace: *"How often do you use LinkedIn from work"* (Table 4-11), which was scaled as follows*:*

Table 4-11 Frequency of LinkedIn use (H10c)

Never	Registered but do not use	Less than once a week	Every 2-3 days	Once to twice per day	Several times a day	Open all the time

4.15.2.7 Demographic and Cultural Factors

Based on the literature review findings, this study also looked into demographic aspects, measuring two areas: demographics and contextual factors, for example cultural factors (see Chapter Three, Sections 3.4.6 and 3.4.7). The demographic and cultural factors considered were age (H11), gender (H12), role in organisation (structural power: H13) and nationality (H14). In addition to the type of social networking sites participants often use, they were asked to specify what leisure or multipurpose SNSs they use, such as Instagram and Snapchat. Although Facebook is now used for job seeking as well, it is still portrayed as primarily a leisure platform. Participants were also asked what career-oriented SNS they use, such as LinkedIn and XIGN. Participants were asked to reveal information about their background as follows:

Culture: Nationality and Organisation. Since the central aim of this study is to examine personality characteristics, knowing that individuals' external factors such as beliefs and culture could potentially influence their behaviour, culture is also considered as a potential influential factor on how employees behave in an organisation. A large body of research has applied the element of cultural values (Hofstede, 1980; Alshehri, 2015; Varadwaj and Rath, 2018), and have shown that they link with many other cultural traits (see Chapter Two, Section 2.6.5 and Chapter Three, Section 3.4.7). Studies have shown that Hofstede's (1980) dimensions of culture can correlate with privacy concerns (Bellman *et al.*, 2004; Cho *et al*., 2009). On the other hand, Hofstede's theory has been criticised for being inconsistent (Ailon, 2008) and drawing conclusions that are too general (McSweeney, 2002).

This study is not able to identify and distinguish the cultural differences of those who are non-Saudis. Those employees in the organisation who are not Saudi nationals are from various backgrounds. Their small numbers would be insufficient and unrepresentative of a particular nationality, for example Pakistani, Egyptian or Indian. In order to avoid a noisy distribution of data, the construct of nationality is used to make a binary distinction between Saudi and non-Saudi. In previous research with a focus similar to that of the present study (Alseadoon, 2014; Sawaya *et al.*, 2017; Albladi and Weir, 2018), nationality has been used as a proxy measure for culture. Therefore, this study has adopted the same approach and substituted nationality for culture.

Nationality (H14) was assessed by asking participants whether they are Saudi citizens or non-Saudi (expatriate). It is relevant to this study to note that Non-Saudis in public organisations in Saudi Arabia are not officially affiliated to the organisation, but rather are sub-contracted for a short period of time to oversee/perform a particular task in the public sector. Due to the country's vast "Saudization" program, 70% of expatriate workers have been terminated in the government sector), as reported in *Gulf Business*: "The Ministry of Civil Service said in September 2017 that it planned to replace all expat staff in the public sector with Saudis. It aims to fill 28,000 roles by the end of 2020" (Gulf Business, 2018; the Ministry of Civil Service has since merged with MHRSD; see Chapter 1).

Role in Organisation. In the pilot study for the survey questionnaire, when participants were asked to state their role in the organisation (MHRSD), many of them misunderstood the intent and/or scope of the question and provided detailed "job descriptions". Therefore, in the larger survey, the question was revised to state their work "level" rather than "role". *Structural power* (H13) was thus assessed by work level (see Table 4-12), using the Saudi workforce index for government employees, under three categories based on type of responsibility (i.e., being in charge and overseeing a larger department, overseeing a section within the department, or nonsupervisory/entry level). The reason behind categorising structural power in three levels is to have better representation of the data and avoid thresholds, making data entry easier, and making it easier for participants to answer.

Participants were asked to state the following:

- Employment level: (1) Top-level management or designee; (2) Department management/ Section supervisor or designee; or (3) Administrative assistant/Office assistant.

Table 4-12 Employee Structural Power Within Organisation

Work level (structural power)	Description
Top-level management or designee	Any employee who holds responsibility for a larger group of employees or is a member of the board of directors. The designation also applies to an assistant of someone in such a position.
Department management/ Section supervisor or designee	Any employee who holds responsibility for a smaller group of employees, such as a section within a department. The designation also applies to an assistant of someone in such a position.
Administrative assistant / office assistant	Entry level or beyond. Employees and assistants who hold responsibilities that do not necessarily involve supervision of other employees and who usual hold routine administrative jobs.

Under the structural power of employees or (role in organisation), their level of information security awareness was given consideration, employees were asked the following in the survey:

- Whether they had received training to identify threats in the IS environment
- Whether they had specifically received training about the online threats involved using a SNS

4.15.2.8 Motivational Factors

Professional advancement motivates use of LinkedIn in several ways:

- Helpful for current and future professional development
- Sharing work-related curriculum vitae posts
- Networking with other professional contacts
- Obtaining peer support from others

Self-presentation is defined as a form of information disclosure (Bronstein, 2013). As such, individuals who are self-presentation-driven are keen to initiate interactions and build relationships. Self-presentation measurement involves:

- Providing personal credentials
- Introducing or telling others about oneself

No pre-existing scales for these two constructs were found in the literature, so two scales were created to measure self-presentation and professional advancement (Alotaibi, 2020). One scale is a 5-point Likert scale (0 = never, 5 = always) that measures *professional advancement* (H15). The 10 items in this scale were based on common user-initiated activities on LinkedIn, such as making contacts and sharing files (Table 4-13). The other scale is binary and measures *self-presentation* (H16), and its 14 items were based on profile features requested or offered by the platform: for example, phone number, work experience (Table 4-14). Internal consistency was measured for both scales, reporting Cronbach's alphas of .899 and .843, respectively. The scales are presented as follows:

Participants were asked to rate on a scale of 1-5 (never, rarely, sometimes, often, always) how often they used LinkedIn for these 10 purposes (Table 4-13).

Table 4-13 Professional Advancement on LinkedIn (Frequency Scale).

Have you connected with professionals that could help you with your professional advancement?
Have you followed other companies that you believe could increase your professional advancement?
Have you shared your work-related CV to companies which you believe could help you with your professional advancement?
Have you shared your work-related CV with professionals with whom you feel can help with your professional advancement?
Have you accepted connections from people whom you don't know but can see that they have many connections themselves?
Have you accepted network connections from people who are connected to your connections?
Have you accepted a connection request on LinkedIn because you recognized the photo?
Have you messaged your connections for support in career or work-related matters?
Have you shared documents, audio or video with connections in order to assist you with a problem?
Have you accepted documents, audio or videos from connections in relation to receiving support from them?

Table 4-14 Self-presentation on LinkedIn (Binary Questions).

Item	**Response Options**
Have you put your work experience history on?	Yes/No
Have you put your Educational history on?	Yes/No
Have you put your licenses on?	Yes/No
Have you put your certificates on?	Yes/No
Have you put your work email address on?	Yes/No
Have you put your work telephone number on?	Yes/No
Have you created an About me Page?	Yes/No
Have you put where you currently work?	Yes/No
Have you put your job title?	Yes/No
Have you put a profile picture?	Yes/No
Have you set your profile to public so anyone can view it?	Yes/No
Have you revealed or updated your current location?	Yes/No
Is your company logo on your profile?	Yes/No

On LinkedIn, as with most SNS applications, users generally provide credentials only once, when they create an account. The binary scale in Table 4-14 measures how much information respondents have put online in relation to their self-presentation, the more information they put online, the more content cyber social engineers have access to, from which these bad actors can glean information and create a more compelling fake profile or other intervention.

4.16 Statistical and Thematic Analytical Techniques

This section presents the methods used to analyse the data from both the quantitative and the qualitative research.

4.16.1 Data Analysis

Key quantitative statistical methods used in this study are briefly described below.

- As described in the preceding sections, Likert scales were employed to measure the constructs in the study model. It is a common and accepted practice to report averages for Likert scores, and to include the "Always" and "Never" scores in the average (Zimet *et al.*, 1990; Michielsen, de Vries and van Heck, 2003). This process was performed in the statistical analysis of the current study as well.
- SPSS 24 (Statistical Package for the Social Sciences)[9] predictive analytics software is used for complex statistical data analysis. In this study, SPSS was used to perfume ANOVA/Kruskal-Wallis tests for significance differences and Logistic regression to investigate relationships between multiple independent variables and a dependent variable.
- Parametric ANOVA (Cardinal and Aitken, 2013) and non-parametric Kruskal-Wallis (Hecke, 2012) tests were used to compare means across demographic groups. When a grouping variable has two levels, ANOVA is equivalent to the two independent samples t-test, which is why for consistency ANOVA results are presented for all grouping variables, including those having two levels. When a grouping variable has two levels, Kruskal-Wallis is equivalent to the Mann-Whitney test for two independent samples, which is why for consistency Kruskal-

[9] IBM SPSS. https://www.ibm.com/products/spss-statistics-gradpack

Wallis results are presented for all grouping variables, including those having two levels.

- Chi-square tests (McHugh, 2013) were used for testing the significance of association between categorical variables (such as the use of social networking sites and demographic variables).
- Logistic regression (Hosmer, Lemeshow and Sturdivant, 2013) was used to test all the hypothesised associations of various independent variables with the binary dependent variable – susceptibility to CSE attacks (1 – yes, 0 – no). Odds ratios (OR) give an idea of how odds of being susceptible change when the independent variable increases by one point. OR statistically significantly exceeding 1 indicate that the independent variable is a risk factor, while OR statistically significantly below 1 indicate that an increase in the independent variable reduced the risk of CSE victimisation.
- Boxplots were employed to visualise the distributions of scale variables; bar charts were used to visualise the frequency distributions of categorical variables.

4.16.2 Qualitative Analysis

In order to ensure rigour when analysing the qualitative data, this researcher followed a number of guidelines for phenomenological analysis (Hycner, 1985, pp. 280-294). The following procedures were employed in recording and analysing the interview data:

1. *Transcription*: The Arabic spoken by the interviewees was not standard Arabic, but rather the Saudi dialect. Their wording was revised to standard Arabic during transcription for better translation and clarity. Moreover, due to the way in which spoken language uses ellipsis, missing phrases were filled in and placed between square brackets when it was clear that these were meant.
2. *Bracketing and phenomenological reduction*: The researcher tried not to presume or assume what the participants would or "should" say.
3. *Listening to the interview for a sense of the whole*: The researcher played back the audio recordings several times and re-read transcribed passages in order to capture words or phrases that may have been missed the first or second time round.

4. *Delineating units of general meaning*: The researcher identified distinct units of meaning within the data "*which express a unique and coherent meaning*" (Hycner, 1985, p. 282). This was achieved by analysing not only the text of the speech, but through examining nonverbal gestures as well, to uncover the intended meaning.

5. *Delineating units of meaning relevant to the research question*: Units of general meaning were reduced to units of meaning relevant to the research question. This was to determine whether the interviewees' statements correspond to and elucidate the research question.

6. *Clustering units of relevant meaning*: The researcher examined the interview data looking for common themes among distinct units of meaning relevant to the research question.

7. *Summarising each individual interview*: The researcher summarised each interview while incorporating the themes elicited from the data. This step was part of the translation process: not all transcribed data was translated. Only the most interesting passages that the researcher deemed of value and relevant to the research question were translated into English. These were statements where participants were in agreement with each other, or supporting, conflicting with or elucidating a quantitative finding. The researcher chose the most salient material from the interview data.

8. *Identifying general and unique themes for all the interviews*: As mentioned in step 6, themes that were common to a number of interviews were identified. These themes from individual interviews were grouped together under a general theme that emerged in several of the interviews.

4.16.3 Organising and Presenting Data Analysis

The analysis has been organised according to the order in which the hypotheses are listed. The relevant data from the two data sources (questionnaires and interviews) were collated so as to produce a cohesive result for each hypothesis. The numerical data for a particular hypothesis has been presented, followed by the qualitative data. This presentation allows relationships, patterns and comparisons across data types to be easily presented and examined.

4.17 Instrument Validity

Neuman (2014) stated that validity "*suggests truthfulness*" and "*refers to how well an idea 'fits' with actual reality*" (p. 212). The validity of the measures and constructs is tested during several stages of the research. First, in the research design phase, the author can ensure that the validity of the measures and constructs is maintained by relying on instruments that have already been used in a similar context. For this reason, the current study has endeavoured to make use of scales found in the existing literature, wherever possible. Second, in conducting the two pilot studies, the researcher was checking for, among other things, whether specific constructs measured similar attributes, that is, the degree to which there was correlation between values. Finally, there are statistical techniques which can be used to test for reliability and validity, and these are applied during the data analysis phase.

The content validity of the study – the extent that measurement instrument items are relevant and representative of a particular construct – was established via the literature review (see Chapters Two and Three) and by reviews carried out by experts (see Section 4.11.4), as recommended by Taherdoost (2016). Similarly, the face validity of the items – the extent to which the items linguistically and analytically look like what is intended to be measured – was checked by experts, including a linguist (Section 4.11.3).

Construct convergent validity is the degree to which different measures of constructs that theoretically should be related, are indeed related. This was assessed with regard to the correlation between the independent variables and the dependent variable by means of regression analysis. The details of these tests are presented in Chapter Five, Section 5.4.

In social science research, external validity "*refers to the degree to which findings can be generalized across social settings*" (Bryman, 2012, p. 390). Bryman noted that external validity can be difficult to establish in qualitative research when it is applied to case studies and small samples. This study involved employees from two sections of a large public sector organisation in Saudi Arabia. The results may be generalisable to other public organisations in Saudi Arabia and similar countries in the Arabian Gulf. It remains to be seen (via study replication) whether this study and its findings are generalisable to other nations or cultures.

With regard to the qualitative measurement instrument (the semi-structured interview), the steps taken to ensure validity were described earlier in Section 4.12.2. In accordance with

the standard process in sequential explanatory design, the interview questions were formed based on the quantitative findings, with a view to explaining any findings that were unexpected or not intuitive. The proposed interview script was reviewed and assessed by an expert in industrial and organisational psychology (see Section 4.12.4 and Appendix I). The script was then revised based on his evaluation and feedback.

4.18 Instrument Reliability

Reliability is "*the consistency of a measure of a concept*" (Bryman 2012, p. 169). According to Bryman (2012), measures should have stability, meaning that they do not change over time. Ideally, an instrument should produce the same score for the same individual every time it is administered. Thus, together with validity, reliability establishes whether the values accurately represent the concepts (Neuman, 2014).

There are a number of threats to measurement reliability. One category of such threats is known as response bias. Response bias refers to the participant response style/set: a pattern showing systematic bias in the respondent's responses. This often happens when a participant is bored or just wants to get done with the survey as quickly as possible, Examples of this are extreme response, in which the respondent always selects the strongest response to avoid thinking through their responses, and bias towards the middle, which is similar to extreme response, but always choosing neutral responses. Another type of response bias is when a participant feels they will be judged by their responses, despite assurances that their responses will be anonymous (Neuman, 2014). Examples of this sort of response bias patterns are acquiescence, which is the tendency to agree to all statements regardless of content, and social desirability, when respondents want to present themselves positively or in a socially acceptable way (Neuman, 2014, p. 233).

The survey questionnaire for this study was designed to minimise response bias where possible. Questions and items were worded as concisely and clearly as possible, to make them short and easy to read and respond to. Some items were reverse-coded so that not all items could be rationally responded to with the same number on the Likert scale. The key items on information security risky habitual behaviour were placed in the middle sections of the survey rather than near the end, so that participants would not be fatigued or bored by the time they reached this set of items.

As with validity, there are established statistical techniques which can be used to test for reliability that are applied during data analysis. The Cronbach's alpha coefficient "*is viewed*

as the most appropriate measure of reliability when making use of Likert scales" (Taherdoost, 2016, p. 33). Cronbach's alpha coefficient values range between 0 and 1: the higher the value, the greater the reliability. According to Taherdoost (2016), it is generally agreed that a Cronbach's alpha of 0.7 is the minimum score for internal consistency, and represents a high level of reliability (p. 33). The reliability analysis of measurement scales is presented in Table 4-15, which shows each construct from the study model, with its resulting Cronbach's alpha.

Table 4-15 Internal Consistency of Measurement Scales Used in the Study

Scale	**Cronbach's alpha**
Openness	0.764
Conscientiousness	0.813
Extraversion	0.802
Agreeableness	0.841
Neuroticism	0.779
Risky habitual behaviour: self-control	0.957
Risky habitual behaviour: level of engagement	0.881
Risk perception	0.803
Willingness to assume risk	0.756
Perceived control of privacy risk	0.716
IT self-efficacy	0.903
Self-presentation	0.843
Professional advancement	0.899
Cyber-social engineering awareness	0.603

The internal consistency is high (all Cronbach's alphas exceed 0.7) for all scales except for the CSE awareness scale. This is not surprising, as that particular scale is comprised of three binary items. They were not aggregated in the analysis, but rather were counted as individual items.

With regard to the qualitative phase of the study, procedures were followed prior to, during and after the interview in order to minimise bias:

- The same interview script was used for all participants. The questions were exactly the same in their wording and in the order in which they were presented and other questions branched out for further clarifications whenever needed.

- The researcher interviewed each participant separately, and privately, in the language of his/her choice (Arabic or English).
- All the interviews were audio recorded, then transcribed and (if in Arabic) translated into English.
- Recordings and transcriptions were cross-checked to catch and correct any errors or omissions made during transcription.
- Themes were identified and coded according to consistent categories.

4.19 Summary of the Chapter

This chapter has presented the methodological process of this study. The philosophical assumptions underpinning the research were outlined. The epistemological stance adopted for this research project was presented: the pragmatic approach, which combines aspects of both positivism and interpretivism. The research methodology, including research design – a holistic single case study, instruments, data collection and sampling techniques, and tools of analysis used in this research, were described and explained. The constructs and their measurement instruments were detailed. Finally, the validity and reliability of the research were addressed. The next chapter, Five, presents the statistical and thematic analysis of the data.

5. Findings

5.1 Introduction

This chapter presents the analysis of the main research question:

Q1. How, and to what extent, do personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering (CSE) victimisation when accessing professional SNS, such as LinkedIn, in government organisations in Saudi Arabia?

The chapter begins by examining the demographic structure of the survey sample, as well as respondents' SNS usage statistics in both types of platforms: CSNS and SNS. Section 5.2 also provides demographic details for the interview participants, including information regarding their professions, areas of specialisation, position and sector of employment. Providing a breakdown of the personal characteristics and personal disposition factors by demographic group is useful for understanding the impact of demographics on susceptibility to online attacks, as well as for developing an approach to preventing risky behaviour in different demographic groups. Using data from both the quantitative and qualitative phases of the study, Section 5.3 describes each of the studied areas, both overall and by demographic groups. These areas are personality traits, personal disposition to risk, risky habitual behaviour demographic and cultural factors, motivation and user susceptibility. Section 5.4 tests the key hypotheses of this study related to the association of personal, behavioural and demographic factors with user susceptibility to CSE victimisation.

5.2 Participants: Demographic Data

In this section, the descriptive statistics for the two samples of participants are presented: the 394 survey respondents and the 15 interview participants.

5.2.1 Survey Respondents: Demographic Data and Usage of Social Networking Sites

Table 5-1 summarises the distribution of respondents by gender, age group, nationality, government sector type and employment level in the organisation. The survey sample is representative of the demographic composition of the MHRSD workforce. Males

comprised three quarters of the sample (74.9%). Most of the respondents were aged 29-39 (66.8%), but other age groups are also represented in the sample, with at least 19 people in each. Almost 87% of respondents were Saudis. Three quarters of the surveyed employees worked in the social development sector. Most participants were lower-level employees, but middle-level managers and top executives were also represented in the sample (20.8% and 4.3%, respectively).

Table 5-1 Summary of Demographic Data of Survey Respondents (N = 394)

Demographics		Count (n)	Percentage %
Gender	Female	99	25.1%
	Male	295	74.9%
Age	18 - 28	28	7.1%
	29 - 39	263	66.8%
	40 - 50	44	11.2%
	51 - 61	19	4.8%
	62 and over	40	10.2%
Nationality	Saudi Arabia	342	86.8%
	Non-Saudi (Expatriate)	52	13.2%
Government Sector Type	Social Development Sector (ORGSDS2)	278	70.6%
	Labor[1] Sector (ORGLS1)	116	29.4%
Work Level in Organisation	Administrative Officer / Assistant (Employee)	295	74.9%
	Department management/Section supervisor or designee	85	21.6%
	Top-level management or designee	14	3.6%

[1] In 2020 the Labor Sector was renamed the Human Resources Sector.

Only 0.5% (2 people) of the surveyed sample reported not using any SNS and 3.3% (13 people) did not use any career-oriented SNS. The majority of respondents reported using some social networking sites at least sometimes. The proportions of respondents who reported using each SNS is presented in Table 5-2.

Table 5-2 SNS and CSNS usage (N = 394)

Platform Classification	n	Usage, % of all respondents
SNS: Facebook	188	48%
SNS: Twitter	299	76%
SNS: Instagram	300	76%
SNS: Snapchat	184	47%
Other SNS	92	23%
CSNS: Bayt	200	51%
CSNS: LinkedIn	362	93%
CSNS: XIGN	62	16%
Other CSNS	52	13%

LinkedIn was by the far the most popular social networking site among the surveyed respondents. More than 9 out of 10 respondents (93%) reported that they used this career-oriented SNS. Instagram and Twitter were the second and the third most popular SNS with over 75% of the sample reporting usage, while Snapchat was the least popular, used by only 47% of respondents. Among other SNS mentioned by respondents, the most popular were WhatsApp (8% of all respondents), YouTube, Reddit and Quora (2% each). Even though these platforms are not usually considered to be social networks, the fact that they were mentioned indicates that messaging apps and – to some extent – forums and video hosting serve the same purpose as more traditional social networks for some people. Only 13% of respondents mentioned "Other Career-oriented Social Networking Sites", with Jadara and Monster recruiting platforms being the most popular (2% of all respondents each). Although these platforms are not fully functioning CSNS, their mentions may be because they include some of the social features found in most modern digital platforms (profiles, messages, chats, audio/video calls), which blurs the distinction between SNS/CSNS and some other platforms.

According to a series of chi-square tests of association between each social network use and each categorical demographic or cultural variable (age, gender, nationality and employment level), almost no statistically significant differences were observed among demographic groups in terms of their choice of SNS. The only association significant at the 5% level was that Bayt usage differed across age groups (Table 5-3). At the 10%

significance level, Instagram usage is associated with employment level (only 50% of top-level employees and 77% of lower and middle-level employees use Instagram) and Saudis more often mentioned "Other" SNS (24.9%) compared to non-Saudis (13.5%), probably because Saudis more often regarded WhatsApp as a social network site.

Table 5-3 Social network use by demographic group

Demographic Group		What career-oriented social networking sites (CSNS) do you use? ***Bayt***		What social networking sites (SNS) do you use? ***Instagram***		What ***OTHER*** social networking sites (SNS) do you use?	
		No	Yes	No	Yes	No	Yes
		Row N %	Row N %	Row N %	Row N %	Row N %	Row N %
Total		49.2%	50.8%	23.9%	76.1%	76.6%	23.4%
Age	18 - 28	32.1%	67.9%	25.0%	75.0%	75.0%	25.0%
	29 - 39	49.4%	50.6%	21.3%	78.7%	77.2%	22.8%
	40 - 50	70.5%	29.5%	25.0%	75.0%	77.3%	22.7%
	51 - 61	26.3%	73.7%	36.8%	63.2%	57.9%	42.1%
	62 and over	47.5%	52.5%	32.5%	67.5%	82.5%	17.5%
Nationality	Saudi Arabia	48.8%	51.2%	24.0%	76.0%	75.1%	24.9%
	Non-Saudi (Expatriate)	51.9%	48.1%	23.1%	76.9%	86.5%	13.5%
Work Level in Organisation	Administrative Officer / Assistant (Employee)	51.5%	48.5%	22.7%	77.3%	78.0%	22.0%
	Department management/Section supervisor or designee	41.2%	58.8%	23.5%	76.5%	71.8%	28.2%
	Top-level management or designee	50.0%	50.0%	50.0%	50.0%	78.6%	21.4%

Shaded cells indicate a significant association between corresponding row and column variables.

Similar usage patterns of social networks in different demographic groups can be explained by the high penetration of social media in people's lives, the fact that the sample was a relatively homogeneous group from a single public sector organisation and the fact that only relatively young and middle-aged respondents were targeted, rather than retired people aged 65+. The absence of major differences in SNS usage among different demographic groups in this sample is beneficial from the statistical analysis perspective, as it will ensure cleaner identification of demographic effects on susceptibility to CSE risks, rather than confounding the effects of experience with SNS. For example, if males turn out to be more susceptible to CSE risks, it will most likely have something to do with differences in personality characteristics between males and females, rather than with the fact that males are less experienced users of SNS in general.

5.2.2 Interview Participants: Demographic Data and Specialisations

Demographic details for the 15 interview participants are shown in Table 5-4.

Table 5-4 Demographic Data for Interview Participants

Table 5.4. Demographic Data for Interview Participants

ID No.	Gender	Age	Nationality	Profession/Specialisation	Position	Sector
IP1	Female	57	Saudi	Sociology	University Faculty	Public
IP2	Male	35	Saudi	Criminology	Security College Faculty	Public
IP3	Male	40	Saudi	Information Technology	IT Center Manager	Public
IP4	Female	37	Saudi	Cyberpsychology Expert	University Faculty	Public
IP5	Male	45	Non-Saudi	Cybercrime Writer/ Reporter	Adjunct College Faculty/ Online Newspaper	Private
IP6	Female	34	Saudi	Computer Science	Assistant Professor	Public
IP7	Male	31	Saudi	Cybersecurity	Executive Manager	Public
IP8	Male	49	Non-Saudi	Computers in Society/ Cybersecurity	Academic/Blogger	Independent
IP9	Female	27	Saudi	Civil Service	HR Specialist	Public
IP10	Female	NA	Saudi	Psychology	University Faculty	Public
IP11	Male	33	Saudi	Information Technology	Expert, FinTech Company	Private
IP12	Female	33	Saudi	InfoSec Expert	Academic Lecturer	Private
IP13	Male	40	Saudi	Information Technology	Systems Analyst	Public
IP14	Female	43	Saudi	Sociology	University Faculty	Public
IP15	Male	45	Saudi	Behavioural Geography & Risk/Education Management	Gov't. Agency Director	Public

As shown in Table 5-4, these participants are professionals from academia and industry. Eight are in various branches of the IT and cybersecurity fields (one is a journalist specialising in cybercrime). Of the remaining 7, there are two psychologists (one in cyberpsychology), two sociologists, a criminologist, a behavioural geographer specialising in risk management and a human resources specialist. Thus, these are effectively a panel of experts. Therefore, it is expected that their views and insights on human susceptibility to cyber-social engineering are informed by their training, experience and expertise.

5.3 Descriptive Analysis of Study Areas

The independent variables (16 constructs and 3 sub-constructs) fall into three main study areas: personality traits, risky habitual behaviour and personal disposition to risk. The dependent variable is user susceptibility to CSE victimisation on LinkedIn. The survey results are described and analysed in the following subsections. The analysis is enriched by the inclusion of the qualitative data from the interviews.

5.3.1 Personality Traits

Five personality traits were measured on multiple item questions measured on seven-point scales (1 – Strongly disagree, 7 – Strongly agree). Summary statistics for each of the scales are presented in Table 5-5.

Table 5-5 Summary statistics for personality traits composite scores (N = 394)

Personality Trait	Mean	SD	Median	Min.	Percentile 25	Percentile 75	Max.
Openness	4.3	1.4	4.5	1.0	3.3	5.5	7.0
Conscientiousness	4.9	1.2	5.0	1.5	4.3	5.8	7.0
Extraversion	4.3	1.5	4.5	1.0	3.3	5.5	7.0
Agreeableness	5.0	1.4	5.0	1.0	4.0	6.0	7.0
Neuroticism	4.0	1.5	4.0	1.0	2.8	5.3	7.0

A comparison of the mean scores for the personality traits across different demographic groups was conducted using a series of ANOVA and Kruskal-Wallis tests. A number of significant differences among demographic groups were identified. Females scored significantly ($p < .001$) higher on extraversion and neuroticism but lower on agreeableness. Women also had significantly higher ($p < .05$) openness and conscientiousness scores than their male colleagues had (Table 5-6).

Table 5-6 Personality Trait Scores by Gender

Personality Trait	Gender				Tests of Significance	
	Female		Male			
	Mean	Standard Deviation	Mean	Standard Deviation	ANOVA p-value	Kruskal-Wallis p-value
Openness	4.55	1.28	4.19	1.49	0.035	0.034
Conscientiousness	5.20	1.17	4.83	1.21	0.009	0.008
Extraversion	5.21	1.22	4.01	1.46	< 0.001	< 0.001
Agreeableness	4.04	1.27	5.27	1.23	< 0.001	< 0.001
Neuroticism	5.00	1.24	3.65	1.43	< 0.001	< 0.001

While most personality traits scores do not differ by age group (Table 5-7), mean neuroticism score significantly increases with age (e.g., M = 2.73, SD = 0.87 for those aged 18-28; and M = 5.06, SD = 1.52 for those aged 62 and over).

Table 5-7 Personality Trait Scores by Age

Personality Trait	Age										Tests of Significance	
	18 - 28		29 - 39		40 - 50		51 - 61		62 +			
	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD	ANOVA p-value	Kruskal-Wallis p-value
Openness	4.08	1.29	4.33	1.43	4.19	1.40	4.07	1.83	4.32	1.52	0.835	0.870
Conscientious-ness	5.04	1.25	4.97	1.18	4.80	1.20	4.37	1.42	4.94	1.27	0.263	0.357
Extraversion	4.11	1.65	4.35	1.45	4.15	1.47	4.33	1.88	4.36	1.52	0.873	0.865
Agreeableness	4.78	1.40	5.00	1.38	5.09	1.36	4.84	1.11	4.80	1.28	0.779	0.660
Neuroticism	2.73	0.87	3.85	1.42	4.29	1.45	4.75	1.54	5.06	1.52	< 0.001	< 0.001

Saudis scored significantly higher on extraversion and agreeableness scales compared to non-Saudis (Table 5-8).

Table 5-8 Personality Trait Scores by Nationality

Personality Trait	Nationality				Tests of Significance	
	Saudi Arabia		Non-Saudi (Expatriate)			
	Mean	Standard Deviation	Mean	Standard Deviation	ANOVA p-value	Kruskal-Wallis p-value
Openness	4.24	1.43	4.60	1.50	0.094	0.094
Conscientiousness	4.95	1.20	4.79	1.26	0.376	0.355
Extraversion	4.42	1.46	3.57	1.48	0.000	0.000
Agreeableness	5.11	1.27	4.00	1.49	0.000	0.000
Neuroticism	4.01	1.48	3.85	1.63	0.467	0.446

An interviewee whose area of study is sociology elaborated on why Saudi Arabian citizens may have scored higher on the agreeableness trait compared to expatriates (non-Saudis). She explained that this trait was fostered in collectivist cultures such as Saudi culture…

> *"Saudi Arabia falls into [the category of] societies that are perceived as collectivist, meaning mutual dependence between people is prevailing. Therefore, they are prone to put the interest of the whole community over one's self-interest […] such as by helping one another, be[ing] good to the elderly, and [Saudis] are raised by strict family and social values that compel them to refrain from arguing with seniors or strangers…*

…and gave detailed examples of the norms and behaviours that indicate agreeableness:

Respecting others can also go beyond one's own interest sometimes… even when they do not agree with someone, it can be common to see a Saudi individual [nod] his/her head and not making the other person feel disappointed for being wrong or hold a dissenting opinion or [a Saudi will] comply with a request [in order] to avoid disappointing [someone] and usually strive to give a helping hand – even to a complete stranger." IP1

Another interview participant reflected on the possible reason that non-Saudis scored lower than their Saudi colleagues did on extraversion and agreeableness. He noted that although the cultural differences might not be large, the socio-economic situation they experience as guest workers may have a greater impact on how (freely) these personality traits are expressed:

"Expatriates from other countries such as parts of the Middle East or Asian countries…may share the same customs and values that induce some to be collaborative and outgoing or polite and pleasing within their community and are eager to [interact with] others... However, these qualities can be expressed differently when they are expatriates in [Arabian] Gulf countries …Being cautious due to the country's labour laws, or [not questioning] instructions, so as to comply and cope within a different environment, could impact on their behaviours and consequently could reshape their habits and impulsive responses. Over time, their emotions and behaviours can be[come] suppressed. For instance, outgoing individuals can turn into introverts, perhaps due to environmental and cultural differences or having the sense of unfamiliarity in this new place and be[ing] wary of whatever consequences might happen should they behave inappropriately with locals known for having strict values – a belief based on misconception for the most part." IP2

Finally, the quantitative analysis shows some significant differences in mean openness scores of employees occupying different levels in the organisation (Table 5-9): lower-level employees (administrative officers/assistants) have the highest mean openness score (M = 4.42, SD = 1.44).

Table 5-9 Personality trait scores by employment level

Personality Characteristics Type	Work Level in Organisation							
	Administrative / Office		Dept. management / Section supervisor		Top-level management / designee		Tests of Significance	
	Mean	SD	Mean	SD	Mean	SD	ANOVA p-value	Kruskal-Wallis p-value
Openness	4.42	1.44	3.88	1.37	3.77	1.60	0.003	0.005
Conscientiousness	4.88	1.20	5.07	1.22	5.04	1.39	0.405	0.274
Extraversion	4.36	1.47	4.21	1.57	3.91	1.51	0.440	0.505
Agreeableness	5.03	1.34	4.78	1.36	4.75	1.63	0.281	0.272
Neuroticism	4.01	1.49	4.03	1.55	3.27	1.21	0.187	0.148

The interviews yielded insights into the openness trait being significant within groups of employees in the lower level of organisation hierarchy. Their responses highlighted that employees at the beginning of their career ladder are periodically seeking to advance their knowledge, which involves being open to new knowledge and experiences:

> *"It is likely that employees occupied in administrative tasks tend to be in a position to seek more knowledge enhancement and to develop themselves, [in ways] such as partaking [in] online learning programs and certificates, [and in] workshops, in order to stand out for future promotions within the organisation."* IP4

One participant noted that knowledge seeking was not confined to lower-level employees, but that management level employees play a role in modelling this information-seeking behaviour along with good InfoSec practices for their lower-level staff. He explained that following and adopting these practices would help administrative staff when they seek promotion and to advance in their careers:

> *"I believe it is a rule of thumb for those at higher levels in companies and organisations to familiarise themselves with technical and administrative updates and developments in order to sustain [last longer or] preferably [advance] further in their positions, along with keeping strong ties with the most important members of the organisation… This will impact on the rest of entities in the organisation, especially [with]in lower levels, to motivate performance and in return respond to such developments by presenting themselves as worthwhile for the next higher position involving much more important tasks …"* IP3

Another interviewee suggested that the openness trait in employees was a positive one from the point of view of an organisation, for the following reason:

> *"I believe that those who read and are?? avid learners and [those who] are curious about knowledge overall and are up to date are far less likely to open a vulnerability hole into the organisation than those who are not [open, i.e., their personality type]."* IP15

However, another interviewee cautioned that knowledge by itself was not sufficient to avoid being susceptible to CSE.

> *"Such knowledge acceleration in administration, or in information technology and security for that matter, is nothing without long years of accumulated experiences… An intellectual person doesn't always mean a wise person practically. They can still be naive in how to respond to deceptive individuals… It's more about life experience than how many books you have read or how many certificates you have. This is why [there is] the general idea that [streetwise] individuals are more favourable in such situations."* IP1

5.3.2 Disposition to Risk

As described in Chapter Three, this study examined four factors related to personal disposition to risk that are applicable in the realm of users' sensitivity to cyber-social engineering: *risk perception*, *willingness to assume risk*, *perceived control of information (privacy risk)* and *IT self-efficacy*. These factors were measured using multiple item seven-point scales (1 = Strongly Disagree, 7 = Strongly Agree). The constructs were analysed by averaging out the corresponding survey items (accounting for the fact that some items needed to be reverse-scaled). Summary statistics for each of the four scales are presented in Table 5-10 and visualised in Figure 5-1.

Table 5-10 Summary statistics for Personal Disposition to Risks *composite scores (N = 394)*

Dispositional Factors	Mean	SD	Min.	Percentile 25	Median	Percentile 75	Max.
Risk Perception (1 – lowest, 7 – highest)	4.42	1.40	1.00	3.50	4.50	5.50	7.00
Willingness to Assume Risk (1 – lowest, 7 – highest)	3.88	1.47	1.00	2.80	3.80	5.00	7.00
Perceived Control of Info (Privacy Risk) (1 – lowest, 7 – highest)	4.69	1.35	1.00	3.67	4.67	5.67	7.00
IT Self-Efficacy (1 – lowest, 7 – highest)	4.58	1.52	1.00	3.50	4.75	5.75	7.00

These results show that, in general, respondents are aware of the risks associated with using SNS and perceive themselves as having some control over them (median values are 4.5 or higher for *risk perception* and *perceived control of information [privacy risks]*). The responses have a high median level for IT self-efficacy (4.6). The distribution of the willingness to assume risk is symmetrical, with most people having a moderate propensity for risk-taking online.

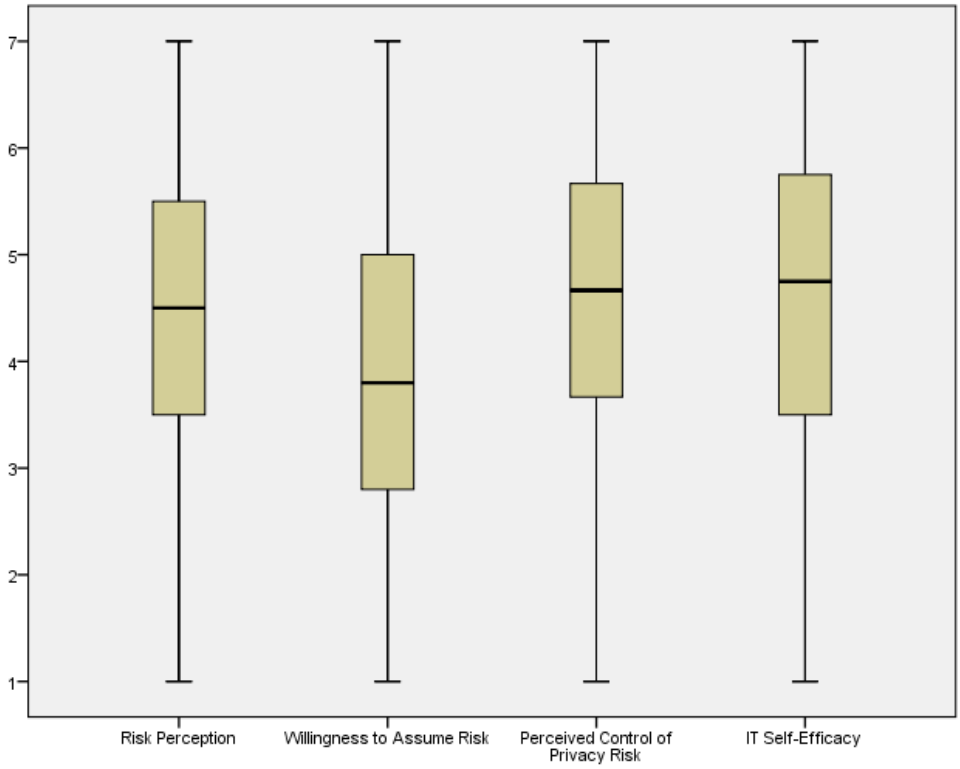


Figure 5-1 Disposition to Risk scales distribution: boxplots

Each 7-point response was recoded into three levels for ease of interpretation: disagree (1-2 points), neutral (3-5 points) and agree (6-7 points). The following sections present the prevalence of each of these groups for each of the items.

Risk Perception

The *Risk Perception* scale includes four items reflecting the perception of the risk involved in providing personal information and credentials on LinkedIn. Chart 5-1 below shows the frequency distributions for the degree of agreement with the existence of each type of risk. The levels of agreement with each of the four statements are similar, with 25% to 31% of respondents agreeing that information sharing on LinkedIn is associated with risk, uncertainty, losses and unexpected problems (Chart 5-1). This accords with the high internal consistency of the scale, discussed in Chapter Four.

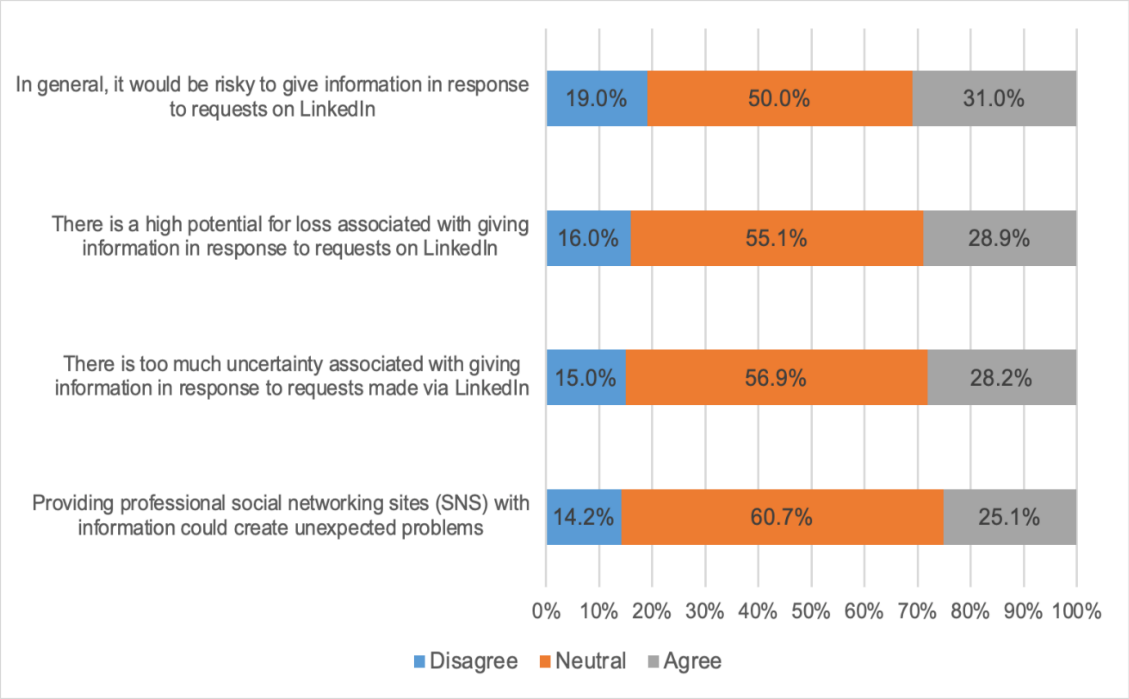


Chart 5-1 Risk Perception Factor

Responses from interviewees provided some indication that SNS users indeed perceived various types and levels of risks associated with engaging on these platforms:

> *"... these are tools of communication, which involves viruses and penetrations of data and stealing your money when you respond to the wrong and deceptive people."* IP1

> *"I once administered a workshop on cybersecurity risks. Some of the students expressed openly, although aware of possible social engineering tactics risks, how rumours and controversial videos/images trending on social media platforms are*

tagged with hundreds of malicious hashtags with links [which] can accidently lead them to seek more about it…" IP7

"… risks of fraud or identity theft and the invasion of virtual communication networks for privacy and harassment in all its forms, along with inappropriate content and spreading rumours." IP8

One interviewee noted that users could play down the risks involved (low risk perception):

"Most likely they arbitrarily minimise the magnitude of whatever bad outcomes [might result], due to users' tendency of curiosity." IP10

Another explained that there were various levels of risk that users ought to take into account:

"…. I do not think that it represents a great risk just because your [LinkedIn] profile is stolen! Because the danger does not lie in tampering with information you show or conceal; the danger, rather, is how your profile can be used as an attack tool to the [other] connected members, or [knowing] the password you are using, as it can be the same in more critical and sensitive accounts such as work emails and Facebook. [This is] because their privacy risks are higher than simply showing the workplace, experiences, or the university from which you graduated." IP15

Willingness to Assume Risks

The *Willingness to Assume Risks* scale includes five items reflecting the respondents' risk-taking likelihood level while on professional SNS platforms. Chart 5-2 below shows the frequency distributions for the degree of risk propensity for each of the items. Slightly more than one quarter of all respondents are willing to take the risk of trying new or unfamiliar career-based SNS platforms, losing money for an attractive LinkedIn job offer process, as well as the risks to their personal information and risks associated with active engagement with the platform's services and features. About one third of respondents are not willing to take such risks, while a neutral willingness to assume risk was the most common response among respondents.

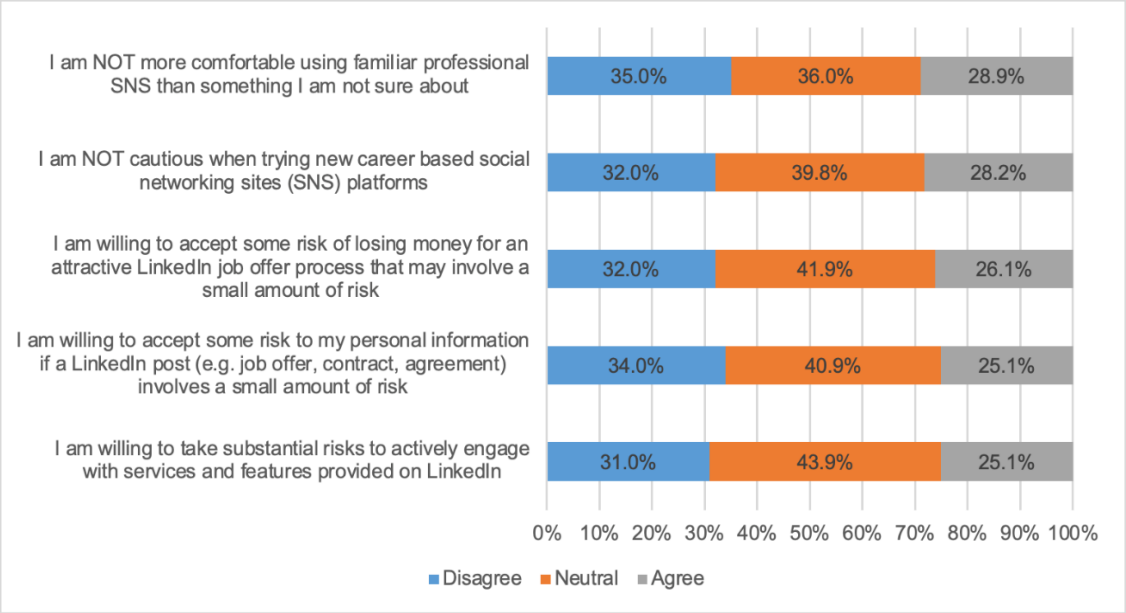


Chart 5-2 Willingness to Assume Risks Factor

On the topic of willingness to assume risk, interview participants often associated this propensity with specific individual characteristics and/or demographic/cultural factors, and these factors have been found in the quantitative phase of this study to influence susceptibility to CSE:

Risk propensity and openness to new experiences (see Section 5.4.1 of this chapter):

> *"...An individual constantly needs to self-learn and explore different aspects of knowledge. [This] can be driven by high curiosity. You see, curiosity can be double-edged in human beings, as it can also at times get you into negative consequences... Of course, that can also apply in any scenario, including online environment[s] ... depending on what a user is looking for or wants, for example, when they are looking to illegally download cracked software they can be vulnerable to harm their computers and their data."* IP10

Risk propensity and career advancement (Sections 5.3.5.2 and 5.4.5):

> *"...the same thing with that [career-oriented SNS]: an employed individual is persistently in need, in this situation, to find a job or even switch jobs. This individual can also make [a] hasty decision, neglecting potential dangers of clicking on phishing links of attractive job applications or opening PDF format job descriptions..."* IP10

Risk propensity and gender (Sections 5.3.4 and 5.4.4):

> *"I as a Muslim woman … would not personally go against my instinct or willingly engage in an action that involves even a low percentage of threat in [the] real world and especially [not] in virtual events, while, others might do otherwise… But let me emphasise that since men are portrayed to be generally more capable physically and are more perceived to gain the sensation of thrill induced by partaking [in] challenging actions, this can explain their willingness to accept a potential threat when engaging with others over the internet compulsively, to uncover what is behind a[n] [al]luring advertisement or request."* IP6

A male participant agreed with the statement above:

> *"Men like to take risks and engage unhesitatingly with strangers online when they [strangers/cyber-social engineers] suddenly seem to share or provide what those men are seeking, either by unknowingly [i.e., without the victim knowing that the cybercriminal has been] follow[ing] their online activities, such as their likes on Instagram and Twitter, or job inquiries posted on LinkedIn, and thus perpetrators work accordingly, using spear phishing… There can be times where a reverse attack happens by offering help to non-existing problem to give a feel of trust through showing willing[ness] to assist."* IP11

Regarding the role of gender with regard to risk propensity, another male interviewee asserted clear differences between the genders:

> *"Of course, the point is, why and how females are less prone than males, statistically, look at the total risk to mortality… I mean even in disaster risk management we had a time when men were always more vulnerable. As for men, they are bolder, and, in the workforce, you see proportionally more men than women, therefore men are more likely to be susceptible than women generally and, in several considerations…. Possibly due to physiological characteristics in them [men] that make them willing to take risks… I mean men are more ready to experience and engage in adventures than women, as they [women] do not like to take risks and fear adventure and are less daring…. This is what makes women less likely to engage in trouble. It has nothing to do with the facts suggesting that women*

are smart or more cautious, I believe it's about physiological and behavioural matters [that] exist in men in general." IP15

Risk propensity and age (Sections 5.3.1 and 5.4.4):

"I once administered a workshop on cybersecurity risks topics. Some of the students expressed openly, although aware of possible social engineering tactics risks, how rumours and controversial videos/images trending on social media platforms … can accidently lead them to seek more about it … Their arrogance of risks and inquisitiveness overcome [them and they engage in] undesirable behaviours." IP7

Risk propensity and nationality (Saudi vs. non-Saudi [Sections 5.3.4 and 5.4.4):

*Residents [expatriates] always fear falling into error, which threatens their career in Saudi Arabia. … Such fear, along with the sense of job insecurity, exists more within expatriates than with Saudis. Saudis feel more secure and sure that they will attain a job eventually, therefore they [Saudis] have a greater [acceptance of] risk of adventure and thus fall [prey] into fraudulent messages." I*P15

When IP15 was asked to elaborate on this point, he added:

"But the resident [expat] renews his/her contract approximately annually. The annual bonus is linked to his/her performance, even in government institutions. Therefore, you find them very careful not to cross red lines or take any gamble which compromises their work permit status. This is why they tend to be more vigilant to cyber threats than others. …[Conversely,] this is what makes some Saudis less vigilant than residents [non- Saudis] to cyber threats, like giving information to others." IP15

Perceived Control of Information (Privacy Risk)

The *Perceived Control of Information (Privacy Risk)* scale includes three items reflecting how users perceive their level of control over their information shared on CSNS. Chart 5-3 below shows the frequency distributions for the level of perceived control for each item. Generally, respondents expressed uncertainty about their control over their privacy on LinkedIn. While 40% of respondents believed they had control over how their personal

information is used by LinkedIn, only a little more than a quarter of respondents expressed confidence in having control over who can get access to their personal information (28%) and control over what personal information is released by LinkedIn (27.2%).

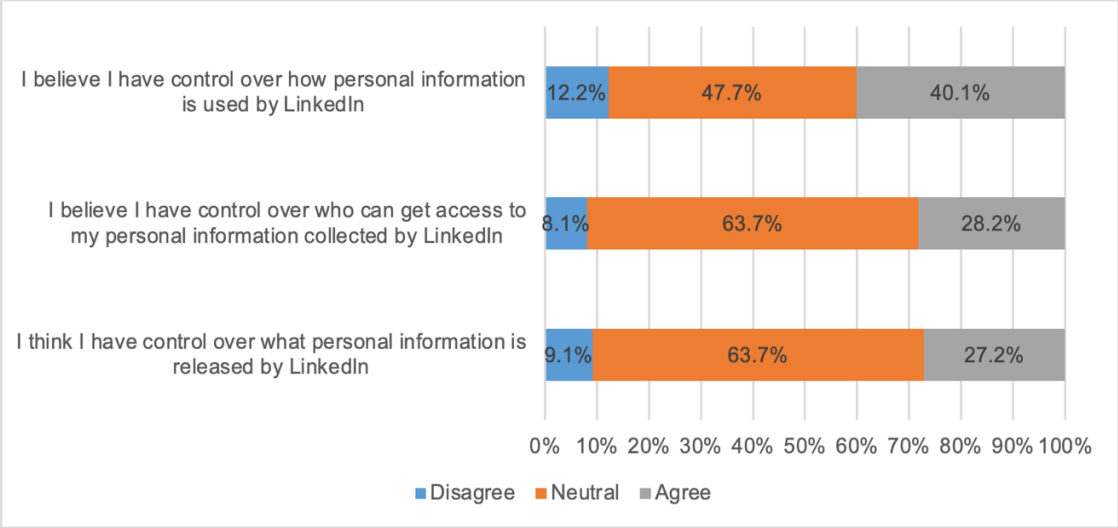


Chart 5-3 Perceived Control of Information (Privacy Risk) Factor

The assessment findings from the qualitative data regarding perceived control of information (privacy risks) amongst employees suggest that users are underestimating the risks to the privacy of their information on LinkedIn and online in general.. Specifically, the interviewees, most of whom were either academics, industry experts or mid- to senior-level management, believed that employees' perceptions of the risks to the privacy of their information would be low. This finding from the qualitative data supports the quantitative findings shown in Chart 5-3.

In the view of several respondents, fear of misjudgement and having insufficient capability of control was predominant in the workplace environment.

> *"For the majority, to express being in control of what of their information is accessed and used by these career social media companies and websites can be confused with what THEY have control of and share by themselves via the privacy settings in their profile… I believe that such knowledge should not necessarily be considered as a reason behind being – or not [being] – a victim of deception, but rather [it] gives us a picture as to what extent employees can be aware and understand the difference between the privilege given to them to control their privacy settings AND the company policy which clause [states] that the data can be shared with a 3rd party for marketing purposes… Usually when people create a*

profile they are in a hurry to join the crowd – they don't care about what to share because they know these platforms are all about sharing and connecting. In the information age, privacy protection is not definite, and information leakage is inevitable." IP3

When asked how information control would be a problem if information leakage is likely to happen anyway, the respondent, an IT centre manager, explained:

"you have to know that these social media websites and applications – in the end – are for-profit companies. Their way of making money is by advertisement campaigns…, selling your information to recruiters and other for-profit parties and subscriptions to get better privileges, like the LinkedIn Premium memberships. For them you are nothing but a product on their table. They have their ways to make you reveal more about yourself, [to make you] engage more to understand your behaviour patterns for marketing purposes. For example, LinkedIn will periodically ask you to put more to your profile to get a complete profile for broader acceptability and benefits… This [tactic] has been made [devised] by them [LinkedIn], not users." IP3

Other interviewees of various professions and educational backgrounds agreed with the above statement, explaining that for the typical user, the perceived risk to the privacy of their information is outweighed by the desire for convenience and other benefits which users expect:

"People learn to follow and trust instructions coming from popular services that are seen everywhere around us, [for instance,] trusting popular banks and social media companies. [Because of] their popularity [people's] personal information are given when asked for. Trust is the foundation between these two things… if people were continuously annoyingly rushed and are compelled by a social media website or application to complete their profile to unlock benefits or to avoid being locked out, the chances are that they will comply, as the sense of incompleteness trigger[s] the feeling of missing out on something in return… Many do not understand that social media policy agreements mention that their data can be given away [used] or sold." IP6 (Assistant Professor in Computer Science)

"The average users do not read the privacy conditions set by social networking sites which alert these users [about] what is required to subscribe to them [the SNS], or what of their information can be used for promotional purposes. And if they read them they do not care about their contents, because they will participate in those platforms anyway…" IP1

They noted that users do not want to go to the trouble or to spend their time reading privacy policies or user agreements:

"The majority of users do not really pay attention to the long pages of privacy policy, and if this happens with companies updating and asking people to accept or deny [a] new information sharing policy, they will accept regardless, even if this is bother[s] them and make[s] them worry about their information, because they do not want to delete their profile and move somewhere else [where] they know [or think] they can't find their colleagues and friends or family." IP15 (Director of a government agency)

"Evaluating users' – especially employees' – control over the privacy of their information can be sensitive. I personally would have to read LinkedIn's user agreement line by line – likewise [the user agreements of] other platforms – to ensure their limit of authorisation to my data and to what extent it's shared [with third parties] from it, and I accept accordingly when I control the access to my profile…" IP3 (Manager of an IT centre)

The IT Manager (IP3) expressed his opinion on rumours that such agreements and policies are not always true, but rather might just be a mechanism to avoid lawsuits as per the privacy act of the hosting country:

"First: the issue of lack of respect for privacy from companies is not an absolute fact that applies on all social media companies. Second: hypothetically, if the companies trade in your data, why not limit the risk [from that] and limit the trading of your data by others, such as websites and other programs and offenders [bad actors] when you are given the privilege of controlling that…. I mean, if some can get your information, why let everyone get it? … Consider the control of privacy feature: many do not, out of recklessness." IP3

IT Self-Efficacy

The *IT Self-efficacy* scale includes four items reflecting an individual's confidence level in their IT skills, with particular reference to their use of SNS. Chart 5-4 below shows the frequency distributions for the degree of confidence expressed regarding each item. Past research suggests that a higher level of self-efficacy can lead to a higher level of awareness and, therefore, to less risky behaviour in a social networking site environment. The levels of confidence in different digital and SNS-related skills were similar, with slightly lower levels of confidence in understanding terms used in SNS privacy policies and agreements (33% agreed).

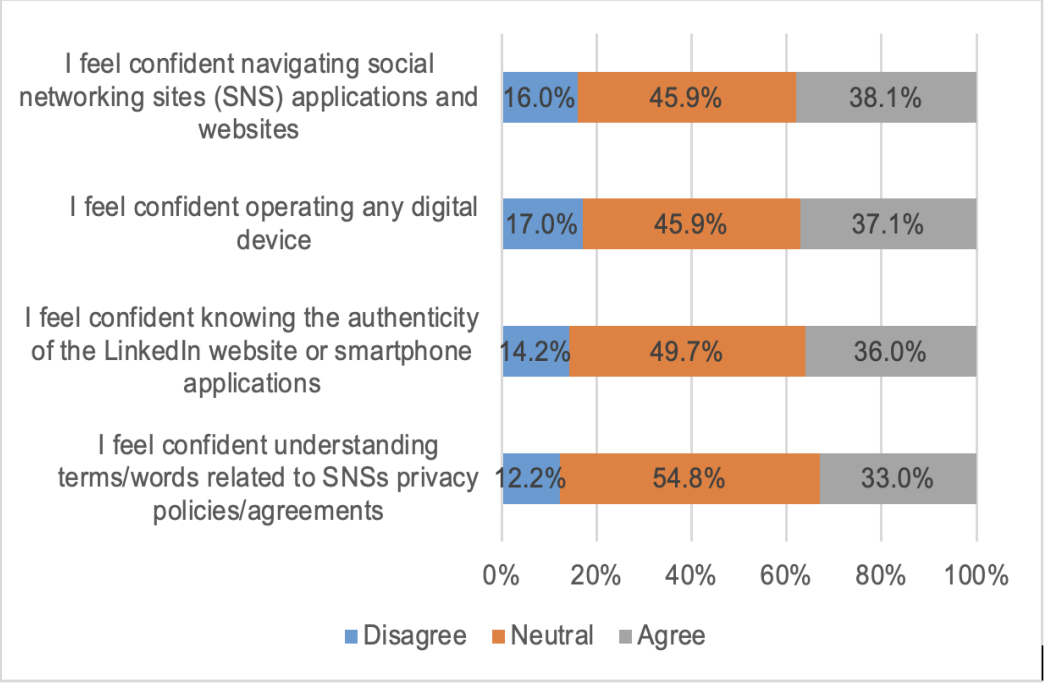


Chart 5-4 IT Self-Efficacy Factor

In line with the quantitative findings regarding IT self-efficacy amongst participating employees, interviewees have placed greater attention on users' IT/InfoSec competence, or their lack of it. As shown in the previous section, several respondents mentioned the importance of understanding terms related to privacy policies/agreements. The most salient responses of these interviewees are as follows:

> *"Computer literacy is a must when operating technologies over the internet for the average user, but this is not the case nowadays, not even [for] those who confidently claim to be experts in IT… Confidence is a rubbery term when it refers to one's*

[own] technological abilities… The question is, in what way and how far a user perceives themselves to be technically confident: [is their confidence] low or high?" IP6

Interviewees mentioned that fear/dislike of being perceived by their peers as incompetent may prevent some employees from admitting that they had low IT self-efficacy:

"Generally, employees claiming attentiveness and knowledge of privacy policy in addition to how one's own information is utilised is predictable, especially in the workplace, where no one likes to be seen [as] less competent. Control and know-how are two concerning factors for employee efficiency. Without the former, it will be perceived as inability and therefore is reported negatively in your [annual] review.]Not having] the latter [know-how] is perceived as ignorance and lack of cleverness and therefore [is also] reported negatively." IP12

"Other users who are showing awareness and knowledge of how or what of their information is handled or accessed aren't really accurate [about it] for the most part, in fact it is simply showing that [I am not ignorant]…" IP1

"the awkwardness of lower-level employees insisting to be perceived as professionals when they lack technical expertise cannot be favourable amongst their colleagues and managers, as it's threatening." IP12

One participant mentioned a financial consequence that resulted from his own inattention to a user agreement:

"…it can be a common thing to see patients neglect reading the prescription leaflet until side effects start showing. [Then] they call their doctor or read the leaflet. I recall once I'd been a [music social media app] premium subscriber for 4 years back in America, and when I decided to cancel my subscription, I intentionally neglected deactivating my subscription… because I knew at that time that my credit card had expired and I wanted to reconsider and organise all of my subscriptions after they got declined due to expiration. Even for accounts that I have but I'm not aware of at this point, which will eventually be sending me renewal emails to update

my card info… Two months later I figured that my music app premium account was still charging me from the expired debit card…" IP13

The incident related by IP13 above spurred this author to look up LinkedIn's user policy and agreement. Indeed, LinkedIn's user agreement (effective August 11, 2020) states under 2.3 Payment:

> *"We may store and continue billing your payment method (e.g., credit card) even after it has expired, to avoid interruptions in your Services and to use to pay other Services you may buy"* (LinkedIn, Policy Agreement)

Two interviewees mentioned potential consequences to organisations resulting from low IT self-efficacy among employees:

> *"Although social media privacy policies were made to protect them legally, it would be better for organisations also to seriously consider what it stipulates, [so as] to avoid technical errors made by its employees or when engaging with outsiders through it [SNS]. This can sometimes hurt the reputation of the organisation in these platforms, especially when sensitive information gets in the hand of cyber criminals … Employers should motivate the untechnical savvy employees to become accustomed to read and understand these policies as well as enhancing their computer skills for a better security behaviour, a better control of their data and understand their limitations. Unfortunately not many have time to read it all or comply"* IP12

> *"I think anyone can fall victim to a phishing attack, regardless of that person's behaviour or personality or their position at the company. Cyberattacks are developing constantly; read the news, you will find even experts in security networks get [their computers] penetrated by one of their employees. You can only reduce [not eliminate] vulnerability."* IP15

5.3.3 Risky Habitual Behaviour

As described in Chapter Three, this study examined three factors of risky habitual behaviour: *information security habitual behaviour*, *level of engagement* and *frequency of*

SNS use at work. The *information security habitual behaviour* and *level of engagement* factors were measured using multiple item questions measured on seven-point scales (1 – Never, 7 – Always). *Frequency of SNS use* was also measured on a seven-point scale (1 – Never, 7 – Open all time). These constructs representing risky habitual behaviours were analysed by averaging out the corresponding survey items (accounting for the fact that some items needed to be reverse-scaled). Higher values correspond to employees engaging in risky behaviour, who are thus exposed to potential CSE attackers as discussed under the heading of Lifestyle/Routine Activity Theory in section 3.1.1. Summary statistics for each of the scales adapted to examine employees' risky habitual behaviours are presented in Table 5-11 and visualised in Figure 5-2.

Table 5-11 Summary statistics for Risky Habitual Behaviour scales composite scores (N = 394)

Risky Habitual Behaviour Factor	Mean	SD	Min.	Percentile 25	Median	Percentile 75	Max.
Risky Habitual Behaviour: *Information Security* (1 – highest information security habitual behaviour, 7 – lowest information security habitual behaviour)	2.28	1.21	1.00	1.30	1.90	3.00	6.60
Risky Habitual Behaviour: Level of Engagement (1 – lowest level of engagement, 7 – highest level of engagement)	2.72	1.42	1.00	1.60	2.20	3.60	6.80
Risky Habitual Behaviour: Frequency of SNS Use at Work (1 – Never, 7 – Open all the time)	3.85	1.65	1.00	3.00	3.00	4.00	7.00

These results show that respondents in general do not engage in habitual risks, which is indicated (in Figure 5-2) by the left-skewed distributions (longer right tail, mean exceeds median for all three scales) with the prevalence of values below 4 points out of 7 (75^{th} percentile does not exceed 4 for any of the scales).

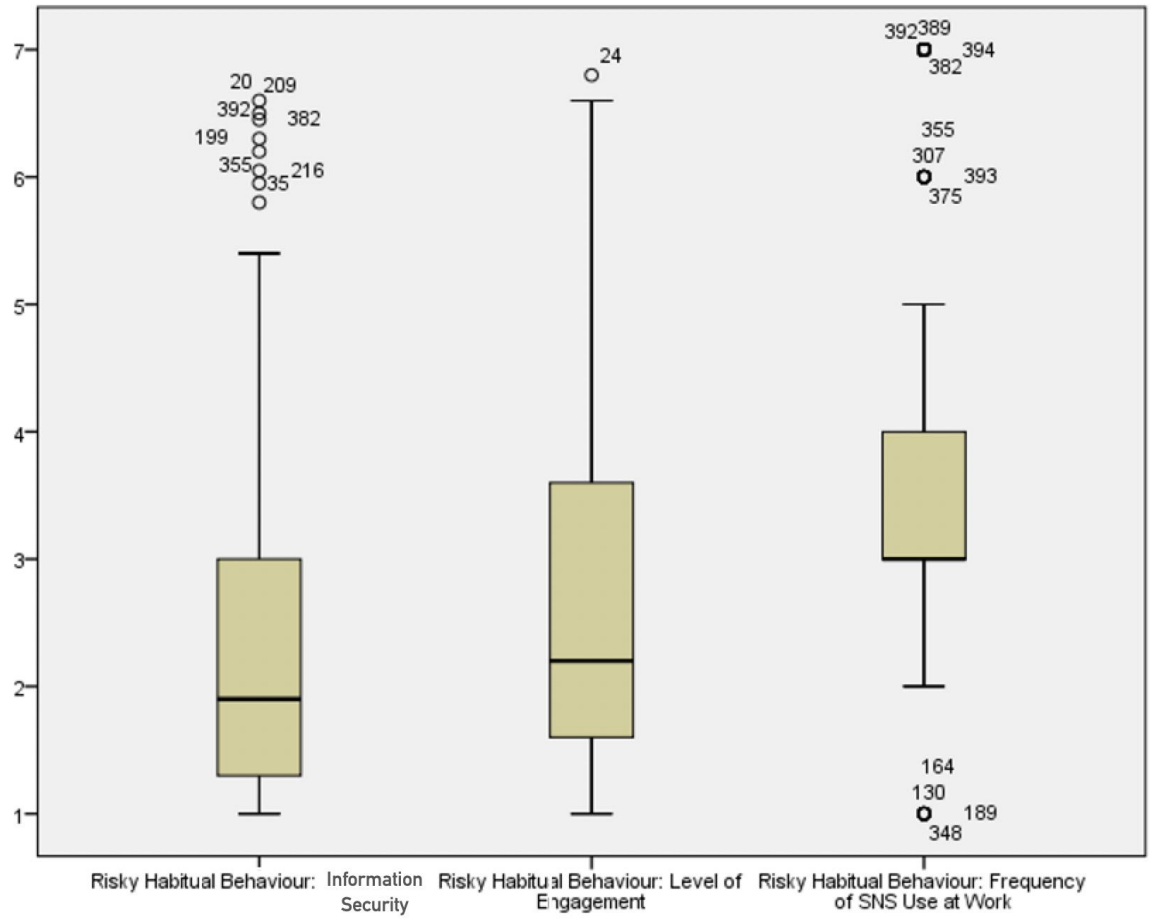


Figure 5-2 Risky Habitual Behaviour scales distribution: boxplots

Each 7-point response was recoded into three levels for ease of interpretation: never, irregularly (once/twice or three times/a few times per month/) and regularly (at least once a week). The following sections present the prevalence of each of these groups for each of the risky habitual practices.

Information Security Behaviour

The *Risky Habitual Behaviour: Information Security* scale consists of 20 items that are relevant to risky practices that employees might have engaged in during the previous 6 months. Chart 5-5 below shows the frequency distributions for the occurrence of each practice.

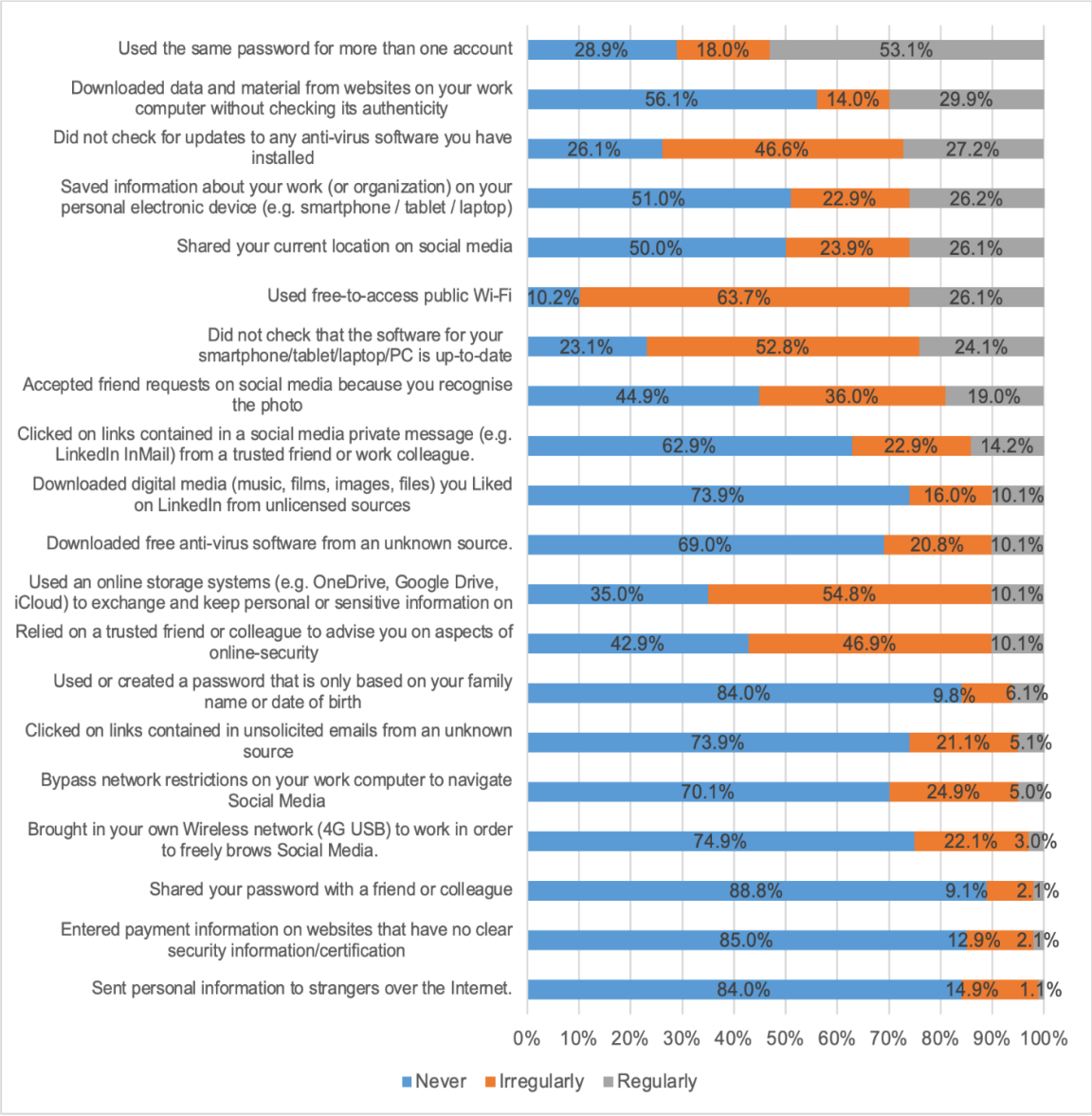


Chart 5-5 Risky Habitual Behaviour: Information Security Factor

Assessment of reckless behaviour helps in determining an employee's weaknesses that increase their likelihood of being susceptible to CSE victimisation. It was found that most respondents never sent personal information to strangers over the Internet (84%), used trivial passwords (84%), entered payment information on unsecure websites (85%) or shared their password with a friend or colleague (89%). The most common risky practices were using the same password for more than one account (53% of respondents do it regularly), downloading data and material from websites on their work computer without checking its authenticity (30%), as well as saving information about their work on their personal devices (26%), sharing their current location on social media (26%) and using free-to-access public Wi-Fi (26%).

Interview participants elaborated on the reasons that users might engage in certain risky IS behaviours:

> *"Saudis, both male and females, are alike in terms of being attracted to the ongoing innovations and technology diffusion among the community – especially for the youngsters… Everyone wants to be involved; if not participating, they want to see what is going on. And so many of them, when intrigued, care about how to get there [into these sites] quickly. And over time they realise that they have multiple accounts starting to pile up here and there, and consequently, [they] choose easy and identical passwords to log in swiftly, overriding necessary common information security behaviours."* IP5

> *"Rumours spreading between users in the society within messaging applications such as WhatsApp and microblogs such as Twitter… can indeed drag those youngsters – and older people alike – to join these SNS platforms to find out more about what is this all about, or the source of a trending controversial topic. Once they are in they are hooked, and gradually spending more time on their smart phones to see – out of curiosity, of course – what these SNS platforms have to offer… Young users, especially, are more attracted to scandals, and through it they swallow the bait [set] by scammers."* IP6

When asked about if such behaviour can exist in the workplace or amongst colleagues, the same interviewee responded:

> *"There are codes of conduct that we and everyone else in the offices should be aware of, however the way each one takes IT [security] precautions seriously is still unclear … but I can assure you that many around me rely blindly on the department overseeing the network here at the university in terms of updates, different types of firewall… I am aware that some still use the work[place] high-speed internet to download [to their laptops] software and movies using file-sharing protocols like BitTorrent which can be infested with viruses before they leave [the office for the day]. While [in other cases] some organisations have access restrictions and so employees bring their own Wi-Fi SIM… browsing SNS platforms for hours, searching for what interest them is out of boredom."* IP6

Another participant also reflected on how employees' IS behaviour can inadvertently be a vector for cyberattacks:

> *"Any system designed on the assumption that the user will make the appropriate decision to protect it is a weak system, and its usefulness and effectiveness will be very limited… Not every employee is a computer expert. Keeping in mind the language used when installing these software and applications… Sometimes such a decision can be a flaw, putting the system and data at risk of [attack by] hackers because of users' ignorance at times, or underestimating threats at times, or adapting low security measures believing that if harm can happen it will affect only them and not the system which they are accessing – that [flawed decision] invites attacks into an intranet network."* IP7

Regarding risky IS behaviour, IP7 added:

> *"Many users do not activate their two-factor authentication method… Such behaviour can lead to their social media profile be stolen and [they are] locked out of it [their account]. Then through it, criminals launch social engineering scams on others... My advice to my employees in the cyberworld is to never think well of people online, or of any URL links they receive. It is better to always doubt everything or action you are about to take… The cyberworld is massive and intangible, many users underestimate the negative outcomes; this is why they still use weak passwords. But such [proper information security] behaviours should be enforced and guided, like using long and difficult passwords. These users in organisations think they are a being protected by the network experts and rely on anti-virus [software], even though they never check if it's up to date. [On the contrary,] this will give them an impression that they do not need to pay attention to their mistakes when they click on a phishing link, because the antivirus will fix the problem."* IP7

Level of Engagement

The *Risky Habitual Behaviour: Level of Engagement* scale includes 5 items reflecting the respondents' security behaviours and the extent of their activities while engaging with features and/or peers over social networking platforms. High engagement with these

practices indicates low levels of caution and is characteristic of risky behaviour. Chart 5-6 below shows the frequency distribution.

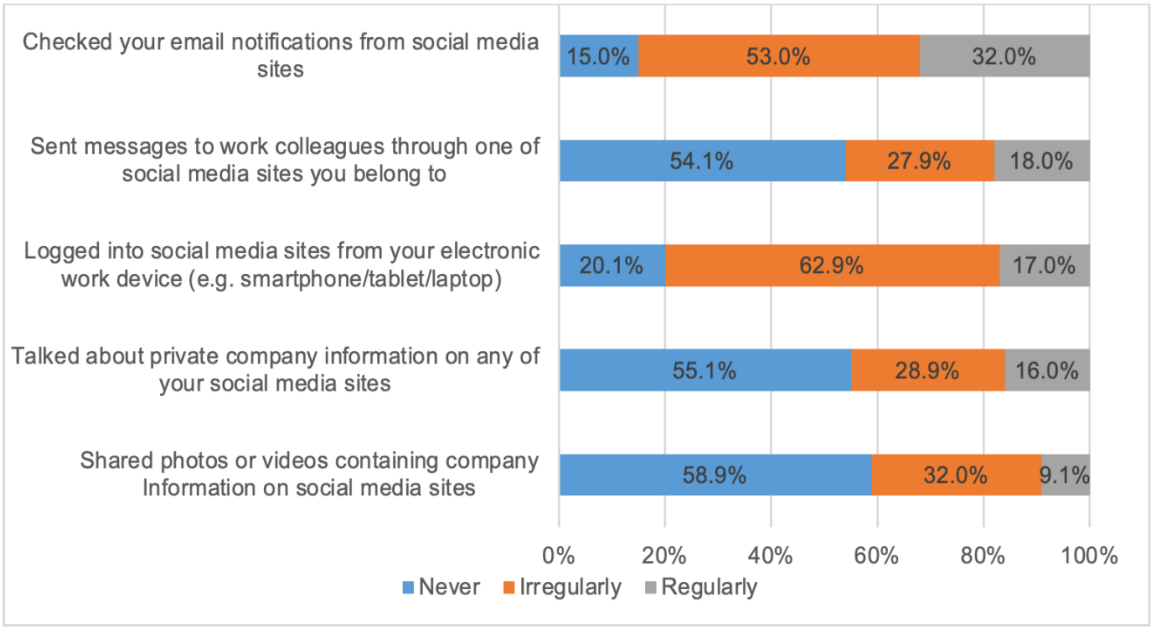


Chart 5-6. Risky Habitual Behaviour: Level of Engagement Factor

Nearly one-third (32%) of respondents regularly check email notifications from social media sites. This behaviour increases cybersecurity risks, because such notifications often contain phishing links. While over half of respondents never send messages to work colleagues through social media sites, 18% of respondents do so regularly, which is also associated with risky behaviour. A similar percentage (17%) reported logging into social media sites from work devices. Over half of respondents avoided talking about private (confidential) company information (55%) or sharing photos or documents containing company information on any social media sites, but a substantial proportion of participants reported doing so at least occasionally.

Frequency of SNS Use

Risky Habitual Behaviour: Frequency of SNS Use was measured by asking participants about the number of times they normally use their professional SNS account while at work (1 – Never ,7 – Open all the time). Almost all respondents (96.2%) use SNS at work at least sometimes, whereas 24.4% of respondents do this regularly. Only 3.8% never use SNS while at work.

The significance of demographic differences (by gender, age, nationality and work level in the organisation) in each of the three components of risky habitual behaviours was tested using parametric (ANOVA) and nonparametric tests (Kruskal-Wallis). No statistically significant differences were found for age, nationality or work level, but statistically significant gender differences (at the 5% significance level) were found in the levels of Information Security (Table 5-12).

Table 5-12 Risky Habitual Behaviour *scales: significance testing of demographic differences*

Scale	Grouping variable	ANOVA significance test	Kruskal-Wallis significance test
Information Security	Gender	F(1, 392) = 3.968, **p = .047**	χ^2 (1) = 4.064, **p = .044**
Information Security	Age	F(4, 389) = 1.127, p = .343	χ^2 (4) = 5.564, p = .234
Information Security	Nationality	F(1, 392) = .670, p = .414	χ2(1) = 0.257, p = .612
Information Security	Work Level	F(2, 391) = 1.041, p = .354	χ^2 (2) = .384, p = .825
Level of Engagement	Gender	F(1, 392) = 3.968, p = .841	χ^2 (1) = .009, p = .923
Level of Engagement	Age	F(4, 389) = .764, p = .344	χ^2(4) = 3.065, p = .547
Level of Engagement	Nationality	F(1, 392) = 3.457, p = .064	χ^2(1) = 3.170, p = .075
Level of Engagement	Work Level	F(2, 391) = .584, p = .558	χ^2(2) = .522, p = .770
Frequency of SNS Use at Work	Gender	F(1, 392) = 3.968, p = .421	χ^2(1) = .715, p = .398
Frequency of SNS Use at Work	Age	F(4, 389) = .564, p = .345	χ^2(4) = 1.59, p = .811
Frequency of SNS Use at Work	Nationality	F(1, 392) = .713, p = .399	χ^2(1) = .374, p = .541
Frequency of SNS Use at Work	Work Level	F(2, 391) = 1.545, p = .215	χ^2(2) = 1.673, p = 0.433

Further analysis (see Table 5-13) shows that males have a higher level of risky habitual behaviours as measured on the information security scale (M = 2.07, SD = 1.09 for females and M = 2.35, SD = 1.25 for males, $p < 0.05$ according to both ANOVA and Kruskal-Wallis tests). Among individual items related to information security habitual behaviour, males, on average, reported higher reliance on a trusted friend or colleague to advise on aspects of online security, as well as being more likely to download free anti-virus software from an unknown source. They are also more likely to save information about their work (or organisation) on their personal electronic device (all p-values < 0.05 according to both ANOVA and Kruskal-Wallis tests).

Table 5-13 Gender differences in the Risky Habitual Behaviour: Information Security Habitual Behaviour *scale and individual items within the scale*

Risky Habitual Behaviour (Information Security Habitual Behaviour)	Gender				Tests of Significance	
	Female (N = 99)		Male (N = 295)			
	Mean	Standard Deviation	Mean	Standard Deviation	ANOVA	Kruskal-Wallis
Risky Habitual Behaviour: *Information Security* (1 – lowest risk, 7 –highest risk)	2.07	1.09	2.35	1.25	F(1, 392) = 3.968, **p = .047**	$\chi^2(1)$ = 4.064, **p = .044**
In the past 6 months relied on a trusted friend or colleague to advise on aspects of online security	1.97	1.41	2.44	1.61	F(1, 392) = 6.827, **p = .009**	$\chi^2(1)$ = 8.728, **p = .003**
In the past 6 months downloaded free anti-virus software from an unknown source	1.51	1.16	1.98	1.72	F(1, 392) = 6.641, **p = .010**	$\chi^2(1)$ = 6.459, **p = .011**
In the past 6 months saved information about your work (or organisation) on your personal electronic device (e.g. smartphone / tablet / laptop)	2.29	1.98	2.79	2.06	F(1, 392) = 4.398, **p = .037**	$\chi^2(1)$ = 6.264, **p = .012**

Asked about risky habitual behaviour on SNS, one participant responded by first listing what he viewed as positive aspects of social media:

> *"…reducing barriers that hinder communication, opening doors to exchanging opinions, expanding opportunities to participate in the expression of opinion and expanding the circle of social relations."* IP8

He then presented what he saw as negative aspects of using SNS:

> *"… risks of fraud or identity theft and the invasion of virtual communication networks for privacy and harassment in all its forms, along with inappropriate content and spreading rumours. … what lies behind these negatives [is] addiction, which is due to gradually increasing the hours spent [on] social media sites or the frequent overuse of social networks without professional or academic necessity."* IP8

Another interviewee remarked that even though people might think of using CSNS as less risky than general SNS, the negative aspects of CSNS can be just as harmful:

> *"[they think] that they are different and the majority of users become addicted to them so that they spend most of their time on mobile devices and I see these*

everywhere I go around me at work. … I tried to leave all sorts of engagement to these social networking platforms for a while, but I went back to it with more strength when I kept following up on my status on a scholarship program pending the results. I went on every social media platform and created a profile to see what others who are in my situation have to say about it, or any possible leaked updates out there. I really wish to find some healthy way to get rid of this bad habit and dependence, which many times has caused my personal information to be leaked unintentionally and increased my procrastination in completing my essential work." IP9

When asked about what sort of information leaked, her response was:

"Oh, I can give you a number of examples [that] happened to friends and family, but some time ago and unbeknownst to me, a stranger started texting me to my WhatsApp from an international number. He or she – I am not sure of their gender – kept me nervous for days for knowing my full name and other information [while] I didn't know who he/she was. And then [that person] started to threaten me. After [that] I realised [this was] much more [dangerous] than I thought… I reported this person to the police. I knew [learned] later that the person might have searched for the same username I used on Twitter…which I never use my real name on, or a photo of myself, but [the person] could have found the same username associated to my Instagram account, although private but my name [is] showing, and then could have googled it and found my obsolete and forgotten Bayt.com profile [CV]. He could have used NumberBook [a caller ID application] to look up my number using my name." IP9

When asked about how individual users' risky practices could have a negative impact on their private information, and risk of its misuse by cyber offenders, IP15 explained:

"Recruitment platforms, like for instance … LinkedIn, will not be seen other than [as] a platform for advertised jobs or linking and communicating with business owners and experts for personal and professional benefits. I do not think that it represents a great risk just because your profile is stolen! Because the danger does not lie in tampering with information you show or conceal; the danger, rather, is how your profile can be used as an attack tool to the [other] connected

members, or [knowing] the password you are using, as it can be the same in more critical and sensitive accounts such as work emails and Facebook. [This is] because their privacy risks are higher than simply showing the workplace, experiences, or the university from which you graduated." IP15

5.3.4 Demographic and Cultural Factors

The significance of demographic differences (by gender, age, nationality and employment level in the organisation) in each of the four factors was tested using parametric (ANOVA) and nonparametric tests (Kruskal-Wallis). No statistically significant differences were found for age, nationality or work level. There were statistically significant gender differences (at the 10% significance level) found in the levels of *willingness to assume risk* (Table 5-14). Males had a higher level of willingness to assume risk (M = 3.67, SD = 1.49 for females and M = 3.96, SD = 1.49 for males, $p < 0.10$ according to both ANOVA and Kruskal-Wallis tests). Among individual items related to willingness to assume risk, on average, males reported higher willingness to take substantial risks to actively engage with services and features provided on LinkedIn, as well as being more likely to share their personal information if a LinkedIn post (e.g., job offer, contract, agreement) involved a small amount of risk. Males also reported being more open to using an unfamiliar professional SNS than females (all p-values < 0.10 according to both ANOVA and Kruskal-Wallis tests).

Interview data supported the some of the quantitative findings, as described below. Participants did not mention age as a factor in relation to CSE risk. When asked about the influence of nationality in relation to risky habitual behaviour, IP1 suggested that it did not play an important role, and explained that other factors were more influential:

The Saudi people are just like [people] anywhere else in the world, [you] have the good and bad, the question is not about their behaviours or character, it is more about their experience in using social media and their awareness and most importantly the situation, these are tools of communication, which involves viruses and penetrations of data and stealing your money when you respond to the wrong and deceptive people. IP1

Table 5-14 Gender Differences in the Willingness to Assume Risk *Scale and Individual Items Within the Scale*

	Gender					
	Female (N = 99)		Male (N = 295)		Tests of Significance	
Items	Mean	SD	Mean	SD	ANOVA	Kruskal-Wallis
Willingness to Assume Risk (1 – lowest, 7 –highest)	3.67	1.49	3.96	1.46	F(1, 392) = 2.909, **p = .089**	$\chi^2(1) = 2.716$, **p = .099**
I am willing to take substantial risks to actively engage with services and features provided on LinkedIn	3.53	2.00	3.97	2.14	F(1, 392) = 3.349, **p = .068**	$\chi^2(1) = 2.974$, **p = .085**
I am willing to accept some risk to my personal information if a LinkedIn post (e.g. job offer, contract, agreement) involves a small amount of risk	3.46	1.98	3.93	2.07	F(1, 392) = 3.808, **p = .052**	$\chi^2(1) = 4.031$, **p = .045**
I am NOT more comfortable using familiar professional SNS than something I am not sure about	3.60	2.10	4.03	2.17	F(1, 392) = 3.027, **p = .083**	$\chi^2(1) = 2.926$, **p = .087**

The qualitative data strongly supported the quantitative findings regarding this relationship. Interview respondents unanimously believed that gender differences play an important role in the level of risk propensity: specifically, male employees were viewed as more willing to take risks than were females, as shown earlier, in the excerpts in Section 5.3.2.2. Unsurprisingly, the way in which female interviewees described this phenomenon differed from the way their male counterparts presented it. Women participants tended to emphasise the socio-cultural reasons behind the gender differences regarding willingness to assume risk. IP10 explained risk propensity from the point of view of women in Saudi Arabia. She stated that despite recent changes in the country's laws and policies:

> *"…to help equalise women's opportunities and rights with men …many Saudis are rooted by strong ties with their religious and cultural values that make women still favour being two steps away from their men, which explains that women's limitations are still accepted by choice and that exceeding their limit is not always an option to partake or a decision they make on their own… To many women here the notion of taking the exact responsibilities as men and doing things on their own can be intimidating, as it can be perceived [as transgressing] beyond the time-honoured accustomed habits."* IP10

Another female participant, IP14, posited this explanation of how men of Saudi nationality approach risk:

> *"It is highly likely that those who fall into fraud are Saudi men more than women. This is because men are perceived as the tentpole of the family, and within the society they are the ones who take responsibilities for the benefit of the family. They are generally expected to deal with personal and family expenses and needs, and deal with the challenges they are facing. Being under the load of responsibility makes them make decisions quickly and restlessly and therefore take actions quickly [too]… One reason why most men in KSA fall victim [to CSE] is [they are] driven by their willingness to be in front of the line, to respond and to engage and [be] more assertive than women, especially in a patriarchal society. However this is diminishing gradually, and women are now holding higher positions in authority with the new government."* IP14

5.3.5 Motivational Factors

Two motivational factors, professional advancement and self-presentation, were measured on multiple item questions.

Professional Advancement

This construct is measured using a five-point scale (1 - never, 2 - rarely, 3 - sometimes, 4 - often, 5 - always) of professional development online activities, consisting of 10 items measuring how often participants used LinkedIn for purposes related to sharing work-related curriculum vitae information, networking with other professional contacts and obtaining peer support from others. A professional advancement score was computed as the average of the 10 items and a series of ANOVA and Kruskal-Wallis tests was conducted to test for significant differences among groups of respondents, based on gender, age, nationality and work level. This analysis indicates that non-Saudis were significantly more (ANOVA $p = .017$, Kruskal-Wallis $p = .019$) actively involved in professional development communication on LinkedIn ($M = 2.61$, $SD = 1.03$) compared to Saudis ($M = 2.25$, $SD = 1.00$). Non-Saudis were more likely to connect with potentially helpful professionals, follow other companies, share their CV to other companies, and share and accept various files more often than were Saudis (Table 5-15).

With regard to those 5 items on which there was a significant difference in professional advancement scores based on nationality, a Saudi professional provided a possible explanation:

> "*…the sense of job insecurity, exists more within expatriates than with Saudis. Saudis feel more secure and sure that they will attain a job eventually…*" IP15

A non-Saudi gave his perspective on how he utilised LinkedIn:

> *"I used to not be active on LinkedIn, but now as part of my work involves SEO – search engine optimising – I am more active than ever, and have more than 500+ connections. Most of these I prefer to approach and approve requests from others on the basis of sharing the same interests as mine… And sometimes [if they] graduated from the same college, [or they have] work experience in the same company… But I also love to add people who are experts to learn from."* IP8

However, even Saudis have engaged in some of these practices when they felt the need to:

> *"Nearly four years ago I was unemployed and was desperately looking for a job until I received [what appeared to be] a highly-paid job offer from an oil company in East Africa. At the beginning, close friends had so many doubts, but I couldn't resist the appealing chance. I decided to request further information and contacted the company headquarters to make sure of the opening. They did in fact confirm, and so I proceeded with the gentleman on LinkedIn representing the company as an HR specialist, until at a later stage [3 weeks later], he requested a small amount of cash in dollars for administration expenses… I then blocked his profile and reported it. But it had took me a while to come to this decision as I was very optimistic because of my need."* IP2

Table 5-15 Professional Advancement *Online Activities by Nationality*

Items	Total		Nationality				Tests of Significance[1]	
			Saudi Arabia		Non-Saudi (Expatriate)			
	Mean	SD	Mean	SD	Mean	SD	ANOVA p-value	Kruskal-Wallis p-value
Connected with professionals that could help you with your professional advancement	2.35	1.40	2.28	1.37	**2.75**	1.49	0.025	0.029
Followed other companies that you believe could increase your professional advancement	2.30	1.30	2.24	1.28	**2.67**	1.37	0.025	0.023
Shared your work-related CV to companies which you believe could help you with your professional advancement	2.22	1.33	2.17	1.31	**2.58**	1.39	0.038	0.045
Shared your work-related CV with professionals with whom you feel can help with your professional advancement	2.30	1.33	2.25	1.32	2.60	1.36	0.081	0.073
Accepted connections from connections whom you don't know but can see that they have many connections themselves	2.29	1.37	2.25	1.37	2.54	1.39	0.160	0.154
Accepted network connections from connections who are connected to your connections	2.25	1.35	2.24	1.35	2.35	1.33	0.596	0.531
Accepted a connection requests on LinkedIn because you recognised the photo	2.38	1.38	2.34	1.38	2.65	1.41	0.123	0.096
Messaged your connections for support in career or work-related matters	2.33	1.42	2.28	1.41	2.63	1.43	0.093	0.072
Shared documents, audio, or video with connections in order to assist you with a problem	2.28	1.43	2.21	1.42	**2.71**	1.46	0.018	0.011
Accepted documents, audio, or videos from connections in relation to receiving support from them	2.32	1.41	2.27	1.42	**2.60**	1.32	0.125	0.039

[1] *p*-values < 0.05 are highlighted.

As shown in Table 5-15, Saudis and non-Saudis did not differ significantly on 5 of the 10 items, namely: *Shared your work-related CV with professionals with whom you feel can help with your professional advancement*, *Accepted connections from connections whom you don't know but can see that they have many connections themselves*, *Accepted network connections from connections who are connected to your connections*, *Accepted a connection requests on LinkedIn because you recognised the photo* and *Messaged your connections for support in career or work-related matters*. Interviewees provided insights as to the reasons behind the commonality of these attitudes and motivations:

> *"LinkedIn, like many other platforms, is another channel for Saudis, men and women alike, to strive to boost their chances of professional opportunities, and to*

feel close to those decision makers and celebrities in all sorts of professions. In Saudi culture, recruitments have always been linked to "wasta" – Arabic for nepotism. LinkedIn and other career SNS platforms had made it possible for those to connect with human resources specialists and government authorities in hopes of benefitting from whatever career chances there might be… This is a country that has mostly been formed on tribal families; it is common to perceive that conflict of interest involving tribal bonds with regard to employment do exist…. Similarly, users could unthinkingly and feel more comfortable to connect and accept requests from those sharing the same surnames or any other type of affiliations, like for example, a person with the last name X connects with another whose last name is X." IP1

"Normally I link to people who I know personally. And if I see a mutual interest is present and demanding at some point during my career, I'd rather link with those with whom I share other connections of my own… It's more comfortable. …Regardless of whether their photo is visible or not, what matters to me is their position and what they share in their content that can enhance and [seem] inviting to share my thoughts and opinions within their timeline." IP9

"Many users are attracted to those who share their interest[s]. Also, they like to make connections with those who look like them in many ways. For example, I like to link and follow those who like Iraqi poems, or experts and geography and environmental behaviouralists, to be specific. I know colleagues who like to link to those who are of the same family, to exploit [this] similarity point in hopes of relocating to a better position in a better place. Such behaviour [results in a] toxic environment to others, but it does unfortunately exist, and at last and absolutely… women." IP15

Self-Presentation

The binary scale of self-presentation consists of 13 yes/no items that measure how much information respondents have put online. The more information that is exposed online, the more information there is for creating a compelling fake profile or other undesirable cyber-

intervention. A self-presentation score was obtained by calculating the proportion of items put online (minimum = 0, maximum = 100) and a series of ANOVA and Kruskal-Wallis tests were conducted to test for the significance of differences among groups of respondents, based on gender, age, nationality and employment level. The average self-presentation score is 44.8%. At the 5% significance level, no demographic differences in this score were found, but at the 10% level self-presentation is significantly higher (ANOVA p = .079, Kruskal-Wallis p = .053) for non-Saudis (M = 51.0, SD = 23.3) than for Saudis (M = 43.9, SD = 27.9). Some differences in individual items are significant at the 5% level: non-Saudis put their certificates and work telephone number on their LinkedIn page more often than Saudis (Table 5-16)

Table 5-16 Self-presentation *Information Placed Online by Nationality*

Items	Total	Nationality		Chi-square test of association p-value[1]
		Saudi Arabia	Non-Saudi (Expatriate)	
company (or organisation) logo	80.2%	79.8%	82.7%	.629
put licences on	70.1%	68.4%	80.8%	.070
put work telephone number on	62.9%	60.8%	76.9%	.025
put certificates on	58.6%	56.7%	71.2%	.049
set profile to "public" so anyone can view it	47.7%	46.8%	53.8%	.342
created an "About me" page	38.6%	37.4%	46.2%	.228
put educational history on	37.6%	36.5%	44.2%	.287
put where currently worked	35.0%	34.2%	40.4%	.385
put a profile picture	33.8%	34.8%	26.9%	.263
revealed or updated current location	32.5%	31.9%	36.5%	.503
put work experience history on	28.9%	28.4%	32.7%	.521
put work email address on	28.7%	27.8%	34.6%	.310
put job title	27.9%	26.6%	36.5%	.137

[1] p-values < .05 are highlighted.

A participant who holds a managerial position in the public sector suggested a specific connection between self-presentation and the motivation for professional advancement within an organisation:

> *I believe it is a rule of thumb for those at higher levels in companies and organisations to familiarise themselves with technical and administrative updates and developments in order to sustain [last longer or] preferably [advance] further in their positions, along with keeping strong ties with the most important members of the organisation… This will impact on the rest of entities in the organisation,*

especially [with]in lower levels, to motivate performance and in return respond to such developments by presenting themselves as worthwhile for the next higher position involving much more important tasks and consequently provoke them to be obedient to stand out among the rest…in a way they are saying look at me, I know better, I deserve more!" IP3

Another interviewee described how the motivation for self-presentation might be manifested on LinkedIn:

"some employees do not necessarily pay attention to whom they are connecting with as long as their [that other user's] profile is portrayed as someone who is professional or a [member of one's own community]. And sometimes their profile photo [falsely] represents a social media star [identifiable from mainstream media] or sometimes poses the sense of authority because of their high credentials and endorsements or a beautiful woman." IP10

5.3.6 User Susceptibility

To figure out whether respondents could be susceptible to cyber-social engineering victimisation attacks that can be traced back to their use of LinkedIn, participants were asked a Yes/No self-report question:

"*In all the time since you have been using LinkedIn have you ever had something bad happen to you (at your work or in your personal life) that you can trace back to your usage of LinkedIn?*" 24.1% of all respondents responded positively to this question. According to the chi-square test results (Table 5-17) males were more likely to have experienced a negative event on LinkedIn than were females (28.1% of males compared to 12.1% of females, $p < 0.001$), while Saudis were more likely than non-Saudis (26.0% vs 11.5%, $p = 0.023$). The results also indicate that the higher the employment level of the employee in the organisation, the less likely respondents were to report negative experiences (28.5% of lower-level employees, 11.8% of middle-level employees and only 7.1% of top-level managers). No statistically significant association between age and susceptibility to CSE victimisation was found; although sample estimates suggest that employees aged 51+ were less susceptible to online attacks in CSNS, the sample size was insufficient to claim that this effect was significant.

Table 5-17 Experience of Online Threats Associated with CSNS Use by Demographic Group

Demographic Group		In all the time since you have been using LinkedIn, have you ever had something bad happen to you (at your work or in your personal life) that you can trace back to your usage of LinkedIn?				Chi-square test of association
		No		Yes		
		Count	Row N %	Count	Row N %	p-value[1]
Total		299	75.9%	95	24.1%	
Gender	Female	87	87.9%	12	12.1%	0.001
	Male	212	71.9%	83	28.1%	
Age	18 - 28	19	67.9%	9	32.1%	0.185
	29 - 39	198	75.3%	65	24.7%	
	40 - 50	31	70.5%	13	29.5%	
	51 - 61	15	78.9%	4	21.1%	
	62 and over	36	90.0%	4	10.0%	
Nationality	Saudi Arabia	253	74.0%	89	26.0%	0.023
	Non-Saudi (Expatriate)	46	88.5%	6	11.5%	
Work Level in Organisation	Administrative Officer / Assistant (Employee)	211	71.5%	84	28.5%	0.002
	Department management/Section supervisor or designee	75	88.2%	10	11.8%	
	Top-level management or designee	13	92.9%	1	7.1%	

[1] *p*-values < 0.05 are highlighted.

Participants were also given the option to elaborate further, in an open-ended follow-up question: *"If you have answered yes to the question, could you briefly explain what happened and how you knew what you did on LinkedIn was the reason?"*

44 respondents explained what happened. Even though the types and consequences of cyberattacks varied widely (viruses, hard drive crashes, creation of fake accounts using the respondent's personal information, stealing of payment details, etc.), most sources of cyberthreat fall into one of a few categories. Of the 44 respondents, the breakdown is: phishing links sent in messages or through messengers (46%); phishing emails with links (13%); fake job invitations to get personal/payment information from applicants (13%); using personal information to create fake profiles (7%); paying for fake products and services online (9%); requests to upload documents containing personal information (5%); or to download and open files, which causes various problems (5%).

Data from the interviews provided insights on some of the survey findings. Respondents were asked whether personality traits could indeed be reflected over SNS or CSNS, or generally over cyberspace, when threat is involved. One interviewee said she believed so:

"Yes, people's characters can be reflected in [their interactions in the] virtual world, yet they should be very careful and ignore [i.e., avoid] the risk. Not by following their intuition, as it's prone to errors, but by following guidelines for safer online surfing set by the SM platform, government information security body and banks… Unfortunately, some people do become victims of a [cyber] threat just because who they are – either too nice, too curious or simply ignorant." (IP1)

However, other participants believed otherwise, and said that in an online setting when faced with cyber threats, factors in offline and online settings differed:

"Not necessarily. People feel much safer online and naturally be themselves in how they operate. A careful individual in society can be as is, or sometimes less [careful] when surfing the net, given the rules and regulations they are used to in real world… there are factors and events that can operate differently in each setting. When I say events, I mean financial difficulties, culture shock, need to vent or express with others of the same group, marital status… But for a cautious individual the difference lies only on the timeframe, as he/she can take more time to respond to a deceptive potential [significant other] due to hesitations … while a desperate [individual] can fully engage with the wrong people and eventually [be] scammed or blackmailed." IP2

"Many individuals in an online context behave differently than when they are in real life. Their personalities can function differently when in a face-to-face situation as all of their senses are present, such as eye contact and/or facial expressions movements. [These] can be crucial to judge credibility … body language can serve as a better instrument to draw a conclusion, especially when they are talking to a potential deceiver… This can be a different case in an online setting, even for the same person with the same personality." IP6

When asked to give examples of how an individual can have different dispositions on CSNS communications versus real time employment (offline):

"For example a SNS user who's known for a particular behaviour or personality can have different reactions, and judgment skills are employed differently when they engage in reality with others and when they engage in the virtual world. Face-to-face recruitments can reveal a lot more for the job seeker to ensure what is

perceived to be a bona fide recruitment process…but given the current situation with the pandemic which... has increased reliance on digital technology… this can be a challenging task. Impersonation of familiar faces is easily done in replicated profiles, and sometimes even in a video call [it] can also be possible with deep-fake technology. Such [an] individual can have different judgements in both [online and offline] situations." IP6

Another participant had a different opinion about users' personality traits as a factor predicting susceptibility to CSE. He suggested that, rather than accounting entirely for a user's susceptibility on SNS, the relationship between susceptibility and personality traits could be mediated by the SNS environment.

"there are individuals who … have thousands of connections or followers, they can be influential either because of their popularity or because they are sweet-tongued [persuasive]. When a new user encounters them they get the impression that they [these influencers are] always right, especially when they see almost everyone seems to cheer them on or endorse them and circulate their content all around. The receiver[user] here even though he/she would hesitate or disagree with them, unconsciously will align to them [in order] to be accepted and feel welcomed, and not eventually get ignored or blocked. I don't believe this is to do with their personality alone; rather, the environment could stimulate other cognitive factors that together [with personality traits] direct to a certain behaviour based on the [user's] need, … what they are looking for, like entertainment, discussion, or even job groups. If you [as a follower of these influencers] undermine them constantly, you will be blocked and lose the chance of being part of a larger group." IP15

The example described by the interviewee above can certainly cultivate social proof, which is a persuasion principle and a common tactic of SE.

Two interviewees reflected that for non-Saudis, the risk might be compounded by their tenuous status as foreign workers in Saudi Arabia:

"…the resident [expat] renews his/her contract approximately annually. The annual bonus is linked to his/her performance, even in government institutions. Therefore, you find them very careful not to cross red lines or take any gamble

which compromises their work permit status. This is why they tend to be more vigilant to cyber threats than others." IP15

"Many expats are single, although well behaved and follow cultural guidelines, but [they] can fall victim to relationship scams and [be] afraid to report it – like over the phone or on Facebook – because this is what they are missing…the drive is the need... and need can be a powerful stimulus to fulfil a necessity." IP2

Cyber-social engineering awareness

The level of information security awareness was assessed by asking participants three questions on whether they received training at work that involved making them aware of online threats related to the use of SNS at work; whether they received training that involved making them aware of online threats in general; and whether they heard of cyber-social engineering. The level of awareness about online threats, and especially those associated with the use of SNS, is low. While 37% of respondents received some training at work that made them aware of online threats, only 31% of surveyed participants received training at work that involved making them aware of threats associated with SNS use. The proportion of those who had heard of cyber-social engineering before is even smaller – 17% (Chart 5-7). A series of pairwise chi-square tests between the corresponding binary responses and categorical variables representing age, gender, nationality and work level did not reveal any significant differences between subgroups based on these characteristics.

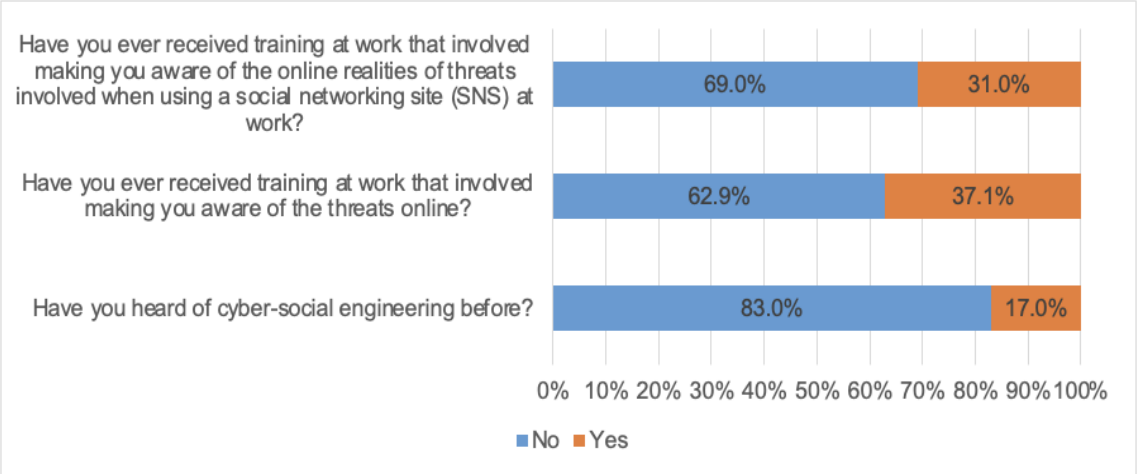


Chart 5-7 Cyber-Social Engineering Awareness

As shown in Table 5-4, 10 of the 15 interview participants were employed in either cybersecurity or IT-related fields. Therefore, it would be expected that the majority of this sample would have undergone ISS training, and that they would be familiar with the concept of cyber-social engineering. Indeed, interviewees mentioned their organisation's efforts at providing ISS training and CSE awareness, or their own awareness of these potential threats to their colleagues.

> *"There are codes of conduct that we and everyone else in the offices should be aware of, however the way each one takes IT [security] precautions seriously is still unclear … but I can assure you that many around me rely blindly on the department overseeing the network here at the university in terms of updates, different types of firewall…"* IP6

> *"… through it [users not activating two-factor authentication], criminals launch social engineering scams on others... My advice to my employees in the cyberworld is to never think well of people online, or of any URL links they receive. It is better to always doubt everything or action you are about to take… The cyberworld is massive and intangible, many users underestimate the negative outcomes..."* IP7

> *"… [they] can fall victim to relationship scams and [be] afraid to report it – like over the phone or on Facebook – because this is what they are missing…the drive is the need.. and need can be a powerful stimulus to fulfil a necessity. But for a cautious individual the difference lies only on the timeframe, as he/she can take more time to respond to a deceptive potential [significant other] due to hesitations … while a desperate [individual] can fully engage with the wrong people and eventually [be] scammed or blackmailed."* IP2

5.4 Testing Relationships

In Sections 5.4.1 – 5.4.6 the conceptual model for this study (see Chapter Three) will be empirically validated using logistic regression. The dependent variable is a binary indicator of susceptibility measured by asking if anything bad happened with the respondent that can be traced back to his/her usage of LinkedIn. In Sections 5.4.1 – 5.4.5 a separate logistic regression model is built for each hypothesis, while in Section 5.4.6 a multivariate stepwise

logistic regression (with backward selection) is applied to the full list of potential explanatory variables. The analysis conducted in Sections 5.4.1 – 5.4.5 presents the bivariate associations between each explanatory variable and the dependent variable – susceptibility. The analysis in Section 5.4.6 is multivariate and presents the influence of each explanatory variables on the dependent variable controlling for other factors. While the latter analysis is less prone to omitted variable bias, the former is also useful as it allows predictions to be made about the behaviour of people when the information is limited to just a single characteristic.

5.4.1 Association between Personality Traits and Susceptibility

Pairwise relationships were tested individually between each personality trait's score and the binary indicator of the susceptibility to CSE attacks on LinkedIn, using bivariate logistic regressions (Table 5-18) to test the significance of the associations. Higher agreeableness (OR[10] = 2.427, $p < .001$), openness (OR = 1.315, $p = .002$) and extraversion (OR = 1.514, $p < .001$) scores are associated with an increased probability of having had a negative experience on LinkedIn. On the contrary, the higher the conscientiousness score, the lower the susceptibility to online threats on LinkedIn (OR = .603, $p < .001$).

Table 5-18 Parameter estimates of bivariate logistic regression models

	B	S.E.	Wald	df	Sig.	Exp(B)	Lower 95% CL	Upper 95% CL
Conscientiousness	-0.507	0.102	24.659	1.000	.000	0.603	0.493	0.736
Constant	1.259	0.484	6.772	1.000	.009	3.522	1.364	9.094
Extraversion	0.415	0.090	21.306	1.000	.000	1.514	1.269	1.807
Constant	-3.031	0.445	46.426	1.000	.000	0.048	0.020	0.115
Agreeableness	0.886	0.131	45.748	1.000	.000	2.427	1.876	3.135
Constant	-5.874	0.748	61.675	1.000	.000	0.003	0.001	0.012
Openness	0.274	0.086	10.032	1.000	.002	1.315	1.111	1.557
Constant	-2.359	0.413	32.679	1.000	.000	0.095	0.042	0.212
Neuroticism	0.021	0.079	0.074	1.000	.786	1.022	0.875	1.192
Constant	-1.232	0.337	13.370	1.000	.000	0.292	0.151	0.565

[10] Odds Ratio. Exponentiated coefficients of the logit model (Exp(B) third column from last of regression tables) correspond to odds ratios, i.e., the number of times the odds of the bad outcome increase if the explanatory variable increases by 1 unit. Odds Ratio equals the exponentiated coefficient of the logistic regression and shows the number of times the odds of having been victimised on LinkedIn increase if the independent variable increases by 1. OR>1 indicates that the higher the value of the independent variable, the higher the risk of victimisation.

To figure out which specific items reflecting personality traits are significantly more characteristic of those who experienced negative events on LinkedIn, mean personality trait scores were compared between those who had experienced negative events on LinkedIn and those who had not. The associated ANOVA results containing information on items that statistically significantly differ between the two groups are presented in Table 5-19.

Table 5-19 Comparing mean values[1] of personality trait scores for individual items using ANOVA

Scale/Item	In all the time since you have been using LinkedIn have you ever had something bad happen (At your work or in your personal life) to you that you can trace back to your usage of LinkedIn?				p-value of the robust test of equality of means
	No		Yes		
	Mean	Standard Deviation	Mean	Standard Deviation	
Openness					
I have thought a lot about the origins of the universe	4.14	1.86	4.85	1.87	0.001
I am highly interested in all fields of science	4.07	1.85	4.82	1.87	0.001
I am fascinated with the theory of evolution	4.09	1.89	4.54	1.87	0.045
Conscientiousness					
I like to keep all my belongings neat and organised	5.04	1.45	4.18	1.50	0.000
I like to have a place for everything and everything in its place	5.11	1.46	4.35	1.55	0.000
I am neat	5.11	1.45	4.57	1.52	0.003
I am organised	5.15	1.46	4.39	1.65	0.000
Extraversion					
I am a very shy person (reverse coded: 7 - strongly disagree)	4.03	1.86	5.03	1.65	0.000
I am quiet (reverse coded: 7 - strongly disagree)	4.53	1.86	4.94	1.54	0.034
I am withdrawn (reverse coded: 7 - strongly disagree)	3.80	1.94	4.67	1.87	0.000
I am silent (reverse coded: 7 - strongly disagree)	4.08	1.91	5.14	1.74	0.000
Agreeableness					
I am always generous when it comes to helping others	4.41	1.68	5.97	1.19	0.000
I always treat other people with kindness	4.88	1.64	5.95	1.24	0.000
I am kind	4.82	1.64	5.81	1.20	0.000
I am sympathetic	4.62	1.66	5.64	1.34	0.000

[1] Grouping variable: susceptibility, only differences significant at the 5% level are included.

According to the comparison on means, three openness item, four extraversion and four agreeableness items are significantly higher for those who had experienced negative events on LinkedIn, while four items measuring conscientiousness are, on average, higher for the other group of respondents.

Table 5-20 gives a summary of hypotheses testing results presented in this subsection.

Table 5-20 Summary of Hypotheses Testing Results: Effects of Personality Characteristics

Hypothesis		Was evidence supporting the hypothesis found?
H1	Employees who express *high levels of conscientiousness are less susceptible* to CSE victimisation on LinkedIn than are those who express low levels of conscientiousness.	Yes, at 1% significance level
H2	Employees who express *high levels of extraversion are more susceptible* to CSE victimisation on LinkedIn than are those who express low levels of extraversion.	Yes, at 1% significance level
H3	Employees who express *high levels of agreeableness are more susceptible* to CSE victimisation on LinkedIn than are those who express low levels of agreeableness.	Yes, at 1% significance level
H4	Employees who express *high levels of openness to experience are more susceptible* to CSE victimisation on LinkedIn than are those who express low levels of openness to experience.	Yes, at 1% significance level
H5	Employees who express *high levels of neuroticism are less susceptible* to CSE victimisation on LinkedIn than are those who express low levels of neuroticism.	No

5.4.2 Association between Disposition to Risk and Susceptibility

The influence of each composite score reflecting disposition to risks on susceptibility to CSE attacks on LinkedIn was individually considered, using bivariate logistic regressions (Table 5-21).

Table 5-21. Parameter estimates of bivariate logistic regression models (dependent variable: susceptibility)

	B	S.E.	Wald	Sig.	Exp(B)	Lower 95% CI	Upper 95% CI
Risk Perception	-0.139	0.082	2.842	0.092	0.871	0.741	1.022
Constant	-0.561	0.361	2.410	0.121	0.571	0.281	1.158
Willingness to Assume Risk	0.191	0.082	5.425	0.020	1.210	1.031	1.422
Constant	-1.911	0.357	28.667	0.000	0.148	0.073	0.298
Perceived Control of Information (Privacy Risk)	-0.200	0.093	4.618	0.032	0.819	0.682	0.982
Constant	-0.244	0.430	0.322	0.571	0.784	0.337	1.820
IT Self-Efficacy	-0.179	0.082	4.825	0.028	0.836	0.712	0.982
Constant	-0.366	0.368	0.989	0.320	0.694	0.337	1.427

The two composite scores that are negatively associated with the probability of having had a negative online security experience with LinkedIn (at the 5% level) are *perceived control of information (privacy risk)* (every additional point decreases the odds by 18%, p = .032) and *IT self-efficacy* (every additional point decreases the odds by 16%, p = .028). Therefore,

those who perceived a higher level of control over risk and those who have higher IT self-efficacy were less likely to experience a negative event on LinkedIn.

The association between the *risk perception* score and susceptibility is statistically significant at the 10% level (p = .092). A one-point increase in this score decreases the odds of experiencing something bad on LinkedIn by 13%. At the same time, a one-point increase in the *willingness to assume risk* score increases the odds of experiencing something bad on LinkedIn by 21% (p = .020). As may be recalled, there were four scale items designed to capture risk perception/disposition (Chapter Four, Table 4-5). Taken together, those four items indicate that people who have higher risk perception believe that there is generally risk associated with sharing information over SNS. The results indicate that those who have a higher *risk perception* score are less likely to experience a negative event on LinkedIn, while those who have a higher *willingness to assume risk* score are more likely to experience a negative even on LinkedIn.

To figure out which specific items reflecting disposition to risk are significantly more characteristic of those who experienced negative events on LinkedIn, means of individual items belonging to scales *willingness to assume risk, perceived control of information (privacy risk)* and *IT self-efficacy* were compared between those who had experienced negative events on LinkedIn and those who had not. The associated ANOVA results containing information on items that statistically significantly differ between the two groups are presented in Table 5-22.

Table 5-22 Comparing mean values of disposition to risk scores for individual items using ANOVA

(grouping variable: susceptibility, only differences significant at the 5% level are included)

Scale/Item	In all the time since you have been using LinkedIn have you ever had something bad happen (At your work or in your personal life) to you that you can trace back to your usage of LinkedIn?				p-value of the robust test of equality of means
	No		Yes		
	Mean	Standard Deviation	Mean	Standard Deviation	
Willingness to assume risk					
I am willing to accept some risk of losing money for an attractive LinkedIn job offer process that may involve a small amount of risk	3.78	2.06	4.27	2.00	0.040
I am willing to accept some risk to my personal information if a LinkedIn post (e.g. job offer, contract, agreement) involves a small amount of risk	3.75	2.04	4.38	2.03	0.009
I am cautious when trying new career based social networking sites (SNS) platforms	3.76	2.08	4.35	1.89	0.011
Perceived control of privacy risk					
I think I have control over what personal information is released by LinkedIn	4.71	1.57	4.25	1.53	0.013
IT Self-efficacy					
I feel confident knowing the authenticity of the LinkedIn website or smartphone applications	4.57	1.60	4.08	1.69	0.016

According to the comparison on means, three items related to *willingness to assume risk* are significantly higher, while one item related to *perceived control of information (privacy risk)* and one item related to *IT self-efficacy* are significantly lower, for those who experienced negative events on LinkedIn (Table 5-23).

Table 5-23 Summary of hypotheses testing results related to effects of personal disposition to risk

Hypothesis		Was evidence supporting the hypothesis found?
H6	Employees who express *high levels of risk perception are less susceptible* to CSE victimisation on LinkedIn than are employees with low levels of risk perception.	Yes, at 10% significance level
H7	Employees who express *high levels of willingness to assume risk are more susceptible* to CSE victimisation on LinkedIn than are employees with low levels of willingness to assume risk.	Yes, at 5% significance level
H8	Employees who *perceive they have control over information* (*privacy risk*) are *less susceptible* to CSE victimisation on LinkedIn than are employees who perceive they have little control over their information.	Yes, at 5% significance level
H9	Employees who express *high levels of IT self-efficacy are less susceptible* to CSE victimisation on LinkedIn than are employees who express low levels of IT self-efficacy.	Yes, at 5% significance level

5.4.3 Association between Risky Habitual Behaviour and Susceptibility

The influence of each Risky Habitual Behaviour score on susceptibility to CSE attacks on LinkedIn was tested individually, using bivariate logistic regressions (Table 5-24) to test the significance of the associations.

Table 5-24 Parameter estimates of bivariate logistic regression models (dependent variable: Susceptibility)

	B	S.E.	Wald	Sig.	Exp(B)
RHBIS	0.158	0.093	2.869	0.090	1.171
Constant	-1.516	0.253	35.979	0.000	0.220
RHBLE	0.166	0.080	4.304	0.038	1.180
Constant	-1.612	0.260	38.560	0.000	0.199
Engagement Frequency	0.045	0.071	0.414	0.520	1.047
Constant	-1.323	0.301	19.344	0.000	0.266

The association between RHBLE (Risky Habitual Behaviour: Level of Engagement) score and susceptibility is statistically significant at the 5% level (p = .038). A one-point increase in this score (i.e. increase in the level of engagement) increases the odds of having experienced something bad on LinkedIn by 18% (1.18 times). The magnitude of the RHBIS (Risky Habitual Behaviour: Information Security) score's influence is similar – a one-point increase in this score (i.e., increase in risks related to Information Security) increases the odds of experiencing a negative incident on LinkedIn by 17% (1.17 times). However, the effect of RHBIS is significant only at the 10% level (p = .09). LinkedIn Engagement Frequency (reflecting the frequency of LinkedIn use at work) is not significantly associated with the risk of experiencing something bad on LinkedIn (p = .520).

To figure out which specific items reflecting risky habitual behaviours are significantly more characteristic of those who experienced negative events on LinkedIn, mean personality trait scores were compared between those who had experienced negative events on LinkedIn and those who had not. The associated ANOVA results containing information on items that statistically significantly differ between the two groups are presented in Table 5-25, which lists the parameter estimates of the multivariate logistic regression model.

Table 5-25 Comparing mean values of risky habitual behaviour scores for individual items using ANOVA

(grouping variable: susceptibility, only differences significant at the 5% level are included)

Scale/Item	In all the time since you have been using LinkedIn have you ever had something bad happen (At your work or in your personal life) to you that you can trace back to your usage of LinkedIn?				p-value of the robust test of equality of means
	No		Yes		
	Mean	SD	Mean	SD	
Risky Habitual Behaviour: Information Security					
Shared your password with a friend or colleague?	1.82	1.59	2.35	2.01	0.020
Used or created a password that is only based on your family name or date of birth?	1.82	1.58	2.34	2.03	0.024
Clicked on links contained in a social media private message (e.g. LinkedIn InMail) from a trusted friend or work colleague.?	1.84	1.59	2.28	2.01	0.050
Downloaded data and material from websites on your work computer without checking its authenticity?	1.82	1.61	2.33	1.96	0.025
Risky Habitual Behaviour: Level of Engagement					
Checked your email notifications from social media sites?	3.11	2.36	3.69	2.36	0.037
Sent messages to work colleagues through one of social media sites you belong to?	3.12	2.35	3.67	2.41	0.050
Shared photos or videos containing company Information on social media sites?	3.10	2.31	3.74	2.49	0.028

According to the comparison on means, four items related to the lack of habitual behaviour with regard to information security and three items corresponding to a higher level of engagement are significantly higher for those who had something bad happen to them over LinkedIn.

Table 5-26 gives a summary of hypotheses testing results presented in this subsection.

Table 5-26 Summary of hypotheses testing results related to the effects of risky habitual behaviour.

Hypothesis		Was evidence supporting the hypothesis found?
H10	Employees with *risky habitual behaviour* (ERHB) on LinkedIn are *more susceptible* to CSE victimisation than are those with lower levels of engagement on LinkedIn.	Yes. Engagement frequency is not significantly associated with the likelihood of victimisation, but lower levels of information security habitual behaviour and, especially, higher levels of engagement increase the probability of becoming victims of CSE.
H10.1	Employees with *low levels of information security habitual behaviour* on LinkedIn (low RHBIS score) are *more susceptible* to CSE victimisation than are those with higher levels of information security habitual behaviour on LinkedIn.	Yes, at 10% significance level
H10.2	Employees with *high levels of engagement* on LinkedIn (RHBLE) are *more susceptible* to CSE victimisation of CSE than are those with lower levels of engagement on LinkedIn.	Yes, at 5% significance level
H10.3	Employees with *high frequency of SNS use* on LinkedIn are *more susceptible* to CSE victimisation than are those with lower frequency of SNS use on LinkedIn.	No

5.4.4 Association between Demographic and Cultural Factors and Susceptibility

While the analysis has already compared user susceptibility by demographic groups and identified significant differences by nationality, gender and work level (as described in Table 5-17), the analysis was univariate and neglected the fact that, in the sample, senior positions are more often occupied by older Saudis, while lower positions are held by younger people and non-Saudis. In this section, the robustness of the findings is checked by presenting the results (in Table 5-27) of a logistic regression model linking the demographic factors to the probability of having experienced a negative event that can be traced back to LinkedIn usage (susceptibility = 1 for negative event, 0 otherwise). This was run by entering all of the demographic variables into the logistic regression model (all the variables turned out to be significant). The analysis is useful as it allows predicting

susceptibility of an employee solely based on his/her demographic characteristics when no information from psychological tests is available. Other things being equal:

- Odds[11] of experiencing cyberthreats on LinkedIn are 3.15 times[12] higher for males than females ($p < 0.001$).
- Odds of experiencing o cyberthreats on LinkedIn are 82%[13] lower for those aged 62 and over compared to those aged 18-28, while other age groups are not significantly different from the baseline group (18-28 years old).
- Odds of experiencing cyberthreats on LinkedIn are 75% lower for non-Saudis than for Saudis (Non-Saudis: exp(B) = .246 < 1 – less likely to be victims).
- Odds of experiencing cyberthreats on LinkedIn are 73% lower for department management/Section supervisors (level 2) and 86% lower for top-level managers (level 3) than for the lowest-level employees (level 1).

Table 5-27 Parameter estimates of multivariate logistic regression model (dep. var. susceptibility)

	B	S.E.	Wald	Sig.	Exp(B)	Lower 95% CL	Upper 95% CL
Constant	-1.159	0.522	4.923	0.026	0.314	0.113	0.873
Gender (reference category: female)							
male	1.147	0.344	11.155	0.001	3.150	1.604	6.180
Age (reference category: 18-28)							
29 - 39	-0.464	0.459	1.024	0.312	0.629	0.256	1.546
40 - 50	-0.141	0.557	0.064	0.801	0.869	0.291	2.588
51 - 61	-0.384	0.737	0.271	0.603	0.681	0.161	2.888
62 and over	-1.706	0.691	6.099	0.014	0.182	0.047	0.704
Nationality (reference category: Saudi)							
Non-Saudi	-1.403	0.465	9.094	0.003	0.246	0.099	0.612
Work Level (reference category: administrative office/assistant employee)							
Department management/Section supervisor or designee	-1.323	0.374	12.549	0.000	0.266	0.128	0.554
Top-level management or designee	-1.989	1.052	3.571	0.059	0.137	0.017	1.076

[11] Odds = Probability(susceptibility = 1)/Probability(susceptibility = 0).
[12] The number of times equals Exp(B).
[13] The odds ratio is represented as a percentage difference by means of the following formula: (Exp(B)-1)*100%.

Therefore, strong support was found of the hypotheses that gender, nationality and structural power in the organisation impact susceptibility to CSE victimisation on LinkedIn, as well as some support for the hypothesis about the influence of age: while people aged 18-61 do not differ significantly in their susceptibility to CSE victimisation, older employees were less likely to experience such online threats.

Table 5-28 gives a summary of hypotheses testing results presented in this subsection.

Table 5-28 Summary of hypotheses testing results related to the effects of demographic characteristics

Hypothesis		Was evidence supporting the hypothesis found?
H1 1	*Older employees are less susceptible* to CSE victimisation on LinkedIn than are younger employees.	Yes. Those over 61 were less susceptible to CSE victimisation than those from younger age groups, at 1% significance level.
H1 2	*Female employees are less susceptible* to CSE victimisation on LinkedIn than are male employees.	Yes. Males were more susceptible to CSE victimisation than females, at 1% significance level.
H1 3	*Employees in senior positions* in the organisation *are less susceptible* to CSE victimisation on LinkedIn than are employees in a junior position.	Yes, at 10% significance level. Employees in a senior position in the organisation were less susceptible to CSE victimisation than were employees in a junior position.
H1 4	The *nationality* of an employee *can increase their susceptibility* to CSE victimisation.	Yes. Saudis were more susceptible than non-Saudis to CSE victimisation, at 1% significance level.

5.4.5 Associations between Motivational Factors and Susceptibility

Table 5-29 presents the results of two bivariate logistic regressions of susceptibility on scores of the motivational factors of self-presentation and professional advancement. The association between self-presentation and susceptibility to bad situations on LinkedIn is non-significant ($p = .198$). At the same time, an increase in the score characterising behaviour pertaining to professional advancement (higher score meaning higher interest in professional advancement), increases the probability of having experienced cybersecurity problems on LinkedIn ($OR = 1.048$, $p < .001$). A possible explanation is that professional advancement involves actively contacting various people on LinkedIn and disclosing sensitive information that may be requested by actual or fake recruiters or potential business partners.

Table 5-29 Parameter estimates of bivariate logistic regression models (dependent variable: susceptibility)

	B	S.E.	Wald	Sig.	Exp(B)
Self-Presentation score	-0.530	0.411	1.661	0.198	0.589
Constant	-0.907	0.216	17.621	0.000	0.404
Professional Advancement Score	0.047	0.012	15.720	0.000	1.048
Constant	-2.302	0.327	49.432	0.000	0.100

To figure out which specific items reflecting professional advancement behaviour on LinkedIn, means of individual items belonging to this scale were compared between those who had negative events on LinkedIn and those who had not. The associated ANOVA results containing information on items that statistically significantly differ between the two groups are presented in Table 5-30.

Table 5-30 Comparing mean values of professional advancement scores for individual items using ANOVA

(grouping variable: susceptibility, only differences significant at the 5% level are included)

Scale/Item	In all the time since you have been using LinkedIn have you ever had something bad happen (At your work or in your personal life) to you that you can trace back to your usage of LinkedIn?				p-value of the robust test of equality of means
	No		Yes		
	Mean	SD	Mean	SD	
Connected with professionals that could help you with your professional advancement	2.20	1.34	2.78	1.42	0.001
Followed other companies that you believe could increase your professional advancement	2.19	1.30	2.66	1.47	0.006
Shared your work related CV to companies which you believe could help you with your professional advancement	2.24	1.31	2.60	1.51	0.039
Shared your work related CV with professionals with whom you feel can help with your professional advancement	2.21	1.33	2.71	1.49	0.005
Accepted connections from connections whom you don't know but can see that they have many connections themselves	2.15	1.30	2.85	1.44	0.000
Accepted network connections from connections who are connected to your connections	2.25	1.34	2.65	1.47	0.019
Accepted a connection requests on LinkedIn because you recognised the photo	2.25	1.36	2.60	1.39	0.032
Messaged your connections for support in career or work related matters	2.23	1.32	2.62	1.47	0.021
Shared documents, audio or video with connections in order to assist you with a problem	2.20	1.34	2.73	1.39	0.002
Accepted documents, audio or videos from connections in relation to receiving support from them	2.22	1.31	2.67	1.50	0.009

Table 5-31 gives a summary of hypotheses testing results presented in this subsection.

Table 5-31 Summary of hypotheses testing results related to the effects of self-presentation and professional advancement on LinkedIn

Hypothesis		Was evidence supporting the hypothesis found?
H15	Users who are *motivated by career advancement* on LinkedIn *are more susceptible* to CSE victimisation than are those who are less motivated in this way.	Yes, at 1% significance level
H16	Users who are *more inclined* than others *to present themselves and their credentials* on LinkedIn *are more* susceptible to CSE victimisation.	No

5.4.6 A Multivariate Logistic Regression Model of Susceptibility Accounting for Each Explanatory Variable

A multivariate stepwise logistic regression (backward LR method with default settings: p-value for entry = .05, p-value for removal = .10) was used to test whether the result of bivariate analyses hold after controlling for other factors. Parameter estimates for the resulting set of explanatory variables selected by the procedure are presented in Table 5-32.

Table 5-32 Parameter estimates of the stepwise multivariate logistic regression model. (dependent variable: susceptibility)

Independent Variables	B	S.E.	Wald	Sig.	Exp(B)	95% C.I.for EXP(B)	
						Lower	Upper
Conscientiousness	-0.838	0.169	24.445	0.000	0.433	0.311	0.603
Extraversion	0.591	0.147	16.097	0.000	1.806	1.353	2.410
Neuroticism	0.294	0.132	5.006	0.025	1.342	1.037	1.737
Openness	0.356	0.130	7.517	0.006	1.427	1.107	1.841
Agreeableness	0.922	0.185	24.724	0.000	2.515	1.748	3.618
RHBIS	0.244	0.128	3.639	0.056	1.277	0.993	1.641
IT Self-efficacy	-0.428	0.118	13.135	0.000	0.652	0.517	0.822
Professional Advancement Score	0.030	0.017	3.014	0.083	1.031	0.996	1.066
Gender (reference category: female)							
male	1.818	0.529	11.813	0.001	6.158	2.184	17.362
Age (reference category: 18-28)							
age: 29-39	-1.338	0.643	4.329	0.037	0.262	0.074	0.925
age: 40-50	-1.451	0.803	3.263	0.071	0.234	0.049	1.131
age: 51-61	-1.839	0.990	3.448	0.063	0.159	0.023	1.107
age: 62+	-3.110	0.940	10.955	0.001	0.045	0.007	0.281
Work Level (reference category: administrative office/assistant (employee)							
Department management/Section supervisor or designee	-1.133	0.472	5.767	0.016	0.322	0.128	0.812
Top-level management or designee	-2.212	1.266	3.051	0.081	0.110	0.009	1.310
Constant	-6.788	1.634	17.254	0.000	0.001		

The signs and the magnitude of effects are similar to those found as part of the bivariate logistic regression analysis. Most associations that were significant in the bivariate analysis were also selected as significant in the stepwise multivariate analysis with a few exceptions: nationality, as well as scores reflecting *risk perception*, *perceived control of information (privacy risk)*, *willingness to assume risk* and *level of engagement*. While the evidence that these variables are significantly associated with susceptibility to negative experience on LinkedIn remains valid, it is likely that the effects of these variables were not direct and were completely or almost completely mediated by some of the significant variables such as RHBIS, IT Self-efficacy, SPA scores and personality traits scores. As a result, when accounting for these mediators, some effects became non-significant. The multivariate logistic regression has thus strengthened the evidence in favour of the direct effect of those significant variables that were eventually included in the model by the stepwise procedure.

Multicollinearity diagnostics were performed for the set of explanatory variables used in the multivariate logistic regression on which Table 5-32 is based, to make sure that standard errors of the parameter estimates are not seriously inflated (Miles, 2014; Thompson et al., 2017). Inflation of a standard error leads to underestimation of the effect's significance. Variance inflation factors (VIFs) were computed for each regressor as follows:

R_j^2 from the regression of regressor *j* on all other regressors shows how much variance of predictor *j* is explained by all other predictors, (i.e., how linearly dependent predictor *j* is on other predictors). The resulting coefficient of determination was used to compute predictor *j*'s variance inflation factor $VIF_j = \frac{1}{1-R_j^2}$. Most VIFs are lower than 2 and none of them exceeds 3.71 – a substantially lower value than a commonly used threshold for detecting multicollinearity (5), implying that the presented model does not suffer from multicollinearity (Table 5-33).

Table 5-33 Variance inflation factors for predictors

Independent Variables	VIF
Conscientiousness	1.451
Extraversion	1.505
Neuroticism	1.507
Openness	1.389
Agreeableness	1.469
RHBIS	1.158
IT Self-efficacy	1.030
Professional Advancement Score	1.235

Gender (reference category: female)	
male	1.674
Age (reference category: 18-28)	
age: 29-39	3.709
age: 40-50	2.506
age: 51-61	1.734
age: 62+	2.525
Work Level (reference category: administrative office/assistant (employee)	
Department management/Section supervisor or designee	1.078
Top-level management or designee	1.057

5.5 Summary of the Chapter

This chapter presents the results of the analysis of 394 completed questionnaires and 15 interviews which examined employee susceptibility to cyber-social engineering (CSE) over LinkedIn. Specifically, this investigation looked at the influence on CSE susceptibility of a number of human aspects. These human factors consist of 18 independent variables in five domains, which are: five personality characteristics, four disposition to risk variables, three independent variables on habitual behaviour, two demographic variables, two cultural variables and two motivational variables. The key findings present a number of interactions (either positive or negative) between hypothesised factors in the extended model of this current study and susceptibility to CSNS attacks. Hypothesis testing was conducted after descriptive outcomes of data and a series of chi-square tests of association between each factor and the categorical demographic or cultural variable, which has been explained in Section 5.2.1. Hypothesis testing was conducted using bivariate logistic regression and multivariate regression. These analyses were performed using SPSS 24 (statistical software package, see Chapter 4).

Key findings of the factors which remained in the final model are summarised below.

For employees of the organisation and controlling for all other factors:

- A 1-unit increase on the conscientiousness scale (i.e., an increase in the level of conscientiousness) *decreases* the odds of being susceptible to CSE victimisation over LinkedIn by 56.7%
- A 1-unit increase on the extraversion scale (i.e., an increase in the level of extraversion) *increases* the odds of being susceptible to CSE victimisation over LinkedIn by 80.6%.

- A 1-unit increase on the agreeableness scale (i.e., an increase in the level of agreeableness) *increases* the odds of being susceptible to CSE victimisation over LinkedIn by 151.5%.
- A 1-unit increase on the openness to experience scale (i.e., an increase in the level of openness to experience) *increases* the odds of being susceptible to CSE victimisation over LinkedIn by 41.2%.
- A 1-unit increase on the neuroticism scale (i.e., an increase in the level of neuroticism) *increases* the odds of being susceptible to CSE victimisation over LinkedIn by 34.2%.
- A 1-unit increase on the IT self-efficacy scale (i.e., an increase in the level of IT self-efficacy) *decreases* the odds of being susceptible to CSE victimisation over LinkedIn by 34.8%.
- A 1-unit increase on the information security risky habitual behaviour scale (i.e., an increase in the level of risky information security habitual behaviour) *increases* the odds of being susceptible to CSE victimisation over LinkedIn by 27.7%.
- Regarding age as a demographic variable, compared to the reference category (18-28):

  - The odds of being susceptible to CSE victimisation over LinkedIn *decreased* by 95.5% for employees aged 62 and over.
  - The odds of being susceptible to CSE victimisation over LinkedIn *decreased* by 84.1% for employees aged 51-61.
  - The odds of being susceptible to CSE victimisation over LinkedIn *decreased* by 76.6% for employees aged 40-50.
  - The odds of being susceptible to CSE victimisation over LinkedIn *decreased* by 73.8% for employees aged 29-39.

Which means that the older the employees are, the less susceptible they are.

- The odds of being susceptible to CSE victimisation over LinkedIn for males are *higher* than for females (reference category) by 6.158 times.

- Compared to administrative office/assistant (employee work level 1), the odds of being susceptible to CSE victimisation over LinkedIn:

  - *decreased* by 67% for department management/section supervisors (work level 2), and
  - *decreased* by 89% for top-level managers (work level 3).

Which means that the higher the employee's level of structural power in the organisation, the less susceptible they are.

- On the motivation factor of professional advancement, a 1-unit increase in this score was found to *increase* the odds of being susceptible to CSE victimisation over LinkedIn by 1.031 times.

Important findings of this study, including the theoretical and practical contributions of these findings, are presented and discussed in Chapter Six.

6. Discussion

6.1 Introduction

As explained in the preceding chapters, the aim of this study is to contribute to the existing literature by identifying underlying causes of employees' susceptibility to CSE victimisation in the workplace. This thesis addresses the following research question:

Q1. How, and to what extent, do personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering (CSE) victimisation when accessing professional SNS, such as LinkedIn, in government organisations in Saudi Arabia?

This research examines susceptibility to CSE in Saudi Arabia's public sector organisations based on employees' personal dispositions and behaviour while using LinkedIn. Many organisations hold large amounts of PII on Saudi citizens and residents that can be exploited by attackers. It is important to examine LinkedIn, the most commonly used CSNS, since users' motivations for engaging on this career-oriented platform are different from those on other platforms such as Facebook, and this difference has the potential to affect their behaviour and susceptibility. To the best of this researcher's knowledge, no other study has investigated susceptibility to CSE victimisation via LinkedIn by examining personality traits in conjunction with personal dispositions and motivations, habitual behaviours, the cultural factors of organisation and nationality, and the demographic factors of age and gender.

Some of the results of this research have confirmed the findings of previous studies, whereas other results of this study contradict or challenge earlier findings. In addition, several new findings have been revealed. In this chapter the research findings are discussed, and the theoretical and practical contributions of this study are presented.

6.2 Study Factors as They Relate to Susceptibility to CSE

In this section, the main findings of the study are discussed, compared and contrasted with findings from the literature on factors influencing user susceptibility to social engineering in cyberspace. The section begins by describing participants' use of CSNS (namely, LinkedIn). The study findings with regard to the factors hypothesised to influence susceptibility to CSE are then discussed. Those factors that increase user susceptibility to

CSE are examined, and findings from both the quantitative and qualitative phases of the study are compared to findings in previous studies.

6.2.1 Use of CSNS

As stated in Chapter Four, the research strategy was based on purposeful sampling of those who use a professional or career-oriented SNS (CSNS). The target sample was employees of MHRSD who used LinkedIn. However, the restrictions placed by MHRSD on this researcher's abilities to contact their employees meant that "not using LinkedIn" could not be a criterion for exclusion in the survey sample. Nevertheless, survey results from the sample of 394 MHRSD employees showed that LinkedIn (LI) was by far the most popular social networking site (362 respondents used it). LI was even more popular than general-purpose SNS such as Facebook: 93% of surveyed respondents reported using LinkedIn as compared to 76% using Twitter and Instagram. Nearly all MHRSD employees (96.2%) reported that they used their professional SNS account at work at least sometimes (i.e., *1 to 3 days/week*). Nearly one quarter (24.4%) of them did so regularly (between *1-2 times a day* and *open all the time*), while a small percentage (3.8%) stated that they either did not have a CSNS or that they never used it while at work. Current data on the use of any type of SNS by employees for personal reasons while at work is surprisingly scarce, but data from the United States via a 2014 Pew Research Center study (N = 2,003) showed that 77% of workers reported using social media at work (Lampe and Ellison, 2016). This study is somewhat dated, however, as it is difficult to find employee usage data related specifically to LinkedIn.

Similar usage patterns of social networks in the different demographic groups examined in this study can be explained by the high penetration of social media in people's lives, the fact that the sample was a relatively homogeneous group from a single public organisation's employees and the fact that only relatively young and middle-aged respondents were targeted, rather than retired people aged 65+.

6.2.2 Personality Traits and Susceptibility

Personality traits, and in particular, those characteristics encapsulated in the Five Factor Model or FFM (*conscientiousness, extraversion, agreeableness, openness to experience* and *neuroticism*) have been identified in the literature as factors explaining or predicting susceptibility to CSE. The research on personality traits has shown that these characteristics

are complex, and that they are influenced by genetic inheritance as well as by environment – that is, by both nature and nurture (Brody and Crowley, 1995). Other researchers who have examined susceptibility to CSE have employed the FFM in their studies precisely because these characteristics are considered to be consistent across nations/cultures and age groups (Heartfield *et al.*, 2016; Frauenstein and Flowerday, 2020). Despite, or perhaps because of, the large and expanding body of research in this domain, the evidence regarding how and whether each of these traits influences vulnerability/susceptibility to cyberattacks has often been conflicting (see Chapter Two, Section 2.8.1). Hence, the five hypotheses regarding the relationship between personality and CSE susceptibility posited for the study model were based on the most common findings in the literature for each trait. Overall, findings of this study revealed significant differences between males and females with regard to personality traits. Notably, females scored higher on conscientiousness (females: $M = 5.20$, males: $M = 4.83$, $p < .01$), openness (females: $M = 4.55$, males: $M = 4.19$, $p = .034$), extraversion (females: $M = 5.21$, males: $M = 4.01$, $p < .001$) and neuroticism (females: $M = 5.00$, males: $M = 3.65$, $p < .001$). The relevance of these findings is discussed in the following subsections.

Conscientiousness

A number of empirical studies have found that users who scored high on the conscientiousness trait were less susceptible to CSE in the email context (Goel *et al.*, 2017; van de Weijer and Leukfeldt, 2017; Frauenstein and Flowerday, 2020) and in the SNS context (Albladi and Weir, 2017; Frauenstein and Flowerday, 2020). In accordance with such findings, this research posited that employees who expressed high levels of conscientiousness would be less susceptible to CSE victimisation on LinkedIn than would their counterparts who expressed low levels of conscientiousness. Unsurprisingly, this hypothesis was strongly supported. Based on a multivariate logistic regression analysis, when controlling for all other variables in the model, a 1-unit increase in the score on the conscientiousness scale decreases the odds of an individual being susceptible to CSE attacks over LinkedIn at the workplace by 57% ($p = .00$).

Conscientiousness consists of sub-traits, one of which is the willingness to comply with rules and norms (Oyibo *et al.*, 2017). The qualitative findings also suggest that individuals who are more conscientious are more careful online. IP2 highlighted that a generally

"*careful individual*" who conscientiously obeys "*rules and regulations*" might still be careful while "*surfing the net*" (e.g., engaging with SNS platforms),

Conscientious individuals are generally viewed by organisations as highly desirable employees (Stevens and Ash, 2001). Moreover, research shows that organisations can encourage conscientious behaviour and that individuals (including employees) can foster this behaviour in themselves, even if their personality is not high on the conscientious scale (Tasselli, Kilduff and Landis, 2018b). However, it is vital that the organisation provide and require up-to-date, appropriate and effective CSE awareness training for all its employees – of any personality type. Specific recommendations are discussed in Chapter Seven.

As is the case with other personality characteristics, the conscientiousness trait can be influenced by other factors such as gender or age. The study findings revealed significant differences ($p < .01$) between men ($M = 4.83$) and women ($M = 5.20$) with regard to conscientiousness However, with regard to other factors investigated in association with the conscientiousness personality trait in this study, in particular, age, nationality (Saudi and non-Saudi employees) and structural power/employment position, no statistically significant difference was found. This and other demographically related differences associated with personality and disposition that emerged from the data are discussed in the relevant sections of this chapter.

Extraversion

The majority of studies agree that individuals who score high on this trait are at higher risk of being victimised by CSE (Parrish *et al.*, 2009; Uebelacker and Quiel, 2014; Alseadoon *et al.*, 2012, 2015; Albladi and Weir, 2017), Therefore, this research posited that employees who expressed high levels of extraversion would be more susceptible to CSE victimisation on LinkedIn than would their colleagues who expressed low levels of this personality trait. Unsurprisingly, this hypothesis was supported. Controlling for all other variables in the model, a 1-unit increase in the score on the extraversion scale increases the odds of an individual being susceptible to CSE attack over LinkedIn by 80% ($p = .000$) at the workplace. It should be noted that the scores for this factor were based on participants' responses to a psychometric test for extraversion in which most of the items were worded to reflect *introversion* (e.g., *I am…very shy*, *…silent*, *…withdrawn*, *…quiet*; see Chapter 5, Table 5-19).

The finding that those who were less susceptible to CSE victimisation had scored lower on the extraversion scale is in accordance with the literature. Employees who are strict about not sharing passwords – and who are, according to the literature, therefore less likely to become victims of CSE – may be viewed by their co-workers as "*unsociable*" (Weirich and Sasse, 2001, p. 142). In other words, their attitudes and behaviours contravene certain social norms in the workplace.

The study findings have revealed significant differences (1% significance level) between men and women with regard to extraversion, which is a trait that generally describes people who are outgoing and social. Female employees scored higher (M = 5.21) on this trait than male employees did (M = 4.01), which according to the literature would suggest that these women are more assertive, sociable, talkative and more likely to disobey policies than are their male counterparts. Surprisingly, this does not accord with this study's qualitative findings that suggest women tend to be more restrained. However, this could be a characteristic that is present amongst females when they are together in a female-only setting and not in a female-male setting; the former is still the norm in Saudi public sector workplaces. A male participant explains: "*in the workforce, you see proportionally more men than women*" (IP15). As explained further by two female participants: "*in KSA ... a patriarchal society*" (IP14) "*women's limitations are still accepted by choice and that exceeding their limit is not always an option*" (IP10).

The finding that females are more extraverted could pose a risk online. Due to the digital distance involved while engaging on CSNS platforms such as LinkedIn, especially when seeking employment, women may feel comfortable enough to be outgoing and expressive. Through this behaviour, they can be easily induced into scams and other types of CSE attacks. However, this study produced no quantitative or qualitative data that explains why females scored higher on extraversion, or how this might play a role in their susceptibility to CSE risks. In fact, the study findings are that, overall, men were more susceptible to CSE victimisation than women were. Further research is needed to examine the relationship between extraversion and gender difference to CSE victimisation over SNS/CSNS.

Looking at the factors of nationality, age and work level, Saudi employees scored higher on the extraversion scale (M = 4.42) than non-Saudis (M = 3.57), whereas no significant differences in levels of this trait were found regarding age and power level. One insight gleaned from the qualitative data was that expatriates from Asian and Middle Eastern countries do express similar personality characteristics with Saudi nationals in that they are

"*outgoing*" and "*eager*" to seek out individuals on LinkedIn who have hundreds of connections to engage and collaborate with (IP2). However, as two interviewees (IP2, 1P15) suggested, socioeconomic and environmental factors could influence and even alter their characteristic behavioural tendencies. In particular, non-Saudis are guestworkers on temporary contracts, so they experience "*job insecurity*", (IP15) and "*Over time, their emotions and behaviours can be[come] suppressed. … outgoing individuals can turn into introverts, … be[ing] wary of whatever consequences might happen should they behave inappropriately*" (IP2). These findings are discussed in more detail under demographics in Section 6.2.5.

Organisations often favour hiring extraverted individuals, because they are outgoing, good communicators and work well in teams (Gupta and Gupta, 2020; Stevens and Ash, 2001). However, hiring managers should be aware of the risks posed to their organisation's cybersecurity from extraverted employees. This and other implications of these findings are discussed in Chapter Seven.

Agreeableness

Previous empirical research examining personality traits and susceptibility to CSE attacks has often omitted agreeableness from their studies. However, two of three studies that did test this relationship found that users who scored high on agreeableness were more susceptible to CSE in the email context (Alseadoon *et al.*, 2015; Frauenstein and Flowerday, 2020) and in the SNS context (Frauenstein and Flowerday, 2020). In contrast, Albladi and Weir (2017) found that high agreeableness scores significantly decreased susceptibility to CSE. In the current study, controlling for all other variables in the model, a 1-unit increase on the agreeableness scale increases the odds of an individual being susceptible to CSE attack over LinkedIn by 151.5% ($p = .000$).

This study also found significant differences in scores of this personality trait related to gender and nationality, whereas differences in agreeableness scores were non-significant as related to age or organisational rank. These findings will be discussed in turn. The quantitative survey results showed that men ($M = 5.27$) scored significantly higher (at 1% significance level) than did women ($M = 4.04$) on this trait. In some populations, this might be a surprising finding, given that individuals high in agreeableness are described as "*compassionate and cooperative*" (Parrish *et al.*, p. 289), which arguably are attributes commonly associated with females. However, male survey participants also responded

positively to items for the agreeableness trait related to helping others and treating people with kindness (e.g., *I am kind, I am sympathetic* and *I am always generous when it comes to helping others*; see Chapter 5, Table 5-19). In order to make sense of this finding, it is helpful to consider it in conjunction with another interesting finding, which was that Saudis scored significantly higher (at 1% significance level) than non-Saudis did on agreeableness.

The qualitative data from the interviews shed some light on this interconnection between gender and nationality. IP1 explained that Saudi culture is "*collectivist, meaning mutual dependence between people*" and that this means Saudis adhere to "s*ocial values that compel them to refrain from arguing with seniors or strangers*" and to "*comply with a request [in order] to avoid disappointing [someone]*". While this explanation might account for Saudi males' high scores in agreeableness, it does not explain the contrasting low scores on this trait by Saudi females. Here again, findings from the qualitative data may offer some insight. All of the female interview participants were of Saudi nationality. Female interviewees expressed their identity "*as a Muslim woman, let alone [i.e., particularly] in Saudi Arabia*" (IP6). Associated with this identity, they implied a need to show reserve: "*many Saudis are rooted by … their religious and cultural values that make women still favour being two steps away from their men … and exceeding their limit is not always an option*" (IP10) and indicated that there was even a degree of apprehension ("*kept me nervous*") when receiving communication from a stranger (IP9). In Arab/Islamic culture, the norm is for women to be reserved and restrained in their behaviour towards males who are not their close relatives. Thus, according to Saudi cultural norms, females would be expected to be uncooperative and not agreeable or compliant when dealing with unsolicited communications, whether offline or online.

As mentioned above, this study found that Saudis (M = 5.11) scored significantly higher (at 1% significance level) than non-Saudis (M = 4.00) did on agreeableness, it is possible that the norms of collectivism are a likely reason for the high scores of Saudi nationals. The corresponding low scores of non-Saudis on this trait require some explanation as well, in which the qualitative data may be helpful. To place this in context, most non-Saudis working on contracts in the Saudi public sector are from majority Muslim and/or Arab countries, whose cultural values (e.g., collectivism, power distance) overlap greatly with those of Saudi society. Therefore, it might be expected that these individuals would also have high agreeableness scores, but as one interviewee explained, although they:

> "*…may share the same customs and values that induce some to be collaborative and outgoing or polite and pleasing… However, these qualities can be expressed differently when they are expatriates in [Arabian] Gulf countries … Being cautious due to the country's labour laws, or [not questioning] instructions, so as to comply and cope within a different environment, could impact on their behaviours and consequently could reshape their habits and impulsive responses*." (IP2)

However, compliance with rules and regulations, as IP2 mentions, is quite different from "*comply[ing] with a request [in order] to avoid disappointing [someone]*" mentioned earlier by IP1. The first type of compliance is a sub-trait of conscientiousness, whereas the second is a sub-trait of agreeableness. Thus, the significant difference in agreeableness scores based on nationality could be because non-Saudis (in their roles as expatriates) are constrained by contextual factors such as their temporary employment contracts.

Uebelacker and Quiel (2014) posited that the relationship between personality traits and susceptibility to social engineering might be mediated by Cialdini's principles of persuasion. Empirical studies (Alkiş and Temizel, 2015; Oyibo *et al.*, 2017) have found that people who had high agreeableness scores were influenced by certain persuasion principles. In particular, agreeable individuals were persuaded by authority, social proof/liking and consistency and commitment, which are three commonly used tactics in social engineering attacks (see Chapter Two, Sections 2.5 & 2.7).

The qualitative findings indicate that agreeableness is a trait in which some of its sub-traits can potentially be consciously controlled by employees. This is supported by recent research showing that personality traits can be consciously changed (Tasselli *et al.*, 2018a, 2018b). Research also has shown that organisations prefer to hire agreeable individuals for their sub-traits of cooperation and empathy (Stevens and Ash, 2001), characteristics that are favoured in employees and managers alike, as they contribute to strong organisational cohesiveness and help to maintain healthy relationships among employees. Considering that agreeableness may increase the likelihood that an employee will use heuristic rather than systematic processing, thus raising their susceptibility to CSE victimisation (Frauenstein and Flowerday, 2020), organisations should be proactive in taking steps to prevent or at least mitigate employee exposure to CSE attack. Recommendations are presented in the Implications section of Chapter Seven.

Openness to Experience

Previous empirical research has produced conflicting results regarding the association between openness to experience and susceptibility to CSE risk. In the email environment, some studies have shown that users scoring high on openness were more susceptible to CSE attacks (Alseadoon *et al.*, 2012, 2015; Halevi *et al.*, 2013a, 2013b), whereas others have shown that individuals who were highly open to experience were less susceptible (Pattinson *et al.*, 2012; Frauenstein and Flowerday, 2020). The limited evidence from previous studies that tested the relationship between FFM traits and vulnerability to CSE in the SNS environment is equally contradictory. Albladi and Weir (2017) found no direct or mediated link between openness and susceptibility, whereas Frauenstein and Flowerday (2020) did find an indirect and positive influence on susceptibility to cyberattacks. Both these studies looked at Facebook, which is not a CSNS.

Despite the lack of evidence in the literature for strong influence in either direction, this study posited that employees who expressed high levels of openness to experience would be more susceptible to CSE victimisation on LinkedIn than would those who expressed low levels of this trait. Surprisingly, this hypothesis was strongly supported. When controlling for all the other variables in the model, a 1-unit increase on the openness scale increases the odds of being susceptible to CSE attacks over LinkedIn at work by 42.7% ($p = .006$).

The study findings have also revealed significant differences in scores of openness to experience related to gender and work level in the organisation. The quantitative survey results showed that women scored significantly higher (at 5% significance level, $M = 4.55$) on openness than did men ($M = 4.19$) on this trait. This finding may be unremarkable when considered against the background of previous research findings on gender differences in personality traits, which have reported variously that higher scores on openness were associated with males or with females (Costa *et al.*, 2001), or that the genders did not differ significantly on this trait (Weisberg, DeYoung and Hirsh, 2011). As discussed later in Section 6.2.5, the qualitative findings did not provide any clarity on the reasons why women in this study sample scored higher on openness.

The quantitative survey results showed significant differences (at 1% significance level) in mean openness scores of employees at different levels of power in the organisation. Specifically, workers at the lowest level scored significantly higher ($M = 4.42$) than did employees in either middle ($M = 3.88$) or top-level management ($M = 3.77$). This was an

interesting finding. Data from the interviews provided insights into the relationship between openness and occupational power position. Interviewees (IP3, IP4) highlighted the importance employees at all levels placed on seeking higher positions within the organisation or to at least maintain their position. One surmised that "*employees occupied in administrative tasks* [i.e., at the lower levels] *tend to … seek more knowledge enhancement and to develop themselves*" and that they did so in hopes of advancing to higher positions within the organisation (IP4). Another interviewee noted the link between openness and ambition, as embodied in an individual's "*need to self-learn and explore in different aspects of science can be driven by high curiosity*" (IP10).

The finding of no significant differences in openness scores by age group was not unexpected. The lack of significant difference on openness with regard to nationality was perhaps more surprising, considering the findings of significant differences between Saudis and non-Saudis on extraversion and agreeableness (Saudis scored significantly higher on both those traits). Following from the qualitative findings, which highlighted that non-Saudis were constrained by their conditional work permits and thus tended to be more restrained than their Saudi colleagues in their attitudes and inclinations, it might have been expected to find a similar effect on their openness scores as well. However, this has not been the case according to the study results.

Gupta and Gupta (2020) found that employees who score high on openness to experience exhibit creativity and help managers to improve job performance. Stevens and Ash (2001) found an association between openness and participatory styles of management and teamwork. However, in an online setting this trait can be problematic to the security of an organisation's network. This is because when individuals engage on SNS and specifically on CSNS, LinkedIn may be mistakenly seen as a "safe" platform on which to network professionally. Uebelacker and Quiel (2014) posited that individuals who score high on openness may be susceptible to social engineering attacks using the scarcity principle. In a LinkedIn setting this may be in the form of fraudulent posts or messages offering free but limited availability places for online courses, which would be attractive to such individuals who want to learn and enhance their knowledge. These targeted employees can fall victim by clicking on "registration" links that circulate spyware and viruses into the organisation's network. Strategies for mitigating these sorts of risks to organisations are discussed in Chapter Seven.

Neuroticism

The evidence from previous empirical studies has tended to show that users who scored high on the neuroticism trait were less susceptible to CSE in the email context (Alseadoon *et al.*, 2015; van de Weijer and Leukfeldt, 2017) and in the SNS context (Albladi and Weir, 2017; Frauenstein and Flowerday, 2020). On the other hand, some previous research showed that neuroticism was associated with higher susceptibility to cyberattacks (Halevi *et al*., 2013a, 2013b; Shappie *et al.*, 2020).

This study hypothesised that employees who expressed high levels of neuroticism would be less susceptible to CSE victimisation on LinkedIn than would those who expressed low levels of this trait. In the multivariate analysis, when controlling for all other variables in the model a 1-unit increase on the neuroticism scale increases the odds of being susceptible to CSE victimisation over LinkedIn at work by 34.2% ($p = .025$). This was an unexpected finding given previous findings in the literature, but if the population sample is considered along with contextual and other factors of the model, some possible explanations may be posited. These factors could have a confounding effect on this trait. For instance, one could argue that people who are nervous/anxious about their career status, or about interpersonal relationships with others, might feel more comfortable doing things online which their neurotic personality hinders them from doing offline. There is some support for this in the qualitative findings. Interviewees noted that "*Many individuals in an online context behave differently than when they are in real life*" (IP6) and that offline contextual and situational factors such as "*financial difficulties, culture shock, [the] need to vent or express [themselves]*" or even being single and seeking companionship can lead to poor judgement and making bad decisions over SNS such as "*fall[ing] victim to relationship scams*" (IP2) or a "hasty decision, neglecting potential dangers of clicking on phishing links of attractive job applications or opening PDF format job descriptions" (IP10).

In the qualitative findings, interestingly, there were several descriptions of behaviour and attitudes of non-Saudis (expatriates) that matched neurotic sub-traits such as fear, insecurity and impulsiveness, for example: "*Residents [expatriates] always fear falling into error … Such fear, along with the sense of job insecurity…*" (IP15). "*Being cautious … so as to comply and cope within a different environment, could impact on their behaviours and consequently could reshape their habits and impulsive responses*" (IP2). However, the association between neuroticism and nationality in the quantitative findings was non-significant. There might be confounding effects that would require further research.

This study also found significant differences in neuroticism scores related to age and gender. These findings will be discussed in turn. Neuroticism is the inverse of emotional stability; individuals who are highly neurotic tend to feel anxious, insecure, nervous and sad (Oyibo *et al.*, 2017; see also Chapters 2 and 3). Women responding to the survey questionnaire scored significantly higher ($M = 5.00$) ($p < .001$) than did men on neuroticism ($M = 3.65$). This result was to be expected as previous empirical research has consistently found that females scored higher than males on this trait (Costa *et al.*, 2001; Weisberg *et al.*, 2011). The qualitative findings echoed the quantitative results to some extent. Female interviewees described themselves as follows: "*I would not personally go against my instinct or to willingly engage in an act that involves even a low percentage of threat*" (IP6) and "*nervous*" about being contacted over SNS by an unknown person (IP9). Although these women were referring to threats of CSE victimisation, these statements are used by this researcher in this context to infer some degree of neuroticism in the women who said them. However, it is understood that they were not specifically referring to themselves as "neurotic".

The literature suggests that employers are not likely to favour hiring highly neurotic personalities. This is because they are (according to the FFM dimensional definition) emotionally unstable, nervous, and lack self-efficacy (Oyibo *et al.*, 2017; Gupta and Gupta, 2020). However, it must be assumed that some proportion of employees in a given organisation will be high scorers on the neuroticism dimension. Therefore, it is important for employers to take into account the specific types of CSE risks posed by such employees. Specific recommendations are discussed in Chapter Seven.

Summary of Discussion about Personality Traits and Susceptibility

The findings presented in Chapter Five suggest that all five of the Big Five personality traits (conscientiousness, extraversion, agreeableness and openness to experience) significantly influenced susceptibility to CSE victimisation, and they did so in the direction posited by the study hypotheses. For employees of the organisation and controlling for all other factors:

- A 1-unit increase on the conscientiousness scale (i.e., an increase in the level of conscientiousness) *decreases* the odds of being susceptible to CSE victimisation over LinkedIn by 56.7%.

- A 1-unit increase on the extraversion scale (i.e., an increase in the level of extraversion) *increases* the odds of being susceptible to CSE victimisation over LinkedIn by 80.6%.
- A 1-unit increase on the agreeableness scale (i.e., an increase in the level of agreeableness) *increases* the odds of being susceptible to CSE victimisation over LinkedIn by 151.5%.
- A 1-unit increase on the openness to experience scale (i.e., an increase in the level of openness to experience) *increases* the odds of being susceptible to CSE victimisation over LinkedIn by 41.2%.
- A 1-unit increase on the neuroticism scale (i.e., an increase in the level of neuroticism) *increases* the odds of being susceptible to CSE victimisation over LinkedIn by 34.2%.

Some findings regarding the relationships between specific personality traits and gender, age, nationality, and employment position (power level) were interesting. In particular, gender stood out as a differentiating factor in all five personality traits: significant differences between females and males were found in scores for each trait. Nationality was a differentiating factor in extraversion and agreeableness, with Saudis scoring significantly higher one both. Power level was a differentiating factor for openness, with lower-level employees scoring higher than their superiors on this trait. Age was significantly and positively associated with neuroticism, in that the trait increased with age. These findings and their implications for organisations merited some probing, and the qualitative data from the semi-structured interviews shed light on some of these relationships.

In any given organisation, it can be assumed that there will be some employees from each category of the Big Five personality traits. Therefore, it is important for employers to consider the specific types of CSE risks posed by individuals with each trait. It is crucial that the organisation provide and require up-to-date, appropriate and effective CSE awareness training for all its employees – of any personality type. Specific recommendations are discussed in Chapter Seven.

6.2.3 Disposition to Risk and Susceptibility

A number of personal dispositions to risk and security have been identified in the literature as influencing users' susceptibility to CSE. This study examined four commonly attributed factors: *risk perception, willingness to assume risk, perceived control of information (privacy risk)* and *IT self-efficacy*. Overall, the study results indicated that MHRSD employees perceived themselves to be at risk by using SNS; moreover, the survey respondents perceived themselves as having some degree of control over those risks. With the exception of IT-self efficacy which had a negative and significant association with CSE victimisation, the factors of risk perception, perceived control of information and willingness to assume risk were not evident in the final logistic regression, Nevertheless, there are some interesting findings that show that high risk perception, high perceived control over information (privacy risk) and willingness to assume risk can pose risks for employees and consequently for organisations. These results are discussed in detail within this section.

IT Self-Efficacy

As explained earlier, IT self-efficacy is based on perceived behavioural control; this construct is also related to origin and control, two concepts from organisational psychology and risk management theory (see Chapters 2 and 3). A higher level of self-efficacy can lead to a higher level of behavioural intention (Nguyen and Kim, 2017) and, therefore, to less risky behaviour in a social networking site environment. Some previous studies on the association of IT self-efficacy with user susceptibility to cyber-social engineering reported no significant relationship (Halevi *et al.*, 2015; Saridakis *et al.*, 2016). Other researchers have found that low levels of IT self-efficacy had a positive influence on susceptibility (Anwar *et al.*, 2017; Kleitman *et al.*, 2018).

This study hypothesised that employees who expressed high levels of IT self-efficacy would be less susceptible to CSE victimisation on LinkedIn than would employees who expressed low levels of this factor. In a multivariate logistic regression, this hypothesis was supported (at 5% significance level). A 1-unit increase on the IT Self-Efficacy scale decreases the odds of being susceptible to CSE over LinkedIn by 34.8% (see Table 5-32 in Chapter 5). In contrast to this study's findings, Saridakis *et al.* (2016) reported finding a

positive, but non-significant, association between higher IT self-efficacy and risk of cybercrime victimisation.

This study found that fewer than 4 in 10 survey participants felt confident in their IT self-efficacy. Moreover, two-thirds of MHRSD employees surveyed did not have confidence in their IT-related abilities, such as navigating SNS applications, operating any digital device, determining the authenticity of well-known websites and applications such as LinkedIn, and understanding the terminology of SNS privacy policies.

The findings from the qualitative data provide some important insights about the quantitative results. One interviewee questioned whether the meaning of "confidence" was universally understood (as the items for IT self-efficacy all used the phrase, *I feel confident…*), commenting, "*Confidence is a rubbery term when it refers to one's [own] technological abilities*" (IP6). Thus it may be inferred that this was a reason for the large proportion of employee responses indicating uncertainty about their IT self-efficacy. On the topic of low IT self-efficacy, interviewees IP6 and IP7 noted that in their workplaces, employees tended to "*rely blindly*" on the organisation's IS infrastructure as if it were failsafe, giving many workers a false sense of security. A number of interview participants (IP1, IP12, IP13, IP15) stressed the importance of employees' IT competence in deterring or preventing CSE attacks. One interviewee likened the problem of low IT self-efficacy to "*patients neglect[ing] reading the prescription leaflet until side effects start showing. [Then] they call their doctor or read the leaflet*" (IP13). This analogy and other statements point to a theme of self-efficacy being preventative (i.e., "medicine" to prevent the "disease") of CSE susceptibility.

It is even more concerning that the vast majority (83%) of MHRSD employees seemed unfamiliar with the term "cyber-social engineering". Yet arguably, although the term might sound new and somewhat technical, they and many people who use online communications and services are certainly already familiar with the concept. They simply know it by a different term, such as deception, phishing, scamming, and so on. The low levels of IT self-efficacy expressed by the survey respondents, combined with this low level of CSE awareness, is concerning. It can be argued that the confidence level versus how employees truly felt about their abilities might be due to a lack of InfoSec training, as the findings of this study on CSE awareness suggest (see Chapter 5, section 5.3.6.1). The implications for organisations, and how they must address these concerns, are discussed in Chapter Seven.

Risk Perception

Previous studies have found a positive relationship between risk perception and adoption of IS security practices (Halevi *et al.*, 2016; van Schaik *et al.*, 2017). Vishwanath *et al.* (2016) found that risk perception (cyber-risk belief) influenced susceptibility to phishing attacks. The findings of this research showed that the majority of employees (nearly 60%) had moderate to low risk perception (disagreeing or only somewhat agreeing that certain items entailed risk). In particular, the survey asked if respondents thought there were risks associated with uncertainty, losses and unexpected problems as a consequence when giving information over SNS. Between 25% and 31% of respondents, that is, 99 to 122 MHRSD employees, strongly agreed that sharing information over LinkedIn was risky. A smaller number (55 to 74) strongly disagreed with this assertion (i.e., they did not perceive such actions to be risky), while 236 to 197 (N = 394) aligned with a more neutral stance on the issue.

The qualitative data presented a different profile of attitudes to risk; however, this was to be expected since the interview sample consisted of experts and academics in the fields of cybersecurity, IT, sociology and the like. There was unanimous agreement among the 15 interviewees that sharing information over CSNS posed *"risks of fraud or identity theft and the invasion of virtual communication networks for privacy and harassments in all its form"* (IP8). They also highlighted the risk of exploitation via fake or highjacked LinkedIn profiles to allure already connected peers or those who were not close acquaintances: "*the danger, rather, is how your profile can be used as an attack tool*" (IP15).

Most interviewees suggested that users would downplay the risk, not believing that they would be victimised. This is indicative of a phenomenon known as "optimistic bias", in which people "*tend to believe that they are less likely to encounter negative events and more likely to encounter positive events than the average person*" (Keaney, 2012, p. 37). Curiosity was posited as a contributing factor to low risk perception while navigating social media: "*they arbitrarily minimise the magnitude of whatever bad outcomes [might result], due to users' tendency of curiosity*" (IP10). Another interesting consequence of sharing information over CSNS highlighted by interviewees was that it could lead to a much greater risk in cases where the duped individual uses the same password with their emails. In such cases, LinkedIn works as a gateway to email accounts, which contain information that is more confidential and sensitive.

Unexpectedly, and contrary to the hypothesis, high risk perception was not found to affect susceptibility, at least in this study sample when controlling for all other factors in the model. This result is consistent with Saridakis *et al.*'s (2016) study, in which they reported that risk perception had an "*insignificant effect*" on cybercrime victimisation (p. 19).

As mentioned above, a large proportion of the survey sample displayed an ambivalent or neutral attitude towards the risks associated with sharing information over LinkedIn. These neutral attitudes and beliefs about cyber risk may explain the finding that risk perception did not have an effect on susceptibility to CSE in this study. Nevertheless, the fact that the majority of employees did not strongly agree that there were risks involved with using SNS/CSNS has serious implications for organisations, as discussed later in Chapter Seven.

Willingness to Assume Risk

Whereas risk perception is about an individual's judgement and beliefs regarding a potential threat, risk propensity (willingness to assume risk), is more about an individual's appetite for and tendency to take the risk while acknowledging its existence. Previous research has shown that an individual's wish to obtain a particular objective (such as a lucrative job offer) can increase a user's willingness to take risks in online contexts (Cases, 2002; Nguyen and Kim, 2017), and that high levels of risk propensity may result in CSE victimisation via CSNS (Saridakis *et al.*, 2016; Krehel, 2016; Nguyen and Kim, 2017).

Based on evidence from previous research, this study posited that employees who expressed high levels of willingness to assume risk would be more susceptible to CSE victimisation on LinkedIn than would employees with low levels of willingness to assume risk. In a bivariate logistic regression, this hypothesis was supported (at 5% significance level): a 1-unit increase on this scale increases the odds of being susceptible to CSE victimisation on LinkedIn at the workplace by 21%. However, after controlling for all of the other variables in the model, this factor did not predict susceptibility to CSE on LinkedIn for this study.

Although there is no link with CSE victimisation, past research and the qualitative interviewees suggest that employees who score high on risk propensity pose a threat to organisations through their willingness to accept risks over LinkedIn (such as by clicking on links in malicious messages in hopes of attaining some reward or opportunity). The quantitative findings show that there is a significant difference between those *Willing to*

accept risks of losing money in an attractive LinkedIn job offer (M = 4.27) compared to those who had not experienced a negative event (M = 3.78). Similarly, those *Willing to risk personal information engaging with posts (i.e. job offers, contracts)* (M = 4.38) compared to those who had not had a negative event from LinkedIn (M = 3.75) Both measurement were on a 7-point scale. This finding accords with previous research, which has shown that the relationship between risk perception and susceptibility to CSE is the inverse of the relationship between risk propensity and CSE susceptibility (Saridakis *et al.*, 2016; Nguyen and Kim, 2017).

As mentioned in the previous section, the majority of the employees in the survey sample exhibited low to moderate risk perception. With regard to risk propensity, between 25% and 30% of respondents in the survey sample indicated their willingness to assume risk. This is including using unfamiliar CSNS platforms; responding to alluring job offers over LinkedIn with the understanding that they might risk losing money as a consequence; and risking the security of their personal information for a job or contract offered via LinkedIn. One third of the sample responded that they were not willing to take these risks, whereas between 36% and 44% of employees gave neutral responses regarding risk propensity.

This study's findings showed that male employees were more willing (M = 3.97, p = .068) than their female colleagues (M = 3.53, p = .068) were, to take risks to engage with services provided via LinkedIn. Men were more likely (M = 3.93, p = .052) than females were (M = 3.46, p = .052), to share their personal information if a purported job offer posted on LinkedIn involved a small amount of risk. Male employees (M = 4.03, p = .08) were also more willing than females were (M = 3.60, p = .08), to use an unfamiliar CSNS. Although these findings are significant at the 10% level, they lend supported by previous research, which has shown that men are generally higher risk-takers than women are (Weber *et al.*, 2002).

Participants interviewed for this study unanimously believed that gender influenced willingness to assume risk. Specifically, males were seen as more willing to take risks, while females were viewed as risk averse. "*Men like to take risks and engage unhesitatingly with strangers online*" (IP11), whereas "*[women] do not like to take risks and … are less daring*" (IP15). Interestingly, the way in which female interviewees described this phenomenon differed from the way their male counterparts presented it. Women participants invariably pointed to social/cultural reasons for the difference in risk propensity, whereas men were likely to mention both social and physiological reasons. It

is possible that the role of subjective and cultural norms may play a mediating role in these gender-based differences.

In addition to gender, thematic analysis of the qualitative data identified other possible factors contributing to an individual's willingness to assume risk. Interview participants mentioned risk propensity in connection with nationality. "*[Expatriates] always fear falling into error, which threatens their career … [Saudis] have a greater [acceptance of] risk of adventure …*" (IP15). As mentioned in Section 6.2, certain personality traits were also mentioned by interviewees in connection with risk, such as openness to new experiences: "[*the need] to self-learn and explore different aspects of knowledge … can be driven by high curiosity [which] can … get you into negative consequences*" (IP10). The relationship between openness and power level within the organisation was also highlighted by interviewees, and this is discussed later, in Section 6.2.6.

Perceived Control of Information (Privacy Risk)

Van Schaik *et al.* (2017) found that perceived control was a significant predictor of precautionary (i.e., risk-reducing) IS behaviour. Therefore, this study posited that employees who perceived they had control over information (privacy risk) would be less susceptible to CSE victimisation on LinkedIn than would their colleagues who perceived they had little control over their information. In a bivariate logistic regression, this hypothesis was supported (at 5% significance level). A 1-unit increase on the perceived control of information scale decreased the odds of experiencing a negative incident on LinkedIn at work by 18%. However, the multivariate stepwise logistic regression omitted this factor; thus, perceived control of information (privacy risk) was removed from the final model (see Table 5-32). This could be due to confounding effects of other factors, which calls for further research.

The quantitative survey responses revealed that just over 40% of MHRSD employees felt confident that they had control over how their personal information was used by LinkedIn. Only 28.2% of employees believed they had control over who could access their personal information, and even fewer (27.2%) felt confident that they had control over which personal information could be released by LinkedIn. It is noteworthy that the majority of MHRSD employees (between 47% and 64%) responded neutrally to these items, indicating that they were unsure about the level of control they exercised over their PII on LinkedIn. These findings suggest that even if some people might imagine how their personal

information is used by LinkedIn (advertising, targeting, recommendation systems), fewer people are aware of the details: what personal information is released by LinkedIn and who can access it.

The qualitative data supplements the quantitative findings. It should be remembered that, in contrast to the survey respondents, who were civil service employees of various ranks but who did not have backgrounds in InfoSec or even IT, many of the interviewees were IT professionals and some were cybersecurity experts. Therefore, their views regarding perceived control of information might be expected to differ noticeably from the attitudes of the MHRSD employees who participated in the survey. Indeed, one interviewee summed up a plausible reason for the seemingly ambivalent beliefs of the survey respondents: "*being in control of what of their information is accessed and used by these career social media companies and websites can be confused with what THEY have control of and share by themselves via the privacy settings in their profile*" (IP3).

As mentioned in Chapter One, the fact that LinkedIn is a SNS aimed at professionals and businesses, there is a common belief that its users need not worry about access by others to their personal information (Cooper and Naatus, 2014). Several interviewees (IP1, IP3, IP6, IP15) also mentioned this trade-off between information privacy and convenience – including the touted career benefits of having a "*complete profile*" on LinkedIn (IP3) – that has come to be expected and accepted by users. Interviewees suggested this was one reason for the apparent lack of concern about what or how much of their PII users have the ability to control. An interesting finding from the qualitative data amongst employees indicated that managers and those at lower administrative levels had different opinions regarding perceived control of information. This finding is discussed in more detail in Section 6.2.5.

Summary of Discussion about Disposition to Risk and Susceptibility

The results presented in Chapter Five demonstrate that, after performing the multivariate logistic regression to account for possible confounding factors, three of the four factors from the study model relating to disposition to risk were omitted. That is, when controlling for all other variables in the model, IT-self efficacy was the only factor in the disposition to risk domain for which the study hypothesis was supported. Findings from the qualitative data also supported this hypothesis: interviewees suggested that employees who had low IT self-efficacy would benefit from clear guidance and IS security awareness and efficacy training in the workplace.

The interviewees provided some interesting insights to explain the relationships as they might occur for individual employees in the workplace, such as individual differences in motivation (e.g., curiosity vs. job insecurity) and gender differences in levels of risk propensity. In this study, risk perception and willingness to assume risk did not show a relationship with susceptibility to CSE risk on LinkedIn,. However, the mean ratings in both factors, risk propensity and risk perception, suggest that the majority of employees did not strongly agree that there were risks involved with using SNS/CSNS, which is concerning. Similarly, on average, male employees exhibit higher levels of risk-taking than their female counterparts. Organisations should take these findings into account (see Chapter 7). In addition, the fact that perceived control of information (privacy risk) was removed from the final model suggests this factor does not predict susceptibility to CSE victimisation over LinkedIn. If people do not perceive themselves to be in control of information, this can still pose risks, and as such is concerning for themselves and for organisations. The implications of all these findings are detailed in Chapter Seven. The model factors relating to risky habitual behaviour and their relationships to CSE susceptibility are discussed next, in Section 6.2.4.

6.2.4 Risky Habitual Behaviour and Susceptibility

In the literature on susceptibility to cyber-based social engineering attacks, habitual behaviour online has been shown to influence an individual's susceptibility to CSE victimisation, whether in the context of email or SNS (Vishwanath, 2014, 2015a, 2015b; Saridakis *et al.*, 2016; Albladi and Weir, 2018, 2020). This current study has focussed on three aspects of user risky habitual behaviour (RHB) on CSNS: *information security habitual behaviour*, *level of engagement* and *frequency of SNS use*. While the survey results showed that the majority of respondents did not generally engage in habitual risks (RHBIS: M = 2.28; Level of Engagement: M = 2.72; Frequency of Use: M = 3.85, on a 7-point scale), almost all respondents (96.2%) used SNS while at work at least sometimes, and only 3.8% never used SNS. Nearly one quarter (24.4%) of respondents reported using their SNS at work on a regular basis (at least once a week). The study findings for each of the three RHB factors are discussed in detail below. Implications for organisations are discussed in Chapter Seven.

Frequency of SNS Use

The quantitative survey responses revealed that the vast majority (96.2%) of employees reported using SNS at work at least occasionally, and nearly one in four (24.4%) of them said they did this at least once a week. Only 15 MHRSD employees in the sample of 394 said they never accessed their SNS while at their workplace. Given the high proportion of employees who did access SNS at work, it would be expected that this behaviour would be remarked upon by the interview participants. In the qualitative data, frequency of use is often not distinguished clearly from level of engagement. Nevertheless, interviewees (IP6, IP8) did mention frequency specifically, as in "*gradually increasing the hours spent [on] social media sites or the frequent overuse of social networks without professional or academic necessity*" (IP8). They also considered that frequency was related to several factors, including the need to be a part of the group (IP5), the attraction of following celebrities and other influencers (IP1), and the need to keep up with the latest happenings (IP6).

This study also investigated the relationship between frequency of SNS use at work and the demographic variables of gender, age, nationality and employee level within the organisation (work level). These associations were found to be non-significant. Indeed, the qualitative data seemed to confirm this finding, as the interviewees variously attributed the frequent use of SNS at work to both genders, to "*youngsters – and older people alike*" (IP6), and to both Saudis and non-Saudis. They did not mention any distinction between management and lower-level staff when it came to frequency of SNS use.

Vishwanath (2014) found that people who used SNS frequently and actively were susceptible to "level 2" CSE attacks that involved scams via requests for the user to provide information to the attacker (see Chapter Two). Other studies also considered frequency of use as one of several indicators of high involvement or engagement on SNS but did not report finding that frequency of SNS use, as a factor on its own, increased susceptibility to CSE attack (Vishwanath, 2015a; Saridakis *et al.*, 2016; Albladi and Weir, 2018). This study hypothesised that employees with high frequency of SNS use on LinkedIn would be more susceptible to CSE victimisation than would those with lower frequency of use of that site. In spite of the support for this relationship found in the qualitative data described in the previous paragraph, this hypothesis was not supported by the quantitative results.

Information Security Habitual Behaviour

Most survey respondents in this study (between 84% and 89%) reported that they never set personal information to strangers over the Internet, used trivial passwords, entered payment information on unsecure websites or shared their password with a friend or colleague. However, the converse of this finding is that up to 16% of the sample (63 MHRSD employees) reported engaging in these risky behaviours at least sometimes during the previous 6 months. Moreover, a number of other risky behaviours were far more common among respondents: using the same password for more than one account (53% said they did so regularly), downloading data and material from websites on their work computer without checking its authenticity (30%), saving information about their work on their personal devices (26%), sharing their current location on social media (26%) and using free-to-access public Wi-Fi (26%). If, during a given 6-month period, 118 employees regularly downloaded potentially unsafe content from websites onto their work computers, this habit can pose a risk to the information security of the organisation in question.

Interview participants provided insights as to the reasons behind or the conditions leading to employees engaging in these risky habitual practices in the workplace. Interviewees observed that in the workplace, employees tended to believe that IS security was the responsibility of the organisation, and that this absolved them of individual responsibility for following cybersecurity protocols (IP6, IP7). One interviewee even alleged that the organisation's own attempts at implementing good cybersecurity practices can backfire, when it puts in place Internet "*access restrictions and so employees bring their own Wi-Fi SIM*" (IP6). This finding suggests the need for further research; its implications for organisations are discussed in Chapter Seven.

In testing their SCAM model, Vishwanath *et al.* (2016) found that the nature of habitual behaviour (force of habit) caused users to react automatically by clicking on links in malicious messages instead of consciously, intentionally following IS security guidelines, which thus led to increased susceptibility to CSE victimisation. In accordance with that and similar previous findings, this study posited that employees with low levels of information security habitual behaviour on LinkedIn i.e., scoring high on *risky* habitual IS behaviour) would be more susceptible to CSE victimisation than would those with higher levels of information security habitual behaviour (i.e., scoring low on *risky* habitual IS behaviour) on CSNS. However, the association between RHBIS scores and CSE susceptibility was statistically significant (at 10% level, $p = .056$).

This study also investigated the relationship between the three risky habitual behaviour sub-factors and the demographic variables of gender, age, nationality and employee level within the organisation (work level). Interestingly, the only significant relationship found was between risky information security habitual behaviour and gender: males had higher levels of risky habitual behaviours than females had: (females: M = 2.07, males: M = 2.35, p = .047). This finding is discussed in more detail in Section 6.2.5.

Level of Engagement

Based on findings from previous research (Vishwanath, 2014, 2015a; Saridakis *et al.*, 2016; Albladi and Weir, 2020), this study hypothesised that employees with high levels of engagement on LinkedIn (RHBLE) would be more susceptible to CSE victimisation than would those with lower levels of engagement on LinkedIn. In a bivariate logistic regression, this hypothesis was supported (at 5% significance level, p = .038). However, when controlling for the effects of other factors in the model, level of engagement was removed as predictor to susceptibility due to possible confounding factors in the model.

The findings of this research also showed that in the 6 months prior to the survey, overall, respondents had moderate to low levels of engagement (M = 2.72) on SNS while at work. Even so, the majority (315 employees, nearly 80%) reported having logged into their SNS from work devices, and 17% of MHRSD employees in this survey stated that they did this regularly (*once a week*, *twice a week* or *always*). At least 180 employees (nearly 46%) had sent messages to work colleagues through social media sites, and 70 employees (18% of respondents) said they did so on a regular basis. One in three MHRSD employees (32%) in the survey sample admitted to checking their email notifications from their SNS on a regular basis, while more than half of them (53%) did so from time to time. A substantial proportion of the employees (41% to 45%) said they had talked about confidential company information or shared photos or documents containing company information on SNS, and between 9% and 16% did this regularly.

The interview participants shared some interesting insights as to why and how employees might participate in such risky behaviours on SNS and CSNS. Being part of the group was mentioned frequently: *"people … don't care about what [they] share because they know these platforms are all about sharing and connecting*" (IP3). "*Everyone wants to be involved … they want to see what is going on*" (IP5). Regarding LinkedIn specifically, "*They have their ways to make you reveal more about yourself, [to make you] engage more*

to understand your behaviour patterns for marketing purposes" (IP3). A number of participants referred to this habitual behaviour as a form of "*dependence*" (IP9), being "*hooked*" (IP6) and even an "*addiction*" (IP8, IP9). Interestingly, one third of the interview participant sample (IP2, IP5, IP6, IP7, IP10) mentioned curiosity as a contributing factor to risky habitual behaviour. This is a factor that should be added to further studies.

Although the level of engagement scale was not a statistically significant predictor for CSE victimisation, the findings of this study are useful for organisations in guiding them to implement targeted strategies proactively, as discussed in Chapter Seven.

Summary of Discussion about Risky Habitual Behaviour and Susceptibility

The results presented in Chapter Five showed that of the three risky habitual behaviour sub-factors, only risky information security habitual behaviour on SNS was found to significantly influence susceptibility to CSE victimisation (at 10% significance level). This single factor from the domain of risky habitual behaviour, along with IT self-efficacy from the domain of disposition to risk, have turned out to outbalance the remaining factors for their respective domains. One explanation for this finding might be that these two factors are related to the ubiquitous and indispensable nature of Internet-connected devices within the workplace (e.g., IoT for businesses like biometric access, security cameras, Zoom/WebEx, VoIP applications, etc.). As such, level of engagement on SNS is a behavioural factor that impacts on IS security, while the attainment of necessary ISS skills for employees operating within the workplace has a role to play in reducing susceptibility to CSE attacks. Such factors can be mediated by other factors of the same group, which suggests the need for further investigation on the roles of perceptual and demographic aspects as mediating influences on susceptibility. However, level of engagement is not evident in the multivariate logistic regression. This may be because it is confounded with other variables. Although it is non-significant, one would argue generally that even the lowest percentage occurrence of these risky behaviours can lead to CSE susceptibility risk.

It should be noted also that, in the multivariate logistic regression analysis and when controlling for the effects of other variables in the model, information security habitual behaviour was the only risky habitual behaviour found to be significantly linked with CSE susceptibility (at 10% significance level). A 1-unit increase in the score on the RHBIS scale increases the odds of being susceptible to CSE victimisation over LinkedIn by 27.7%.

Another important finding was that nearly one quarter (24.4%) of employees in the sample reported using their SNS at work on a regular basis (at least once a week). This last group are at high risk of CSE victimisation, according to a report from SANS Institute which highlights the increase in security risks to enterprise networks and their data when their employees use social media at work (Chi and Wanner, 2011). In this study, RHBIS was the only factor found to be significant predictors of susceptibility in this study when controlling for the effect of other factors at 10% level Although other risky habitual behaviours in terms of level of engagement and frequency of SNS, were not found to be significant predictors of susceptibility in this study, risky habitual behaviours by employees pose serious cybersecurity threats to organisations. These implications and some recommended practices are discussed in Chapter Seven.

6.2.5 Demographic and Cultural Factors and Susceptibility

Demographic factors such as age, gender, education, nationality/culture and socioeconomic status are often included in research on user susceptibility to cybercrime (Parrish *et al.*, 2009; Alseadoon, 2014; Heartfield *et al.*, 2016: Norris *et al.*, 2019). As explained in Chapter Two, certain demographic factors have been shown to influence perceptual, behavioural and motivational factors (Bonem *et al.*, 2015). This study looked at four demographic factors: gender, age, work level within the organisation (structural power) and nationality. As explained in Chapter Three, the latter two factors can be classified as cultural factors, as they pertain to organisational and national culture (Hofstede, 1980), respectively. Previous research regarding how and whether each of these factors influences susceptibility to cyberattacks has produced conflicting findings (see Chapter Two, Section 2.8.5). Therefore the four hypotheses regarding the relationship between demographic factors and susceptibility to CSE posited for the Model of Susceptibility to CSE Victimisation on LinkedIn were based on the most common findings in the literature for each trait. Overall, this study's findings showed that age, gender, and nationality each had a significant influence on susceptibility to CSE victimisation. Work level/structural power in the organisation was not shown to influence CSE susceptibility to a significant degree, but the qualitative data revealed some interesting findings regarding differences between lower- and higher-level employees within the organisation. These findings are detailed below.

Age

Age is one of those demographic factors that is typically included in the data collection in research on susceptibility to cybercrime via social engineering, but not always investigated as an independent variable. One of the reasons for this is that a large proportion of these studies are conducted on undergraduate student populations, which obviously do not differ greatly according to age. Of those studies that did include age as a factor, some found that age was inversely related to susceptibility to cybercrime (Leukfeldt and Yar, 2016), whereas others found that certain age groups (usually 18-25 years, or in that approximate range) were more susceptible than others (Sheng *et al.*, 2010; Saridakis *et al.*, 2016), but there was no directional relationship (whether positive or negative) between age and CSE susceptibility across the age groups. For instance, Saridakis *et al.* (2016) found that users in the 29-38 and 49-58 age groups were less at risk of cybercrime victimisation than those in the 18-28 cohort.

Based on evidence from previous research, this study hypothesised that older employees would be less susceptible to CSE victimisation on LinkedIn than would younger employees. This hypothesis was strongly supported: employees in the oldest age group (62+ years) were less susceptible (at 1% significance level) to CSE victimisation than were those from younger age groups. When controlling for all the other factors in the model using multivariate logistic regression, when compared to the 18-28 age group: the odds of being susceptible to CSE victimisation over LinkedIn decreased by 73.8% for age group 29-39, by 76.6% for age group 40-50, by 84% for age group 51-61, and by 95% for ages 61 and over. This finding is not surprising, but it is interesting. An inverse relationship is evident: the older the employees are, the less susceptible they are.

One plausible reason for this finding comes via another quantitative finding. For the survey sample of this study, the mean neuroticism score showed a statistically significant increase with age. Specifically, mean neuroticism scores significantly increased with age (e.g., M = 2.73 for those aged 18-28, and M = 5.06 for those aged 62 and above). This finding is interesting from a couple of angles. This relationship might be linked to risk propensity, which also is associated (but negatively) with age: risk aversion, which is the opposite of risk propensity, increases with age (Hadlington, 2018). Indeed, Bonem *et al.* (2015) found that age was a mediating factor for risk perception and risk propensity. Furthermore, Whitty *et al.* (2015) had posited that elderly people, being less IT-savvy, would be less aware of cybersecurity risks making them more likely to share passwords than people in younger

age groups would. To the contrary and unexpectedly, Witty *et al.* (2015) found that the senior citizens were less likely to share passwords. Witty *et al.* (2015) did not speculate as to why that age demographic might be averse to sharing passwords but other research has found that employees who were strict about not sharing passwords were judged by their co-workers as "*paranoid*" (Weirich and Sasse, 2001), which is a sub-trait of neuroticism. Although neuroticism was not tested in Weirich and Sasse's (2001) study, it is possible that this trait, rather than age, may have been the direct influencing variable in both this current study and in that of Witty *et al.* (2015). Thus, it is not unreasonable to suggest that higher scores on neuroticism might be the reason behind senior citizens being less susceptible. The qualitative data did not provide any insight as to why this might be the case. The relationship between age and neuroticism as it pertains to CSE susceptibility may require further investigation in future.

Age might also be linked to structural power (work level), as discussed later, in that subsection. The qualitative findings did not reveal any further insights into the relationship between age and susceptibility.

Gender

Of the four demographic factors investigated as part of this study, gender is the most commonly examined in the literature on susceptibility to cyber-social engineering. Many studies have found that gender is an influencing factor in susceptibility to CSE victimisation; however, the research is not in agreement as to whether males or females are the more susceptible of the two genders. Some research indicates that due to their higher risk propensity (Byrnes *et al.*, 1999), men may be more likely than women would be to fall victim to CSE attack and, conversely, that women are usually more cautious than men are (Hadnagy, as quoted by Mills, 2010). However, the majority of studies have found that women are more susceptible than men are to CSE attack, due to lower IT self-efficacy, higher levels of engagement online and/or risky cybersecurity behaviours (Sheng *et al.*, 2010; Halevi *et al.*, 2013a, 2013b; Blythe *et al.* 2011; Greitzer *et al.*, 2014; Algarni *et al.*, 2014, 2017; Leukfeldt and Yar, 2016; Anwar *et al.*, 2017; Goel *et al.*, 2017; Airehrour *et al.*, 2018; Arend *et al.*, 2020; Albladi and Weir, 2020).

This study posited that female employees would be less susceptible to CSE victimisation on LinkedIn than would male employees. When controlling for all the other variables in the model, (with females as the reference category) the odds of being susceptible to CSE

victimisation on LinkedIn was 6.2 times higher for males. Thus, this study's finding differs from the great majority of previous studies on the relationship of gender to CSE susceptibility. The qualitative findings on the issue of gender and susceptibility to CSE are interesting. The overall opinions of the interviewees did not point to any expected difference in susceptibility based on gender alone, but rather in association with other factors. These are discussed in turn, below.

As discussed earlier in this chapter, men's and women's scores on a number of other factors differed significantly. As expected, males and females differed in their levels of risky habitual behaviour. Men were more likely to save information about their work (or organisation) on their personal electronic devices, to download free anti-virus software from an unknown source and to rely on a trusted friend or colleague to advise on aspects of online security (Chapter 5, Section 5.3.3). This finding was confirmed by the qualitative data, as detailed in Section 6.2.3. This higher level of engagement by males in risky habitual behaviour accords with the finding in this study and in the literature that males are more willing to assume risk than are females. Moreover, if an employee has the intention to download illegal software, this may be an indication of other closely related risky InfoSec behaviours, such as seeking out and downloading other unsafe forms of software or media files.

There were also clear differences between the genders in scores on a number of personality traits: women ($M = 5.20$) scored significantly higher than men ($M = 4.83$), did on the conscientiousness ($p < .01$) and neuroticism scales (females: $M = 5.0$, males: $M = 3.65$, $p < .001$), and significantly lower than men did on agreeableness (females: $M = 4.04$, males: $M = 5.27$, $p < .001$). With regard to conscientiousness, this suggests that females are more careful and more likely to obey policies than males are. This finding from the quantitative survey is supported by the qualitative findings as well. One interviewee stressed that "*women [were] less likely to engage in trouble*" (IP15), which implies that women tend to be more cautious and try to avoid negative consequences. IP15 suggested that this might be due to physiological cues that could influence how women interact with others. This agrees with what InfoSec expert Christopher Hadnagy stated: "*women are more cautious by nature and that makes them less susceptible to social-engineering attacks*" (Mills, 2010). This could explain the higher scores by women on the conscientiousness scale.

High scores on conscientiousness and neuroticism and low scores on agreeableness are all associated with lower susceptibility to CSE victimisation in the literature, as discussed in

Section 6.2.2 above and in Chapters Two and Three. Two of these score results are associated with lower susceptibility in this study as well, neuroticism being the exception. However, the female survey participants in this study also scored higher than their male counterparts on extraversion ($p < .001$) and openness ($p < .05$), both of which would indicate higher susceptibility to CSE attack according to the literature and to this study's findings. These latter two scores were in contradiction to expectations, and as such they require further examination in studies carried out within the same context.

As mentioned in Section 6.2.2, female employees also scored significantly higher ($M = 521$, $p < .001$) than their male colleagues did on extraversion ($M = 4.01$). This was an unexpected finding, so the qualitative data were reviewed for further insights. However, nothing in the interview data pointed to a possible reason why women in Saudi Arabia might score higher than men on this trait. In fact, the qualitative data indicated that women, at least in the Saudi Arabian context, were expected to be, and felt, more inhibited in their behaviour in public, especially around men. Nevertheless, the interview participants suggested that gender does play a role in influencing some attitudes and behaviours that are often associated with certain personality traits, such as conscientiousness. IP6, IP10 and IP14 all asserted that women in Saudi Arabia —whether by choice or due to the influence of cultural and traditional norms — preferred to uphold and accept conventional social standards.

It is evident from the qualitative findings that culture plays a role in what makes women more conscientious and self-disciplined, which can in turn influence their level of susceptibility: for instance, they are less likely to respond to deception due to societal expectations that as females they should be cautious when dealing with strangers, as explained in the section on Agreeableness. However, such reservedness was not expected of women when they were in the company of other females, and when interacting online with others whom they perceive/believe to be women, those who are natural extraverts may very well feel less inhibited in their behaviour.

Examining whether openness to experience is viewed in a gendered way in the qualitative data could shed some light on the apparent contradiction in higher female scores on this trait and their lower susceptibility to CSE victimisation, and conversely, the lower male scores on this trait and their higher susceptibility. Indeed, there was some indication of assumed gender differences in this trait. Paradoxically, however, interviewee participants seemed to believe that the opposite was true. A male participant asserted, "*men are more*

ready to experience and engage in adventures than women [are]" (IP15), while a female interviewee explained that for Saudi women "*...the notion of taking the exact responsibilities as men and doing things on their own can be intimidating*" (IP10). The reasons behind the apparent contradiction in the gender differences in openness scores relative to their susceptibility to CSE victimisation remain unclear.

Work Level Within Organisation

Previous research on the relationship between power level and CSE susceptibility is limited. Williams *et al.* (2017a) suggested that lower-level employees in an organisation might have higher levels of susceptibility to cyber-based social engineering attacks. Indeed, Aurigemma and Mattson (2017) found that senior level employees had higher perceived behavioural control than those in lower positions within the organisation, and thus the former exhibited stronger IS security compliance. Other research has indicated that this relationship is mediated by culture, whether that be the organisational culture of the workplace or the national culture of the employees (Bullée *et al.*, 2017; Williams *et al.*, 2017a).

Based on the limited evidence available from previous research, this study hypothesised that employees in senior positions in the organisation would be less susceptible to CSE victimisation on LinkedIn than would employees in a junior position. When controlling for all other factors in the study model, the odds of exposure to CSE attack on LinkedIn decreased by 67.8% for mid-level managers and supervisors ($p = .016$) and by 89% for employees at the top levels, when compared to administrative levels. Which means that the higher the work level (structural power), the less susceptible they are.

Findings from the qualitative data amongst employees suggested that top managers and those at lower administrative levels differed in their perceived control of information/privacy risk (this factor represents perceived behavioural control in the study model). Bearing in mind that most of the interviewees were either academics or in mid- to upper-level management positions, a number of interview participants (IP3, IP6, IP15) asserted that employees in general were concerned that they were insufficiently able to control their information. At least one interviewee (a university lecturer) posited that employees, particularly those in the lower ranks, were afraid to show that they did not have the control and IT self-efficacy expected of them, as "*it will be perceived as inability and therefore is reported negatively in your [annual] review*" (IP12).

An interesting quantitative finding with regard to power level and openness scores was mentioned in Section 6.2.2. As mentioned in that section, this study found significant differences (at 1% significance level) in mean openness scores of employees at different work levels. Specifically, staff at the lowest level scored significantly higher (M = 4.42) than did employees in either mid-level (M = 3.88) or top-level management (M = 3.77). The interviews yielded insights into the openness trait being significant within groups of employees in the lower level of organisation hierarchy. Several of the responses (IP1, IP3, IP4, IP15) highlighted that employees at the beginning of their career ladder are periodically seeking to advance their knowledge, and thus are more open to learning new things and trying new experiences. However, due to this openness, *"…without long years of accumulated experiences… They can still be naive in how to respond to deceptive individuals*" (IP1). This in turn could explain why lower-level employees would be more susceptible, since higher levels of the openness trait were found to increase the odds of being susceptible to CSE victimisation.

Structural power might also be linked to age. When controlling for all other factors, employee susceptibility to CSE decreased 67.8% for those in the middle management ranks as compared to the reference category of administrative office/assistant. Being in the top level of management (assuming that upper-level management are in the oldest age group) decreased the probability of susceptibility by up to 89%. However, having a higher rank does not always mean the employee is older, as employees of younger age might hold top management positions. Nevertheless, in the quantitative survey sample, senior positions were more often occupied by older employees, while lower-level positions were held by younger employees.

Finally, another interesting highlight from the quantitative survey which coupled with an auxiliary finding: in both the survey questionnaire and the semi-structured interviews, participants were asked Yes/No questions about their awareness of the technical term "cyber-social engineering", and if they had received training at work to be aware of threats, both online and via SNS at work. No significant association was found between their responses and their work levels. However, as described in Sections 6.2.3 and 6.2.4 above, the qualitative responses highlighted that the interviewees were concerned about the lack of awareness on the part of employees. The interviewees also offered an explanation as to why lower-level employees (the majority of survey respondents at 74.9%) might be the more likely to be susceptible. The expert interviewee participants suggested that this was

due to administrative/clerical employees' relatively low levels of risk perception, perceived control of information and IT self-efficacy, and their higher levels of openness and curiosity. These insights ought to be considered seriously, since between 248 and 327 of MHRSD employees received no training at work to raise awareness of online threats and SNS threats at the workplace, nor had they heard of cyber-social engineering. The implications of these findings for organisations in general are discussed in Chapter Seven.

Nationality

In the literature on susceptibility to CSE over social networking sites, nationality is not often examined as an associated factor. Nevertheless, some studies have reported that nationality, via its cultural values and norms, can affect users' susceptibility to CSE victimisation (Al-Hamar *et al.*, 2010; Rocha Flores, 2016; Albladi and Weir, 2018). As described in Chapters Two and Three, the direction and degree of influence is mediated by certain cultural dimensions. For instance, Williams *et al.* (2017a) suggested that collectivist cultures tended to place greater emphasis on adherence to social norms and discouraged nonconformity. Thus, if the majority of employees in an organisation tended to circumvent IS security protocols, individual employees would be more likely to flout those rules as well.

Considering the findings of previous research, this study posited that the nationality of an employee could increase that employee's susceptibility to CSE victimisation. However, nationality was not a statistically significant variable in the final multivariate logistic regression model. Despite the non-significant finding for nationality as it related to CSE susceptibility, the survey results showed differences between non-Saudi employees and their Saudi colleagues in scores on two personality characteristics: extraversion and agreeableness. Interestingly, and also as described in Section 6.2.2, the qualitative data from the interviews highlighted descriptions of Saudis that matched these two traits in particular, such as ""*Saudis, both male and females … Everyone wants to be involved [in SNS communities]*" (IP5 on extraversion) and "*social values that compel them to refrain from arguing with seniors or strangers*" (IP1, on agreeableness).

As mentioned in the literature, the direction of influence between nationality and CSE susceptibility depends on sub-factors of nationality (e.g., cultural norms) that have not been examined in this study model, it is necessary to look to the qualitative data for insights as to what these sub-factors might be, and how they might influence susceptibility to CSE

victimisation. It was posited in Chapters Two and Three that two of Hofstede's (1980) cultural dimensions, collectivism and power distance, seemed particularly relevant to Saudi culture as the national culture is manifested among the employees of an organisation. With regard to nationality as a factor, collectivism was mentioned specifically (IP1) and described in essence: "*Expatriates … may share the same customs and values [as Saudi nationals] that induce some to be collaborative … within their community… However, these qualities can be expressed differently when they are expatriates in [Arabian] Gulf countries …Being cautious due to the country's labour laws, or [not questioning] instructions, so as to comply and cope within a different environment, could impact on their behaviours*" (IP2).

From the interview data, it emerged that for non-Saudi employees, differences related to nationality seemed to be rooted, not in their own culture, but rather in their socio-economic position in Saudi society as contract workers in a foreign country, without job security. One participant noted that non-Saudis have to navigate "*environmental and cultural differences or having the sense of unfamiliarity in this new place and be[ing] wary of whatever consequences might happen should they behave inappropriately*" (IP2). Although the difference in personality trait scores between Saudi nationals and non-Saudi expatriates in the survey sample seem stark, there are socio-economic factors that could account for these differences between the two populations. Thus, there might be confounding factors which indicate the need for further research.

Summary of Discussion about Demographic and Cultural Factors and Susceptibility

The results presented in Chapter Five showed that of the four demographic and cultural factors, three (age, gender and nationality) were found to significantly influence susceptibility to CSE victimisation. After controlling for all of the other factors, gender remained a significant influence (reference category: female) for male employees, the odds of being susceptible to CSE victimisation over LinkedIn increased by 6.158 times ($p = .001$). This finding was in contrast to the majority of previous research, and the qualitative findings from this study suggest that there are cultural factors that impact this relationship.

Nationality was ruled out in the final model after controlling for all of the other factors. Work level within the organisation was the only factor not found to significantly influence CSE susceptibility; yet as expected, employees in the management/supervisory level were

significantly (p = .016) less susceptible to CSE victimisation than were those at the top level (p = .081), when controlling for all of the other factors. This may be because power position is confounded by personality traits and nationality; however, further research is needed in order to investigate these relationships.

Several interesting intersections between personality traits, personal dispositions, and demographics emerged as a result of the comparison between the quantitative and the qualitative findings. For instance, neither willingness to assume risk nor nationality were found to be statistically significant predictors of susceptibility to CSE in the quantitative study, but the qualitative analysis suggests that these factors may have a role to play in the way they interact with other factors that are significant predictors, such as gender, age and a number of personality traits.

These findings have added new dimensions to the understanding – although still far from complete – of the roles played by demographic and cultural variables in influencing an individual's susceptibility to being victimised by cyber-social engineering. Some of these new dimensions have been highlighted in the qualitative findings, such as the way culture adds a gendered dimension to the way personality traits may be expressed online versus offline.

6.2.6 Motivational Factors and Susceptibility

Motivation is encapsulated in TPB via behavioural intention, which is influenced by beliefs/attitudes and subjective norms (Baker and White, 2010). Motivation is also a key component of persuasion theory (Chapter 2, Section 2.7). Albladi and Weir (2017, 2018) found that motivation to use SNS increased users' disposition to risk and led to users engaging in risky IS habitual behaviours, such as disclosing personal information over SNS. Two factors have been identified by Kim and Cha (2017) as being primary motivations for users of LinkedIn: professional advancement and self-presentation. In the Model of Susceptibility to CSE Victimisation on LinkedIn (Figure 6-1), these two factors are posited to positively influence CSE susceptibility. The study findings regarding these factors are discussed in this section.

Professional Advancement

This study's survey found that LinkedIn was the CSNS of choice among MHRSD employees, with 93% of respondents using that CSNS. Based on findings from previous research that empirically tested the relationship between motivation for SNS use and CSE susceptibility (Albladi and Weir, 2017, 2018), this study hypothesised that users who were motivated by career advancement on LinkedIn would be more susceptible to CSE victimisation than would those who were less motivated in this way. This hypothesis was strongly supported (p = .000). However, when controlling for the effects of other variables in the study model, professional advancement has maintained its impact on susceptibility with significance at 10% level.

The drive for achievement in one's career is a primary motivation for users of LinkedIn (Kim and Cha, 2017; LinkedIn, 2020). Research on susceptibility to CSE that incorporates career-oriented motivations is lacking (and this is one of the justifications for the present study).

This study also found that non-Saudis were significantly more actively involved in professional development communication on LinkedIn (M = 2.61) compared to Saudis (M = 2.25). Non-Saudis were more likely to connect with potentially helpful professionals, follow other companies, share their CV to other companies, and share and accept various files more often than were Saudis (see Table 5-15 in Chapter 5). To compare this with data from another culture, a study in the United States reported that 78% of workers who used SNS for work-related purposes found it "*useful for networking or finding new job opportunities. 71%... [found CSNS] useful for staying in touch with others in their field… [while] 56% [found it] useful for connecting with experts*" (Lampe and Ellison, 2016, p. 5). The qualitative data supported this finding regarding motivation: IP1 mentioned that "*LinkedIn, like many other platforms, is another channel for Saudis…to strive to boost their chances of professional opportunities*". Five other interviewees (IP2, IP3, IP8, IP11 and IP15) all concurred with this view.

There is no clear or direct support in the qualitative data for the quantitative finding regarding the association between professional advancement and susceptibility to CSE victimisation. However, the interview data indicates that since expatriates are hired on short-term (annual) contracts, they can feel pressured by job insecurity and as such are motivated to try to advance their careers by seeking out additional opportunities and

networking with others online. For instance, "*financial difficulties, culture shock…, marital status… Many expats are single… [they] can fall victim to relationship scams*" (IP2). These motivations can induce them to engage online and particularly LinkedIn.

As mentioned in Chapter Four, the items designed to measure professional advancement (see Chapter 5, Table 5-15) were suggested by an expert in organisational psychology. According to the survey findings, non-Saudis were more likely to connect with potentially helpful professionals, follow other companies, share their CV to other companies, and share and accept various files more often than were Saudis (Table 5-15). All of these behaviours significantly increased the probability of exposure to a negative event on LinkedIn (at 1% significance level for all items except *sharing your work-related CV to other companies*, which was significant at 5% level ($p = .039$). These practices are concerning for organisations. Such networking behaviours would be considered "normal" in an offline context for career advancement, and in some online contexts such as LinkedIn, a platform which is portrayed as a networking site for professionals. LinkedIn is ranked as the most trusted of all the major SNS platforms and has maintained this number one spot in trustworthiness every year from 2017 to 2020 (Schomer, 2019; Insider Intelligence, 2020). Employees motivated by career and professional advancement can be exploited through a number of CSE methods (Wilcox *et al.*, 2014; Silic and Back, 2016). The salient practices on this scale (Table 5-15) exhibit the persuasion principles of reciprocity and scarcity. Bad actors can find it easily to obtain access through these risky motivation-based practices. LinkedIn and any other platform pose CSE risks, especially when accessed from within organisations. Further implications for organisations are discussed in detail in Chapter Seven.

Overall, the MHRSD employees in this study are not engaging in risky practices with regard to being motivated for career advancement. There are no significant differences between demographic groups except for nationality. Non-Saudis were more likely ($M = 2.60$, $p = .03$) than their Saudi counterparts ($M = 2.32$) to be in the habit of sharing and accepting files from online connections in relation to receiving support from those connections. This behaviour points to Cialdini's principle of reciprocity, which is a common tactic of CSE attackers. It should be noted, however, that these principles apply generally to all cultures and nationalities. The quantitative findings also concord with the findings from the qualitative data, where a non-Saudi interviewee suggested that non-

Saudis were less secure in their current jobs (Section 6.2.2) and felt the need to be proactive in professional development and in advancing their careers (Section 6.2.5):

> "*… on LinkedIn … I am more active than ever, and have more than 500 connections. … I prefer to approach and approve requests from others on the basis of sharing the same interests as mine… [or they have] work experience in the same company*" (IP8, non-Saudi).

Saudi employees engaged in such behaviour for similar motivations:

> "*I kept following up on my status on a scholarship program pending the results. I went on every social media platform and created a profile to see what others who are in my situation have to say about it, or any possible leaked updates out there."* (IP9, Saudi)

Reciprocity and unity were two persuasion principles that emerged prominently from the qualitative data regarding career advancement, in particular with reference to Saudi nationality. Interviewees mentioned the cultural norm of "*wasta*" or nepotism that is expected in Saudi Arabia as part of the job seeking process (IP1, IP15). Cultural knowledge of this phenomenon can be used for malicious purposes by cyber-social engineers over LinkedIn and other CSNS or job-seeking platforms. In fact, exploiting this phenomenon online can be easier than in the offline context, where it might be difficult to reach certain target victims. Online, it is easier convince the intended victim that they are of the same tribe or family group. Once the victim is deceived, the unity principle can be successfully employed – or deployed. As found with a number of other factors mentioned in the previous sections of this chapter, there can be confounding effects on both susceptibility and professional advancement from demographic and personality factors. In considering these findings it must be remembered that non-Saudis accounted for only 13% of the entire sample (52 participants, $N = 394$).

Self-Presentation

The motivation to tell others about oneself, or self-presentation, is not unique to LinkedIn users as opposed to users of general purpose SNS. However, as explained in Chapters Two and Three, due to the functions of LinkedIn and other CSNS as job-seeking and career-advancing platforms, the nature of the information presented by users on LinkedIn and similar sites can be more sensitive and valuable to cybercriminals and other bad actors

(Talent, 2016). Previous studies have found that the presentation of personally identifying information on social media networks increases the risk of susceptibility to CSE attack (Edwards *et al.*, 2017; Albladi & Weir, 2017).

In line with such research findings, this study posited that users who were more inclined than others to present themselves and their credentials on LinkedIn would be more susceptible to CSE victimisation. Surprisingly, this hypothesis was not supported by the quantitative findings ($p = .198$). Nevertheless, of the survey respondents who had experienced a negative event on LinkedIn, 7% of them reported that their personal information had been used to create fake or cloned profiles. While this happened to a relatively small number of MHRSD employees in the survey, the potential for serious cybersecurity threat to the organisation via such vectors is real (Breitenbacher and Osis, 2020).

The survey data showed that non-Saudis put their certificates and work telephone number on their LinkedIn page more often (76.9%) than Saudis did (60.8%) (at 5% significance level). Such behaviour of posting certificates can be exploited by cyber-social engineers to obtain more sensitive information such as date of graduation or even birth certificate and passport information. With this level of sensitive PII, they can easily launch other schemes, including identity theft. Likewise, phone numbers can be exploited in offline social engineering schemes, especially if extension numbers are provided, by impersonating other colleagues in a different branch of the organisation.

The data from the semi-structure interviews indicated that one common manifestation of self-presentation on LinkedIn was by increasing the number of one's connections as much as possible, and that in doing so, the user did not exercise reason or good judgement:

"*some employees do not necessarily pay attention to whom they are connecting with as long as their [that other user's] profile is portrayed as someone who is professional or a [member of one's own community]. … [they connect with a stranger who] poses the sense of authority because of their high credentials and endorsements…*" (IP10)

"*Many users are attracted to those who share their interest[s]. Also, they like to make connections with those who look like them in many ways*." (IP15)

"*Usually when people create a profile they are in a hurry to join the crowd – they don't care about what to share because they know these platforms are all about sharing and connecting*." (IP3)

Self-presentation was also a motivation that could blind the user to "…*risks of fraud or identity theft and the invasion of virtual communication networks for privacy and harassment in all its forms*" (IP8). Interviewees noted that they knew of colleagues and other employees who Moreover, the inclination to present more personal information than was necessary was often a function of wanting to "*join the crowd*" and do what everyone else on the platform seemed to be doing (IP3). Thus, from the qualitative data it appears there are other factors influencing the self-presentation motivation, such as the principles of unity, reciprocity and authority, as well as personality traits like extraversion, openness and agreeableness.

Summary of Discussion about Motivational Factors and Susceptibility

This study found that MHRSD employees who were motivated by career advancement on LinkedIn were more susceptible to CSE victimisation than were their colleagues who were less motivated by professional advancement. On the second factor, there was no significant difference in susceptibility to CSE attack for users who were more inclined to present themselves and their credentials on the CSNS platform. Regarding the difference in susceptibility between these two categories of LinkedIn motivation (career advancement and self-presentation), perhaps simply placing one's CV (or the contents of it) on LinkedIn is so common – nearly every user has to present this information about themselves to some extent – that it is not in and of itself a risky thing to do. But those who are motivated by career advancement are willing to take the extra (risky) step of sending more personal details to a supposed recruiter and even to provide details about what they exactly do in their job at their current company, inadvertently exposing company/organisational secrets. This may be the additional level of risk that is not found in self-presentation alone.

6.3 Emerging Behavioural Factor from the Qualitative Data: Favouritism

Users' motivations over social media platforms can differ and are often related to the main purpose of a particular SNS, such as making friends, staying in touch with family, dating, gaming, academic research exchange and professional networking (Kim and Cha, 2017). Generally, motivations can be influenced by need and expected reward (Rybnicek, Bergner and Gutschelhofer, 2019). In an organisational context, according to the U.S. Federal Merit Systems Protection Board, "*favoritism occurs when human capital decisions are based on*

personal feelings and/or relationships and NOT on objective criteria, such as assessments of ability, knowledge, and skills" (Merit Systems Protection Board, 2011, p. 1). The qualitative findings have revealed that when employees are motivated by professional advancement on CSNS, the element of favouritism can play a role. Specifically, there is a cultural perception or belief that achieving career advancement such as placement in a higher, more powerful or more lucrative position, can be facilitated though nepotism, as these interview participants have stated:

> *"In Saudi culture, recruitments have always been linked to "wasta" – Arabic for nepotism. LinkedIn and other career SNS platforms had made it possible for those to connect with human resources specialists and government authorities in hopes of benefitting from whatever career chances there might be… This is a country that has mostly been formed on tribal families; it is common to perceive that conflict of interest involving tribal bonds with regard to employment do exist…. Similarly, users could unthinkingly and feel more comfortable to connect and accept requests from those sharing the same surnames or any other type of affiliations, like for example, a person with the last name X connects with another whose last name is X."* (IP1)

> *"Most of these I prefer to approach and approve requests from others on the basis of sharing the same interests as mine… And sometimes [if they] graduated from the same college, [or they have] work experience in the same company…"* (IP8)

Just as in the real world, nepotism and favouritism can also take place on a more accessible social networking platform; in both online and offline contexts this process operates based on similarities in the form of sharing the same tribe/family surname, or in some cases having attended the same university or sharing cultural interests. This invoking of shared backgrounds is a function of Cialdini's (2001) seventh persuasion principle – unity.

> *"I like to link and follow those who like Iraqi poems, or experts and geography and environmental behaviouralists, to be specific. I know colleagues who like to link to those who are of the same family, to exploit [this] similarity point in hopes of relocating to a better position in a better place." (IP15)*

With regard to cultural knowledge about a tribal-based society, Maisel (2014) found that the "*network of tribal affiliations ensured a layer of trust between members*" (p. 118). As Huff and Kelly (2003) noted, "*The quality of social interactions between individuals in a*

collectivist culture depends heavily on whether they belong to the same in-group" (p. 83). Such knowledge, should cyber-social engineers become aware of it, can be used to deceive users into believing that the cybercriminal is from their same tribe or affiliation (e.g., by cloning a CSNS profile of an actual member of the same group, especially an authoritative figure). Thus, the user will feel more comfortable with the CSE attacker and be more open to exploitation of their trust. Such motivations and cultural expectations in professional networking can be exploited by social engineers who have cultural knowledge. For instance, the offender could launch a reverse CSE ploy by having the victim initiate the connecting and approaching phase (see Chapter Two, Section 2.5).

Such a potential mediating factor needs further exploration. The factor of favouritism among employees/managers might be measured using a set of scale items consisting of statements about actions entailing favouritism. The relationship between CSE victimisation and favouritism, as a motivational factor for a potential gullible victim, is a potential area of future research that merits further work.

6.4 Summary of Findings

Research on the factors that influence user susceptibility to cybercrime victimisation via SNS (as opposed to via email) is still limited. As far as this author has been able to determine, no other study has investigated how and to what extent personality traits, disposition to risk, habitual behaviour, cultural factors of organisation and nationality, individual motivations, age and gender are each associated with susceptibility to victimisation from cyber-social engineering via LinkedIn. This thesis represents the first study to empirically examine this combination of factors, quantitatively and qualitatively, and specifically in the context of employees of government organisations in Saudi Arabia.

The findings from this study have confirmed a number of findings from previous research, but it has also contradicted or even challenged other findings from earlier studies. The ways in which this study's findings differ from those of previous research, and the possible explanations for these differences, have been discussed in the previous sections of this chapter. This study has also revealed a number of new findings about susceptibility to CSE attack which contributes to knowledge of this domain (see Section 6.5). Some of these findings may be considered "common sense", whereas other findings seem to be counterintuitive. This section recaps these findings in brief.

This research investigated the ways and the extent to which personal characteristics and other factors play a role in an employee's likelihood of being susceptible to CSE victimisation when accessing professional SNS such as LinkedIn. The Model of Susceptibility to CSE Victimisation on LinkedIn (Chapter Three, Figure 3-6 and this chapter, Figure 6-1) was proposed to test which factors might influence CSE susceptibility. The model was tested on 16 factors and three sub-factors across five domains (personality traits, disposition to risk, risky habitual behaviours, demographic factors, cultural factors and motivations), as detailed in Sections 6.2.2 to 6.2.6. Based on the results of the analysis, a modified Model of Susceptibility to CSE Victimisation on LinkedIn has been proposed (Figure 6-2).

After considering potential confounding effects of the overall factors in the hypothesised model, the final model eliminated two of these 13 factors. Of the remaining 11 factors, seven had positive associations with CSE susceptibility, while four had negative associations with susceptibility to CSE victimisation, as shown in the final model (Figure 6-2).

The most interesting findings of this study are those related to gender differences. There is a greater risk of susceptibility to CSE victimisation for male employees. Males scored higher than females did in the agreeableness trait. Men also scored higher on willingness to assume risk and exhibiting the habit of engaging in risky information security behaviours, based on the means and on the multiple regression analysis. This is possibly due to their willingness to assume risk, as the bivariate regression indicated.

Another noteworthy finding is that those who scored higher in neuroticism can also pose risks to the organisation due to their susceptibility to CSE attacks over LinkedIn. This is interesting, as previous findings regarding susceptibility over SNS have suggested otherwise (Albladi and Weir, 2017; Frauenstein and Flowerday, 2020). Previous studies have found that women are more susceptible to deception online, whereas this study has found that men are more susceptible. Again, this contradicts other studies conducted in the SNS context (Albladi and Weir, 2020). Saridakis *et al.* (2016) found no gender effect on susceptibility to cybercrime.

With regard to age, based on the multivariate regression analysis, this study has found that those in the oldest group (aged 62+) were markedly less susceptible than those in younger age groups, and that the younger the employee, the more susceptible they are to CSE attacks on LinkedIn in the workplace. This finding accords with that of Saridakis *et al.* (2016) that those aged 29-58 were less likely to be victimised by cybercrime than those aged 18-28. Moreover, this study has found that susceptibility to CSE attacks is reduced further with each consecutively older age group.

Bivariate regression analysis suggests that some of the influencing factors that were posited in the proposed Model of Susceptibility to CSE Victimisation on LinkedIn (Figure 6-1) to have singular and direct influences on the dependent variable were not evident in the multivariate logistic regression. This may be because they are being confounded with other variables. Future work may be required to investigate these possible relationships.

In this study, cognitive/perceptual factors did not influence susceptibility to CSE victimisation. In contrast, factors that pertain to InfoSec practices and IT self-efficacy – that is, factors that entail engagement between humans and technology – had a stronger influence. For example, gender and information security habitual behaviour are two factors in the Model of Susceptibility to CSE Victimisation on LinkedIn that, when combined (while excluding personality traits), resulted in the finding that men, on average, engaged

in riskier IS habitual behaviour than women did. However, there remain questions as to whether other factors may be mediating or confounding these relationships. Moreover, among the survey participants there was a strikingly low level of awareness of the term "cyber-social engineering", but it seems likely that although the specific term was unfamiliar to them, the concept was not, as they would have heard of and understood the general meaning of associated terms like phishing, scamming, cybercrime, and the like.

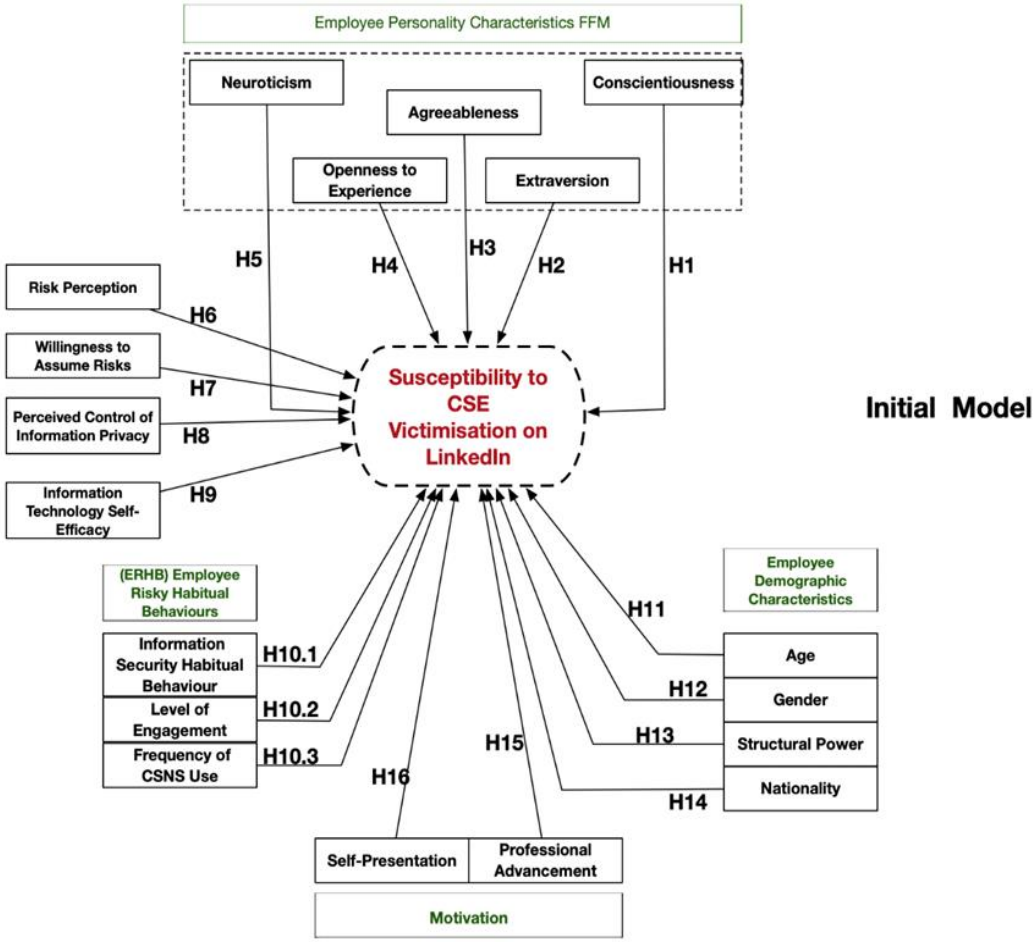


Figure 6-1 Hypothesised Model of Susceptibility to CSE Victimisation on LinkedIn

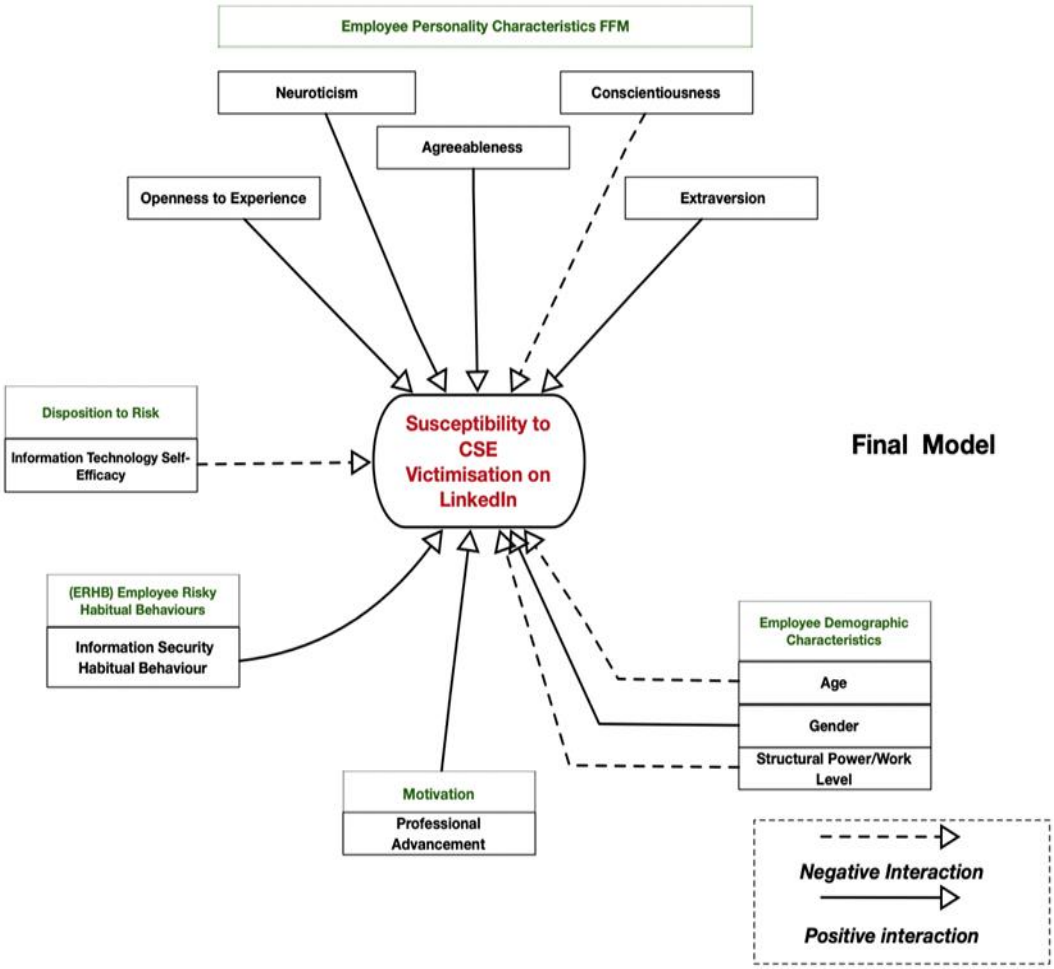


Figure 6-2 Modified Model of Susceptibility to CSE Victimisation on LinkedIn

Figure 6-2 presents the initial framework that can be applied in different workplace settings and contexts (e.g., managers and employees of public or private sector organisations, or faculty members and final year students of educational institutions) who are motivated by professional advancement and self-presentation when accessing professional career-oriented social networking sites such as LinkedIn, Bayt, Indeed and Xing. The framework is novel since it is geared towards identifying individual strengths and weaknesses in professional users and those seeking employment through CSNS platforms, as it provides a more comprehensive view via various human aspects (totalling 18 factors), examining their susceptibility to cyber-social engineering. This framework is the first of its kind to have been applied in a knowledge-exchange SNS context, as opposed to the previously examined multipurpose SNS such as Facebook. Unlike previous frameworks in the

literature, this study accounts for the ubiquitous use of Internet-connected devices in the workplace and the habitual behaviour of users, as well as assessing direct impact of employees' personality traits on their susceptibility to CSE attacks. The framework constructs, when applied in mixed method research as opposed to adopting only a quantitative method, will help to reveal unpredicted motivational factors. The follow-up qualitative phase of this study also contributes to knowledge as it has revealed that favouritism is a motivational factor that can lead individuals using CSNS to be susceptible to CSE victimisation.

6.5 Contributions

This study makes a number of contributions to current knowledge, as well as for practical application. These are detailed in this section.

6.5.1 Contribution to Knowledge (Theoretical)

Using a sequential explanatory design, this study has addressed susceptibility to cyber-based social engineering (CSE) over social media platforms. A number of factors that contribute to susceptibility were addressed. These are personality characteristics, dispositions to risk, risky habitual behaviour, demographics and motivations. The setting (LinkedIn) that is the focus of this study is different from settings in previous research.

A number of findings of this study's extended model concord with some previously identified factors impacting susceptibility to CSE risks. Moreover, the findings shed light on some apparent contradictions that may be due to the different ways in which these relationships function in various environments, such as online settings and cultural contexts. This study has proposed new factors, namely, professional advancement as a motivation and risky habitual behaviour information security (RHBIS), both of which impact susceptibility to CSE on SNS platforms in the workplace. This study relied on a number of theories, concepts and models, such As lifestyle/routine activity theory or LRAT (Cohen and Felson, 1979; Hindelang *et al.*, 1978; Sampson and Wooldredge, 1987), risk perception, cultural dimensions (Hofstede, 1980; Hofstede *et al.*, 2010), personality characteristics from the Five Factor Model or FFM (John and Srivastava, 1999), persuasion principles (Cialdini, 2001, 2016) and overarched by the theory of planned behaviour or TPB (Ajzen, 1985).

This study has also addressed a number of gaps in the current literature and previous research. Consequently, it proposes a more holistic model of susceptibility to CSE risks over career-based platforms for organisations.

The deficiencies identified in the literature include:

- LinkedIn as a setting has been the focus of this study, which as far as the author is aware, is the first study to examine CSE susceptibility on professional-based networking platforms in the workplace.
- Previous research has looked at factors statistically. This study, however, digs deeper uncover and understand the mechanisms behind how and why users in the workplace may be victimised.
- There is no single, universally accepted framework assessing susceptibility to cyber-social engineering. As a result, there is a lack of coherence in the literature. A number of previous CSE susceptibility studies have examined various cognitive, behavioural, motivational and perceptual factors based on prior studies. This study combines these factors into a single model.
- Studies of cyber-social engineering in the information system literature generally focus on a small number of factors individually, such as behavioural and perceptual factors. Previous studies have not examined susceptibility to CSE over SNS directly and comprehensively, from all five aspects (behavioural, personality, cognitive, demographic and motivational) at once. These factors that have been unearthed in the literature could help to understand user weaknesses from a wider perspective than limiting the investigation to fewer factors.
- There has been a lack of studies on the SNS environment that collectively examine the effects of behavioural (e.g., risky behaviour), perceptual, demographic (e.g., gender, structural power), motivational (e.g., career advancement) and personality/individual dispositional factors, on CSE risks. In particular, the models produced by such studies have not included structural power/level of work and professional advancement as a motivational factor to predict SNS use (Kim and Cha, 2017), in the context of CSE risks while accessing SNS by employees in public sector organisations.

- Although the model tested by Saridakis *et al.* (2016) was selected for its applicability to this study, it did not look at a broad set of user behaviours. In their model, the human behavioural dimension was examined through frequency of use. This present study has broadened this scope, branching out to examine user behaviour in terms of frequency/time spent, level of engagement with SNS features and overall InfoSec habitual behaviour. Through this broader lens, the final model has shown that habitual InfoSec behaviour is a predictor of susceptibility to CSE victimisation while engaging with SNS. This is important, as the success or failure of protective InfoSec measures (despite the user's individual weakness) may depend on provided that user's level (low or high) of risky habitual information security behaviour. Low levels of risky behaviours entail a minimum standard level of security behaviours, such as complying with established safe practices and use of IT (e.g., changing passwords periodically and minimising interaction with others over CSNS). These security behaviours could prevent or at least mitigate any harm caused by an unintentional insider threat.

- There has been a lack of research extending investigations to include a qualitative phase, as previous studies have largely relied on quantitative methods alone, especially studies involving personality characteristics. Saridakis *et al.* (2016) noted that one of the limitations of their study was that it lacked a qualitative component, and they recommended that future research (such as this current study) include "*interpretive research*" in order to explain some of the "*intricate phenomena*" uncovered by the quantitative study, and to gain "*an in-depth understanding of user behaviours and motivations*" (p. 327). Indeed, in this study the qualitative findings have indicated that culture (e.g., religion and conventional social values) influences the way in which personality traits can be expressed by employees. The interviewees suggested that some sub-traits may even become supressed, such as in the case of expatriate workers.

This study has aimed at addressing the above-mentioned gaps in the following ways:

- Unlike previous studies, this model examines personality traits as a direct influence, rather than as an indirect one with mediating factors (Albladi and Weir, 2017; Frauenstein and Flowerday, 2020), nor simply as an auxiliary finding (e.g., Algarni *et al.*, 2014). Additionally, FFM has been shown to interact with demographic factors.

- LinkedIn has unique specifications compared to other SNS contexts (such as Facebook) examined in previous research. This study has investigated not only how, but why employees use LinkedIn. A developed and reliable measure was implemented to assess user motivation and, qualitatively, the intention behind the motivation. Following this, another factor has emerged from the qualitative data associated with professional advancement: favouritism. CSE offenders can exploit such motivations and perceptions to induce those who are seeking to connect, be endorsed or relocate within the public sector.
- This study has examined structural power (employment level/position), in particular, how the role of work level amongst employees influences their susceptibility to CSE risk. This has been proposed previously as a possible impacting factor in the literature (Williams *et al.*, 2017a) as employees in lower positions tend to have less self-efficacy than those at higher levels (Guinote, 2007, as cited by Williams *et al.*, 2017a), but had not been previously empirically examined in a context such as that of this study. This factor was adapted for its relevance to the context of this study (the workplace) and was encapsulated under demographic factors in the three work level divisions examined. To the best of this researcher's knowledge, this is the first study to examine structural power (work level) from a quantitative and a qualitative perspective in the context of cyber-based social engineering attacks over SNS.
- Behavioural and perceptual aspects have been examined qualitatively as well as quantitatively, focussing on individuals in the workplace, where IT infrastructure and its peripherals function as frontline guardians. This study has concluded that susceptibility can indeed be increased by an insider's weakness in being dependent on the organisation's IT security infrastructure, consequently downplaying CSE threats. this relationship can be influenced by environmental and inherited factors, where culture and gender play major roles in decreasing or increasing susceptibility. The qualitative data revealed that even when the majority of employees do perceive that there are risks to engaging on CSNS and they are not (for the most part) engaging in risky habitual behaviour, the element of curiosity, combined with taking the InfoSec infrastructure of the organisation for granted (the seatbelt effect), can increase their susceptibility to CSE victimisation.

- Finally, as mentioned under motivational factors above, a factor has emerged from this study which pertains to the way in which a culturally based (expectation of) behaviour is manifested on career-oriented online networking platforms. This factor is favouritism. This emerging factor can be leveraged by fraudsters online, potentially increasing susceptibility in reverse social engineering facilitated by the principles of reciprocation and unity, as explained in Sections 6.2.6 and 6.4.

6.5.2 Practical Contribution

This study makes a significant contribution to understanding and addressing a pivotal issue in information security. Cyber-social engineering offenders still pose significant security risks to individuals and organisations (Tessian, 2020). The human aspect in this study refers to employees' disposition to risks, their motivations, and their behaviour online such as level of engagement and time spent. The main practical contribution of this study is to help IT and IS practitioners to understand that the human element is a serious threat as well as a vital asset to their organisation's InfoSec. Aided by this understanding, they can develop effective strategies (see Section 7.3) to address the issue of CSE attacks on employees at companies or organisations. The organisational context from which this study gathered its data is considered one that is highly sensitive to attacks and poses national risks due to its current reliance on interconnected civil data. This study has revealed that a substantial proportion of employees did not receive proper and periodical awareness training regarding online threats.

Strong, safe IS habitual behaviour through ensuring that employees take responsibility, in coordination with guidance from the organisation's IT department, for all aspects of online activity in terms of using secure passwords, updating antivirus software, not sharing sensitive information, not saving work documents on the cloud, not using the same password for multiple accounts, and so on. All these IS security behaviours can reduce victimisation. It only takes one employee to fail in their judgment and disposition to risk, or with a personality trait that increases their susceptibility; but by adhering to and implementing good InfoSec practices, this can prevent a successful CSE attack. The practical implications of the research findings as they pertain to both organisations and individuals are part of the practical contribution of this study. These are presented in Chapter Seven.

7. Implications, Limitations and Future Work

7.1 Introduction

This chapter presents the implications of this research and proposes some recommendations for practice that have emerged from this study. Finally, the limitations of the study are discussed and suggestions for future research provided.

7.2 Implications of Findings

As noted throughout this thesis, it is a commonly accepted premise in the InfoSec literature that the human element is the weakest link in any organisation's information security chain (Hu *et al.*, 2015; Vishwanath *et al.*, 2016). Indeed, it is crucial to realise that one weak or broken link is all it takes to jeopardise an organisation's entire system. Having said that, some cybersecurity experts note that, conversely, human beings "*may be the most vital link when it comes to attacks that are always morphing, in particular those aimed directly at humans*" (Kassner, 2020, para. 18). Bearing these two points in mind, the findings of this study hold serious implications for the information security and safety of two principal stakeholders: the organisation and the employee (the CSNS user).

7.2.1 Implications for Organisations

It is not uncommon to read on an organisation's home page the claim that its most precious resource is its workforce: the employees. Arguably, hiring extraverted employees could be favourable for organisations generally, as such individuals are more outgoing and do not have the tendency to be withdrawn. The characteristics of extraverted people can be beneficial in teamwork; for example, they may maintain healthy relationships with their fellow colleagues in the workplace (Gupta and Gupta, 2020). Organisations also prefer to hire individuals who exhibit agreeableness traits, due to their tendency to work well in teams and to show empathy (Stevens and Ash, 2001). On the other hand, these traits can indeed be a double-edged sword. Employees who exhibit these traits are more inclined to respond to and engage with malicious messages over social media platforms generally, as per this study and previous research in the context of social media have contended.

Another personality trait often favoured by organisations when hiring is found in employees who show openness to experience, as they are viewed as being highly creative problem solvers and can facilitate performance enhancement (Gupta and Gupta, 2020). Open individuals also make good managers due to their tendency towards participatory management styles and team building (Stevens and Ash, 2001). However, in an online setting this trait can be problematic to the security of an organisation's network, as it has been found in this study to predict susceptibility to CSE victimisation over LinkedIn.

As discussed in Chapter Six (Section 6.2.2), an unexpected finding of this study was that higher levels of neuroticism can increase susceptibility to CSE attacks. Although hiring managers tend not to seek out candidates with neurotic personalities due to their emotional instability and low self-efficacy (Oyibo *et al.*, 2017; Gupta and Gupta, 2020), it can be assumed that in any organisation some employees will be neurotic personality types. Therefore, it is necessary that organisations understand the sorts of risks posed by such individuals.

Mitigation of the risks of CSE attacks due to personality characteristics can be achieved by implementing a number of proactive and preventative measures. Human resources managers should conduct personality trait assessments of new hires and current employees. Organisations should incorporate validated psychometric evaluations as part of their recruitment platform. Such evaluation can be provided in an empowering, rather than a demeaning way, via "personal strengths and weaknesses" tests (e.g., StrengthsFinder, High5, etc.). The accurate identification of personality traits can help employers to tailor their organisation's InfoSec defence strategies, such as educating employees about how their own personal characteristics can play a role in either preventing or succumbing to phishing attacks. These efforts can be included as integration modules in SETA programs (Security, Education, Training, Awareness). Employees should be provided with and required to pass courses and training about the dangers that risky information security behaviours pose to themselves, their colleagues and their organisation. As per this study's findings, training should be targeted to those employees whose profiles indicate they are more at risk: younger employees, males, those who are motivationally driven with high level engagement on social media and lower-level employees in the organisation.

As shown in Chapter Five and explained in Chapter Six, the level of awareness among the survey participants about online threats – and especially, threats associated with the use of SNS – is low. Although 37% of employees received some training at work that made them

aware of online threats, only 31% of employees received training at work that involved making them aware of threats associated with SNS use. The proportion of those who had heard of cyber-social engineering was even smaller: 17% (Chapter 5, Chart 5-7). To put it another way, the vast majority of employees surveyed had no knowledge of what cyber-social engineering was.

The findings of this study regarding employees' low levels of CSE awareness indicate a lack of IS security training. Organisations should focus on the replacing the false sense of confidence with affirmation by exposing employees to intensive cybersecurity modules and awareness messaging. IT self-efficacy can impact overall work productivity as well as information security for an organisation. Until employees believe in their own abilities to do a task, they will not realise their aptitude to do that task; this is the case as well with online environment risks. The higher the perceived IT self-efficacy on aspects of CSE attacks over CSNS, the more unrealistic is the picture they have about their true abilities (Petersen, n.d.). This is something organisations should address. IT self-efficacy of employees needs to be measured and ensured by their IT departments, and not by non-IT employees about themselves. Organisations should implement more IS awareness training and workshops by looking at CSE and risks associated with CSNS. This is particularly important for organisations that hold sensitive PII.

Although risky habitual behaviour with regard to level of engagement and frequency of SNS use was not found to be a significant predictor of susceptibility in this study, risky information security habitual behaviour was. In particular, a number of practices were common among employees: using free-to-access public Wi-Fi, saving information about their work on their personal devices, using the same password for more than one account, downloading data and material from websites on their work computer without checking its authenticity and sharing one's current location on social media. These risky InfoSec practices entail serious threats to an organisation's security. Supervisors and managers need to liaison with their IT departments to enforce restrictions on access to platforms and to monitor employee usage of computers.

Organisations must work proactively to mitigate potential future risk as part of business continuity and disaster preparedness and recovery schemes. Most importantly, IT departments of organisations should implement strategies to control employee engagement over SNS in the workplace. This would include enforcing usage policies for Internet-connected devices (such as prohibiting the use of personal mobile devices in the workplace

using work Wi-Fi, or tethering work computers using personal phones or modems), monitoring employee workstation antivirus updates, installing security/surveillance cameras and using performance-tracking software, along with Threat Detection Response (TDR) systems. Organisations should also create an easy way for employees to approach and access IT support, such as an SMS number or portal to directly and safely report suspicious messages.

Organisations should work to minimise potential threats that may be posed by the career advancement motivations of its employees. In particular, organisations should regulate and monitor or even prevent access to social media platforms, along with implementing education and training in all the native languages of its employees, in order to raise awareness of threats involved in online and in particular in SNS environments.

7.2.2 Implications for Individuals

In this study, personality traits, perceptual factors and other individual differences have been examined as to their role in and influence on susceptibility to persuasion and deception. Individuals in their role as employees can be prone to malicious persuasive tactics and respond to them. Risky habitual IS practices and the user's level of engagement have been shown in previous research to impact (either to facilitate or to mitigate) the success of CSE attacks. This study found that indeed, RHBIS predicts susceptibility to CSE victimisation. As explained in the literature, the habit of saving information about work (and/or the organisation) on personal electronic devices can also be abused from a different location by a potential insider threat (such as a bad actor colleague) to launch attacks targeting the careless employee. This unsuspecting employee is referred to in the literature as an unintentional insider threat (UIT, see Chapter 2). Nearly half of all respondents in the survey sample had accepted friend requests on social media "*because they recognised their photo*" (Chart 5-5). This behaviour can be exploited to launch CSE attacks via impersonation/profile cloning vectors. An easy vector of attack would be stealing that co-worker's password, since the most common risky practice was using the same password for more than one account (this study found that 53% of respondents did this regularly). A younger employee who scores high in openness to experience could be a UIT if he/she were to trust a colleague to that extent. The behaviours described on the scale related to SNS usage (e.g., using free open-access public Wi-Fi, downloading unverified software,

showing one's location, etc.) can jeopardise the information security of an organisation as well as the employee.

As mentioned in the previous section, employees (SNS users) are considered the organisation's first line of defence; they are the most important entity to consider when addressing cyber-social engineering. This study has shown that employees engage in a number of risky behaviours that can serve as entry points for hackers who deploy social engineering schemes. This is a clear indication that users need to be educated to understand the risks and implications, not only for organisations but also on themselves, anywhere they engage online. Allowing cyber-attackers such easy access can bring harm to the employees as well as to their organisation. Individuals need to be enabled and feel empowered to exercise informed judgement, to know that a certain amount of suspicion can be beneficial and to understand that intangible threats can lead to tangibly harmful outcomes.

Employees should not rely blindly on their organisation's InfoSec infrastructure to keep them and their workplaces secure. Rather, individual employees should be proactive and learn how to spot potential cyberthreats. Employees should report any suspicious messages to their IT department. Moreover, those in the IT department should be part of the system: aside from launching SNS and email phishing tests, they should facilitate a channel for their non-IT colleagues to easily report threats.

Although in this study risk propensity did not predict susceptibility, both the quantitative and qualitative findings have shown that high levels of willingness to assume risk are evident in the male employees. This is a concern for Saudi Arabian organisations, in which three of every four employees are male. Employees with high risk propensity know that a threat might exist, yet they continue to engage in risky practices and behaviours. From the qualitative data, experts have used words to explain these sorts of weakness, such as *naïve*, *reckless*, *giving into curiosity*, *over-reliant*, *careless*.

Employees with such dispositions towards risk need to be more sceptical of what they encounter on SNS, to learn how to investigate and distinguish between a genuine and a fraudulent message. Equipped with high IT self-efficacy, they will be less likely to respond (e.g., by clicking on a link) to unknown persons but rather go to the official channel and inquire about the source of the message. If they receive a message though LinkedIn about a job vacancy or a promotion, individuals (employees) need to refrain from engaging directly, and instead, to check with the supposed company or recruiter through their official

websites or through their verified social media profile (that uses a verification badge). Employees using LinkedIn and other CSNS should be aware that account authenticity is not measured by the number of followers or connections, or the presence of an organisation's or known member's image or logo alone. Individual users should use strong passwords on LinkedIn and other social media accounts and periodically change those passwords. Employees should refrain from storing sensitive and work-related data on commercial cloud accounts. They should avoid uploading CVs which contain personal identifying information like national IDs, department phone number/extensions, mobile phone numbers, and/or addresses that can be exploited in impersonation attacks online or offline.

7.3 Limitations

Every research project has its limitations. The limitations particular to this study are listed and explained as follows:

- Due to ethical and privacy rules established by the CSNS platform provider (LinkedIn) and the organisation (MHRSD), the researcher was not permitted to launch real scenario-based CSE experiments using LinkedIn profiles or LinkedIn emails to employees in the organisation. Launching a simulated attack would have been useful to elicit "*realistic response behaviour*" from participants (Jones and Towse, 2018, p. 84).
- Although TPB was employed as an overarching theory, only two of the model's 18 constructs (structural power/work level and nationality/culture) represented subjective norms. In this study normative influence as a motivational factor was emphasised less than other factors. Nevertheless, subjective norms emerged from the interview data as a potentially salient set of factors, especially in explaining certain findings from the quantitative data regarding gender and susceptibility.
- As it was not possible to use an experiment to test for susceptibility, the dependent variable (susceptibility to CSE victimisation) was measured using a self-report approach. A substantial proportion of the participants did not identify the type of CSE vector. Of the 95 respondents who reported having "*something bad happen to them traced back to their usage of LinkedIn*", only 44 stated what that incident entailed.

- In this study the dependent variable (susceptibility to CSE victimisation) was measured as a dichotomous Yes/No variable, whereas other aspects of CSE susceptibility such as frequency of prior exposure to/experience with CSE victimisation, intensity of the attack/victimisation, timing of prior CSE victimisation, and harm caused by that negative experience, were not examined.
- This study lacks a follow-up phase that could have been conducted either with a focus group or through interviews with individuals drawn from the survey sample after the quantitative phase. This strategy could help explore causations of CSE susceptibility on LinkedIn by asking those participants who had responded "Yes" (that they had experienced a negative event), why they might have been victimised by the CSE schemes they reported, and to provide further insights about their reported incidents.
- Every PhD study is limited by time and resources: perhaps the greatest constraint is that the research is carried out by a single researcher. This researcher has initially made many efforts to obtain permission to collect data from seven different public sector organisations in Saudi Arabia. The process took months to get approval and permission from only one such organisation. Thus, this research is based on a single case study, which in itself can be a limitation in terms of generalisability of the data. Examining the cases of other organisations could strengthen findings with regard to representation.
- This cross-sectional study investigates employee's susceptibility to CSE victimisation over LinkedIn at the workplace at a particular moment in time. Like most technology, SNS evolve over time, and SNS usage and its associated risks also continue to evolve and change. Due to these circumstances, generalising the findings of this study to other employees in public sector organisations in Saudi Arabia requires caution. Nevertheless, this study is valuable in offering insights into employee attitudes, motivations and behaviours regarding risk of cyber-social engineering over CSNS. The findings would also be useful as a historical data point in a longitudinal analysis. This highlights the need for longitudinal studies to explore how susceptibility to victimisation through CSE may change over time and what factors contribute to this change.

- Due to gender segregation at the workplace, female participants were not observed directly by the (male) researcher while they completed the survey questionnaire. The researcher was able to observe only the male employees during the survey. This disparity could have caused issues that were raised with the survey, which the researcher would be unaware of.
- Nationality was found to be unsuitable to be examined as a factor in Saudi public sector organisations. This is because Saudi Arabia is enforcing the "Saudization" program, which mandates the hiring of Saudi employees in place of non-Saudis. Thus, the study sample contained only a small proportion of non-Saudi employees, and to categorise those few individuals by their separate nationalities (e.g., Indian, Lebanese, Pakistani, Syrian) would have resulted in groups so small in number as to have been of little analytical value.
- The wording of some of the questionnaire items could be improved. As an example, one item in the 20-item RHBIS scale stated "*Sent personal information to strangers over the Internet*". Nowhere in the survey was a definition of "*strangers*" provided. Therefore, responses to this item may depend entirely on each participant's personal definition of the term. For instance, in the LinkedIn context, with so many connections, many of whom a user might exchange comments with on a post of mutual interest, would a user consider those connections to be strangers because they have never met in real life and only ever have communicated via LinkedIn? Or would the participat not consider them to be strangers for the purpose of responding to this item?
- Likert scales were used for most of the survey items. In spite of their usefulness, Likert scales have a number of disadvantages. Cohen *et al.* (2007) listed the following drawbacks: (1) Researchers may mistakenly "*infer a degree of sensitivity and subtlety*" from the responses that is not supported by the data; (2) "*There is no assumption of equal intervals between the categories*"; (3) There is no way to know if respondents are being truthful or not; (4) Respondents are necessarily limited in their responses to the set of provided options, thus they are "*condemned to silence for want of a category*" (p. 327). Despite these concerns, however, Likert scales as a measurement instrument remain a staple in survey research (Neuman, 2014).

7.4 Recommendations for Future Research

The present study has focussed on the impact on susceptibility to CSE of a range of factors: personality characteristics, disposition to risks, risky information security behaviours, motivations and demographics. Future work is suggested in the following areas:

1) Susceptibility was measured by self-reported victimisation incidents. Future research could focus on proactively investigating those individuals in categories deemed (based on the findings of this and previous studies) to have higher susceptibility to CSE victimisation. In particular, a future study could investigate susceptibility to attacks via stimulating phishing emails with LinkedIn themes using characteristics of Cialdini's principles of influence (Chapter 2, Section 2.7 & Table 2-2) over career-oriented social networking sites. Such as "*Do you know (name)*?" with a photo of an authoritative figure, "*You have an InMail message, click to view*", designing a post embedded in the email that convey a promising news for the workforce with a "like button".

2) Subjective norms can be examined in future research in the context of SNS and susceptibility to CSE; this would be particularly valuable where the organisations of interest are in societies which score high on the cultural dimensions of collectivism and power distance.

3) As mentioned in Section 7.4, one limitation of this study was the inability (due to being denied permission) to conduct actual LinkedIn environment CSE attacks. Future research could apply this study's extended model by testing the dependent variable (susceptibility to CSE victimisation) using an experiment. A study design that included role-play experiments in the real LinkedIn environment would provide a wealth of data and could strengthen the findings of the current study.

4) The study model could be extended to account for other factors, for example, the effect of the number of LinkedIn connections on susceptibility to CSE victimisation.

5) This study could be applied to other contexts: for instance, other social media platforms for entertainment or business purposes (e.g., Snapchat, Skype). Such platforms have been increasing in prominence and popularity due to the "new normal" of fewer in-person interactions. This new normal has affected business, education and arts/entertainment because of recent global and regional catastrophic

incidents (e.g., pandemics and natural disasters). Therefore, it is expected that online interaction via social media platforms will continue to increase.

6) As with other IT-related fields, the domain of CSE research is one in which the technologies and user practices change rapidly. This this research is highly time sensitive. Furthermore, susceptibility to CSE victimisation is a phenomenon that varies according to the context and the user's own level of awareness and knowledge. Thus, research and the knowledge base for this field needs to be kept up to date. Moreove Bullée *et al.* (2017) argued that there was a need for longitudinal studies to examine how the attitudes and behaviours of those who have been previously victimised by CSE attacks change over time.
7) Since the study focussed on personality traits as having a direct impact on susceptibility, future research could utilise personality traits as predictors to investigate their impact, both direct and indirect, on each of the factors examined in this study. Such a multi-relational study would yield further insights into the mediating relationships between personality traits and the factors of each of the other domains examined in this study – demographic, dispositional/perceptual, behavioural and motivational – in addition to their relationships with the dependent variable (susceptibility to CSE victimisation).
8) The study's statistical analysis and subsequent discussion have shown differing findings when running both bivariate and multivariate regression analysis. These discrepancies can indicate possible confounding effects. Future research could employ structural equation modelling (SEM) to reveal these confounding effects.
9) This study could be strengthened in by obtaining qualitative data from those who participated in the first quantifying phase. However, the organisation in which the survey was conducted has to date refused permission for the researcher to contact the participants individually.
10) This study has focussed for the most part on Saudi Arabian citizens in both phases of data collection, and the focus of the investigation was a public sector organisation in Saudi Arabia. Future research could expand the findings by investigating different populations that are representative of various countries and cultures, as well as in other contexts such as medical staff in hospitals, military personnel, or multinational employees in private sector companies.

7.5 Summary

This chapter has presented the implications of the findings on both organisations and the individual (the employee). This chapter has also discussed the limitations of this study as well as future research directions. In spite of the limitations of this research, it makes a significant practical contribution to public sector organisations in Saudi Arabia and the Arabian Gulf. This study provides empirical data that emphasises the pressing need for organisations to take extra precautions by up-to-date training and education of their employees. Organisations ought to seriously consider the psychological, behavioural and demographically-based weaknesses that influence employees while accessing CSNS. For instance, as mentioned earlier in this thesis, the general view of LinkedIn is that it is a site on which users do not need to be cautious about publicly displaying their personal information or photos, since this CSNS is geared towards business and professional activity (Cooper and Naatus, 2014). This study has highlighted the fact that the great majority of employees are unaware of what cyber-social engineering is, and thus they are unable to accurately assess the risks that CSE poses to them in the workplace. The findings from this study also indicate an emerging motivational factor, favouritism.

Employees are considered a frontline defence to help prevent breaches of their own personal data and to prevent consequently harming the organisation's sensitive data. This is especially critical when risky information security behaviours, IT-self efficacy, personality traits, motivation for professional advancement, gender, age and structural power to were found to predict susceptibility to CSE victimisation. The quantitative and the qualitative findings in this study indicate that risky habits with regard to information security are concerning. However, the positive view of this is that visible habitual behaviours can be identified, and thus addressed and controlled, more easily than other less visible aspects such as cognitive (i.e., perceptual) factors. If employees can comply with safe use practises, it will overcome other perceptual and personality weaknesses. As some cybersecurity experts have observed, the human being (the employee) that is usually depicted as the weakest link for an organisation's cybersecurity can be empowered to become a strong and vital link in that InfoSec system.

REFERENCES

Aburrous, M., Hossain, M.A., Dahal, K. and Thabtah, F. 2010. Experimental case studies for investigating e-banking phishing techniques and attack strategies. *Cognitive Computation*, 2(3), 242–253. https://doi.org/10.1007/s12559-010-9042-7

Acquisti, A. and Gross, R. 2006. Imagined communities: Awareness, information sharing, and privacy on the facebook. In: Danezis G., Golle P. (Eds.) *Privacy Enhancing Technologies*. *PET 2006*. *Lecture Notes in Computer Science*, vol. 4258. Berlin: Springer, pp. 36-58. https://doi.org/10.1007/11957454_3

Ailon, G. 2008. Mirror, mirror on the wall: Culture's consequences in a value test of its own design. *Academy of Management Review*, 33(4), 885–904. https://doi.org/10.5465/AMR.2008.34421995

Airehrour, D., Nair, N.V. and Madanian, S. 2018. Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user-reflective mitigation model. *Information*, 9(5), p. 110. (Switzerland). doi: 10.3390/info9050110

Ajzen I. 1985. From intentions to actions: A theory of planned behavior. In J. Kuhl and J. Beckmann, eds. *Action control*. SSSP Springer Series in Social Psychology. Berlin, Heidelberg: Springer, pp. 11–39. doi: 10.1016/0749-5978(91)90020-T

Ajzen, I., and Fishbein, M. 1980. *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Alarcon, G.M., Lyons, J.B., Christensen, J.C., Klosterman, S.L., Bowers, M.A., Ryan, T.J., Jessup, S.A. and Wynne, K.T. 2018. The effect of propensity to trust and perceptions of trustworthiness on trust behaviors in dyads. *Behavior Research Methods*, 50(5), 1906–1920. https://doi.org/10.3758/s13428-017-0959-6

Alarishi, J. 2012. مليار دولار خسائر البنوك السعودية بسبب الجرائم الإلكترونية - أخبار السعودية | صحيفة عكاظ. [USD 1bn in Saudi bank losses due to cybercrime]. *Okaz* [online newspaper]. https://www.okaz.com.sa/article/449185/ (Accessed 17 September 2018).

Albladi, S. and Weir, G.R.S. 2016. Vulnerability to social engineering in social networks: A proposed user-centric framework. In: *2016 IEEE International Conference on*

Cybercrime and Computer Forensic (ICCCF). IEEE, pp. 1–6. https://doi.org/10.1109/ICCCF.2016.7740435

Albladi, S.M. and Weir, G.R.S. 2017. Personality traits and cyber-attack victimisation: Multiple mediation analysis. *Internet of Things Business Models, Users, and Networks*, pp. 1–6. doi: 10.1109/CTTE.2017.8260932

Albladi, S.M. and Weir, G.R.S. 2018. User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, 8(1). doi: 10.1186/s13673-018-0128-7

Albladi, S.M. and Weir, G.R.S. 2020. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, 3(7). https://doi.org/10.1186/s42400-020-00047-5

Alcantara, E. 2010. Darknet intelligence secrets revealed. *United States Cybersecurity Magazine*. https://www.uscybersecurity.net/darknet-intelligence-secrets-revealed/ (Accessed 16 September 2018).

Alexander, M. 2016. Understanding and reducing social engineering attacks 1. SAND Institute InfoSec Reading Room. https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972 (Accessed 25 November 2017).

Algarni, A.A. 2016. *The impact of source characteristics on users' susceptibility to social engineering victimization in social networks: Mixed method study based on Facebook*. PhD Thesis. https://eprints.qut.edu.au/95604/1/Abdullah Ayed M_Algarni_Thesis.pdf (Accessed 29 September 2017).

Algarni, A. 2013. Social engineering in social networking sites: Phase-based and source-based models. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 508–515. doi: 10.7763/IJEEEE.2013.V3.278

Algarni A. 2019. What message characteristics make social engineering successful on Facebook: The role of central route, peripheral route, and perceived risk. *Information*; 10(6), 211. https://doi.org/10.3390/info10060211

Algarni, A., Xu, Y. and Chan, T. 2014. Social engineering in social networking sites: The art of impersonation. In: *2014 IEEE International Conference on Services Computing*, pp. 797–804. IEEE. https://doi.org/10.1109/SCC.2014.108

Algarni, A., Xu, Y. and Chan, T. 2017. An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, 26(6), 661–687. doi: 10.1057/s41303-017-0057-y

Al-Hamar, M., Dawson, R. and Guan, L. 2010. A culture of trust threatens security and privacy in Qatar. *10th IEEE International Conference on Computer and Information Technology, 2010*. IEEE, pp. 991–995. doi: 10.1109/CIT.2010.182

Alkış, N. and Temizel, T.T. 2015. The impact of individual differences on influence strategies. *Personality and Individual Differences*, 87, 147–152. https://doi.org/10.1016/j.paid.2015.07.037

Almakrami, H.A. 2015. *Online self-disclosure across cultures: A study of Facebook use in Saudi Arabia and Australia*. https://eprints.qut.edu.au/84494/4/Hashem Almakrami Thesis.pdf (Accessed 15 April 2018).

Alotaibi, M.K.N. 2020. Employees' interest in professional advancement on LinkedIn increases susceptibility to cyber-social engineering: An empirical test. In: Clarke N., Furnell S. (eds). 2020. *Human Aspects of Information Security and Assurance*. *HAISA 2021*. *IFIP Advances in Information and Communication Technology*, vol 593. Springer, Cham. https://doi.org/10.1007/978-3-030-57404-8_7

Alseadoon, I. 2014. *The impact of users' characteristics on their ability to detect phishing emails*. PhD Thesis. https://eprints.qut.edu.au/72873/1/Ibrahim Mohammed A_Alseadoon_Thesis.pdf (Accessed 7 December 2018).

Alseadoon, I., Chan, T., Foo, E. and Gonzáles Nieto, J.M. 2012. Who is more susceptible to phishing emails? A Saudi Arabian study. *23rd Australasian Conference on Information Systems*, pp. 1-11. https://www.researchgate.net/publication/237010027_Who_is_More_Susceptible_to_Phishing_Emails_A_Saudi_Arabian_Study

Alseadoon, I., Othman, M.F.I. and Chan, T. 2015. What is the influence of users' characteristics on their ability to detect phishing emails? In: Sulaiman, H., Othman, M., Othman, M., Rahim, Y., and Pee, N. (Eds), *Advanced Computer and Communication Engineering Technology. Lecture Notes in Electrical Engineering*, vol 315. Springer, Cham, pp. 949–962. doi: 10.1007/978-3-319-07674-4_89

Alseadoon, I., Othman, M.F.I., Foo, E. and Chan, T. 2013. Typology of phishing email victims based on their behavioural response. In: Shim, J.P., Hwang, Y., and Petter, S. (Eds.) *Proceedings of the Nineteenth Americas Conference on Information Systems.* Association for Information Systems (AIS), http://aisel.aisnet.org/, pp. 3716-3724

Al-Shargie, F., Tariq, U., Mir, H., Alawar, H., Babiloni, F. and Al-Nashash, H. 2019. Vigilance decrement and enhancement techniques: A review. *Brain Sciences*, 9(8), 178. https://doi.org/10.3390/brainsci9080178

Alshehri, H.A.D. 2015. *A framework for the implementation of B2C e-commerce in Saudi Arabia: A comparative study of Saudis living in Saudi Arabia and those living in the UK, and the perception of Saudi companies*. PhD Thesis, University of Salford, UK. https://core.ac.uk/download/pdf/42588959.pdf (Accessed 2 August 2020)

Alzamil, Z.A. 2012. Information security awareness at Saudi Arabians' organizations. *International Journal of Information Security and Privacy*, 6(3), 38–55. doi: 10.4018/jisp.2012070102

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. and Xu, L. 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, pp. 437–443. doi: 10.1016/j.chb.2016.12.040

Arend, I., Shabtai, A., Idan, T., Keinan, R. and Bereby-Meyer, Y. 2020. Passive- and not active-risk tendencies predict cyber security behavior. *Computers & Security*, 96, 101929. https://doi.org/10.1016/j.cose.2020.101929

Armstrong, M.E., Jones, K.S., Siami Namin, A. and Newton, D.C. 2018. What vulnerability assessment and management cybersecurity professionals think their future colleagues need to know. In: *Proceedings of the 49th ACM Technical Symposium on Computer Science Education – SIGCSE '18* (pp. 1082–1082). New York: ACM Press. https://doi.org/10.1145/3159450.3162250

Asharq Al-Awsat. 2020. Saudi royal decree forms 3 new ministries, merges 2 others. *Asharq Al-Awsat* [newspaper], 25 February 2020. https://english.aawsat.com//home/article/2149016/saudi-royal-decree-forms-3-new-ministries-merges-2-others

Assaad, R. and Barsoum, G. 2019. Public employment in the Middle East and North Africa. *IZA World of Labor 2019*, 463. doi: 10.15185/izawol.463 https://wol.iza.org/articles/public-employment-in-the-middle-east-and-north-africa/long

Auchard, E. and Paul, K. 2017. Saudi agency says country targeted in cyber spying campaign. | *Reuters Internet News*, 20 November 2017. https://www.reuters.com/article/us-saudi-cyber/saudi-agency-says-country-targeted-in-cyber-spying-campaign-idUSKBN1DK27M (Accessed 7 February 2019).

Aurigemma, S. and Mattson, T. 2017. Privilege or procedure: evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers & Security*, 93, http://dx.doi.org/doi: 10.1016/j.cose.2017.02.006

Awad, N.F. and Ragowsky, A. 2008. Establishing trust in electronic commerce through online word of mouth: An examination across genders. *Journal of Management Information Systems*, 24(4), 101-121.

Bagrow, J.P., Liu, X. & Mitchell, L. 2019. Information flow reveals prediction limits in online social activity. *Nature Human Behaviour* [online], 3, pp.122–128. https://doi.org/10.1038/s41562-018-0510-5 (Accessed 29 July 2020).

Bailey, J.L., Mitchell, R.B. and Jensen, B.K. 2008. Analysis of student vulnerabilities to phishing. In *Americas Conference on Information* Systems (AMCIS) 2008 Proceedings, 271, pp. 1–10. http://aisel.aisnet.org/amcis2008/271

Baker, K. and White, K. 2010. Predicting adolescents' use of social networking sites from an extended theory of planned behaviour perspective. *Computers in Human Behavior*, 26(6), 1591-1597. https://doi.org/10.1016/j.chb.2010.06.006

Bandura, A. 1989. This week's citation classic: Bandura A. Self-efficacy: Toward a unifying theory of behavioral change [*Psychological Review*, 84(1977), 191-215]. *Current Contents*, 20, 15 May 1989. http://garfield.library.upenn.edu/classics1989/ A1989U419500001.pdf

Bansal, G., Zahedi, F. M. and Gefen, D. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems.* doi: 10.1016/j.dss.2010.01.010.

Barlett, C.P. 2019. *Predicting Cyberbullying*. London: Academic Press. https://doi.org/10.1016/C2018-0-00531-9

Barnett, E. 2011. Social networks are easier targets for cyber criminals. *The Telegraph*, 19 January 2011. https://www.telegraph.co.uk/technology/news/8267489/Social-networks-are-easier-targets-for-cyber-criminals.html

Barrilleaux, B. and Wang, D. 2018. Spreading the love in the LinkedIn feed with creator-side optimization [Blog post]. *LinkedIn Engineering*, 16 October 2018. https://engineering.linkedin.com/blog/2018/10/linkedin-feed-with-creator-side-optimization

Baruah, T.D. 2012. Effectiveness of social media as a tool of communication and its potential for technology enabled connections: A micro-level study. *International Journal of Scientific and Research Publications*, 2(5). www.ijsrp.org (Accessed 2 February 2019).

Baskerville, R. and Myers, M.D. 2004. Special issue on action research in information systems: Making IS research relevant to practice: Foreword. *MIS Quarterly*, 28(3), 329-335. https://doi.org/10.2307/25148642

Beldad, A. 2015. Sharing to be sociable, posting to be popular: Factors influencing non-static personal information disclosure on Facebook among young Dutch users. *International Journal of Web Based Communities*, 11(3-4), 357-374. doi:10.1504/IJWBC.2015.072132

Beldad, A. 2016. Sealing one's online wall off from outsiders: Determinants of the use of Facebook's privacy settings among young Dutch users. *International Journal of Technology and Human Interaction*, 12(1), 21-34. doi:10.4018/IJTHI.2016010102

Bellman, S., Johnson, E.J., Kobrin, S.J. and Lohse, G.L. 2004. International differences in information privacy concerns: A global survey of consumers. *Information Society*, 20(5), 313–324. https://doi.org/10.1080/01972240490507956

Benenson, Z., Gassmann, F. and Landwirth, R. 2017. Unpacking spear phishing susceptibility. In *Lecture Notes in Computer Science*. Springer, Cham, pp. 610–627. doi: 10.1007/978-3-319-70278-0_39

Bertocci, P.A. 1988. *The person and primary emotions. Recent research in psychology*. New York: Springer. doi: 10.2320/matertrans.MC200825

Bilge, L. *et al.* 2009. All your contacts are belong to us: Automated identity theft attacks on social networks. *WWW 2009*. doi: http://doi.acm.org/10.1145/1526709.1526784

Biography.com (eds.). 2014. *Frank Abagnale Biography*. Biography.com website. A&E Television Networks. https://www.biography.com/people/frank-abagnale-20657335 (Accessed 1 February 2018).

Blythe, M., Petrie, H. and Clark, J.A. .2011. F for fake: Four studies on how we fall for phish. *CHI '11: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, May 2011, pp. 3469–3478. https://doi.org/10.1145/1978942.1979459

Bond, C.F. and DePaulo, B.M. 2006. Accuracy of deception judgments. *Personality and Social Psychology Review*, 10(3), 214–234. doi: 10.1207/s15327957pspr1003_2

Bonem, E.M., Ellsworth, P.C. and Gonzalez, R. 2015. Age differences in risk: Perceptions, intentions and domains. *Journal of Behavioral Decision Making*, 28(4), 317-330. https://doi.org/10.1002/bdm.1848

boyd, d. 2008. Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *International Journal of Research into New Media Technologies*, 14(1), 13–20. doi: 10.1177/1354856507084416

boyd, d.m. and Ellison, N.B. 2007. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230. doi: 10.1111/j.1083-6101.2007.00393.x

Boyden, P. 2021. All you need to know about LinkedIn fraud [Blog post]. *FraudWatch International*, 16 February 2021. https://fraudwatchinternational.com/all/all-you-need-to-know-about-linkedin-fraud/

Breitenbacher, D. and Osis, K. 2020. Operation In(Ter)Ception: Targeted attacks against European aerospace and military companies [white paper]. *ESET*, June 2020.

https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf

Brislin, R.W. 1970. Back-translation for cross-cultural research. J*ournal of Cross-Cultural Psychology*, 1(3), 187–216. https://doi.org/10.1177/135910457000100301

Broadband Search. 2020. Average time spent daily on social media (latest 2020 data) [blog post]. *Broadband Search*, 2020. https://www.broadbandsearch.net/blog/average-daily-time-on-social-media

Brody, N. and Crowley, M.J. 1995. Environmental (and genetic) influences on personality and intelligence. In: Saklofske D.H., Zeidner M. (eds). *International Handbook of Personality and Intelligence. Perspectives on Individual Differences*. Springer, Boston, MA. https://doi.org/10.1007/978-1-4757-5571-8_4

Bronstein, J. 2013. Personal blogs as online presences on the internet: Exploring self-presentation and self-disclosure in blogging. *Aslib Proceedings*, 65(2), pp. 161-181. https://doi.org/10.1108/00012531311313989

Bryman, A. 2012. *Social research methods* (4th edn). Oxford University Press.

Buchanan, T. and Benson, V. 2019. Spreading disinformation on Facebook: Do trust in message source, risk propensity, or personality affect the organic reach of "fake news"? *Social Media and Society*, 5(4). https://doi.org/10.1177/2056305119888654

Bullée, J.-W., Montoya, L., Junger, M. and Hartel, P. 2017. Spear phishing in organisations explained. *Information & Computer Security*, 25(5), 593–613. https://doi.org/10.1108/ICS-03-2017-0009

Bullée, J.-W.H., Montoya, L., Pieters, W., Junger, M. and Hartel, P. 2018. On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. Journal of Investigative Psychology and Offender Profiling, 15(1), 20–45. doi: 10.1002/jip.1482

Bunch, J., Clay-Warner, J. and Lei, M.-K. 2015. Demographic characteristics and victimization risk: Testing the mediating effects of routine activities. *Crime & Delinquency*, 61(9), 1181–1205. https://doi.org/10.1177/0011128712466932

Burke Johnson, R. Onwuegbuzie, A.J. and Turner, L. 2007. Toward a definition of mixed methods research. *Journal of Mixed Methods Research*, 1, 112-133. DOI: 10.1177/1558689806298224

Butavicius, M, Parsons, K., Pattinson, M., Mccormac, A., Calic, D. and Lillie, M. 2017. Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. In: Clarke, N.L. and Furnell, S.M. (eds.). 2017. *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018)*. Plymouth: Centre for Security, Communications & Network Research. https://pdfs.semanticscholar.org/e098/5512826c150b243efe7cb35a514b21ce272c.pdf

Byrnes, J.P., Miller, D.C. and Schafer, W.D. 1999. Gender differences in risk taking: A meta-analysis. *Psychological Bulletin*, 125(3), 367–383. doi: 10.1037/0033-2909.125.3.367

Cardinal, R.N. and Aitken, M.R. 2013. *ANOVA for the behavioral sciences researcher*. Psychology Press.

Carey, W.P. 2007. The gentle science of persuasion, part six: Scarcity [Online article]. *W.P. Carey News*, 14 Feb 2007. Arizona State University. https://news.wpcarey.asu.edu/20070214-gentle-science-persuasion-part-six-scarcity

Carter, N.T. Guan, L., Maples, J.L., Williamson, R.L. and Miller, J.D. 2016. The downsides of extreme conscientiousness for psychological well-being: The role of obsessive compulsive tendencies. *Journal of Personality*, 84(4), pp. 510–522. doi: 10.1111/jopy.12177

Cases, A.-S. 2002. The perceived risk and risk-reduction strategies in Internet shopping. *International Review of Retail, Distribution and Consumer Research.* doi: 10.1080/09593960210151162

CERT-UK. 2015. *An Introduction to Social Engineering*. https://info.publicintelligence.net/UK-CERT-SocialEngineering.pdf (Accessed 29 August 2018).

Chaiken, S. 1980. Heuristic versus systematic information processing and the use of source versus message cues in persuasion, *Journal of Personality and Social Psychology*. doi: 10.1037//0022-3514.39.5.752

Chang, H.H. and Chen, S.W. 2008. The impact of online store environment cues on purchase intention. *Online Information Review*, 32(6), 818–841. https://doi.org/10.1108/14684520810923953

Cherdantseva, Y. and Hilton, J. 2013. A reference model of information assurance & security. In *Proceedings - 2013 International Conference on Availability, Reliability and Security*, ARES 2013. doi: 10.1109/ARES.2013.72

Chi, M. and Wanner, R. 2011. Reducing the risks of social media to your organization security policy and social media use: *GIAC (GSEC) Gold Certification Security Policy and Social Media Use*. SANS Institute. https://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749 (Accessed 4 September 2018).

Chitrey, A., Singh, D. and Singh, V. 2012. A comprehensive study of social engineering based attacks in India to develop a conceptual model. *International Journal of Information & Network Security*, 1(2), 45–53. doi: 10.11591/ijins.v1i2.426

Cho, M. and Kim, G. 2017. A cross-cultural comparative analysis of crowdfunding projects in the United States and South Korea. *Computers in Human Behavior*, 72, 312–320. doi: 10.1016/j.chb.2017.03.013

Cho, H., Rivera-Sánchez, M. and Lim, S.S. 2009. A multinational study on online privacy: global concerns and local responses. *New Media & Society*, 11(3), 395–416. https://doi.org/10.1177/1461444808101618

Choi, K-S. and J.R. Lee. 2017. Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, 73, 394-402. https://doi.org/10.1016/j.chb.2017.03.061

Choo, K. R., Smith, R. and McCusker, R. 2007. Future directions in technology-enabled crime. *Australian Institute of Criminology 2007*, 78, 53–54. http://www.aic.gov.au/media_library/publications/rpp/78/rpp078.pdf (Accessed 27 November 2017).

Choo, T.-H. 1964. Communicator credibility and communication discrepancy as determinants of opinion change. *Journal of Social Psychology*, 64(1), 65–76. doi: 10.1080/00224545.1964.9919544

Chu, A.M.Y and So, M.K.P. 2020. Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability*, 12, 3163. doi:10.3390/su12083163

Chua, W.F. 1986. Radical developments in accounting thought. *Accounting, the Social and the Political*, 61(4), 601-632. https://doi.org/10.1016/b978-008044725-4/50009-6. http://www.jstor.org/stable/247360 (Accessed 14 June 2020).

Cialdini, R. 2016. *Pre-Suasion: A revolutionary way to influence and persuade*. New York: Simon & Schuster.

Cialdini, R. 2020. *Principles of persuasion*. Influence at Work [website]. https://www.influenceatwork.com/principles-of-persuasion/

Cialdini, R.B. 2001. *Influence: Science and practice* (4th edn). New York: HarperCollins. https://www.researchgate.net/publication/229067982_Influence_Science_and_Practice

Cialdini, R.B. *et al.* 1999. Compliance with a request in two cultures: The differential influence of social proof and commitment/consistency on collectivists and individualists, *Culture and Compliance*. https://journals.sagepub.com/doi/pdf/10.1177/0146167299258006 (Accessed 4 December 2018).

Cialdini, R.B., Trost, M.R. and Newsom, J.T. 1995. Preference for consistency: The development of a valid measure and the discovery of surprising behavioral implications. *Journal of Personality and Social Psychology*, 69(2), 318–328. doi: 10.1037/0022-3514.69.2.318

Cleary, S. and Kelly, L. 2017. Irish engineer claims fake recruiter 'catfished' him out of job after contacting him on LinkedIn. *Independent.ie*, 15 June 2017. https://www.independent.ie/business/in-the-workplace/irish-engineer-claims-fake-recruiter-catfished-him-out-of-job-after-contacting-him-on-linkedin-35799579.html (Accessed 26 November 2018).

Clement, J. 2019a. LinkedIn – Statistics & Facts. *Statista*, 1 Aug 2019. https://www.statista.com/topics/951/linkedin/ (Accessed 29 July 2020).

Clement, J. 2019b. U.S. Leading LinkedIn usage reasons according to users in the United States as of 3rd quarter 2019. *Statista*, 18 Nov 2019. https://www.statista.com/statistics/276593/us-adults-reasons-to-use-social-networking-sites/ (Accessed 29 July 2020).

Cofrin, A.E. 2011. Security concerns in the nomological network of trust and Big 5: First order and second order [conference paper]. https://www.semanticscholar.org/paper/Security-Concerns-in-the-Nomological-Network-of-and-Cofrin/32837d2dfdfa0463e294eaeb497451f3d6f6139c?p2df

Cohen, L.E. and Felson, M. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44: 588–608. DOI: 10.2307/2094589

Cohen, L., Manion, L. and Morrison, K. 2007. *Research methods in education*, 6th edn. Abingdon: Routledge.

Collin, P. Rahilly, K., Richardson, I. and Third, A. 2011. Literature review: The benefits of social networking services [academic report]. (April), p. 29. http://www.uws.edu.au/__data/assets/pdf_file/0003/476337/The-Benefits-of-Social-Networking-Services.pdf (Accessed 21 November 2018).

Connelly L.M. 2008. Pilot studies. *Medsurg Nursing: Official Journal of the Academy of Medical-Surgical Nurses*, 17(6), 411–412.

Connolly, L.Y., Lang, M., Gathegi, J. and Tygar, D.J. 2017. Organisational culture, procedural countermeasures, and employee security behaviour. *Information and Computer Security*, 25(2), 118–136. doi: 10.1108/ICS-03-2017-0013

Conteh, N.Y. and Schmick, P.J. 2016. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31–38. doi: 10.19101/ijacr.2016.623006

Corritore, C.L., Kracher, B. and Wiedenbeck, S. 2003. On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, 58(6), 737–758. doi: 10.1016/S1071-5819(03)00041-7

Costa, P.T. and McCrae, R.R. 1992. *Professional manual: Revised NEO personality inventory (NEO-PI-R) and NEO five-factor inventory (NEO-FFI)*. Odessa, FL: Psychological Assessment Resources. doi: 10.1037//1040-3590.4.1.5.

Costa, P.T. Jr., Terracciano, A., and McCrae, R.R. 2001. Gender differences in personality traits across cultures: Robust and surprising findings. *Journal of Personality and Social Psychology*, 81, 322–331.

Counter Threat Unit Research Team (CTU). 2017. The curious case of Mia Ash: Fake persona lures Middle Eastern targets. *Secureworks Threat Analysis*, [report] 27 July 2017. https://www.secureworks.com/research/the-curious-case-of-mia-ash

Creswell, J.W. and Plano Clark, V.L. 2007. *Designing and conducting mixed methods research*. London: Sage.

Cvrcek, D., Kumpost, M., Matyas, V. and Danezis, G. 2006. A study on the value of location privacy. *In Proceedings of the 5th ACM workshop on privacy in electronic society – WPES '06*. New York: ACM Press, p. 109. doi: 10.1145/1179601.1179621

Dalal, R.S. and Gorab, A.K. 2016. Insider threat in cyber security: What the organizational psychology literature on counterproductive work behavior can and cannot (yet) tell us. In S.J. Zaccaro, R.S. Dalal, L.E. Tetrick, and J.A. Steinke (Eds.), *Series in applied psychology. Psychosocial dynamics of cyber security* (pp. 92–110). Routledge/Taylor & Francis Group.

D'Arcy, J., Hovav, A. and Galletta, D. 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98. doi: 10.1287/isre.1070.0160

Darker, C. 2013. Risk perception. In: Gellman, M.D., Turner, J.R. (eds). *Encyclopedia of Behavioral Medicine* (p. 110). New York, NY: Springer. https://doi.org/10.1007/978-1-4419-1005-9_866

Darwish, A., Zarka, A. El and Aloul, F. 2012. Towards understanding phishing victims' profile. *2012 International Conference on Computer Systems and Industrial Informatics, ICCSII 2012*, June 2012, pp. 10–15. doi: 10.1109/ICCSII.2012.6454454

Das, T. K. and Teng, B.-S. 2004. The risk-based view of trust: A conceptual framework. *Journal of Business and Psychology*, 19(1), 85–116. doi: 10.1023/B:JOBU.0000040274.23551.1b

Das, S., Kim, A., Tingle, Z. and Nippert-Eng, C. 2019. All about phishing: Exploring user research through a systematic literature review (HAISA 2019). *ArXiv*, abs/1908.05897. https://arxiv.org/abs/1908.05897

Davis, J. 2020. Phishing attacks evade security with Google services, social engineering [News report]. *Health IT Security*, 23 November 2020. https://healthitsecurity.com/news/phishing-attacks-evade-security-with-google-services-social-engineering

DeJonckheere, M. and Vaughn, L.M. 2019. Semistructured interviewing in primary care research: a balance of relationship and rigour. *Family Medicine and Community Health*, 7(2), e000057. https://doi.org/10.1136/fmch-2018-000057

DeKay S. 2009. Are business-oriented social networking web sites useful resources for locating passive jobseekers? Results of a recent study. *Business Communication Quarterly*, 72(1), 101-105. doi:10.1177/1080569908330378

Deutsch, M. 1958. Trust and suspicion. *Journal of Conflict Resolution*, 2(4), 265–279. https://doi.org/10.1177/002200275800200401

Deutsch, M. 1960. The effect of motivational orientation upon trust and suspicion. *Human Relations*, 13, 123–139. https://doi.org/10.1177/001872676001300202

de Vries, R.S. 2017. A methodology for quantifying the level of cybersecurity awareness. Master Thesis. Leiden University, The Hague, Netherlands. https://openaccess.leidenuniv.nl/bitstream/handle/1887/64574/Vries_R_de_2018_CS.pdf?sequence=2

Dhillon, G. and Backhouse, J. 2001. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11, 127–153. http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/DhillonBackhouse2001_ISJ_11_1_review_paper.pdf

Di Giunta, L.L., Alessandri, G., Gerbino, M., Luengo Kanacri, P., Zuffiano, A., and Caprara, G.V. 2013. The determinants of scholastic achievement: The contribution of personality traits, self-esteem, and academic self-efficacy.

Learning and Individual Differences, 27, pp. 102–108. doi: 10.1016/j.lindif.2013.07.006

Digman, J.M. 1990. Personality structure: Emergence of the Five-Factor Model. *Annual Review of Psychology*, 41, 417-440. https://doi.org/10.1146/annurev.ps.41.020190.002221

Donnellan, M.B., Oswald, F.L., Baird, B.M. and Lucas, R.E. 2006. The Mini-IPIP scales: Tiny-yet-effective measures of the Big Five Factors of Personality. *Psychological Assessment*, 18(2), 192–203. https://doi.org/10.1037/1040-3590.18.2.192

Dreibelbis, R.C., Martin, J., Coovert, M.D. and Dorsey, D.W. 2018. The looming cybersecurity crisis and what it means for the practice of industrial and organizational psychology. *Industrial and Organizational Psychology*, 11(2), 346-365. DOI: https://doi.org/10.1017/iop.2018.3 https://www.cambridge.org/core/journals/industrial-and-organizational-psychology/article/looming-cybersecurity-crisis-and-what-it-means-for-the-practice-of-industrial-and-organizational-psychology/4D676BE58747D375AC531D9A46446723/core-reader#

Dudovskiy, J. 2018. *The ultimate guide to writing a dissertation in business studies: A step-by-step assistance* [e-book]. Business Research Methodology. https://research-methodology.net/product/the-ultimate-guide-to-writing-a-dissertation-in-business-studies-a-step-by-step-assistance-january-2018-edition/

Dwyer, C., Hiltz, and Passerini. 2007. Trust and privacy concern within social networking sites: A Comparison of Facebook and MySpace. *Americas Conference on Information Systems Proceedings*, 339, pp. 12–31. https://aisel.aisnet.org/amcis2007/339/

Earle, T.C. and Cvetkovich, G. 1997. Culture, cosmopolitanism, and risk management. *Risk Analysis*, 17(1), 55–65. https://doi.org/10.1111/j.1539-6924.1997.tb00843.x

Earle, T.C. and Cvetkovich, G.T. 1995. *Social trust: Toward a cosmopolitan society*. Westport, CT: Praeger.

Edwards, M. Larson, R., Green, B., Rashid, A. and Baron, A. 2017. Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security*, 69, 18–34. doi: 10.1016/j.cose.2016.12.013

Egelman, S. and Peer, E. 2015. Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS). In: *CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 2873–2882. https://doi.org/10.1145/2702123.2702249

Eisend, M. 2006. Source credibility dimensions in marketing communication – A generalized solution. *Journal of Empirical Generalisations in Marketing Science*, 10(2), 1–33. https://www.empgens.com/article/source-credibility-dimensions-in-marketing-communication-a-generalized-solution/

Ellison N.B. and Boyd, D.M. 2013. Sociality through social network sites. In: William H. Dutton (ed.) *The Oxford Handbook of Internet Studies*. Oxford University Press. DOI: 10.1093/oxfordhb/9780199589074.013.0008

Elnaim, B. and Al-Lami, H. 2017. The current state of phishing attacks against Saudi Arabia university students. *International Journal of Computer Applications Technology and Research*, 6(1), 42–50. www.ijcat.com42 (Accessed 1 December 2018).

Enos, F., Benus, S., Cautin, R.L., Graciarena, M., Hirschberg, J. and Shriberg, E. 2006. Personality factors in human deception detection: Comparing human to machine performance. In *Proceedings of the Annual Conference of the International Speech Communication Association – INTERSPEECH 2006*. doi: 10.1.1.448.5012 https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.448.5012&rep=rep1&type=pdf

Erdheim, J., Wang, M. and Zickar, M.J. 2006. Linking the Big Five personality constructs to organizational commitment. *Personality and Individual Differences*, 41(5), 959–970. doi: 10.1016/j.paid.2006.04.005

Evans, A.M. and Revelle, W. 2008. Survey and behavioral measurements of interpersonal trust. *Journal of Research in Personality*, 42, 1585–1593. doi:10.1016/j.jrp.2008.07.011

Eysenck, H.J. 1990. Genetic and environmental contributions to individual differences: The three major dimensions of personality. *Journal of Personality*, 58(1), 245–261. doi: 10.1111/j.1467-6494.1990.tb00915.x

Ferreira, A., Coventry, L. and Lenzini, G. 2015. *Human aspects of information security, privacy, and trust*. Edited by T. Tryfonas and I. Askoxylakis. Cham: Springer International Publishing (Lecture Notes in Computer Science). doi: 10.1007/978-3-319-20376-8.

Festinger, L. 1957. *A theory of cognitive dissonance*. Stanford, CA: Stanford University Press.

FINRA Investor Education Foundation. 2013. *Financial fraud and fraud susceptibility in the United States*. Research report from a 2012 national survey. FINRA Investor Education Foundation. https://www.finrafoundation.org/files/financial-fraud-and-fraud-susceptibility-united-states-research-report-2012-national-survey (Accessed 17 August 2018).

Fire, M., Goldschmidt, R. and Elovici, Y. 2013. Online social networks: Threats and solutions survey. *IEEE Communication Surveys & Tutorials Online*, 16(4), 1–20. doi: 10.1109/COMST.2014.2321628.

Fishbein, M.A. and Ajzen, I. 1975. *Belief, attitude, intention and behaviour: An introduction to theory and researc*h. Reading, MA: Addison-Wesley. https://www.researchgate.net/publication/233897090_Belief_attitude_intention_and_behaviour_An_introduction_to_theory_and_research

Fleming, P., Watson, S.J., Patouris, E., Bartholomew, K.J. and Zizzo, D.J. 2017. Why do people file share unlawfully? A systematic review, meta-analysis and panel study. *Computers in Human Behavior*, 72, 535–548. doi: 10.1016/j.chb.2017.02.014

Ford, J.B. 2016. Cost vs credibility: the student sample trap in business research. *European Business Review, 28*(6), pp. 652-656. https://doi.org/10.1108/EBR-08-2016-0100

Forrester, B. and den Hollander, K. 2016. The role of social media in the intelligence cycle. In Broome, B.D. *et al.* (eds), *Next-Generation Analyst IV*, 18 - 19 April 2016, 9851. *Proceedings of SPIE - The International Society for Optical Engineering*, p. 98510G. doi: 10.1117/12.2242530

FraudWatch International. 2017. UAE, the GCC region and the importance of increasing Phishing Awareness [online article], *FraudWatch International*, 7 June 2017.

https://fraudwatchinternational.com/phishing/uae-gcc-phishing-awareness/ (Accessed 16 September 2018).

Frauenstein, E.D. and Flowerday, S. 2020. Susceptibility to phishing on social network sites: A personality information processing model, *Computers & Security*, 94, 101862. https://doi.org/10.1016/j.cose.2020.101862

Freudenburg, W.R. 1993. Risk and recreancy: Weber, the division of labor, and the rationality of risk perceptions. *Social Forces*, 71(4), 909–932. https://doi.org/10.1093/SF/71.4.909

Frumento, E. *et al.* 2016. The role of social engineering in evolution of attacks [Gov't report]. *Advanced Social Engineering and Vulnerability Assessment Framework* (DOGANA). European Commission Horizon 2020 Programme. https://www.dogana-project.eu/images/PDF_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf (Accessed 2 December 2018).

Furnell, S. 2010. Jumping security hurdles. *Computer Fraud & Security*, 2010(6), 10–14. doi: 10.1016/S1361-3723(10)70067-1

Furnell, S. and Rajendran, A. 2012. Understanding the influences on information security behaviour. *Computer Fraud & Security*, 2012(3), 12-15. doi: 10.1016/S1361-3723(12)70053-2

Garbarino, E. and Strahilevitz, M. 2004. Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research*, 57(7):768-775. doi: 10.1016/S0148-2963(02)00363-6

Gastellier-Prevost, S., Granadillo, G.G. and Laurent, M. 2011. Decisive heuristics to differentiate legitimate from phishing sites. In 2011 *Conference on Network and Information Systems Security*. IEEE, pp. 1–9. doi: 10.1109/SAR-SSI.2011.5931389

Gardikiotis, A. and Crano, W.D. 2015. Persuasion theories. In J.D. Wright (Ed.), *International Encyclopedia of the Social & Behavioral Sciences* (2nd edn). Oxford: Elsevier. doi: 10.1016/B978-0-08-097086-8.24080-4

General Authority for Statistics. 2019. *Population Estimates, 2019.* https://www.stats.gov.sa/en/43 (Accessed 2 August 2020).

Gevers, W. 2020. COVID-19 cyberattacks are placing organizations at increased risk. *Saudi Gazette*, 20 May 2020. https://saudigazette.com.sa/article/593366 (Accessed 3 August 2020).

Gkika, S., Skiada, M., Lekakos, G. and Kourouthanasis, P. 2016. Investigating the role of personality traits and influence strategies on the persuasive effect of personalized recommendations. In: *4th Workshop on Emotions and Personality in Personalized Systems* (EMPIRE), p. 9. http://ceur-ws.org/Vol-1680/paper2.pdf

Gneezy, A. 2017. Field experimentation in marketing research. *Journal of Marketing Research*, 54(1), 140–143. doi: 10.1509/jmr.16.0225

GlobalWebIndex. 2016. *GWI Social 2016 Summary Report: GlobalWebIndex's quarterly report on the latest trends in social networking*. https://www.slideshare.net/globalwebindex/globalwebindex-social-q1-summary-report (Accessed 3 February 2019).

Global Media Insight. 2019. *Saudi Arabia Social Media Statistics 2019*. 29 October 2019. https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/

Goel, S., Williams, K. and Dincelli, E. 2017. Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1), pp. 22–44. doi: 10.17705/1jais.00447

Goldberg, L.R. 1990. An alternative "description of personality": The Big-Five factor structure. *Journal of Personality and Social Psychology*, 59(6), 1216-1229. https://projects.ori.org/lrg/PDFs_papers/Goldberg.Big-Five-FactorsStructure.JPSP.1990.pdf

Goldberg, L.R. 1992. The development of markers for the Big-Five factor structure. *Psychological Assessment*, 4(1), 26-42. https://doi.org/10.1037/1040-3590.4.1.26

Goldberg, L.R. 1999. A broad-bandwidth, public-domain, personality inventory measuring the lower-level facets of several five-factor models. In: I. Mervielde, I.J. Deary, F. De Fruyt, and F. Ostendorf (Eds.), *Personality psychology in Europe* (Vol. 7, pp. 7–28). Tilburg, The Netherlands: Tilburg University Press.

Goldkuhl, G. 2004. Meanings of pragmatism: Ways to conduct information systems research. *2nd International Conference on Action in Language, Organisations and*

Information Systems (*ALOIS-2004*), 17-18 March 2004, Linköping University, Sweden. http://www.vits.org/publikationer/dokument/457.pdf

Goldkuhl, G. 2008. What kind of pragmatism in information systems research? Special Interest Group on Pragmatist IS Research (SIGPrag). Association for Information Systems. AIS SIG Prag Inaugural Meeting, Dec 14, 2008, Paris.

Goodey, P. 2015. *Salesforce CRM: The definitive admin handbook* (3rd edn). Packt Publishing. https://books.google.ie/books?id=sftzBgAAQBAJ&pg=PP1&lpg=PP1&dq=successfully+administer+Salesforce+CRM+and+Salesforce+mobile+implementations+with+best+practices+and+realworld+scenarios&source=bl&ots=nmEAnKssu3&sig=KhCGUPTQrc6hjF36ixW_xGK5kg8&hl=en&sa=X&v (Accessed 18 August 2018).

Gosling, S. D., Rentfrow, P.J. and Swann, W.B., Jr. 2003. A very brief measure of the Big Five personality domains. *Journal of Research in Personality*, 37, 504-528. https://doi.org/10.1016/S0092-6566(03)00046-1

Gov.SA. 2020. *Unified National Platform*. https://www.my.gov.sa/wps/portal/snp/pages/agencies

Grabosky, P. 2001. Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10(2):243–249. https://doi.org/10.1177/a017405

Gragg, D. 2003. A multi-level defense against social engineering. *SANS Reading Room*, Paper 920. 13 March 2003. SANS Institute. https://www.sans.org/reading-room/whitepapers/engineering/paper/920

Gray, R. 2018. Common LinkedIn phishing scams and how to prevent them [Blog post]. Wandera, 17 September 2018. https://www.wandera.com/common-linkedin-scams-and-how-to-prevent-them/

Greenspan, S. 2009. *Annals of gullibility: Why we get duped and how to avoid it*. Praeger Publishers.

Greitzer, F.L., Strozer, J.R., Cohen, S., Moore A.P., Mundie, D. and Cowley, J. 2014. Analysis of unintentional insider threats deriving from social engineering exploits. In *2014 IEEE Security and Privacy Workshops*. IEEE, pp. 236–250. doi: 10.1109/SPW.2014.39

Grimes, G.A., Hough, M.G., Mazur, E. and Signorella, M.L. 2010. Older adults' knowledge of Internet hazards. *Educational Gerontology*, 36(3), 173–192. https://doi.org/10.1080/03601270903183065

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. 2018. Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345–358. doi: 10.1016/j.cose.2017.11.015.

Gulf Business. 2018. Saudi terminates more than 70% of foreign staff in government jobs. *Gulf Business* [Online magazine], 30 October 2018. https://gulfbusiness.com/saudi-terminates-more-than-70-foreign-staff-government-jobs/ (Accessed 4 March 2020).

Gülseçen, S. and Kubat, A. 2006. Teaching ICT to teacher candidates using PBL: A qualitative and quantitative evaluation. Educational Technology and Society, 9(2), 96-106. https://www.jstor.org/stable/jeductechsoci.9.2.96?seq=1

Gupta, N. and Gupta, A.K. 2020. Big Five Personality traits and their impact on job performance of managers in FMCG sector. *International Journal of Recent Technology and Engineering*, 8(5), 3104-3109. DOI:10.35940/ijrte.E6406.018520 https://www.ijrte.org/wp-content/uploads/papers/v8i5/E6406018520.pdf

Hadlington, L. 2017. Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(2017), e00346. doi: 10.1016/j.heliyon.2017.e00346

Hadlington, L. 2018. Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, 12(1), 269-281. DOI: 10.5281/zenodo.1467909

Hadlington, L., Binder, J. and Stanulewicz, N. 2021. Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Computers in Human Behavior*, 114, 106557. https://doi.org/10.1016/j.chb.2020.106557

Hadnagy, C. 2011. *Social engineering: The art of human hacking*. Indianapolis: Wiley. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470639539.html (Accessed 30 October 2017).

Halevi, T., Lewis, J. and Memon, N. 2013a. A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web: WWW '13*. Companion. New York, NY: ACM Press, pp. 737–744. doi: 10.1145/2487788.2488034

Halevi, T., Lewis, J. and Memon, N. 2013b. Phishing, personality traits and Facebook. *arXiv*:1301.7643. http://arxiv.org/abs/1301.7643 (Accessed 22 April 2018).

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., . . . Chen, J. 2016. Cultural and psychological factors in cybersecurity. In *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services* – IIWAS '16, pp. 318–324. doi: 10.1145/3011141.3011165

Halevi, T., Memon, N. and Nov, O. 2015. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *SSRN* [electronic journal], January 2015. doi: 10.2139/ssrn.2544742

Hallikainen, P. 2015. Why people use social media platforms: Exploring the motivations and consequences of use. In: Mola L., Pennarola F., Za S. (eds) *From Information to Smart Society. Lecture Notes in Information Systems and Organisation*, vol 5. Springer, Cham. https://doi.org/10.1007/978-3-319-09450-2_2

Hamid, T. 2017. Threats grow in Saudi Arabia's cyber sector. *ComputerWeekly.com*, 29 March 2017. http://www.computerweekly.com/news/450415661/Threats-grow-in-Saudi-Arabias-cyber-sector (Accessed 27 November 2017).

Harvard Kennedy School. 2019. The labor market in Saudi Arabia: background, areas of progress, and insights for the future. *Evidence for Policy Design*. August 2019. Cambridge, MA: Harvard University https://epod.cid.harvard.edu/sites/default/files/2019-08/EPD_Report_Digital.pdf (Accessed 2 August 2020).

Hecke, T.V. 2012. Power study of ANOVA versus Kruskal-Wallis test. *Journal of Statistics and Management Systems*, 15(2-3), 241-247. https://doi.org/10.1080/09720510.2012.10701623

Henshel, D., Sample, C., Cains, M. and Hoffman, B. 2016. Integrating cultural factors into human factors framework and ontology for cyber attackers (pp. 123-137). In:

Advances in human factors in cybersecurity. *Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity*, 27-31 July 2016, Orlando, Florida, USA. DOI: 10.1007/978-3-319-41932-9_11

Herath, T. and Rao, H.R. 2009a. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T. and Rao, H.R. 2009b. Protection motivation and deterrence: a framework for security policy compliance in organisations, *European Journal of Information Systems*, 18(2), 106-125. DOI:10.1057/ejis.2009.6

Hichang Cho, Rivera-Sánchez, M. and Lim, S. 2009 A multinational study on online privacy: global concerns and local responses. *New Media & Society*, 11(3), 395–416. doi: 10.1177/1461444808101618

Hindelang, M.J., Gottfredson, M.J. and Garofalo, J. 1978. *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

Hoadley, C.M., Xu, H., Lee, J.J. and Rosson, M.B. 2010. Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*, 9(1), 50-60. https://doi.org/10.1016/j.elerap.2009.05.001

Hofstede, G. 1980. *Culture's consequences: International differences in work-related values*. Beverly Hills, CA: Sage.

Hofstede, G., Hofstede, G.J., and Minkov, M. 2010. *Cultures and organizations: Software of the mind: Intercultural cooperation and its importance for survival*. New York: McGraw-Hill Professional.

Holt, T.J. and Bossler, A.M. 2009. Examining the applicability of lifestyle-routine activity theory for cybercrime victimisation. *Deviant Behaviour*, 30, 1–25. https://doi.org/10.1080/01639620701876577

Holt. T.J., van Wilsem, J., van de Weijer, S., Leukfeldt, R. 2018. Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*, 38(2):187-206. doi:10.1177/0894439318805067

Hohwü, L., Lyshol, H., Gissler, M., Jonsson, S.H., Petzold, M. and Obel, C. 2013. Web-based versus traditional paper questionnaires: a mixed-mode survey with a Nordic perspective. *Journal of Medical Internet Research*, 15(8), e173. https://doi.org/10.2196/jmir.2595

Holtfreter, K., Reisig, M.D., Pratt, T.C. and Holtfreter, R.E. 2015. Risky remote purchasing and identity theft victimization among older Internet users. P*sychology, Crime & Law*, 21, 681–698. doi:10.1080/1068316X.2015.1028545

Hosmer, D.W., Jr., Lemeshow, S. and Sturdivant, R.X. 2013. *Applied logistic regression*. Wiley.

Hovland, C.I., Janis, I.L. and Kelley, H.H. 1953. *Communication and persuasion: Psychological studies of opinion change*. New Haven, CT: Yale University Press.

Huff, L. and Kelly, L. 2003. Levels of organizational trust in individualist versus collectivist societies: A Seven-Nation Study. *Organization Science*, 14(1), 1-106. https://doi.org/10.1287/orsc.14.1.81.12807

Hussey, J. and Hussey, R. 1997. *Business research: A practical guide for undergraduate and postgraduate students*. London: Macmillan.

Hycner, R.H. 1985. Some guidelines for the phenomenological analysis of interview data. *Human Studies*, 8, 279–303. https://doi.org/10.1007/BF00142995

IDCARE. 2018. LinkedIn security. *Learning Centre – Fact Sheets*. https://www.idcare.org/fact-sheets/linkedin-security (Accessed 27 February 2019).

Ifinedo, P. 2019. End user nonmalicious, counterproductive computer security behaviors: Concept, development, and validation of an instrument. *Security and Privacy*, 2019(2), e66. https://doi.org/10.1002/spy2.66

Information Security Media Group (ISMG). 2016. *Email security: Social engineering report* [industry report]. Princeton, NJ, USA: Agari.

Insider Intelligence. 2020. Facebook ranks last in digital trust among consumers. *Business Insider*, 24 September 2020. https://www.businessinsider.com/facebook-is-consumers-least-trusted-social-media-platform-2020-9

International Personality Item Pool: A Scientific Collaboratory for the Development of Advanced Measures of Personality Traits and Other Individual Differences [online]. http://ipip.ori.org/

Interpol. 2015. *Social engineering fraud: Questions and answers*. December 2015, pp. 1–4. https://www.interpol.int/Media/Files/Crime-areas/Financial-crime/Social-engineering-fraud/

Interpol. 2017. Types of social engineering fraud / Social engineering fraud / Financial crime / Crime areas / Internet / Home - INTERPOL, International police - Financial Crimes. https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud (Accessed 24 November 2017).

Irani D., Balduzzi M., Balzarotti D., Kirda E. and Pu C. 2011. Reverse social engineering attacks in online social networks (pp. 55–74). In: Holz T., Bos H. (eds.) *Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2011*. *Lecture Notes in Computer Science*, vol. 6739. Springer. https://doi.org/10.1007/978-3-642-22424-9_4

Isen, A.M. and Patrick, R. 1983. The effect of positive feelings on risk taking: When the chips are down. *Organizational Behavior and Human Performance*, 31(2), 194–202. doi: 10.1016/0030-5073(83)90120-4

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. 2007. Social phishing. *Communications of the ACM*, 50(10), 94–100. doi: 10.1145/1290958.1290968

Jalali, M.S., Bruckes, M., Westmattelmann, D. and Schewe, G. 2020. Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research*, 22(1), e16775. https://doi.org/10.2196/16775

Jacob, C., Guéguen, N. and Boulbry, G. 2018. How proof of previous donations influences compliance with a donation request: Three field experiments. *International Review on Public and Nonprofit Marketing*, 15(1-8). doi: 10.1007/s12208-017-0187-x

Jacoby, J., Troutman, T., Kuss, A. and Mazursky, D. 1986. Experience and expertise in complex decision making. In *NA - Advances in Consumer Research* (vol. 13, pp. 469-472). Richard J. Lutz (ed.). Provo, UT: Association for Consumer Research.

http://www.acrwebsite.org/search/view-conference-proceedings.aspx?Id=6533 (Accessed 5 December 2018).

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. 2007. Social phishing. *Communications of the ACM*, 50(10), 94–100. doi: 10.1145/1290958.1290968

John, O.P. and Srivastava, S. 1999. The Big Five Trait taxonomy: History, measurement, and theoretical perspectives. In L.A. Pervin and O.P. John (Eds.), *Handbook of personality: Theory and research* (pp. 102–138). Guilford Press.

Johnston, A.C., Warkentin, M. and Siponen, M. 2015. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113–134. doi: 10.25300/MISQ/2015/39.1.06

Jones, H.S. and Towse, J. 2018. Examinations of email fraud susceptibility: Perspectives from academic research and industry practice (pp. 80-97). In: J. McAlaney, L.A. Frumkin and V. Benson, eds. *Psychological and behavioral examinations in cyber security*. IGI Global. DOI: 10.4018/978-1-5225-4053-3.ch005

Junger, M, Montoya, L. and Overink, F.-J. 2017. Priming and warnings are not effective to prevent social engineering attacks. doi: 10.1016/j.chb.2016.09.012

Junglas, I. and Spitzmüller, C. 2006. Personality traits and privacy perceptions: An empirical study in the context of location-based services. In *International Conference on Mobile Business. ICMB 2006*. doi: 10.1109/ICMB.2006.40

Kaptein, M., De Ruyter, B., Markopoulos, P. and Aarts, E. 2012. Adaptive persuasive systems: A study of tailored persuasive text messages to reduce snacking. *ACM Transactions on Interactive Intelligent Systems*, 2(2), Article 10. http://doi.acm.org/10.1145/2209310.2209313

Kassner, M. 2020. Cybersecurity pros: Are humans really the weakest link? [Blog post] *TechRepublic*, 21 December 2020. https://www.techrepublic.com/article/cybersecurity-pros-are-humans-really-the-weakest-link

Kawulich, B. 2012. Selecting a research approach: Paradigm, methodology and methods. In: C. Wagner, B. Kawulich, and M. Garner, eds. *Doing social research: A global context*. London: McGraw-Hill, pp. 51-61.

Keaney, A.M. 2012. *Risk perceptions on social networking sites: An investigation of age and other factors*. PhD thesis. Trinity College, University of Dublin.

Kee, J. 2008. *Social engineering: Manipulating the Source* (whitepaper). https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-source-32914 (Accessed 26 November 2018).

Keinan, R. and Bereby-Meyer, Y. 2017. Perceptions of active versus passive risks, and the effect of personal responsibility. *Personality and Social Psychology Bulletin*, 43(7), 999–1007. doi: 10.1177/0146167217703079

Kelly, C. 2020. 95% of Saudi businesses hit by cyber attack in the past year. ITP.net, [online news report] 11 August 2020. https://www.itp.net/news/93516-95-of-saudi-businesses-hit-by-cyber-attack-in-the-past-year

Kemp, S. 2020. Digital 2020: Saudi Arabia. *Data Reportal*. 12 February 2020. https://datareportal.com/reports/digital-2020-saudi-arabia (Accessed 3 August 2020).

Kennedy, A. and Parsons, A. 2012. Macro-social marketing and social engineering: a systems approach. *Journal of Social Marketing*, 2(1), 37–51. doi:10.1108/20426761211203247

Khanna, S. 2016. Don't fall victim to the newest phishing scam. *Journal of Accountancy*, 24 October 2016. https://www.journalofaccountancy.com/newsletters/2016/oct/phishing-scam-executive-impersonation.html (Accessed 30 January 2019).

Kim, K.J. and Joukov, N. 2016. *Information science and applications (ICISA) 2016*. Berlin: Springer.

Kim, M. and Cha, J. 2017. A comparison of Facebook, Twitter, and LinkedIn: Examining motivations and network externalities for the use of social networking sites. *First Monday*, 22(11). doi: 10.5210/fm.v22i11.8066

King, Z.M. Henshel, D.S, Flora, L., Cains, M.G., Hoffman, B. and Sample, C. 2018. Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology*, 5 February 2018, 39. doi: 10.3389/fpsyg.2018.00039

Kirichenko, L., Radivilova T. and Carlsson, A. 2017. Detecting cyber threats through social network analysis: short survey. *SocioEconomic Challenges*, 1(1), 20-34. arXiv:1805.06680

Kleitman, S., Law, M.K.H. and Kay, J. 2018. It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLoS ONE* 13(10), e0205089. https://doi.org/10.1371/journal.pone.0205089

Knowles, C. 2020. Cyber attacks use LinkedIn to target companies and employees. *SecurityBrief – Cybersecurity and Threat News for Europe, the Middle East & Africa*, [online news report] 19 June 2020. https://securitybrief.eu/story/cyber-attacks-use-linkedin-to-target-companies-and-employees

Kongsved, S.M., Basnov, M., Holm-Christensen, K. and Hjollund, N.H. 2007. Response rate and completeness of questionnaires: a randomized study of Internet versus paper-and-pencil versions. *Journal of Medical Internet Research*, 9(3), e25. https://doi.org/10.2196/jmir.9.3.e25

Kontaxis, G., Polakis, I., Ioannidis, S. and Markatos, E.P. 2011. Detecting social network profile cloning. In *2011 IEEE International Conference on Pervasive Computing and Communications Workshops*. PERCOM Workshops 2011, pp. 295–300. doi: 10.1109/PERCOMW.2011.5766886

Korzaan, M.L. and Boswell, K.T. 2008. The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, 48(4), 15-24. doi: 10.1080/08874417.2008.11646031

Koochaksaraee, A.A. 2019. *End-user security & privacy behaviour on social media: Exploring posture, proficiency & practice*. Master Thesis. University of Ottawa, Ontario, Canada. https://ruor.uottawa.ca/bitstream/10393/39310/3/Akbari_Koochaksaraee_Amir_2019_thesis.pdf

Krasnova, H., Spiekermann, S., Koroleva, K. and Hildebrand, T. 2010. Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), 109–125. https://doi.org/10.1057/jit.2010.6

Krasnova, H. and Veltri, N. F. 2010. Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *2010 43rd Hawaii International Conference on System Sciences*. IEEE, pp. 1–10. doi: 10.1109/HICSS.2010.307

Krombholz, K. Hobel, H., Huber, M. and Weippl, E. 2015. Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122. doi: 10.1016/j.jisa.2014.09.005

Krehel, O. 2016. The rise of LinkedIn fraud. *Secure Connection* [blog], 22 February 2016. CSO. https://www.csoonline.com/article/3036072/the-rise-of-linkedin-fraud.html

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F. and Hong, J. 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2), Article 7, 31 pages. doi: 10.1145/1754393.1754396

Kvale, S. 1996. *InterViews: An introduction to qualitative research interviewing*. Thousand Oaks, CA: Sage.

Lacey, D., Salmon, P. and Glancy, P. 2015. Taking the bait: A systems analysis of phishing attacks', *Procedia Manufacturing*, 3, 1109–1116. doi: 10.1016/j.promfg.2015.07.185

Lalor, J.G., Casey, D., Elliott, N. … Begley, C. 2013. Using case study within a sequential explanatory design to evaluate the impact of specialist and advanced practice roles on clinical outcomes: the SCAPE study. *BMC Medical Research Methodology*, 13(55). https://doi.org/10.1186/1471-2288-13-55

Lampe, C. and Ellison, N.B. 2016. *Social media and the workplace* [Report]. Pew Research Center Internet & Technology, 22 June 2016. https://www.pewresearch.org/internet/2016/06/22/social-media-and-the-workplace/ (Accessed 14 February 2021).

LaRose, R. 2010. The problem of media habits. *Communication Theory*, 20, 194–222. doi: 10.1111/j.1468-2885.2010.01360.x

Lavrakas, P.J. 2008. Priming. *Encyclopedia of survey research methods*. Thousand Oaks, CA: Sage. http://dx.doi.org/10.4135/9781412963947.n399

Lawler, J.P., Molluzzo, J.C. and Doshi, V. 2012. An expanded study of net generation perceptions on privacy and security on social networking sites (SNS). *Information*

Systems Education Journal, 10(1), 21-32. http://isedj.org/2012-10/N1/ISEDJVol10No1.pdf (Accessed 2 December 2018).

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H. 2014. Information security awareness and behavior: A theory-based literature review. *Management Research Review*, 37(12), 1049–92. doi: 10.1108/mrr-04-2013-0085

Lee, A.S. and Hubona, G. 2009. A scientific basis for rigor in information systems research. *Management Information Systems Quarterly*, 33(2), 237-262. https://aisel.aisnet.org/misq/vol33/iss2/4

Lee, J.K., and Rao, H.R. 2007. Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government-citizens online interactions in a turbulent environment. *Decision Support Systems*, 43(4), 1431-1449. https://doi.org/10.1016/j.dss.2006.04.008

Legal Dictionary. 2017. General deterrence. LegalDictionary.net https://legaldictionary.net/general-deterrence/

Leukfeldt, E.R. and Yar, M. 2016. Applying Routine Activity Theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280. doi: 10.1080/01639625.2015.1012409

Levine, T.R. and McCornack, S.A. 1991. The dark side of trust: Conceptualizing and measuring types of communicative suspicion. *Communication Quarterly*, 39(4), 325-340. doi: 10.1080/01463379109369809

Likert, R. 1932. A technique for the measurement of attitudes. *Archives of Psychology*, 140, 5–55. https://legacy.voteview.com/pdf/Likert_1932.pdf (Accessed 1 October 2020).

LinkedIn. 2020. Statistics, About us. *LinkedIn Pressroom*. https://news.linkedin.com/about-us#Statistics (Accessed 14 December 2020).

Linkov, V., Zámečník, P., Havlíčková, D. and Pai, C.-W. 2019. Human factors in the cybersecurity of autonomous vehicles: Trends in current research. *Frontiers in Psychology*, 10, 995. https://doi.org/10.3389/fpsyg.2019.00995

Lumen. Attitudes and persuasion. *Psychology* [online course]. OpenStax College. http://cnx.org/contents/4abf04bf-93a0-45c3-9cbc-2cefd46e68cc@4.100:1/Psychology.

https://courses.lumenlearning.com/psychology2x4master/chapter/attitudes-and-persuasion/ (Accessed 31 October 2020).

Lystig Fritchie, L. and Johnson, K.K.P. 2003. Personal selling approaches used in television shopping. *Journal of Fashion Marketing and Management*, 7(3), 249-258. doi: 10.1108/13612020310484807

Lyons, J.B., Stokes, C.K., Eschleman, K.J., Alarcon, G.M. and Barelka, A.J. 2011. Trustworthiness and IT suspicion: An evaluation of the nomological network. *Human Factors*, 53(3), 219–229. https://doi.org/10.1177/0018720811406726

Madden, T.J., Ellen, P.S. and Ajzen, I. 1992. A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin*, 18(1), 3-9. doi: 10.1177/0146167292181001

Madnick, S. 1978. Management policies and procedures needed for effective computer security. *Sloan Management Review*, 20(1), 61-74. https://pubmed.ncbi.nlm.nih.gov/10239542/

Maisel, S. 2014. The new rise of tribalism in Saudi Arabia. *Nomadic Peoples*, 18(2), 100-122. http://www.jstor.org/stable/43123948

Malek, C. 2019. Saudi Arabia 'a prime target for hackers,' cyber experts warn [online news report]. *Arab News*, 8 September 2019. https://www.arabnews.com/node/1551186/saudi-arabia

Malhotra, N.K., Kim, S.S. and Agarwal, J. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Marinova, I. 2020. 28 Need-to-know remote work statistics of 2020. *Review 42*, 24 September 2020. https://review42.com/remote-work-statistics/

Martin, J. 1973. *Security, accuracy, and privacy in computer systems*. Englewood Cliffs, NJ: Prentice-Hall.

Martinko, M.J, Gundlach, M.J, and Douglas, S.C. 2002. Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective. *International Journal of Selection and Assessment*, 10(1-2), 36-50. doi: 10.1111/1468-2389.00192

Mayer, R.C., Davis, J.H., & Schoorman, F.D. 1995. An integrative model of organizational trust. *Academy of Management Review*, 20, 709-734. https://doi.org/10.2307/258792

McBride, M., Carter, L. and Warkentin, M. 2012. *Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies*. RTI International – Institute for Homeland Security Solutions. Washington, DC: U.S. Department of Homeland Security.

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T. and Pattinson, M. 2017a. A reliable measure of Information Security Awareness and the identification of bias in responses. *Australasian Journal of Information Systems*, 21, 1–12. https://doi.org/10.3127/ajis.v21i0.1697

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. 2017b. Individual differences and Information Security Awareness. *Computers in Human Behaviour*, 69, 151-156. https://doi.org/10.1016/j.chb.2016.11.065

McCrae, R.R. and Costa, P.T. 1987. Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology*, 52 (1): 81–90. doi:10.1037/0022-3514.52.1.81

McGregor, S.L.T. and Murnane, J.A. 2010. Paradigm, methodology and method: intellectual integrity in consumer scholarship. *International Journal of Consumer Studies*, 34(4), 419–427. https://doi.org/10.1111/j.1470-6431.2010.00883.x

McHugh, M.L. 2013. The chi-square test of independence. *Biochemia Medica*, 23(2), 143-149.

McKnight, D.H., Choudhury, V. and Kacmar, C. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 227-359. https://doi.org/10.1287/isre.13.3.334.81

McSweeney, B. 2002. Hofstede's model of national cultural differences and their consequences: A triumph of faith - A failure of analysis. *Human Relations*, 55(1), 89–118. doi: 10.1177/0018726702551004

Mearns, M.B., Matthiesen, K.B. and Eid, S.B. 2011. Personality and social psychology using the Job Demands–Resources model to investigate risk perception, safety

climate and job satisfaction in safety critical organizations. Scandinavian Journal of Psychology, 52(5), 465-475. doi: 10.1111/j.1467-9450.2011.00885.x

Mercado, B.K. 2017. *Cyber counterproductive work behaviors: Measurement, prediction, and means for reduction*. PhD dissertation. City University of New York (CUNY). https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=3079&context=gc_etds

Merit Systems Protection Board. 2011. Understanding Favoritism – MSPB takes a closer look at what the concept of favoritism means. *Issues of Merit*, (2011, July), 1–7. www.mspb.gov

Metev, D. 2020. How much time do people spend on social media? [63+ facts to like, share and comment]. *Review 42*, 4 July 2020. https://review42.com/how-much-time-do-people-spend-on-social-media/

Meyer, Z. 2020. Never click on this kind of Zoom invite. You'll thank us forever. *FastCompany*, 7 December 2020. https://www.fastcompany.com/90582864/never-click-on-this-kind-of-zoom-invite-youll-thank-us-forever

Michielsen, H.J., de Vries, J. and van Heck, G.L. 2003. Psychometric qualities of a brief self-rated fatigue measure: The Fatigue Assessment Scale. *Journal of Psychosomatic Research*, 54(4), 345–352. https://doi.org/10.1016/s0022-3999(02)00392-6

Microsoft. 2018. *Microsoft Security Intelligence Report*, vol. 23. https://info.microsoft.com/rs/157-GQE-382/images/EN-US_CNTNT-eBook-SIR-volume-23_March2018.pdf (Accessed 18 August 2018).

Miles, J. 2014. Tolerance and variance inflation factor. *Wiley StatsRef: Statistics Reference Online*. https://onlinelibrary.wiley.com/doi/10.1002/9781118445112.stat06593

Mills, C. 2017. *Cyber security strategy* [govt. report], December 2017. Castle Point Borough Council (UK). https://www.castlepoint.gov.uk/download.cfm?doc=docm93jijm4n3296.pdf&ver=6099

Mills, D. 2009. Analysis of a social engineering threat to information security exacerbated by vulnerabilities exposed through the inherent nature of social networking websites. In *2009 Information Security Curriculum Development Conference – InfoSecCD '09* (pp. 139-141). doi: 10.1145/1940976.1941003

Mills, E. 2010. Social engineering 101 (Q & A). *CNET*. cnet.com. https://www.cnet.com/news/social-engineering-101-q-a/ (Accessed 27 November 2018).

Milne, G.R., Labrecque, L.I. and Cromer, C. 2009. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3), pp. 449–473. doi: 10.1111/j.1745-6606.2009.01148.x

Mingers, J. 2001. Combining IS research methods: Towards a pluralist methodology. *Information Systems Research*, 12(3), 240-259. doi: 10.1287/isre.12.3.240.9709

Ministry of Communications and Information Technology (MCIT). 2018a. NCSC releases report on cyber threats, risks for Q3-2017. 02 Jan 2018. https://www.mcit.gov.sa/en/media-center/news/99093

Ministry of Communications and Information Technology (MCIT). 2018b. NCSC releases '2017-Q4 Threats And Risk Report'. 06 May 2018. https://www.mcit.gov.sa/en/media-center/news/99558

Ministry of Human Resources and Social Development. 2020a. *About Ministry* [Arabic-language webpage]. https://hrsd.gov.sa/ar/node/433 (Accessed 20 September 2020).

Ministry of Human Resources and Social Development. 2020b. *About Ministry* [English-language webpage]. https://hrsd.gov.sa/en/node/433 (Accessed 20 September 2020).

Ministry of Human Resources and Social Development. 2020c. *Overview* [LinkedIn profile page]. LinkedIn. https://www.linkedin.com/company/ministry-of-human-resources-and-social-development-ksa/about/ (Accessed 26 September 2020).

Mitnick, K.D. and Simon, W.L. 2001. *The art of deception: Controlling the human element of security*. Wiley. http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf (Accessed 30 October 2017).

Modic, D., Anderson, R. and Palomäki, J. 2018. We will make you like our research: The development of a susceptibility-to-persuasion scale. *PLoS ONE*, 13(3), e0194119. https://doi.org/10.1371/journal.pone.0194119

Montañez, R., Golob, E. and Xu, S. 2020. Human cognition through the lens of social engineering cyberattacks. *Frontiers in Psychology*, 11, 1755. https://doi.org/10.3389/fpsyg.2020.01755

Moody, G. D., Galletta, D.F. and Dunn, B.K. 2017. Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems*, 26(6), 564–584. https://doi.org/10.1057/s41303-017-0058-x

Mouton, F., Malan, M.M, Leenen, L. and Venter, H.S. 2014. Social Engineering Attack Framework. *Information Security for South Africa* [conference], Johannesburg, August 2014. pp 1–9. doi: 10.1109/ISSA.2014.6950510 (Accessed 7 November 2017).

Mueller, R. 2009. FBI Dir. Robert Mueller talks cybersecurity [video, duration: 1:28:00]. *CNET YouTube* channel. https://www.youtube.com/watch?v=M1PzM51JF5s&feature=emb_title (Accessed 22 December 2019).

Muncaster, P. 2017. Phishers spread malicious links via hacked LinkedIn accounts. *Infosecurity Magazine*, 15 September 2017. https://www.infosecurity-magazine.com/news/phishers-spread-hacked-linkedin/

Mundie, M. 2014. Unintentional insider threats: Social engineering [Technical note]. *CERT Insider Threat Center*, January 2014, p. 82. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=77455

Muniz, J. and Lakhani, A. 2013. *Web penetration testing with Kali Linux: A practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux* [e-book]. Packt Publishing. https://doc.lagout.org/security/Pen%20Testing/Web%20Penetration%20Testing%20with%20Kali%20Linux.pdf

Myers, M. and Avison, D. (eds.) 2002. *Qualitative research in information systems*. London: Sage. https://doi.org/10.4135/9781849209687

Nagy, J. and Pecho, P. 2009. Social networks security. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies* (pp. 321–325). IEEE. doi: 10.1109/securware.2009.56

National CyberSecurity Authority (NCA). 2020. About NCA. https://nca.gov.sa/en/pages/about.html (Accessed 3 August 2020).

National Information Center (NIC). 2020. Saudi Data & AI Authority. *Main Duties*. https://www.my.gov.sa/wps/portal/snp/pages/agencies/agencyDetails/

Neuman, W.L. 2014. *Social research methods: Qualitative and quantitative approac*hes (7th International edn). Harlow, UK: Pearson. http://letrunghieutvu.yolasite.com/resources/w-lawrence-neuman-social-research-methods_-qualitative-and-quantitative-approaches-pearson-education-limited-2013.pdf

Nguyen, Q.N. and Kim, D.J. 2017. Enforcing information security protection: Risk propensity and self-efficacy perspectives. *HICSS*. doi:10.24251/HICSS.2017.601

Norris, G., Brookes, A. and Dowell, D. 2019. The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, 34(3). doi: 10.1007/s11896-019-09334-5

Nuno, A. and St. John, F.A.V. 2015. How to ask sensitive questions in conservation: A review of specialized questioning techniques. *Biological Conservation*, 189, 5-15. DOI: 10.1016/j.biocon.2014.09.047

Orlikowski, W.J. and Baroudi, J.J. 1991. Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1-28. DOI: 10.1287/isre.2.1.1

Otuteye, E. and Siddiquee, M. 2015. Overcoming cognitive biases: A heuristic for making value investing decisions. *Journal of Behavioral Finance*, 16(2), 140–149. doi: 10.1080/15427560.2015.1034859

Oxford English Dictionary (OED). 2020a. *Definition of "susceptibility"* [online]. Oxford University Press. https://www.lexico.com/definition/susceptibility (Accessed 2 August 2020).

Oxford English Dictionary (OED). 2020b. *Definition of "cognition"* [online]. Oxford University Press. https://www.lexico.com/definition/cognition (Accessed 20 October 2020).

Oyibo, K, Orji, R. and Vassileva, J. 2017. Investigation of the influence of personality traits on Cialdini's persuasive strategies. In R. Orji, Reisinger, M., Busch, M., Dijkstra, A., Kaptein, M., and Mattheiss, E. (eds.) *Proceedings of the Personalization in Persuasive Technology Workshop, Persuasive Technology 2017*, Amsterdam, 4-6 April 2017. http://ceur-ws.org/Vol-1833/4_Oyibo.pdf

Pahnila, S., Siponen, M. and Mahmood, A. 2007. Employees' behavior towards IS security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences – 2007*, 156b.

Palmer, D. 2017. How these fake Facebook and LinkedIn profiles tricked people into friending state-backed hackers. *ZDNet*. https://www.zdnet.com/article/how-these-fake-facebook-and-linkedin-profiles-tricked-people-into-friending-state-backed-hackers/ (Accessed 16 September 2018).

Parkinson, J., David, P. and Rundle-Thiele, S. 2017. Self-efficacy or perceived behavioural control: Which influences consumers' physical activity and healthful eating behaviour maintenance? *Journal of Consumer Behaviour*, 16(5), 413– 423. https://doi.org/10.1002/cb.1641

Parrish, J.L., Bailey, J.L. and Courtney, J.F. 2009. A personality based model for determining susceptibility to phishing attacks. *Southwest Decision Sciences Institute (SWDSI) annual meeting*, pp. 285–296. http://swdsi.org/swdsi2009/Papers/9J05.pdf (Accessed 29 September 2018).

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. 2010. *Human factors and information security: Individual, culture and security environment* [report]. Command, Control, Communications and Intelligence Division. Defence Science and Technology Organisation (Australia). October 2010. https://apps.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C. 2013. Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In: *IFIP Advances in Information and Communication Technology* (Vol. 405, pp. 366–378). https://doi.org/10.1007/978-3-642-39218-4_27

Parsons, K., Butavicius, M., Pattinson, M., Calic, D., Mccormac, A. and Jerram, C. 2016. Do users focus on the correct cues to differentiate between phishing and genuine emails? *ArXiv* Preprint ArXiv:1605.04717, 1–10.

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(C), 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Patel, R.S. 2013. Kali Linux social engineering: effectively perform efficient and organized social engineering tests and penetration testing using Kali Linux. Packt Publishing. https://books.google.ie/books/about/Kali_Linux_Social_Engineering.html?id=w11uAgAAQBAJ&redir_esc=y (Accessed 1 December 2018).

Pattinson M., Butavicius M., Parsons K., McCormac A., Calic D. 2015a. Factors that influence information security behavior: An Australian web-based study (pp. 231-241). In: Tryfonas T., Askoxylakis I. (eds) *Human Aspects of Information Security, Privacy, and Trust. HAS 2015. Lecture Notes in Computer Science*, vol. 9190. Springer, Cham. https://doi.org/10.1007/978-3-319-20376-8_21

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. and Jerram, C. 2015b. Examining attitudes toward information security behaviour using mixed methods (pp. 57–70). In: *Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*. https://dblp.org/rec/conf/haisa/2015.html

Petersen, E. n.d. Self-efficacy theory in the workplace [online article]. *Chron*, undated. houstonchronicle.com. https://smallbusiness.chron.com/selfefficacy-theory-workplace-10330.html (Accessed 23 March 2021).

Petty, R.E. and Cacioppo, J.T. 1986. The elaboration likelihood model of persuasion. In L. Berkowitz (ed.), *Advances in experimental social psychology*. San Diego, CA: Academic Press, pp. 123-205.

Pinder, C.C. 2014. *Work motivation in organizational behavior* (2nd edn). New York: Psychology Press.

Pitesa, M. and Thau, S. 2013a. Compliant sinners, obstinate saints: How power and self-focus determine the effectiveness of social influences in ethical decision making. *Academy of Management Journal*, 56(3), 635–658. doi: 10.5465/amj.2011.0891

Pitesa, M. and Thau, S. 2013b. Masters of the universe: How power and accountability influence self-serving decisions under moral hazard. *Journal of Applied Psychology*, 98(3), 550–558. doi: 10.1037/a0031697

Ponemon Institute. 2012. *2012 Cost of cyber crime study: United States* [research report]. October 2012. https://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6 .pdf (Accessed: 3 December 2018).

Pratt, T.C., Holtfreter, K. and Reisig, M.D. 2010. Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47, 267–296. https://doi.org/10.1177/0022427810365903

Pratt, T.C. and Turanovic, J.J. 2016. Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, 11(3), 335-354. DOI: 10.1080/15564886.2015.1057351

Proofpoint. 2018. *2018 State of the phish report* [Industry report]. Proofpoint. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish (Accessed 18 August 2018).

Quiel, S. 2013. *Social engineering in the context of Cialdini's psychology of persuasion and personality traits*. Bachelor thesis, Hamburg University of Technology. https://www.sva.tuhh.de/ (Accessed 25 October 2018).

Qin, T. and Burgoon, J.K. 2007. An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *2007 IEEE Intelligence and Security Informatics*, pp. 152-159. doi: 10.1109/ISI.2007.379548

Rao, U.H. and Nayak, U. 2014. *The InfoSec handbook: An introduction to information security*. Apress Open. Edited by S.D. (Intel) Saswata Mishra (Apress), Steve Weiss (Apress). New York: Heinz Weinheimer. doi: 10.1007/978-1-4302-6383-8

Reed, M.B., Bruch, M.A. and Haase, R.F. 2004. Five-Factor Model of Personality and career exploration. *Journal of Career Assessment*, 12(3), 223–238. doi: 10.1177/1069072703261524

Rehman, U.U., Khan, W.A., Saqib, N.A. and Kaleem, M. 2013. On detection and prevention of clickjacking attack for OSNs. In *Proceedings of the 2013 11th International Conference on Frontiers of Information Technology* (FIT '13). IEEE Computer Society, USA, 160–165. doi: https://doi.org/10.1109/FIT.2013.37

Reidl, R., Hubert, M. and Kenning, P. 2010. Are there neural gender differences in online trust? An fMRI study on the perceived trustworthiness of eBay offers. *MIS Quarterly*, 34(2), 397-428. doi: 10.5555/2017458.2017469

Reyns, B.W. 2013. Online routine and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, 50, 216-238. https://doi.org/10.1177/0022427811425539

Reyns, B.W., Henson, B. and Fisher, B.S. 2011. Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Rhee, H., Ryu, Y.U. and Kim, C. 2012. Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221-232. doi:10.1016/j.cose.2011.12.001

Rhodes, R.E. and Courneya, K.S. 2004. Differentiating motivation and control in the Theory of Planned Behavior. *Psychology, Health & Medicine*, 9(2), 205-215. DOI: 10.1080/13548500410001670726

Robinson, S.L. and Bennett, R.J. 1995. A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal*, 38(2), 555–572. doi:10.5465/256693

Rolland, J.-P. 2002. The cross-cultural generalizability of the Five-Factor Model of Personality. In McCrae, R.R., and Allik, J. (eds) *The Five-Factor Model of Personality across cultures*. Boston, MA: Springer, pp. 7–28. doi: 10.1007/978-1-4615-0763-5_2

Rocha Flores, W. 2016. *Shaping information security behaviors related to social engineering attacks*. PhD Thesis. Royal Institute of Technology, Stockholm, Sweden. https://www.diva-portal.org/smash/get/diva2:925493/FULLTEXT02.pd

Rocha Flores, W., Holm, H., Nohlberg, M. and Ekstedt, M. 2015. Investigating personal determinants of phishing and the effect of national culture. *Information and Computer Security*, 23(2), 178-199. doi: 10.1108/ICS-05-2014-0029

Romm-Livermore, C. and Setzekorn, K. 2009. *Social networking communities and e-dating services: Concepts and implications*. Hershey, PA: Information Science Reference. https://www.igi-global.com/book/social-networking-communities-dating-services/917

Ropeik, D. 2002. Understanding factors of risk perception. *Nieman Reports* (Winter 2002). https://niemanreports.org/articles/understanding-factors-of-risk-perception/

Rotter, J.B. 1967. A new scale for the measurement of interpersonal trust. *Journal of Personality*, 35(4), 651–665. https://doi.org/10.1111/j.1467-6494.1967.tb01454.x

Rotter, J.B. 1980. Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35(1), 1–7. https://doi.org/10.1037/0003-066X.35.1.1

Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C. 1998. Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), 393–404. https://www.researchgate.net/publication/50313187_Not_So_Different_After_All_A_Cross-discipline_View_of_Trust

Rowe, B., Halpern, M., Lentz, T. and Wood, D. 2012. *Understanding cyber security risk preferences: A case study analysis inspired by public health research*. Institute for Homeland Security Solutions, 76. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.454.518&rep=rep1&type=pdf

Royal Society (Great Britain). 1992. *Risk: analysis, perception and management*. Royal Society. https://www.abebooks.co.uk/9780854034673/Risk-Analysis-Perception-Management-Report-0854034676/plp (Accessed 21 November 2018).

Rybnicek, R., Bergner, S. and Gutschelhofer, A. 2019. How individual needs influence motivation effects: a neuroscientific study on McClelland's need theory. *Review of Managerial Science*, 13, 443–482. https://doi.org/10.1007/s11846-017-0252-1

Saeed, F. Gazem, N., Mohammed, F. and Busalim, A. (eds.) 2019. *Recent trends in data science and soft computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology* (IRICT 2018). Cham: Springer. doi: 10.1007/978-3-319-99007-1

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Abdul Ghani, N. and Herawan, T. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Safianu, O., Twum, F. and Hayfron-Acquah, J.B. 2016. Information system security threats and vulnerabilities: Evaluating the human factor in data protection. *International Journal of Computer Applications*, 143(5), 8–14. doi: 10.5120/ijca2016910160

Salgado, J.F. 2002. The Big Five personality dimensions and counterproductive behaviors. *International Journal of Selection and Assessment*, 10(1-2), 117-125. https://doi.org/10.1111/1468-2389.00198

Salgado, J.F., Moscoso, S. and Anderson, N. 2013. Personality and counterproductive work behavior (pp. 606-632). In N. Christiansen and R. Tett, eds. *Handbook of Personality at Work*. New York: Routledge. https://doi.org/10.4324/9780203526910

Saß, H. 2001. Personality disorders. *International encyclopedia of the social & behavioral sciences*. Pergamon, pp. 11301–11308. doi: 10.1016/B0-08-043076-7/03763-3

Sam, H.K., Othman, A. and Nordin, Z.S. 2005. Computer self-efficacy, computer anxiety, and attitudes toward the Internet: A study among undergraduates in Unimas. *Educational Technology and Society*, 8(4), 205-219. https://www.researchgate.net/publication/220374593_Computer_Self-Efficacy_Computer_Anxiety_and_Attitudes_toward_the_Internet_A_Study_among_Undergraduates_in_Unimas

Samani, R. 2010. Re-defining the human factor. *Infosecurity*, 7(2), 30–33. doi: 10.1016/S1754-4548(10)70039-5

Samani, R. and McFarland, C. 2015. Hacking the human operating system. The role of social engineering within cybersecurity [online industry report]. Intel Security/McAfee. https://icscsi.org/library/Documents/Threat_Intelligence/McAfee%20-%20Hacking%20the%20Human%20OS.pdf

Sampson, R. and J. Wooldredge. 1987. Linking the micro- and macro-level dimensions of lifestyle-routine activity and opportunity models of predatory victimization. *Journal of Quantitative Criminology*, 3, 371-393. https://doi.org/10.1007/BF01066837

Sanders, G.B. 2016. *Opportunities and risks in online gaming environments*. PhD thesis. Faculty of Science and Engineering, University of Plymouth, UK. http://hdl.handle.net/10026.1/8083 (Accessed 1 December 2018).

Sandy, C., Rusconi, P. and Li, S. 2017. Can humans detect the authenticity of social media accounts? On the impact of verbal and non-verbal cues on credibility judgements of twitter profiles. In: *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*. Exeter, 2017, pp. 1-8. https://doi.org/10.1109/CYBConf.2017.7985764

Saridakis, G. Benson, V., Ezingeard, J.-N. and Tennakoon, H. 2016. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting & Social Change*, 102, 320–330. doi: 10.1016/j.techfore.2015.08.012

Saucier, G. and Goldberg, L.R. 2002. Assessing the Big Five: Applications of 10 psychometric criteria to the development of marker scales. In: B. De Raad & M. Perugini (Eds.), *Big Five assessment* (pp. 29–58). Seattle, WA: Hogrefe and Huber Publishers.

Saunders, M., Lewis, P. and Thornhill, A. 2015. *Research methods for business students* (7th edn). Harlow: Pearson Education Limited.

Saunders, M.N.K. and Townsend, K. 2016. Reporting and justifying the number of interview participants in organization and workplace research. *British Journal of Management*, 27(4), 836-852. https://doi.org/10.1111/1467-8551.12182

Sawaya, Y. Sharif, M., Christin, N., Kubota, A., Nakarai, A. and Yamada, A. 2017. Self-confidence trumps knowledge. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. New York: ACM Press, pp. 2202–2214. doi: 10.1145/3025453.3025926

Sawahel, W. 2015. Arab universities are vulnerable to cyberattacks, experts say. *Al-Fanar Media*. https://www.al-fanarmedia.org/2015/12/arab-universities-are-vulnerable-to-cyber-attacks-experts-say/ (Accessed 1 December 2018).

Sawyer, B.D. and Hancock, P.A. 2018. Hacking the human: The prevalence paradox in cybersecurity. *Human Factors*, 60(5), 597–609. https://doi.org/10.1177/0018720818780472

Scannell, K. 2016. Cyber crime: How companies are hit by email scams. *Financial Times*, 24 February 2016. https://www.ft.com/content/19ade924-d0a5-11e5-831d-09f7778e7377 (Accessed: 27 November 2017).

Schaeken, M. 2018. *Information security awareness measuring & social engineering 2.0*. Assessment of information security awareness (ISA) in the Belgian healthcare sector using an enhanced HAIS-Q. Master's thesis. Open Universiteit Nederland. http://dspace.ou.nl/bitstream/1820/9761/1/Schaeken M IM9806 AF scriptie.pdf

Schomer, A. 2019. Digital trust report 2019: Popular social media platforms ranked by consumer trust metrics. *Business Insider*, 16 October 2019. https://www.businessinsider.com/the-digital-trust-report-2019-enterprise-edge?r=US&IR=T

Schein, E.H. 1984. Coming to a new awareness of organizational culture. *MIT Sloan Management Review*, Winter 1984 (15 January 1984). https://sloanreview.mit.edu/article/coming-to-a-new-awareness-of-organizational-culture/

Seethaler, R. and Rose, G. 2003. Application of psychological principles to promote travel behaviour change. *26th Australasian Transport Research Forum* (ATRF

’03), Wellington, New Zealand, 1-3 October 2003. https://trid.trb.org/view/704005

Seidenberger, S. 2016. A new role for human resource managers: Social engineering defense. *Cornell HR Review*, 20 September 2016. https://hdl.handle.net/1813/73018 (Accessed: 31 October 2017).

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems* (CHI ’10). doi: 10.1145/1753326.1753383

Sherman, D.K. and Cohen, G.L. 2010. Self-affirmation theory. In *Encyclopedia of Identity*. Sage Reference. doi: 10.4135/9781412979306

Sherry, S.B., Hewitt, P.L., Flett, G.L. Lee-Baggley, D.L. and Hall, P.A. 2007. Trait perfectionism and perfectionistic self-presentation in personality pathology. *Personality and Individual Differences*, 42(3), 477–490. doi: 10.1016/j.paid.2006.07.026

Shin, D.H. 2010. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, 22(5), 428–438. doi: 10.1016/j.intcom.2010.05.001

Shrum, L.J., Liu, M., Nespoli, M. and Lowrey, T.M. 2013. Persuasion in the marketplace: How theories of persuasion apply to marketing and advertising. In J.P. Dillard and L. Shen (eds.), *The SAGE handbook of persuasion: Developments in theory and practice* (pp. 314–330). Sage. http://dx.doi.org/10.4135/9781452218410.n19

Siegrist, M. 2021/2019. Trust and risk perception: A critical review of the literature. *Risk Analysis*, 41(3), 480-490. Special Issue: 40 Years of Social Sciences in Risk Research Reconsidered, March 2021. First published 02 May 2019. https://doi.org/10.1111/risa.13325

Siegrist, M., Cvetkovich, G. and Roth, C. 2000. Salient value similarity, social trust, and risk/benefit perception. *Risk Analysis*, 20(3), 353–362.

Silic, M. and Back, A. 2016. The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior*, 60, 35–43. doi: 10.1016/j.chb.2016.02.050

Sillence, E. Briggs, P., Harris, P. and Fishwick, L. 2006. A framework for understanding trust factors in web-based health advice. *International Journal of Human-Computer Studies*, 64(8), 697–713. doi: 10.1016/j.ijhcs.2006.02.007

Sitkin, S.B. and Pablo, A.L. 1992. Reconceptualizing the determinants of risk behavior. *Academy of Management Review*, 17(1), 9–38. doi: 10.5465/AMR.1992.4279564

Skeels, M.M. and Grudin, J. 2009. When social networks cross boundaries. In *Proceedings of the ACM 2009 International Conference on Supporting Group Work* (GROUP '09), May 2009. New York: ACM Press, pp. 95-104. doi: 10.1145/1531674.1531689

Snyder, J., Carpenter, D. and Slauson, G.J. 2007. MySpace.com – A social networking site and social contract theory. Information Systems Education Journal, 5(2), 1-11. http://proc.edsig.org/2006/3333/ISECON.2006.Snyder.pdf (Accessed: 2 December 2018).

Solano, J. 2015. Dangerous scams now on LinkedIn. Maalbeek Valley (blog). https://josepsolano.wordpress.com/2015/03/18/dangerous-scams-now-on-linkedin/ (Accessed: 17 August 2018).

Srivastava, S., John, O.P., Gosling, S.D. and Potter, J. 2003. Development of personality in early and middle adulthood: Set like plaster or persistent change? *Journal of Personality and Social Psychology*, 84(5), 1041–1053. https://doi.org/10.1037/0022-3514.84.5.1041

Stoeber, J., Otto, K. and Dalbert, C. 2009. Perfectionism and the Big Five: Conscientiousness predicts longitudinal increases in self-oriented perfectionism. *Personality and Individual Differences*, 47(4), 363–368. doi: 10.1016/j.paid.2009.04.004

Symantec. 2013. Security 1:1, Part 3: Various types of network attacks. *Symantec Connect Community*, 27 December 2013. https://www.symantec.com/connect/articles/security-11-part-3-various-types-network-attacks (Accessed: 8 November 2018).

Symantec 2015. Cybercriminals are leveraging social networks and apps to do their dirty work. *Internet Security Threat Report 2015*. https://www.itu.int/en/ITU-

D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf (Accessed: 2 February 2019).

Schwämmlein and Wodzicki, 2012. What to tell about me? Self-presentation in online communities. *Journal of Computer-Mediated Communication*, 17(4), 387-407. https://doi.org/10.1111/j.1083-6101.2012.01582.x

Sears, D.O. 1986. College sophomores in the laboratory: Influences of a narrow data base on social psychology's view of human nature. *Journal of Personality and Social Psychology*, 51,515-530. https://doi.org/10.1037/0022-3514.51.3.515

Sebescen, N. and Vitak, J. 2017. Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the Association for Information Science and Technology*, 68(9), 2237–2247. doi:10.1002/asi.23851

Scotland, J. 2012. Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English Language Teaching*, 5(9), 9–16. https://doi.org/10.5539/elt.v5n9p9

Shappie, A.T., Dawson, C.A. and Debb, S.M. 2020. Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, 9(4), 475–480. https://doi.org/10.1037/ppm0000247

Sheng, S. Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. 2010. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. New York: Association for Computing Machinery, pp. 373–382. doi: 10.1145/1753326.1753383

Simons, H.W. 1976. *Persuasion*. Addison-Wesley.

Siponen, M., Mahmood, M.A. and Pahnila, S. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–24. doi: 10.1016/j.im.2013.08.006

Slovic, P., Peters, E., Finucane, M. and MacGregor, D.G. 2005. Affect, risk, and decision making. *Health Psychology*, 24(4 Suppl), S35-S40. DOI: 10.1037/0278-6133.24.4.S35

Solon, O. and Farivar, C. 2019. Millions of people uploaded photos to the Ever app. Then the company used them to develop facial recognition tools. *NBC News*, 9 May 2019. https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371

Spector, P.E., Fox, S., Penney, L.M., Bruursema, K., Goh, A. and Kessler, S. 2006. The dimensionality of counterproductivity: Are all counterproductive behaviors created equal? *Journal of Vocational Behavior*, 68, 446-460. https://doi.org/10.1016/j.jvb.2005.10.005

Stanton, M. 2010. The systemic epistemology of the specialty of family psychology. In: *The Wiley-Blackwell Handbook of Family Psychology* (pp. 5–20). London: Blackwell. https://doi.org/10.1002/9781444310238.ch1

Steinmetz-Wood, M., Pluye, P. and Ross, N.A. 2019. The planning and reporting of mixed methods studies on the built environment and health. *Preventive Medicine*, 126, 105752. https://doi.org/10.1016/j.ypmed.2019.105752

Stevens, C. and Ash, R. 2001. Selecting employees for fit: Personality and preferred managerial style. *Journal of Managerial Issues*, 13(4), 500-517. http://www.jstor.org/stable/40604367

Stoltenberg, C.D. and McNeill, B.W. 1984. *Source, message, and recipient factors in counseling and psychotherapy*. Paper presented at the APA Convention, Toronto, Canada, August 1984. https://files.eric.ed.gov/fulltext/ED251783.pdf

Straub, D.W. 1990. Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276. doi: 10.1287/isre.1.3.255 https://www.researchgate.net/publication/220079472_Effective_IS_Security_An_Empirical_Study

Stroll, A. and Martinich, A.P. 2020. Epistemology. *Encyclopædia Britannica*. 23 April 2020. https://www.britannica.com/topic/epistemology

Taher, A. 2019. Saudi Arabia's efforts to ensure cyber security: A pillar of Vision 2030. *Majalla*, 25 January 2019. https://eng.majalla.com/node/65466/saudi-arabia%E2%80%99s-efforts-to-ensure-cyber-security%C2%A0

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(3), 28-36. hal-02546799

Talent. 2016. Cyber security – how LinkedIn profiles are a goldmine for hackers [blog post]. *Talent*, December 2016. https://www.talentinternational.com.au/blog/2016/12/cyber-security-how-linkedin-profiles-are-a-goldmine-for-hackers

Tasselli, S., Kilduff, M. and Landis, B. 2018a. Becoming more conscientious [online article]. *Harvard Business Review*. 30 March 2018. https://hbr.org/2018/03/becoming-more-conscientious

Tasselli, S., Kilduff, M. and Landis, B. 2018b. Personality change: Implications for organizational behavior. *Academy of Management Annals*, 12(2). [published online] https://doi.org/10.5465/annals.2016.0008

TechCentral.ie. 2017. Germany unmasks fake Chinese LinkedIn profiles [online article]. *TechCentral.ie*. https://www.techcentral.ie/germany-unmasks-fake-chinese-linkedin-profiles/ [Accessed August 20, 2018].

Terrill, C. 2017. What you need to know now about cybersecurity and social media. *Forbes*. https://www.forbes.com/sites/christieterrill/2017/04/28/what-you-need-to-know-now-about-cybersecurity-and-social-media/ (Accessed: 2 February 2019).

Tessian. 2020. Securing the future of hybrid working [report]. Tessian. September 2020. https://www.tessian.com/research/the-future-of-hybrid-working/

Thomas, J.E. 2018. Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business and Management*, 13(6), 1-24. https://doi.org/10.5539/ijbm.v13n6p1

Thompson, C.G., Kim, R.S., Aloe, A.M., & Becker, B.J. 2017. Extracting the variance inflation factor and other multicollinearity diagnostics from typical regression results. *Basic and Applied Social Psychology*, 39(2), 81-90. https://doi.org/10.1080/01973533.2016.1277529

Trend Micro. 2020. What is social media phishing? Trend Micro. https://www.trendmicro.com/en_vn/what-is/phishing/social-media-phishing.html

Trimpop, R.M. 1994. *The psychology of risk taking behaviour*. Amsterdam: Elsevier Science.

Trumbo, C.W. 1999/2006. Heuristic-systematic information processing and risk judgment. *Risk Analysis*, 19(3), 391-400. https://doi.org/10.1111/j.1539-6924.1999.tb00415.x

Trumbo, C.W. 2002. Information processing and risk perception: An adaptation of the heuristic-systematic model. *Journal of Communication*, 52(2), 367–382. doi: 10.1111/j.1460-2466.2002.tb02550.x

Tversky, A. and Kahneman, D. 1974. Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124–1131. doi: 10.1126/science.185.4157.1124

Uebelacker, S. and Quiel, S. 2014. The social engineering personality framework. In Proceedings – *4th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2014*. Co-located with 27th IEEE Computer Security Foundations Symposium, CSF 2014 in the Vienna Summer of Logic 2014, pp. 24–30. doi: 10.1109/STAST.2014.12

United States Code. 2014. Information security. Definitions. 44 US Code 3552(b)(3). https://www.law.cornell.edu/uscode/text/44/3552#b_3

U.S.-Saudi Business Council. 2020. *Saudi Arabia's emergence in cyber technology*. U.S.-Saudi Business Council, Featured Articles, [online article] 29 January 2020. http://ussaudi.org/saudi-arabias-emergence-in-cyber-technology/

Vakhitova, Z.I., Reynald, D.M. and Townsley, M. 2016. Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, 32(2), 169–188. https://doi.org/10.1177/1043986215621379

van de Weijer, S.G.A. and Leukfeldt, E.R. 2017. Big Five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, 20(7), 407–412. doi: 10.1089/cyber.2017.0028

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. and Kusev, P. 2017. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75, pp. 547-559. http://dx.doi.org/10.1016/j.chb.2017.05.038

van Schaik, P., Jansen, J., Onibokun, J., Camp, J. and Kusev, P. 2018. Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, 78, 283–297. https://doi.org/10.1016/j.chb.2017.10.007

Varadwaj, K. and Rath, S. 2018. Cultural consequences of Big Five traits: Comparing urban, rural and tribal students. *IOSR Journal of Humanities and Social Science*, 23(5), 11–16. doi: 10.9790/0837-2305091116

Vennekens, J. 2015. The influence of tribalism in the Middle East. *International Perspective*. http://www.internationalperspective.be/insight/2015/09/the-influence-of-tribalism/ (Accessed: 4 December 2018).

Venkatesh, V., Brown, S.A. and Bala, H. 2013. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 37(1), 21–54. https://doi.org/10.25300/MISQ/2013/37.1.02

Venkatesh, V., Brown, S.A. and Sullivan, Y.W. 2016. Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems*, 17(7), 435–494. https://pdfs.semanticscholar.org/9848/5554a32a8ae3249fc6ed10a15ff20444e1f6.pdf

Verizon. 2018. *Data Breach Investigations Report, 11th edition*. http://bfy.tw/HJvH (Accessed: 28 February 2019).

Vishwanath, A. 2014. Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, 20(1), 83– 98. https://doi.org/10.1111/jcc4.12100

Vishwanath, A. 2015a. Diffusion of deception in social media: Social contagion effects and its antecedents. *Information Systems Frontiers*, 17(6), 1353–1367. doi: 10.1007/s10796-014-9509-2

Vishwanath, A. 2015b. Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication*, 20. doi: 10.1111/jcc4.12126

Vishwanath, A. 2017. Getting phished on social media. *Decision Support Systems*, 103, pp. 70–81. doi: 10.1016/j.dss.2017.09.004

Vishwanath, A., Harrison, B. and Ng, Y.J. 2016. Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146–1166. doi: 10.1177/0093650215627483

Vishwanath, A. Herath, T., Chen, R., Wang, J. and Rao, H.R. 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), 576–586. doi: 10.1016/j.dss.2011.03.002

Wallston, K. 2001. Control beliefs: Health perspectives (pp. 2724-2726). In N.J. Smelser, Paul B. Baltes, eds. *International Encyclopedia of the Social & Behavioral Sciences*. Pergamon. https://doi.org/10.1016/B0-08-043076-7/03799-2

Walsham, G. 1993. *Interpreting information systems in organizations*. Chichester, UK: Wiley.

Waldman, A.E. 2016. Privacy, sharing, and trust: The Facebook study. *Case Western Law Review*, 67(1), 193. http://scholarlycommons.law.case.edu/caselrev/vol67/iss1/10 (Accessed 17 November 2018).

Wang, Y.D. and Emurian, H.H. 2005. An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, 21(1), 105–125. doi: 10.1016/j.chb.2003.11.008

Wani, M.A. and Jabin, S. 2018. A sneak into the Devil's Colony – Fake profiles in online social networks. *arXiv*, 30 May 2017. https://arxiv.org/abs/1705.09929v2 (Accessed: 30 January 2019).

Warner-Søderholm, G. Bertsch, A., Sawe, E., Lee D., Wolfe, T. Meyer, J. Engel, J. Fatilua, U.N. 2018. Who trusts social media? *Computers in Human Behavior*, 81, 303–315. doi: 10.1016/j.chb.2017.12.026

Warren, M., Leitch, S. and Rosewall, I. 2011. *Attack vectors against social networking systems: The Facebook example* [conference paper]. 9th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5 -7 December 2011. doi: 10.4225/75/57b54ba6cd8cc

Wasson-Blader, K. 2009. Have you established your professional network yet? *American Medical Writers Association Journal*, 24(1), 26–27. https://cdn.ymaws.com/www.amwa.org/resource/resmgr/journal/Issues/2009/2009v24n1.pdf

Weber, E.U., Blais, A.-R. and Betz, N.E. 2002. A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making*, 15(4), 263–290. https://doi.org/10.1002/bdm.414

Weber, R. 2004. Editor's comments: The rhetoric of positivism versus interpretivism: A personal view. *MIS Quarterly*, 28(1), iii-xii. https://doi.org/10.2307/25148621

Wei, Z., Zhao, Z. and Zheng, Y. 2019. Following the majority: Social influence in trusting behavior. Frontiers in Neuroscience, 13(February), 89. doi: 10.3389/fnins.2019.00089

Weirich, D. and Sasse, M.A. 2001. Pretty good persuasion: A first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on new security paradigms* (NSPW '01), pp. 137-143. doi: 10.1145/508171.508195

Weisberg, Y.J., DeYoung, C.G. and Hirsh, J.B. 2011. Gender differences in personality across the ten aspects of the Big Five. *Frontiers in Psychology*, 2, 1 August 2011, 178. https://doi.org/10.3389/fpsyg.2011.00178

Whitty, M., Doodson, J., Creese, S. and Hodges, D. 2015. Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1), 1-5. doi: 10.1089/cyber.2014.0179

Wicks, A.C. and Freeman, R.E. 1998. Organization studies and the new pragmatism: Positivism, anti-positivism, and the search for ethics. *Organization Science*, 9(2), 123–140. https://doi.org/10.1287/orsc.9.2.123

Wilcox, H., Bhattacharya, M. and Islam, R. 2014. Social engineering through social media: An investigation on enterprise security. *Communications in Computer and Information Science*, 490, 243–255. doi: 10.1007/978-3-662-45670-5

Williams, E.J., Beardmore, A. and Joinson, A.N. 2017a. Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412–421. doi: 10.1016/j.chb.2017.03.002

Williams, E., Morgan, P. and Joinson, A.N. 2017b. Press accept to update now: Individual differences in susceptibility to malevolent interruptions. *Decision Support Systems*, 96, 119-129. DOI: 10.1016/j.dss.2017.02.014

Williams, E., Hinds, J. and Joinson, A.N. 2018. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1-13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Williams, S. 2020a. IT leaders fear increase risk of cyber attacks while working from home. *SecurityBrief*, [online news report] 29 September 2020. https://securitybrief.eu/story/it-leaders-fear-increase-risk-of-cyber-attacks-while-working-from-home

Williams, S. 2020b. Cyberattacks up 400% compared to pre-COVID-19 levels. *SecurityBrief*, [online news report] 2 October 2020. https://securitybrief.eu/story/cyberattacks-up-400-compared-to-pre-covid-19-levels

Williams, S. 2020c. Secureworks: Remote working exposes new security vulnerabilities. *SecurityBrief*, [online news report] 19 October 2020. https://securitybrief.eu/story/secureworks-remote-working-exposes-new-security-vulnerabilities

Willis, J., Jost, M. and Nilakanta, R. 2007. *Foundations of qualitative research: Interpretive and critical approaches* [electronic resource]. Thousand Oaks, CA: Sage.

Wolff, K., Larsen, S. and Øgaard, T. 2019. How to define and measure risk perceptions, *Annals of Tourism Research*, 79, 102759. https://doi.org/10.1016/j.annals.2019.102759

Workman, M. 2008. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662–674. doi: 10.1002/asi.20779

World Bank. 2018. *Country profile: Saudi Arabia*. https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=C

ountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=SAU [Accessed 2 August 2020].

World Health Organisation (WHO). 2020a. Gender. *Gender, equity and human rights: Glossary of terms and tools*. https://www.who.int/gender-equity-rights/knowledge/glossary/en/

Wright, R.T. and Marett, K. 2010. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, 27(1), 273–303. doi: 10.2753/MIS0742-1222270111

Xu, H., Dinev, T., Smith, H.J. and Hart, P. 2008. Examining the formation of individual's privacy concerns: toward an integrative view. In: *Proceedings of the 29th International Conference on Information Systems* (ICIS), Paper 6. http://aisel.aisnet.org/icis2008/6

Yin, R.K. 2009. *Case study research: Design and methods*, 4th edn. Thousand Oaks, CA: Sage.

Yokoyama, M.H. 2016. How social network sites (SNS) have changed the employer–employee relationship and what are the next challenges for human resource (HR)? *REGE – Revista de Gestão*, 23(1), 2–9. doi: 10.1016/j.rege.2015.11.001

Young, H., van Vliet, T., van de Ven, J., Jol, S. and Broekman, C. 2018. Understanding human factors in cyber security as a dynamic system. In Nicholson D. (eds) *Advances in Human Factors in Cybersecurity*. AHFE 2017. *Advances in Intelligent Systems and Computing*, vol. 593, pp. 244-254. Springer, Cham. https://doi.org/10.1007/978-3-319-60585-2_23

Zhu, Y., Wang, X., Zhong, E., Liu, N., Li, H. and Yang, Q. 2012. Discovering spammers in social networks. *Proceedings of the National Conference on Artificial Intelligence*, 26(1). https://ojs.aaai.org/index.php/AAAI/article/view/8116

Zainal, Z. 2007. Case study as a research method. *Jurnal Kemanusiaan*, 9(June), 1-6. https://jurnalkemanusiaan.utm.my/index.php/kemanusiaan/article/view/165

Zhitomirsky-Geffet, M. and Bratspiess, Y. 2015. Perceived effectiveness of social networks for job search, *Libri*, 65(2), 105-118. doi: https://doi.org/10.1515/libri-2014-0115

Zhao, C., Street, D.L. and Hinds, P. 2012. How and to whom people share: The role of culture in self-disclosure in online communities. *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, pp. 67–76. doi: 10.1145/2145204.2145219

Zimet, G.D., Powell, S.S., Farley, G.K., Werkman, S. and Berkoff, K.A. 1990. Psychometric characteristics of the multidimensional scale of perceived social support. *Journal of Personality Assessment*, 55(3-4), 610-617. doi: 10.1080/00223891.1990.9674095

Zubiaga, A. and Ji, H. 2014. Tweet, but verify: Epistemic study of information verification on twitter. *Social Network Analysis and Mining*, 4(163). https://doi.org/10.1007/s13278-014-0163-y

APPENDICES

APPENDIX A

	Extraversion	Conscientiousness	Neuroticism	Openness to Experience	Agreeableness	Environment/ CSE Trajectory	Sample Size / Type of Study	Demographic Characteristics	Setting	Personality Traits Measurement
	Findings of Personality Traits and Their link to Susceptibility to Cyber-Attacks (e.g., CSE)									
Frauenstein and Flowerday (2020)	High score→heuristic/systematic→ no effect on susceptibility	High score→less heuristic → (ds)	High score→high systematic→ (ds)	High score→high heuristic/systematic→ (ds)	High score→high heuristic→ (is)	Facebook Phishing E-mail	215 students (online survey)	(114 male, 101 female) of final year students	3 different sites of South African university	44-Item Big-Five Inventory (BFI)
Cusack and Adedokun (2018)	High score→ (is)	n/a	n/a	n/a	High score → (is)	None (qualitative approach choosing five participants had experienced SE attacks)	5	none	none	unknown
Weijer and Leukfeldt (2017)	n/a	High score → (ds)*	High score → (ds)	n/a	n/a	Phishing E-mail, SMS,	3,648 respondents, 550 cybercrime victims, 2,585 nonvictims (Primarily survey study)	age average 51.29, 46.9% =men, 89.9 of Dutch origin,	Households (public) in The Netherlands	50-item International Personality Item Pool (IPIP)
Albladi and George (2017)	Strongest significant effect	Strong significant effect, high score →(ds)	High score→(ds)	No effect	Significant negative effect, high score →(ds)	CSE in Facebook (SNS)	316 (scenario-based) (survey study)	Ages 18-55, mix genders unknown percentage, no findings on demographic	Saudi students/ 2 universities, Saudi Arabia	10-Item Personality short version of Big-Five
Pattinson *et al.* (2012)	High score → (ds)	No significant impact	No significant impact	High score → (ds)	Negative effect to - informed of- genuine emails	E-mail emulation (images of phishing and genuine emails)	117 N=59 unaware, N=58 aware of phishing, genuine email (survey study)	64 business students, 53 psychology students	University, Australia	44-Item Big-Five Inventory (BFI)

Halevi, *et al.* (2013)	**n/a**	**n/a**	**High score → (is)****	**n/a**	**n/a**	**Prize phishing E-mail experiment, Facebook privacy setting behaviour used to assess information disclosure only**	**100 students from science & engineering disciplines (survey study)**	**(83 male, 17 female)**	**Community College, USA**	**NEO-PI FFM 60-Item**
Goel *et al.* (2017)	**n/a**	**High score → High suspicions →(ds)**	**n/a**	**n/a**	**n/a**	**phishing E-mail experiment**	**7225 responds to experimental phishing emails,1975 opened email, 974 clicked on the embedded link, and only 206 completed survey**	**female (n=1,5051) more responsive to emails out of males (n=924),(female =495) clicked on link vs. males (469), business and social science background more likely to open email than humanities majors,**	**University, USA**	**Self-report commercial personality inventory**
Halevi *et al.* (2015)	**n/a**	**High score → (is) (with low-risk perception)**	**n/a**	**n/a**	**n/a**	**Official company E-mail experiment**	**N=40 Stage1: survey link stage2: experimental (spear-phishing emails aiming to people of consciousness trait,**	**(30 men, 10 women) women are more susceptible to phishing, n=5 (18-24), n=22 (25-29), n=8 Ages (30-34), n=5 Ages (35-39)**	**Employees of a large company, India**	**20-items/Mini-IPIP scale** (Donnellan et al. 2006)
Alseadoon *et al.* (2012)	**High score → (is)**	**n/a**	**n/a**	**High score → (is)**	**n/a**	**University phishing E-mail**	**N = 200 undergraduate student phase, Survey study: part 1: questionna**	**Ages 18-25 (males) computer science discipline**	**University, Saudi Arabia**	**10-Item Personality short version (TIPI)**

Appendix A: to Attacks in SNS Through the Traits of users Susceptibility email and on environments Personality (FFM).

increased
decreased
n/a indicates the trait in their findings.

FFM Appendix: Findings in CSE Victimisation

susceptibility →(is)**
susceptibility →* (ds)
was not highlighted

Personality Traits Susceptibility to Studies

							ire on personality traits, part 2: phishing email experiment launched then part 2: survey on experience.			(Gosling et al. 2003)
Alseadon *et al. (2015)*	**High score → (is) with significant relationship**	**high score → (is) with significant relationship**	**High score → (ds) with significant relationship**	**High score → (is) with significant relationship**	**High score → (is) with significant relationship**	**College Phishing E-mail experiment**	**N= 383, survey of personality trait only on Australian students' sample, study not cross cultural to personality factor per se.**	**N =196 (Saudi Arabian), N =187 (Australian, 69.5% men 18-25, 30.5% women 26-35), all undergraduate students**	**Saudi Arabian college, Australian college**	**10-Item Personality Inventory (TIPI)** (Gosling et al. 2003)
Parrish Jr. et al. (2009)	**High score → (is)**	**High score → (ds)**	**High score → (ds)**	**High score → (ds)**	**High score → (is)**	**Theoretical/Review Paper**				**n/a**
Uebelacker and Quiel (2014)	**High score → (is)**	**High score → (ds)**	**High score → (is)**	**High score → (is)**	**High score → (is)**	**Theoretical /Review paper**				**n/a**

APPENDIX B

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

وزارة العمل
والتنمية الاجتماعية
المملكة العربية السعودية

السلام عليكم ورحمة الله وبركاته

تفيد وزارة العمل والتنمية الاجتماعية أنه لا مانع من قيام الطالب / محمد خالد العتيبي هوية رقم ([redacted]) والمبتعث للدكتوراه من قبل وزارة التعليم اعتباراً من تاريخ 7 أكتوبر 2019 حتى 7 يناير 2020 بالقيام بجمع البيانات اللازمة من الموظفين بالقطاعات التابعة للوزارة في المملكة العربية السعودية لمدة 3 أشهر تخص دراسته في الهندسة الاجتماعية على شبكات التواصل الاجتماعي "

هذا وقد تم اصدار هذا الخطاب بناء على طلب منه، وذلك لتقديمة للملحقية الثقافية بإيرلندا دون أدنى مسؤلية على الوزارة.

الختم

مدير عام الإدارة العامة لتقنية المعلومات

مساعد عبد الله العتيبي

APPENDIX C (8 Pages)

Responses to Required Amendments

1. Semi-structured interview process has been changed to be conducted from online (see highlights) as per The Corona Guidelines 2020 (Research during pandemics, conflict and natural disasters) dated 17 March 2020 by Andrea J. Nightingale **(updated 20/7/2020)**

2. Please remove reference to video recordings in the interview consent form if they are not being used. All references to video have been removed.

3. Please proofread the Survey Information Sheet and correct for typos.

   Typos corrected. Also, punctuation corrected, and some rephrasing done to improve clarity and grammatical accuracy.

4. The Information Sheets should indicate the length of time required, a statement on de-briefing, the adherence to relevant legislation, e.g. GDPR, illicit activities, provision for verification of direct quotations, etc. where relevant – not all are relevant to both Information Sheets.

Length of time: Previously included in information sheet for interviews, now added to information sheet for survey. See attached document for survey and for interviews.

Debriefing: There is a statement on debriefing in the information sheet for the interviews. It is not anticipated to be needed for the survey, which is intended to be self-contained.

Update (20 June): The last part of the 'debriefing' section has been rewritten and the following sentence has been added to this section and to the 'Privacy' section of the information sheets for the Survey and the Interview:

Although the data will be collected in Saudi Arabia (KSA), the analysis may be undertaken within the EU, so the data collected has to comply with the GDPR.

Although the data will be collected in Saudi Arabia (KSA), the analysis may be undertaken within the EU, so the data collected has to comply with the GDPR. Data will be encrypted and stored in a secure password- protected cloud device which will remain offline at all times until names and organizations are replaced with distinctive code to insure anonymity.

Legislation: As the study will be conducted in Saudi Arabia and the participants are not EU citizens, GDPR does not apply. Notes on reporting of illicit activities are included: -

Informed consent form for survey:

page 5. Informed consent form for interview: Update (20 June 2019): The following sentence has been added to 'Debriefing' and to the information sheets for the Survey and the Interview:

page 6. Information sheet

Although the data will be collected in Saudi Arabia (KSA), the analysis may be undertaken within the EU, so the data collected has to comply with the GDPR

Verification of direct quotations:

Participants will receive a copy of interview transcript and will be invited to request changes or deletion of any parts which they feel are inaccurate. (See page 8 of the attached document)

5. The estimated time for completion of the survey at 10 minutes is unrealistic for a 13-page survey, this should be amended.

   Suggested time has been changed to 30 minutes. See pages 6 and 10 of the attached documents.

School of Computer Science and Statistics
Research Ethics Application

Part A

Project Title: The Influence of Personal Characteristics and Other Factors on The Susceptibility of Public Sector Employees to Cyber-Social Engineering Through LinkedIn; A Mixed-Methods Sequential Explanatory Study

Name of Lead Researcher (student in case of project work): .....Mohammed Khaled N. Alotaibi. .....

Name of Supervisor: .....Dr. Aideen M. Keaney.....

TCD E-mail: malotaib@tcd.ie Contact Tel No.: +353874037027

Course Name and Code (if applicable) ..... Doctor in Philosophy, Computer Science/ Information Systems Track

Estimated start date of survey/research: 01/05/2019..... .....……

I confirm that I will (where relevant):

- Familiarize myself with the Data Protection Act and the College Good Research Practice guidelines http://www.tcd.ie/info_compliance/dp/legislation.php;
- Tell participants that any recordings, e.g. audio/video/photographs, will not be identifiable unless prior written permission has been given. I will obtain permission for specific reuse (in papers, talks, etc.)
- Provide participants with an information sheet (or web-page for web-based experiments) that describes the main procedures (a copy of the information sheet must be included with this application)
- Obtain informed consent for participation (a copy of the informed consent form must be included with this application)
- Should the research be observational, ask participants for their consent to be observed
- Tell participants that their participation is voluntary
- Tell participants that they may withdraw at any time and for any reason without penalty
- Give participants the option of omitting questions they do not wish to answer if a questionnaire is used
- Tell participants that their data will be treated with full confidentiality and that, if published, it will not be identified as theirs
- On request, debrief participants at the end of their participation (i.e. give them a brief explanation of the study)
- Verify that participants are 18 years or older and competent to supply consent.
- If the study involves participants viewing video displays then I will verify that they understand that if they or anyone in their family has a history of epilepsy then the participant is proceeding at their own risk
- Declare any potential conflict of interest to participants.
- Inform participants that in the extremely unlikely event that illicit activity is reported to me during the study I will be obliged to report it to appropriate authorities.
- Act in accordance with the information provided (i.e. if I tell participants I will not do something, then I will not do it).

Signed: ..... Date: **May 8, 2019**

Lead Researcher/student in case of project work

Part B

Please answer the following questions.		***Yes/No***
Has this research application or any application of a similar nature connected to this research project been refused ethical approval by another review committee of the College (or at the institutions of any collaborators)?		No
Will your project involve photographing participants or electronic audio or video recordings?		Yes (audio rec)
Will your project deliberately involve misleading participants in any way?		No
Does this study contain commercially sensitive material?		No
Is there a risk of participants experiencing either physical or psychological distress or discomfort? If yes, give details on a separate sheet and state what you will tell them to do if they should experience any such problems (e.g. who they can contact for help).		No
Does your study involve any of the following?	Children (under 18 years of age)	No
	People with intellectual or communication difficulties	No
	Patients	No

School of Computer Science and Statistics
Research Ethical Application Form

Details of the Research Project Proposal must be submitted as a separate document to include the following information:

1. Title of project
2. Purpose of project including academic rationale
3. Brief description of methods and measurements to be used
4. Participants - recruitment methods, number, age, gender, exclusion/inclusion criteria, including statistical justification for numbers of participants
5. Debriefing arrangements
6. A clear concise statement of the ethical considerations raised by the project and how you intend to deal with them
7. Cite any relevant legislation relevant to the project with the method of compliance e.g. Data Protection Act etc.

Part C

I confirm that the materials I have submitted provided a complete and accurate account of the research I propose to conduct in this context, including my assessment of the ethical ramifications.

Signed: ..... Date: 8 - May 2019
Lead Researcher/student in case of project work

There is an obligation on the lead researcher to bring to the attention of the SCSS Research Ethics Committee any issues with ethical implications not clearly covered above.

Part D

If external or other TCD Ethics Committee approval has been received, please complete below.

External/TCD ethical approval has been received and no further ethical approval is required from the School's Research Ethical Committee. I have attached a copy of the external ethical approval for the School's Research Unit.

Signed: ..... Date: .....
Lead Researcher/student in case of project work

Part E

If the research is proposed by an undergraduate or postgraduate student, please have the below section completed.

I confirm, as an academic supervisor of this proposed research that the documents at hand are complete (i.e. each item on the submission checklist is accounted for) and are in a form that is suitable for review by the SCSS Research Ethics Committee

Signed: ..... Date: 8th May 2019.
Supervisor

Completed application forms together with supporting documentation should be submitted electronically to the online ethics system - https://webhost.tchpc.tcd.ie/research_ethics/ When your application has been reviewed and approved by the Ethics committee, hardcopies with original signatures should be submitted to the School of Computer Science & Statistics, Room 104, Lloyd Building, Trinity College, Dublin 2.

Ethics Application Guidelines – 2016

CHECKLIST

Please ensure that you have submitted the following documents with your application:

1.	• SCSS Ethical **Application Form**	
2.	• **Participant's Information Sheet** must include the following: a) Declarations from Part A of the application form; b) Details provided to participants about how they were selected to participate; c) Declaration of all conflicts of interest.	
3.	• **Participant's Consent Form** must include the following: a) Declarations from Part A of the application form; b) Researchers contact details provided for counter-signature (your participant will keep one copy of the signed consent form and return a copy to you).	
4.	• **Research Project Proposal** must include the following: a) You must inform the Ethics Committee **who** your intended participants are i.e. are they your work colleagues, class mates etc. b) How will you recruit the participants i.e. **how** do you intend asking people to take part in your research? For example, will you stand on Pearse Street asking passers-by? c) If your participants are under the age of 18, you must seek both parental/guardian AND child consent.	
5.	• Intended **questionnaire**/survey/interview protocol/screen shots/representative materials (as appropriate)	
6.	• **URL** to intended on-line survey (as appropriate)	

Notes on Conflict of Interest

1. If your intended participants are work colleagues, you must declare a potential conflict of interest: you are taking advantage of your existing relationships in order to make progress in your research. It is best to acknowledge this in your invitation to participants.
2. If your research is also intended to direct commercial or other exploitation, this must be declared. For example, *"Please be advised that this research is being conducted by an employee of the company that supplies the product or service which form an object of study within the research."*

Notes for questionnaires and interviews

1. If your questionnaire is **paper based**, you must have the following **opt-out** clause on the top of each page of the questionnaire: *"Each question is optional. Feel free to omit a response to any question; however the researcher would be grateful if all questions are responded to."*
2. If you questionnaire is **on-line**, the first page of your questionnaire must repeat the content of the information sheet. This must be followed by the consent form. If the participant does not agree to the consent, they must automatically be exited from the questionnaire.
3. Each question must be **optional**.
4. The participant must have the option to '**not submit, exit without submitting'** at the final submission point on your questionnaire.
5. If you have open-ended questions on your questionnaire you must warn the participant against naming **third parties**: "*Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised."*
6. You must inform your participants regarding **illicit activity**: "*In the extremely unlikely event that illicit activity is reported I will be obliged to report it to appropriate authorities."*

Research Project Proposal

1. Title of project

The Influence of Personal Characteristics and Other Factors on The Susceptibility of Public Sector Employees to Cyber-Social Engineering Through LinkedIn: A Mixed-Methods Sequential Explanatory Study

2. Purpose of this project including academic rationale

This research aims to offer a rich and deep understanding of the impact of personal characteristics and other factors upon government organization employees' susceptibility to the risks of cyber-social engineering (CSE) in the Kingdom of Saudi Arabia. Factors to be studied include demographics, risk perception, willingness to assume risk, perceived control over privacy risk, computer self-efficacy, and level of engagement. For the government of Saudi Arabia, the results of this study will provide insights to help determine human aspects of employees and managers that can influence their perceptual and behavioural fallibilities in respect of the risks of cyber-social engineering when accessing social networking sites in work environments. It will consequently shed light on potential risks to sensitive data held by these organizations. It is anticipated that this research will provide insights which will support appropriate decision-making in relation to employees' use of cyber-based networking platforms and the development or enhancement of appropriate IS security strategies and policies to achieve safe use of these platforms across the public sector in Saudi Arabia.

3. Brief description of methods and measurements to be used in

This study involves mixed methods and multiple case studies. The primary data gathering will be done using two approaches. First, questionnaires will be distributed in paper form in each affiliated department under the selected organization. A quantitative data analysis will be conducted using the SPSS software package. Second, semi-structured interviews will be conducted, however, in light of the current situation with COVID-19, and in compliance with Trinity College Dublin and the Health Departments of Ireland and Saudi Arabia, semi-structured interviews will not be conducted face-to-face. Instead, participants will be interviewed remotely, either by telephone or online (i.e., Zoom, Skype, or Hangouts), according to their preference. Participants will also be contacted by email or social networking platforms. Qualitative data analysis will be carried out by transcribing the interview recordings for analysis after translation in terms of categories and themes, based on factors influencing susceptibility to CSE in the workplace.

4. Participants - recruitment methods, numbers, age, gender, exclusion/inclusion criteria, including statistical justification for numbers of participants.

A formal request for recruitment of participants will commence through direct verbal communication via phone calls to initially obtain formal permission from the head office. Upon receiving permission to conduct both quantitative and qualitative data collection, an internal informal written communication, such as a letter or email, will be circulated to department personnel potentially willing to voluntarily take part in this study. The number of participants anticipated for the quantitative study is approximately 300- 500 employees and managers, drawn from departments and subcontracts, all of which are affiliated to one main ministry. This is based on the estimate that the Ministry of Human Resources and Social Development (formerly Ministry of Labor and Social Development) in Saudi Arabia has an average of 10,000 personnel. The number of people who will be interviewed is approximately 15- 20 participants, including: employees and managers, higher education faculty members, and experts in the field of IS. There are no exclusion criteria.

5. Debriefing arrangements

I have already met some of the affiliated officials working under the ministry who will potentially be interviewed. I have asked them if they are interested in participating in this research and they have agreed to do so, subject to official approval from the ministry, which has already been requested. Other informants will be identified using the snowball method, as well as based on direct contact with targeted employees under the authority of local managers/officials while complying with precautionary measures as directed by officials in light of COVID-19 pandemic and as per "*The Corona Guidelines 2020 (Research during pandemics, conflict and natural disasters)"* dated 17th March 2020 by Andrea J. Nightingale. Direct contact will also be through mediated contacts, such as experts and faculty members and other participants. Participants in the survey will also be invited on a separate form to indicate their willingness to be contacted for the interview. Summaries of the interviews will be checked with the informants to ensure their accuracy. Results of the study will be available to participants when the study has been completed.

TRINITY COLLEGE DUBLIN
INFORMED CONSENT FORM - Survey

APPENDIX C1

LEAD RESEARCHERS: Mohammed Khaled N. Alotaibi

BACKGROUND OF RESEARCH: This research investigates employees' susceptibility to cyber-social engineering while accessing professional social networking sites SNSs (i.e. LinkedIn) in public sector organisations that are affiliated under Saudi Arabia's Ministry of the Interior. Its objective is to investigate how and to what extent employees' personal characteristics and other factors can influence their susceptibility. The factors to be investigated include *risk perception; willingness to assume risk; perceived control over privacy risk; computer self-efficacy; demographic background;* and *level of engagement in LinkedIn usage*.

This study will involve a mixed-methods research approach that combines questionnaires and interviews. This questionnaire will take around 10 minutes to complete.

PUBLICATION: The result of this project may appear in papers, books, journal articles and presentations at conferences, but you will not be identified in any of these reports. Individual results will be aggregated anonymously, and research reported on aggregate results.

Please take your time to read the following declaration and sign it if you are willing to participate in the survey.

DECLARATION:

- I am 18 years of age or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction.
- I understand the description of the research that has been provided to me.
- I agree that my data is used for scientific purposes and I have no objection to my data being published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to the appropriate authorities.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.

By signing this document, I consent to participate in this study, and consent to the data processing necessary to enable my participation and to achieve the research goals of this study.

PARTICIPANT'S NAME:

PARTICIPANT'S SIGNATURE: **Date:**

Statement of investigator's responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

RESEARCHER'S CONTACT DETAILS: E-mail: malotaib@tcd.ie **Tel No: +966**[redacted]

INVESTIGATOR'S SIGNATURE:

Date: **8 May 2019**

TRINITY COLLEGE DUBLIN
INFORMED CONSENT FORM - Interview

APPENDIX C2

LEAD RESEARCHERS: Mohammed Khaled N. Alotaibi

BACKGROUND OF RESEARCH: This research investigates employees' susceptibility to cyber-social engineering while accessing professional social networking sites (specifically, LinkedIn) in public sector organisations that are linked to the Ministry of the Interior's National Information Center (NIC) in Saudi Arabia. Its objective is to investigate how, and to what extent, employees' personal characteristics and other factors can influence their susceptibility. Factors to be investigated include *risk perception; willingness to assume risk; perceived control over privacy risk; computer self-efficacy and employees' demographics;* and *level of engagement on LinkedIn*.

This study will involve a mixed-methods research approach that combines questionnaires and interviews. The remote interview is expected to take about 30 – 45 minutes and will be recorded using a digital voice recorder, if that is acceptable to you. Otherwise, handwritten notes will be taken. If a voice recorder is in use, you may ask at any time to stop recording temporarily or permanently.

PUBLICATION: The result of this project may appear in papers, books, journal articles and presentations at conferences, but you will not be identified in any of these reports. No recordings will be made available to anyone other than the researcher, nor will any such recordings be replayed in any public forum or presentation of the research. Individual results will either be aggregated anonymously or quoted from the interview findings, and research reported on the aggregated results.

Please take your time to read the following declaration and sign it.

DECLARATION:

- I am 18 years of age or older and am competent to provideconsent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction.
- I understand the description of the research that has been provided tome.
- I agree that my data is used for scientific purposes and I have no objection to my data being published in scientific publications in a way that does not reveal myidentity.
- I understand that if I make illicit activities known, these will be reported to the appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation, have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researcher or research team.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.

By signing this document, I consent to participate in this study, and consent to the data processing necessary to enable my participation and to achieve the research goals of this study.

PARTICIPANT'S NAME:
PARTICIPANT'S SIGNATURE: **Date:**

Statement of investigator's responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

RESEARCHER'S CONTACT DETAILS: E-mail: malotaib@tcd.ie **Tel No: +966[redacted] (KSA)**

INVESTIGATOR'S SIGNATURE:
Date:May 8, 2019

Although the data will be collected in Saudi Arabia (KSA), the analysis may be undertaken within the EU, so the data collected has to comply with the GDPR. Data will be encrypted and stored in a secure password- protected cloud device which will remain offline at all times until names and organisations are replaced with distinctive code to insure anonymity.

6. A clear concise statement of the ethical considerations raised by the project and how you intend to deal with them

There are no ethical considerations in this project other than respecting the confidentiality of the interviewees' comments. There are no sensitive social, political, medical or sexual issues involved in this research. All interviewees will be adults.

I confirm that I will abide by the School of Computer Science and Statistics Ethical Guidelines and I will inform the committee if there is any ethically relevant variation to the project as described in this application.

Signature of Applicant:  **Date:** **May 8, 2019**

TRINITY COLLEGE DUBLIN

INFORMATION SHEET FOR PROSPECTIVE PARTICIPANTS – Survey

This sheet should inform participants of the following as appropriate to the study:

- The background context of the research explaining its relevance
- The procedures relevant to the participant within this particular study
- Declaration of the conflicts of interest
- The voluntary nature of participation: the right to withdraw and to omit individual responses without penalty
- The expected duration of the participant's involvement
- Anticipated risks/benefits to the participant
- The provisions for debriefing after participation
- Preservation of participant and third-part anonymity in analysis, publication and presentation of resulting data and findings
- Cautions about inadvertent discovery of illicit activities
- Provision for verifying direct quotations and their contextual appropriateness

Of course, the information sheet for participants will differ according to the study at hand. It should provide all information necessary for informed consent.

TRINITY COLLEGE DUBLIN

INFORMATION SHEET FOR PROSPECTIVE PARTICIPANTS – Interview

This sheet should inform participants of the following as appropriate to the study:

- The background context of the research explaining its relevance
- The procedures relevant to the participant within this particular study
- Declaration of the conflicts of interest
- The voluntary nature of participation: the right to withdraw and to omit individual responses without penalty
- The expected duration of the participant's involvement
- Anticipated risks/benefits to the participant
- The provisions for debriefing after participation
- Preservation of participant and third-part anonymity in analysis, publication and presentation of resulting data and findings
- Cautions about inadvertent discovery of illicit activities
- Provision for verifying direct quotations and their contextual appropriateness
- No recordings will be made available to anyone other than the research/research team nor will any such recordings be played in any public forum or presentation of the research.

Of course, the information sheet for participants will differ according to the study at hand. It should provide all information necessary for informed consent.

TRINITY COLLEGE DUBLIN
INFORMATION SHEET FOR PROSPECTIVE PARTICIPANTS – Survey

My Name is Mohammed Khaled N. Alotaibi. I am a Ph.D. student in the School of Computer Science and Statistics at Trinity College Dublin. You are being invited to take part in a research study investigating how, and to what extent, personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering when accessing LinkedIn. Factors to be investigated include: *demographics; risk perception; willingness to assume risk; perceived control over privacy risk; computer self-efficacy;* and *level of engagement*. The study specifically concerns the personnel of government organisations in Saudi Arabia. Please take your time to read the following information.

I am asking between 300 – 500 employees to take part in this survey to investigate the likelihood of susceptibility to cyber-social engineering on professional social networking sites (SNS) in the workplace. Your participation in this study is voluntary and you can withdraw from it at any time without penalty.

If you decide that you would like to take part, I would ask you to fill in this survey at your convenience. You will not have to do anything particular to prepare for this survey. Each question is optional; however, I would be grateful if you could respond to all.

You may or may not benefit directly from participating in this research, but you will be helping to advance awareness, knowledge and understanding of human aspects relating to the safe use of cyber-based social networking platforms accessed in public organisations. It will help us to understand which characteristics make employees vulnerable to deceptive attacks by cyber-social engineers on professional social networking sites. The results of this research will be available to you on request.

Time required
The questionnaire will take approximately 30 minutes to complete.

Conflict of interest
There are no known conflicts of interest associated with this research project. The author whose name is highlighted above certifies that he has NO affiliations with or involvement in any of the organizations that are taking part in the project. There will be no incentives, coercion or undue influence of research participants to take part in filling in the questionnaire. There are no anticipated ethical issues in this project, other than respecting the confidentiality of your responses. There are no sensitive social, political, medical or sexual issues involved in this research.

Privacy and Confidentiality
The result of this project may appear in papers, books, journal articles and presentations at conferences, but you will not be identified or identifiable in any of these reports unless you wish to be so identified. Individual results will be aggregated anonymously, and pseudonyms will be used for the organization department names so that they will not be identifiable in what is written. Completed surveys and information consent forms will only be available to the researcher and will be destroyed after the thesis has been examined.

In the extremely unlikely event that illicit activity is reported, the researcher will be obligated to report it to the appropriate authorities.

The project is funded by Saudi Arabia's Ministry of Education. However, they will not have access to the data.

Although the data will be collected in Saudi Arabia (KSA), the analysis may be undertaken within the EU, so the data collected has to comply with the GDPR

Further information
If you have any questions about this research, you can ask now or at any point during the study.

Email: malotaib@tcd.ie Tele No: +96654[redacted] (KSA)

INFORMATION SHEET FOR PROSPECTIVE PARTICIPANTS – Interview

APPENDIX C6

My Name is Mohammed Khaled N. Alotaibi. I am a Ph.D. student in the School of Computer Science and Statistics at Trinity College Dublin. You are being invited to take part in a research study investigating how, and to what extent, personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering when accessing LinkedIn. The factors to be investigated include: *demographics; risk perception; willingness to assume risk; perceived control over privacy risk; computer self-efficacy;* and *level of engagement*. The study specifically concerns employees in government organisations in Saudi Arabia.

Please take your time to read the following information.

I am asking between 15-20 people (employees/managers, experts and faculty members in the field of IS security and other interdisciplinary backgrounds i.e. cyberpsychology) to take part in a remote interviews via telephone or online (i.e. Zoom, Skype, hangouts) to investigate their views on susceptibility to cyber-social engineering on professional social networking sites (SNS) in the workplace. Your participation in this study is voluntary and you can withdraw from the study at any time withoutpenalty.

If you decide that you would like to take part, I will hold the interview in your workplace at a time that suits you. The interview will last about 30 - 45 minutes. You will not have to do anything to prepare for this interview. Each question is optional; however, I would be grateful if you could respond to all.

You may or may not benefit directly from participating in this research, but you will be helping to advance awareness, knowledge and understanding of human aspects relating to the safe use of cyber-based social networking platforms accessed in public organisations and to understand what characteristics make employees vulnerable to deceptive attacks by cyber-social engineers on professional social networking sites. The results of this research will be available to you on request.

Conflict of interest

There are no known conflicts of interest associated with this research project. The author whose name is highlighted above certifies that he has NO affiliations with or involvement in any of the organizations that are participating in the study. There will be no incentives, coercion or undue influence of research participants to take part in the recorded interviews. There are no anticipated ethical issues in this project, other than respecting the confidentiality of your responses. There are no sensitive social, political, medical or sexual issues involved in this research.

Privacy and Confidentiality

With your permission, I will record the interview on a digital voice recorder to make sure that I remember what we talked about. I will turn off the recorder, temporarily or permanently, at any time if you are not comfortable with a particular part of the discussion being recorded. The result of this project may appear in papers, books, journal articles and presentations at conferences, but you will not be identified or identifiable in any of these reports unless you wish to be so identified. No recordings will be made available to anyone other than the researcher, nor will any such recordings be replayed in any public forum or presentation of the research. Pseudonyms will be used for your and the organizations name so you will not be identifiable in what is written. Completed interview records/audio transcriptions and information consent forms will only be available to the researcher and will be destroyed after the thesis has been examined.

In the extremely unlikely event that illicit activity is reported, the researcher will be obligated to report it to the appropriate authorities.

The project is funded by Saudi Arabia's Ministry of Education. However, they will not have access to the data.

Although the data will be collected in Saudi Arabia (KSA), the analysis may be undertaken within the EU, so the data collected has to comply with the GDPR

Verification of interview records

After the interview has been transcribed, you will receive a copy of the transcription. You will be asked to confirm the accuracy of the record and you can make changes or delete any parts which you feel are incorrect.

Further information

If you have any questions about this research, you can ask now or at any point during the study.

Email: malotaib@tcd.ie Tele No: +96654[redacted](KSA)

APPENDIX D

The Survey Questionnaire

Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin
Ollscoil Átha Cliath | The University of Dublin

Welcome

Thank you for taking the time to answer the following survey. Within the survey you will be asked to provide limited background information, your Big Five Personality profile and questions related to potential factors that could make an individual susceptible to risks of cyber-social engineering occurring on professional social networking sites.

- Your participation in this study is voluntary and you can withdraw from the study at any time without penalty.
- The survey should take you around 10 to 15 minutes to complete.
- I would welcome any comments or suggestions you have, please add them to the space provided at the end of the survey.

Confidentiality

The information you provide is anonymous; you cannot be identified from this questionnaire. The completed survey will only be accessed by the researcher (see below) and the data will be destroyed after examination of the dissertation has been completed. The information will be collated statistically and anonymously, you will not be identifiable.

Since the information you provide is anonymous. We ask that you please answer each question honestly as this will help ensure that we can make the greatest impact with our research.

Should you have any further questions please use the following to reach me:

Mr. Mohammed K. Alotaibi

Discipline of Statistics and Information Systems

School of Computer Science and Statistics

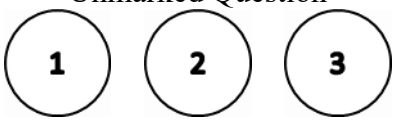
Trinity College Dublin, Ireland

Tel: +96654 (KSA), +353874037027 (Ireland)

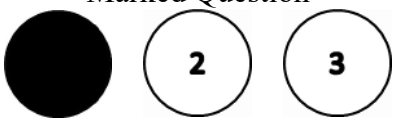
Email: malotaib@tcd.ie

Please answer each of the following question by filling in the bubble of your choice on the scantron sheet provided. Be sure that the bubble area is completely filled with answers that apply to you. Please use pencil, if you can, in the event you wish to change your answer.

Unmarked Question



Marked Question

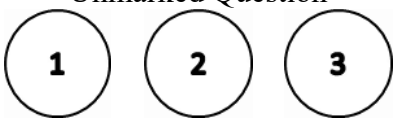


Q1. What social networking sites (SNS) do you use?	1	2	3	4	5
	Facebook	Twitter	Instagram	Snapchat	Other, please specify on answer sheet

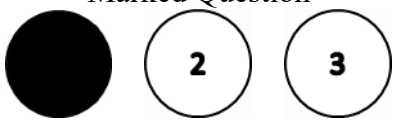
Q2. What career-oriented social networking sites (CSNS) do you use?	1	2	3	4
	Bayt	LinkedIn	XIGN	Other, please specify on answer sheet

Please answer each of the following question by filling in the bubble of your choice on the scantron sheet provided. Be sure that the bubble area is completely filled with answers that apply to you. Please use pencil, if you can, in the event you wish to change your answer.

Unmarked Question



Marked Question



Q3. Are you?	1	2
	Male	Female

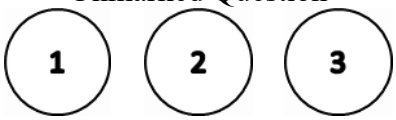
Q4. How old are you?	1	2	3	4	5
	18 - 28	29 - 39	40 -50	51 - 61	Over 62

Q5. What is your Nationality	1	2
	Saudi Arabia	Non-Saudi (expatriate), please specify in answer sheet
Q6. You work at:	1	2
	Labor Sector	Social Development Sector

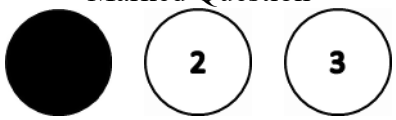
Q7. Do you work on?	1	2	3
	Top-level management or designee	Department management/Section supervisor or designee	Administrative Officer/Assistant (Employee)

Please answer each of the following question by filling in the bubble of your choice on the scantron sheet provided. Be sure that the bubble area is completely filled with answers that apply to you. Please use pencil, if you can, in the event you wish to change your answer.

Unmarked Question



Marked Question



How likely would you be to agree or disagree with the following statements?

	Strongly Disagree	Disagree	Slightly Disagree	Neither Disagree or Agree	Slightly Agree	Agree	Strongly Agree
Q8. I have thought a lot about the origins of the universe.	1	2	3	4	5	6	7
Q9. I like to keep all my belongings neat and organized	1	2	3	4	5	6	7
Q10. I am a very shy person	1	2	3	4	5	6	7
Q11. I am always generous when it comes to helping others	1	2	3	4	5	6	7
Q12. I always treat other people with Kindness	1	2	3	4	5	6	7
Q13. Sometimes I get so upset I feel sick to my stomach	1	2	3	4	5	6	7
Q14. I am highly interested in all fields of science	1	2	3	4	5	6	7
Q15. I like to have a place for everything and everything in its place	1	2	3	4	5	6	7
Q16. I am kind	1	2	3	4	5	6	7
Q17. When I am under great stress I often feel like I am about to break down	1	2	3	4	5	6	7
Q18. I am quiet	1	2	3	4	5	6	7
Q19. I am fascinated with the theory of evolution	1	2	3	4	5	6	7
Q20. I am neat	1	2	3	4	5	6	7
Q21. I am sympathetic	1	2	3	4	5	6	7
Q22. I am withdrawn	1	2	3	4	5	6	7
Q23. My feelings are easily hurt	1	2	3	4	5	6	7
Q24. I would enjoy being a theoretical scientist	1	2	3	4	5	6	7
Q25. I am organized	1	2	3	4	5	6	7
Q26. I am quiet	1	2	3	4	5	6	7
Q27. I often have headaches when things are not going well	1	2	3	4	5	6	7

Please answer each of the followings question by filling in the bubble of your choice on the scantron sheet provided. Be sure that the bubble area is completely filled with answers that apply to you. Please use pencil, if you can, in the event you wish to change your answer.

In the past 6 months have you?

	Never	Once	Two or three times	A few times per month	Once a week	A few times per week	Always
Q28. Shared your password with a friend or colleague	1	2	3	4	5	6	7
Q29. Used or created a password that is only based on your family name or date of birth	1	2	3	4	5	6	7
Q30. Used the same password for more than one account	1	2	3	4	5	6	7
Q31. Used an online storage systems (e.g. OneDrive, Google Drive, iCloud) to exchange and keep personal or sensitive information on	1	2	3	4	5	6	7
Q32. Entered payment information on websites that have no clear security information/certification	1	2	3	4	5	6	7
Q33. Used free-to-access public Wi-Fi	1	2	3	4	5	6	7
Q34. Relied on a trusted friend or colleague to advise you on aspects of online-security	1	2	3	4	5	6	7
Q35. Downloaded free anti-virus software from an unknown source.	1	2	3	4	5	6	7
Q36. Bypass network restrictions on your work computer to navigate SNSs.	1	2	3	4	5	6	7
Q37. Brought in your own Wireless network USB to work in order to brows SNSs.	1	2	3	4	5	6	7
Q38. Checked that the software for your smartphone/tablet/laptop/PC is up-to-date.	1	2	3	4	5	6	7
Q39. Downloaded digital media (music, films, games) you Liked on LinkedIn from unlicensed sources	1	2	3	4	5	6	7
Q40. Shared your current location on social media	1	2	3	4	5	6	7
Q41. Accepted friend requests on social media because you recognise the photo.	1	2	3	4	5	6	7
Q42. Clicked on links contained in unsolicited emails from an unknown source	1	2	3	4	5	6	7
Q43. Sent personal information to strangers over the Internet.	1	2	3	4	5	6	7
Q44. Clicked on links contained in a LinkedIn InMail from a trusted friend or work colleague.	1	2	3	4	5	6	7
Q45. Checked for updates to any anti-virus software you have installed.	1	2	3	4	5	6	7
Q46. Downloaded data and material from websites on your work computer without checking its authenticity	1	2	3	4	5	6	7
Q47. Stored company information on your personal electronic device (e.g. smartphone/tablet/laptop)	1	2	3	4	5	6	7

Please answer each of the followings question by filling in the bubble of your choice on the scantron sheet provided. Be sure that the bubble area is completely filled with answers that apply to you. Please use pencil, if you can, in the event you wish to change your answer.

In the past 6 months have you?

	Never	Once	Two or three times	A few times per month	Once a week	A few times per week	Always
Q48. Logged into social media sites from your electronic work device (e.g. smartphone/tablet/laptop)	1	2	3	4	5	6	7
Q49. Checked your email notifications from social media sites	1	2	3	4	5	6	7
Q50. Talked about private company information on any of your social media sites	1	2	3	4	5	6	7
Q51. Sent messages to work colleagues through one of social media sites you belong to	1	2	3	4	5	6	7
Q52. Shared photos or videos containing company Information on social media sites	1	2	3	4	5	6	7

The following questions relate to your thoughts, behaviours and experience with regards to using LinkedIn as a professional career social networking service. If you have a LinkedIn account we would appreciate the following questions.

	1	2	3	4	5	6	7
Q53. How often do you use LinkedIn at work?	Never	Registered but do not use	Less than once a week	Every 2-3 days	Once to twice per day	Several times a day	Open all the time

Please indicate how likely you are to agree or disagree with the following statements

	Strongly Disagree	Disagree	Slightly Disagree	Neither Disagree or Agree	Slightly Agree	Agree	Strongly Agree
Q54. In general, it would be risky to give information in response to requests on LinkedIn.	1	2	3	4	5	6	7
Q55. There is a high potential for loss associated with giving information in response to requests on LinkedIn.	1	2	3	4	5	6	7
Q56. There is too much uncertainty associated with giving information in response to requests made via LinkedIn	1	2	3	4	5	6	7
Q57. Providing professional SNS sites with information could create unexpected problems	1	2	3	4	5	6	7

Please answer each of the following questions by filling in the bubble of your choice on the scantron sheet provided. Be sure that the bubble area is completely filled with answers that apply to you. Please use pencil, if you can, in the event you wish to change your answer.

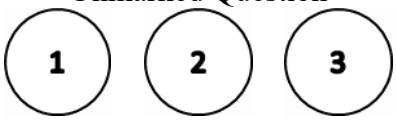
Please indicate how likely you are to agree or disagree with the following statements

	Strongly Disagree	Disagree	Slightly Disagree	Neither Disagree or Agree	Slightly Agree	Agree	Strongly Agree
Q58. I am willing to take substantial risks to actively engage with services and features provided on LinkedIn	1	2	3	4	5	6	7
Q59. I am willing to accept some risk of losing money if a LinkedIn job offer process involves a small amount of risk	1	2	3	4	5	6	7
Q60. I am willing to accept some risk to my personal information if a LinkedIn post (e.g. job offer, contract, agreement) involves a small amount of risk.	1	2	3	4	5	6	7
Q61. I am NOT more comfortable using familiar professional SNS than something I am not sure about.	1	2	3	4	5	6	7
Q62. I am NOT cautious when trying new career based SNS platforms.	1	2	3	4	5	6	7
Q63. I believe I have control over who can get access to my personal information collected by LinkedIn.	1	2	3	4	5	6	7
Q64. I think I have control over what personal information is released by LinkedIn.	1	2	3	4	5	6	7
Q65. I believe I have control over how personal information is used by LinkedIn.	1	2	3	4	5	6	7
Q66. I feel confident operating a digital device.	1	2	3	4	5	6	7
Q67. I feel confident understanding terms/words relating to SNSs privacy policies/agreements	1	2	3	4	5	6	7
Q68. I feel confident navigating SNSs applications and websites.	1	2	3	4	5	6	7
Q69. I feel confident knowing/recognizing the authenticity of LinkedIn website/profiles or smartphone app.	1	2	3	4	5	6	7

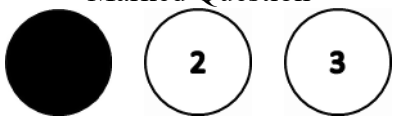
Please turn the page over

Please answer each of the following question by filling in the bubble of your choice on the scantron sheet provided. Be sure that the bubble area is completely filled with answers that apply to you. Please use pencil, if you can, in the event you wish to change your answer.

Unmarked Question



Marked Question



On LinkedIn…

	Yes	No
Q70. Have you put your work experience history on?	1	2
Q71. Have you put your Educational history on?	1	2
Q72. Have you put your licences on?	1	2
Q73. Have you put your certificates on?	1	2
Q74. Have you put your work email address on?	1	2
Q75. Have you put your work telephone number on?	1	2
Q76. Have you created an About me Page?	1	2
Q77. Have you put where you currently work?	1	2
Q78. Have you put your job title?	1	2
Q79. Have you put a profile picture?	1	2
Q80. Have you set your profile to public so anyone can view it?	1	2
Q81. Have you revealed or updated your current location?	1	2
Q82. Is your company logo on your profile?	1	2

On LinkedIn…

	Never	Rarely	Sometimes	Often	Always
Q83. Have you connected with professionals that could help you with your professional advancement?	1	2	3	4	5
Q84. Have you followed other companies that you believe could increase your professional advancement?	1	2	3	4	5
Q85. Have you shared your work related CV to companies which you believe could help you with your professional advancement?	1	2	3	4	5
Q86. Have you shared your work related CV with professionals with whom you feel can help with your professional advancement?	1	2	3	4	5

Q87. Have you accepted connections from connections whom you don't know but can see that they have many connections themselves?	1	2	3	4	5
Q88. Have you accepted network connections from connections who are connected to your connections?	1	2	3	4	5
Q89. Have you accepted a connection requests on LinkedIn because you recognized the photo?	1	2	3	4	5
Q90.Have you messaged your connections for support in career or work related matters?	1	2	3	4	5
Q91. Have you shared documents, audio or video with connections in order to assist you with a problem?	1	2	3	4	5
Q92. Have you accepted documents, audio or videos from connections in relation to receiving support from them?	1	2	3	4	5

The following questions relate to your experience regarding cyber social engineering. Please answer this questions as honestly as possible as it would help increase the accuracy of the research. Your responses will be anonymous.

	Yes	No
Q93. Have you heard of cyber-social engineering before?	1	2
Q94. Have you ever received training at work that involved making you aware of the threats online?	1	2
Q95. Have you ever received training at work that involved making you aware of the online realities of threats involved when using a SNS at work?	1	2
Q96. In all the time since you have been using LinkedIn have you ever had something bad happen (At your work or in your personal life) to you that you can trace back to your usage of LinkedIn?	1	2

Q97. If you have answered yes to question 97 could you briefly explain what happened and how you knew what you did on LinkedIn was the reason?

"Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised."

Answer sheet

Paper ID	

Q1 ① ② ③ ④ ⑤	**Q28** ① ② ③ ④ ⑤ ⑥ ⑦	**Q55** ① ② ③ ④ ⑤ ⑥ ⑦
Q2 ① ② ③ ④	**Q29** ① ② ③ ④ ⑤ ⑥ ⑦	**Q56** ① ② ③ ④ ⑤ ⑥ ⑦
Q3 ① ②	**Q30** ① ② ③ ④ ⑤ ⑥ ⑦	**Q57** ① ② ③ ④ ⑤ ⑥ ⑦
Q4 ① ② ③ ④ ⑤	**Q31** ① ② ③ ④ ⑤ ⑥ ⑦	**Q58** ① ② ③ ④ ⑤ ⑥ ⑦
Q5 ① ②	**Q32** ① ② ③ ④ ⑤ ⑥ ⑦	**Q59** ① ② ③ ④ ⑤ ⑥ ⑦
Q6 ① ②	**Q33** ① ② ③ ④ ⑤ ⑥ ⑦	**Q60** ① ② ③ ④ ⑤ ⑥ ⑦
Q7 ① ② ③	**Q34** ① ② ③ ④ ⑤ ⑥ ⑦	**Q61** ① ② ③ ④ ⑤ ⑥ ⑦
Q8 ① ② ③ ④ ⑤ ⑥ ⑦	**Q35** ① ② ③ ④ ⑤ ⑥ ⑦	**Q62** ① ② ③ ④ ⑤ ⑥ ⑦
Q9 ① ② ③ ④ ⑤ ⑥ ⑦	**Q36** ① ② ③ ④ ⑤ ⑥ ⑦	**Q63** ① ② ③ ④ ⑤ ⑥ ⑦
Q10 ① ② ③ ④ ⑤ ⑥ ⑦	**Q37** ① ② ③ ④ ⑤ ⑥ ⑦	**Q64** ① ② ③ ④ ⑤ ⑥ ⑦
Q11 ① ② ③ ④ ⑤ ⑥ ⑦	**Q38** ① ② ③ ④ ⑤ ⑥ ⑦	**Q65** ① ② ③ ④ ⑤ ⑥ ⑦
Q12 ① ② ③ ④ ⑤ ⑥ ⑦	**Q39** ① ② ③ ④ ⑤ ⑥ ⑦	**Q66** ① ② ③ ④ ⑤ ⑥ ⑦
Q13 ① ② ③ ④ ⑤ ⑥ ⑦	**Q40** ① ② ③ ④ ⑤ ⑥ ⑦	**Q67** ① ② ③ ④ ⑤ ⑥ ⑦
Q14 ① ② ③ ④ ⑤ ⑥ ⑦	**Q41** ① ② ③ ④ ⑤ ⑥ ⑦	**Q68** ① ② ③ ④ ⑤ ⑥ ⑦
Q15 ① ② ③ ④ ⑤ ⑥ ⑦	**Q42** ① ② ③ ④ ⑤ ⑥ ⑦	**Q69** ① ② ③ ④ ⑤ ⑥ ⑦
Q16 ① ② ③ ④ ⑤ ⑥ ⑦	**Q43** ① ② ③ ④ ⑤ ⑥ ⑦	**Q70** ① ②
Q17 ① ② ③ ④ ⑤ ⑥ ⑦	**Q44** ① ② ③ ④ ⑤ ⑥ ⑦	**Q71** ① ②
Q18 ① ② ③ ④ ⑤ ⑥ ⑦	**Q45** ① ② ③ ④ ⑤ ⑥ ⑦	**Q72** ① ②
Q19 ① ② ③ ④ ⑤ ⑥ ⑦	**Q46** ① ② ③ ④ ⑤ ⑥ ⑦	**Q73** ① ②
Q20 ① ② ③ ④ ⑤ ⑥ ⑦	**Q47** ① ② ③ ④ ⑤ ⑥ ⑦	**Q74** ① ②
Q21 ① ② ③ ④ ⑤ ⑥ ⑦	**Q48** ① ② ③ ④ ⑤ ⑥ ⑦	**Q75** ① ②
Q22 ① ② ③ ④ ⑤ ⑥ ⑦	**Q49** ① ② ③ ④ ⑤ ⑥ ⑦	**Q76** ① ②
Q23 ① ② ③ ④ ⑤ ⑥ ⑦	**Q50** ① ② ③ ④ ⑤ ⑥ ⑦	**Q77** ① ②
Q24 ① ② ③ ④ ⑤ ⑥ ⑦	**Q51** ① ② ③ ④ ⑤ ⑥ ⑦	**Q78** ① ②
Q25 ① ② ③ ④ ⑤ ⑥ ⑦	**Q52** ① ② ③ ④ ⑤ ⑥ ⑦	**Q79** ① ②
Q26 ① ② ③ ④ ⑤ ⑥ ⑦	**Q53** ① ② ③ ④ ⑤ ⑥ ⑦	**Q80** ① ②
Q27 ① ② ③ ④ ⑤ ⑥ ⑦	**Q54** ① ② ③ ④ ⑤ ⑥ ⑦	**Q81** ① ②

Q82 ① ②

Q83 ① ② ③ ④ ⑤

Q84 ① ② ③ ④ ⑤

Q85 ① ② ③ ④ ⑤

Q86 ① ② ③ ④ ⑤

Q87 ① ② ③ ④ ⑤

Q88 ① ② ③ ④ ⑤

Q89 ① ② ③ ④ ⑤

Q90 ① ② ③ ④ ⑤

Q91 ① ② ③ ④ ⑤

Q92 ① ② ③ ④ ⑤

Q93 ① ②

Q94 ① ②

Q95 ① ②

Q96 ① ②

Q97 ① ②

(Q1) _____

_____

_____

(Q2) _____

_____

_____

"Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised."

Q97 _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

THANK YOU FOR TAKING THE TIME TO COMPLETE THE SURVEY

APPENDIX E

Table 4.3: Items Changed in Questionnaire, Retaining Intended Meaning.

Variable	Statement	Changed to	Rationale
RHBIS Item 28	Sharing passwords with friends and colleagues.	Shared your password with a friend or colleague	Clarity in Arabic version
RHBIS Item 29	Using or creating passwords that are not very complicated (e.g. family name and date of birth).	Used or created a password that is only based on your family name or date of birth	Clarity in Arabic version
RHBIS Item 30	Using the same password for multiple professional SNS sites.	Used the same password for more than one account	Clarity in Arabic version
RHBIS Item 31	Using online storage systems to exchange and keep personal or sensitive information.	Used an online storage system (e.g. OneDrive, Google Drive, iCloud) to exchange and keep personal or sensitive information on	Experts
RHBIS Item 32	Entering payment information on websites provided through LinkedIn that have no clear security information/certification	Entered payment information on websites that have no clear security information/ certification	Clarity in Arabic version
RHBIS Item 36	Disabling the anti-virus on my work computer so that I can download information/documents shared by users on LinkedIn.	Bypass network restrictions on your work computer to navigate SNSs.	Clarity in Arabic version/Experts
RHBIS Item 37	Bringing in my own USB to work in order to transfer data onto it.	Brought in your own Wireless network USB to work in order to brows SNSs.	Experts
RHBIS Item 38	Checking that applications on my smartphone/tablet/laptop/PC are up to date through the Organisation's network. (reverse coded)	Checked that the software for your smartphone/tablet/laptop/PC is up-to-date.	Clarity in Arabic version/Experts
RHBIS Item 39	Downloading digital material (Videos, Documents, Applications) from LinkedIn users regardless of its authenticity.	Downloaded digital media (music, films, games) you liked on LinkedIn from unlicensed sources	Clarity in Arabic version
RHBIS Item 40	Sharing/revealing my current location on LinkedIn.	Shared your current location on social media	Clarity in Arabic version

RHBIS Item 41	Accepting connection requests on LinkedIn because you recognise the photo.	Accepted friend requests on social media because you recognise the photo.	Clarity in Arabic version
RHBIS Item 42	Clicking on links contained in unsolicited LinkedIn Inbox messages from an unknown source	Clicked on links contained in unsolicited emails from an unknown source	Clarity in Arabic version
RHBIS Item 43	Sending personal information/ credentials to unknown employers over LinkedIn	Sent personal information to strangers over the Internet	Clarity in Arabic version
RHBIS Item 47	Storing organisations information/materials on my personal electronic device (e.g. smartphone/tablet/laptop)	Stored company information on your personal electronic device (e.g. smartphone/tablet/laptop)	Clarity in Arabic version
Risk Perception Item 57	Providing professional SNS sites with information would involve many unexpected problems.	Providing professional SNS sites with information could create unexpected problems	Clarity in Arabic version
Willingness to Assume Risk Item 59	I am willing to accept some risk of losing money if a LinkedIn job offer involves an insignificant amount of risk.	I am willing to accept some risk of losing money if a LinkedIn job offer process involves a small amount of risk.	Clarity in Arabic version
Willingness to Assume Risk Item 60	I am willing to accept some risk to my personal information if a LinkedIn career opportunity (e.g. job post offers, contracts, agreements) involves an insignificant amount of risk.	I am willing to accept some risk to my personal information if a LinkedIn post (e.g. job offer, contract, agreement) involves a small amount of risk.	Clarity in Arabic version
Willginess to Assume Risk item 61	I am more comfortable using familiar professional SNS than something I am not sure about	I am NOT more comfortable using familiar professional SNS than something I am not sure about	Expert to avoid (chrismas-treeing) , grab attention.
Willignness to Assume Risk item62	I am cautious when trying new career based SNS platforms	I am NOT cautious when trying new career based SNS platforms	Expert to avoid (chrismas-treeing) , grab attention.
IT Self-Efficacy Item 66	I feel confident operating a personal computer.	I feel confident operating a digital device.	Clarity in Arabic version

IT Self-Efficacy Item 67	I feel confident understanding terms/words relating to SNS policy agreements	I feel confident understanding terms/words relating to SNSs privacy policies/agreements	Experts
IT Self-Efficacy Item 69	I feel confident knowing/recognizing the authenticity of a LinkedIn website or smartphone app.	I feel confident knowing/recognizing the authenticity of LinkedIn website/profiles or smartphone app.	Experts

APPENDIX F

FINAL REPORT FOR EVALUATION OF THE SURVEY AIMED AT EVALUATING

To what extent do personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering (CSE) victimisation when accessing professional SNSs, such as LinkedIn, in government organisations in Saudi Arabia?

By William Welsh

Industrial and Organisational Psychologist

1. Your Research

From reading through your research I found the factors you want to measure to be sound however there are some inconsistencies in your wording which I strongly suggest you fix and make consistent across your whole research paper; and this is really for your own benefit.

For example:

a) Personality Traits <- This is missing in your 1.1 Significance of Research

b) Susceptibility to risk of CSE attack on professional SNS. <- Again you need to be clear. All professional SNS or just LinkedIn.

c) Personal disposition (risk perception, risk propensity (willingness to assume risk), perceived control of privacy risk, Computer self-efficacy) Computer Self-efficacy is separate in 1.1 but included as part of personal disposition in 2.9.3

d) Behaviour/habitual (level of engagement on LinkedIn) <- Just re-write to Habitual behaviour in 1.1 as it is reflected in 2.9.4

e) Demographics (consisting of age, gender, nationality, role in organisation (manager/subordinates))

So just be so sure about that. Make it consistent across all headings, wording and your model.

If possible you should provide the reliability (α = internal consistency) and validity information of the instruments you are using, if you can, even if you intend to adjust the scale. This will give researchers an indication of the validity of the instrument as your research already points to the validity of constructs being measured quite well.

Furthermore with regards to your sample size. Ideally I would say 500 would be better. Run the calculator again once you have finalized your survey and the constructs/dimensions it measures and then see. If you wish to publish your results in a journal, that would definitely one of the deciding factors that they could deny you publication on. From my personal experience I sent my online survey, for my research, to 5000 participants and only received 279 viable datasets back. So working on that estimation and adding to the fact that it will be paper based. You should get enough data back, especially if you call the participants into a prepared survey room and ask them to quickly fill out the survey.

2 | Page

2. Constructs for your Research

I think the model of your research should be expanded and changed based upon your own research that you provided me with. I will outline that below. I believe this will help ensure the soundness of your research.

I understand your supervisors concern around constructing a whole new instrument to measure the constructs. It can backfire spectacularly. So if you can find a measure that can meet your needs according YOUR SPECIFIC needs i.e Measuring susceptibility on Linked. Go for it. But right now I don't see another option available to you.

I honestly don't think the picture images are as useful in proving that an individual is susceptible in the survey context. I would rather use an instrument that measures user behaviour validated by similar instruments measuring similar constructs. You have to think about time here as well and the disposition of the individuals maybe wanting to leave as quickly as possible.

I think you should give consideration about publishing this in the International Journal of Human-Computer Studies. As well as using that journal and others like it to help answer any fundamental questions that you still have.

Because! Here is an interesting article published by the International Journal of Human-Computer Studies that you might find very useful

https://www.sciencedirect.com/science/article/pii/S1071581918303628

Especially since you included the authors already as two of your references

So I am going outline how I would construct the instrument here.

2.1 Susceptibility to CSE Victimisation

Firstly Susceptibility to CSE Victimisation on Linked should be based on the constructs as you defined it in your research:

1. Self-presentation

2. Professional Development

As you have stated:

> Users of job-related social networking platforms are motivated by self-presentation and professional advancement (Kim and Cha 2017). Self-presentation is a form of information disclosure (Bronstein, 2013). As such, individuals who are self-presentation driven are keen to initiate interactions and build relationships (Schwämmlein and Wodzicki 2012). These motives of career advancement can be seen as an element that could be exploited by fake recruiter scams. LinkedIn members are found to be significantly more likely than Facebook users to allow public access to their professional and educational data (Zhitomirsky-Geffet and Bratspiess 2009), but there is little research specifically addressing these users' attitudes and dispositions toward potential cyber risk.

3 | Page

(1) - Never

Because from your research you have stated:

> LinkedIn can be an attractive SNS platform for cyber-social engineers as it holds the professional profiles of employees (Eichler et al., 2012), sometimes including their official company email addresses; credentials that can be exploited through a number of cyber-social engineering methods (Silic and Back, 2016b; Wilcox, Bhattacharya and Islam, 2014a). These attacks are typically launched over four phases, as presented in the next section.
> The scarcity principle was used, for instance, in a recent incident as reported in Independent.ie (2017), when a social engineer posted a bogus job vacancy on LinkedIn with a link to apply. The job vacancy stressed that applicants must apply within a limited timeframe.
>
> Quiel (2013) explains the 'social proof principle' as being used when a cyber attacker acts as a self-proclaimed expert in cybersecurity, purposely to connect with actual IT experts. This method enhances the trustworthiness of their profile, as the more people the attacker is connected to, the more 'social proof' it provides that the fake account is real. This also allows the attacker to benefit from the 'like principle', as we tend to trust people who are like us.
>
> Similarly, the 'authority principle' is used by social engineers to create profiles impersonating someone with a high organisational status, and this can also influence users (Frumento et al., 2016; Khanna, 2016)
> Finally, 'reciprocity' is a strong social norm that urges us to repay others for what we have received from them. This principle is used by social engineers in SNS when they offer a favour in advance of the attack to increase compliance (Algarni, 2016). This can encourage users to click on a malicious link (Quiel, 2013).
>
> The existing literature on the utilisation of these principles in the context of IT security does not show if they can be empirically tested. Studies have used these principles to identify the psychological concepts that explain a situation of influence, such as to raise sales in the marketing domain (Cialdini, 2001; Gneezy, 2017; Lystig Fritchie and Johnson, 2003), or as persuasion for various social behavioural changes (Seethaler and Rose, 2003; Jacob, Guéguen and Boulbry, 2018). Algarni (2016), however suggests that Cialdini's principles are not sufficient for examining an individual's susceptibility; he applies constructs of source credibility to see how, and to what extent, individuals' judgements are influenced by the encountered source when they are exploited for malicious attacks. Caldini's principles were used by Algarni et al. (2014) as guidance to design role-play experimental attacks.
>
> In the online context, Corritore, Kracher and Wiedenbeck (2003), Wang and Emurian (2005), and Albladi and Weir (2017) highlight that the level of trust can vary between individuals and in different contexts. They also suggest that the likelihood of an individual trusting another over the internet can vary,

2.2 Personal Disposition

With regards to personal disposition as its sub factors:

1. Risk perception

2. Willingness to assume risk on Linkedin

3. Perceived Control of Information Privacy Risk

4. Computer Self-Efficacy

I think you should just change the wording of the scale.

(1) – Strongly Disagree

5 | Page

2.5 Social engineering approaches

The concern that you have been having is if the susceptibility scale actually measures susceptibility on LinkedIn.

The easiest way to determine that is if the participant indicates he or she has been a victim since he or she created a LinkedIn account.

Therefore you will measure whether the individual has been a victim of cyber-social engineering by asking them if they ever have. You can incorporate that into the survey or ask in the qualitative interviews. If you ask it in the interviews however you will need to have some sort of identification to link the survey results to the interview.

I would use those images in the qualitative approach instead and make use of the TAT (Thematic apperception test) type of approach. Where you ask them "what think of the image" and you present a whole bunch of images and gauge and record their responses using an electronic recorder or video, with their consent of course. Since you would be able to capture more nuance from what they say which would give you more insight into the heuristics they use in judging what is happening on the image to be "safe".

3. Reliability and Validity

This report will deal with two types of validity in general, namely content and face validity since it relates to initial construction of the survey and its evaluation. However construct and criterion validity will be mentioned as it is necessary to have this for the statistical analysis of the survey results.

Content validity as I have expressed before relates to the specific questions you use and how you frame those questions in relation to measuring the dimension. The way you judge content validity is by a panel of experts who evaluate each question and determine which questions they want to keep or change. I did this specifically for the Personal Disposition to security and risks of CSE victimisation on LinkedIn dimension.

Face validity isn't really a measure you can quantify, however it is important because if a survey looks legitimate then participants will be more accepting of it. What contributes to face validity that relates to wording used, spelling, grammar and the scale used. Personal preference and inexperience or experience can alter the face validity of a survey. For example for your survey I outlined the wording of the scale. I reworded the scale so that it makes more "sense" for the participant.

Right now you cannot measure construct validity. As you can only do that after you have gathered the data, checked the reliability and did a factor analysis. However you can to some degree assure it by using previous instruments that

8 | Page

Users on LinkedIn use the site for professional advancement (helpful for professional future, sharing work-related curriculum vitae posts, networking with other professional contacts, obtaining peer support from others) and, secondly, for self-presentation (providing personal credentials, introducing or telling others about oneself). These motivations can be misused by a social engineer masquerading as an employer (Misra and Goswami, 2017), a job seeker or a colleague.

Therefore any individual who engages in a high degree of professional development and self-presentation behaviour exposes herself or himself to cyber social engineering.

2.1.1 Self-presentation

Where self-presentation as you define it as is:

Self-presentation is a form of information disclosure (Bronstein, 2013). As such, individuals who are self-presentation driven are keen to initiate interactions and build relationships.

For self-presentation:

- Providing personal credentials
- Introducing or telling others about oneself

2.1.2 Professional development:

- Helpful for professional future
- Sharing work-related curriculum vitae posts
- Networking with other professional contacts,
- Obtaining peer support from others

Because you only provide your credentials once when you create your account, you should think about using two scales. Firstly a binary scale and a frequency scale

Where the binary scale measures how much information you have put online in relation to your self-presentation. Since the more information you put online the more cyber social engineers can gleam information and create a more compelling

With frequency scale indicating the frequency of professional development you engage in online, since the more active you are the more likely it is that you will be exposed to cyber social engineering.

As a result I think you should measure the frequency of activity and use the following scale.

(5) - Always
(4) - Often
(3) - Sometimes
(2) - Rarely

- Nationality

2.4.2.2 Organisation

- Manager level
- Receiving training to identify threat in the IS environment
- Specifically received training about the online threats involved using a SNS

In relation to your research

For businesses that increasingly rely on remote collaboration, online channels of communication, online platforms and tools for virtual communication, CSE poses a serious threat to the security of their organisation's data centres. This corresponds with the growing trend towards BYOD, or 'bring your own device', which is linked by Krombholz et al. (2015)

Combining online tools in both private and business environments provides cyber attackers with many new opportunities for malicious operations

While employees are periodically made aware of security issues and given training programs to address potential threats in IS environments, the training does not include the online realities of threats involved when using SNS at work

Conversely, organisations that have not yet experienced serious cyber-attacks and have not trained their employees about social engineering threats will end up having different cyber-risk beliefs, and, consequently, poorer risk perception (Algarni et al. 2014).

Furthermore, D'Arcy, Hovav and Galletta (2009) and McBride et al. (2012) emphasised the significant threat to organisations from employees' failure to observe good information security practices and a lack of compliance with mitigation actions to limit exposure to cyber threats. Statistically, 92% of the data breaches within the public sector were due to social breaches (Verizon, 2018), in which policies were bypassed by unwitting employees. They highlight the importance of employees being periodically kept updated and informed of new CSE methods to refresh their mind on information security awareness; as successful cyber-attacks are associated with "behavior or an attitude of an organization and/or its members towards protecting the organization's information assets" (Alzamil, 2012, p.38).

In addition, a study by Pitesa and Thau (2013) found that individuals who are in powerful positions, such as 'managers' within an organisation, are generally more able to thwart social influence techniques than those who are in lower positions, 'employees/subordinates'. They attribute this to the higher-powered individuals typically being more able to act on their own personal preferences, which, in turn makes them less likely to submit to persuasive and influential messages. Conversely, less powerful individuals need to depend more on outsiders, which makes them more susceptible to scams. According to Alzamil (2012), who carried out a comparative study of managers and employees in relation to the influence of InfoSec awareness on their daily business, there is a lack of training and policy enforcement in Saudi organisations

6. The Paper based Survey

Breakdown of questions:

Questions	Constructs being measured
3 to 7	Demographics and Contextual Factors
8 to 27	Personality traits
28 to 47	Risky Habitual behaviours Self-Control - Hadlington (2017) Risky Cybersecurity behaviour Scale
48 to 52	Risky habitual behaviour - Levels of Engagement
53	LinkedIn usage at work
54 to 57	Risk Perception
58 to 61	Willingness to assume risk on LinkedIn
62 to 71	Preceived Control of informaiton Privacy Risk
71 to 83	Susceptability to Cyber Social Engineering Vitcimisation on LinkedIn - Self-Presentation
84 to 93	Susceptability to Cyber Social Engineering Vitcimisation on LinkedIn - Professional Advancement
94 to 96	Cyber social engineering awareness (Contextual Factors)
97 to 98	Victim of a cyber social engineering

Survey Expert Review

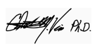
My name is Dr. Christopher M. Via, and I have reviewed and consolidated the survey contents provided to me by Mr. Alotaibi. My Undergraduate, Graduate, and PhD degrees are from Embry-Riddle Aeronautical University in Daytona Beach, Florida. I have instructed courses on Intro to Human Factors Psychology, Cognitive Psychology, Memory and Cognition, Human-Computer Interaction, and Abnormal Psychology. I have spent the greater part of my academic and post-academic career designing, teaching, administering, analyzing, validating, and reporting on surveys within the academic community as well as for small and medium-sized businesses.

I have reviewed the survey for Mr. Alotaibi and assessed it for construct validity. Small changes were made to some of the answer options as they were vague in nature and could have been a source of confusion for participants. Some answer options appeared to measure multiple things at once, and as such, changes in punctuation were implemented to address the dissonance between the researcher's intent and the participant's receipt.

Regarding the pictures at the end of the survey, several discussions were had between Mr. Alotaibi and I to determine what, in the world of all that is possible, were the actions that our participants could face. In the end, I determined that it would be more efficient for him to measure susceptibility by asking participants a self-report question.

Moving forward, my concern with this research project is the length of the questionnaire. An ideal survey should have 8 or fewer matrix type questions. Of course, breaking the matrix questions apart with some smaller dichotomous answer options or multiple-choice options would be ideal to prevent "Christmas-Treeing" in which participants click straight down or select random answers to complete the survey faster. Unfortunately, this simply isn't possible. As it stands, the survey currently will take participants about 15 minutes to complete.

Respectfully,
Dr. Christopher M. Via



APPENDIX G

وزارة العمل
والتنمية الاجتماعية
المملكة العربية السعودية

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

الي من يهمه الأمر

السلام عليكم ورحمة الله وبركاته

تفيد وزارة العمل والتنمية الاجتماعية ان المرشح للدكتوراه/ محمد خالد ناصر العتيبي سجل مدني رقم/[redacted] والمبتعث من قبل وزارة التعليم قد انتهى من جمع البيانات المطلوبة من قبلنا لدراسته الميدانية حيث انها تتعلق بمجال بحثه في الامن السيبراني عبر شبكات التوصل الاجتماعي في مكان العمل، وذلك لمرحلة الدكتوراه في جامعة دبلن / كلية ترينتي في إيرلندا.

حيث بدأ البحث بتاريخ ٢٠١٩/١٠/٠٧م وانتهى بتاريخ ٢٠٢٠/٠١/٠٧م، وقد تم إصدار هذا الخطاب بناء على طلبه، وذلك لتقديمة إلى (الملحقية الثقافية السعودية بدبلن).

ولكم تحياتي ،،

مدير عام الإدارة العامة لتقنية المعلومات

مساعد بن عبد الله العتيبي

الختم

وزارة العمل والتنمية الاجتماعية
الإدارة العامة لتقنية المعلومات

APPENDIX H

Trinity College Dublin
The University of Dublin

Interview Protocol

Susceptibility to Cyber-Social Engineering Through LinkedIn

TCD research ethical application

Please note: each question may be modified as the research proceeds but will remain broadly alongthe lines set out.

To answer the research question:

How, and to what extent do personal characteristics and other factors play a role in an employee's likelihood of being susceptible to cyber-social engineering (CSE) victimisation when accessing professional SNSs, such as LinkedIn, in government organisations in Saudi Arabia?

Three categories of informants will be interviewed:

1. Employees/Managers working in these organisations
2. IS security Experts
3. Faculty members in educational institutions.

Do you know what cyber-social engineering on SNS is?
Have you encountered CSE on SNS? How did you identify that and what was your response? Generally, can you perceive the threat of cyber-social engineering carried out on social media on organisations? How?

I would like to get your opinions on the likelihood of employees who are working in [organisation name] becoming vulnerable to cyber-social engineering attacks when accessing LinkedIn.

How, and to what extent, can the following personal characteristics [what makes an individual who he (or she) is…] impact their risks of cyber-social engineering (CSE) attacks on LinkedIn? :

Personality Domain	*Definition*
Extraversion	*[friendly, sociable, like being with other people]*
Conscientiousness	*[Being careful and serious about completing duties]*
Openness to experience	*[Interested in trying new things]*
Agreeableness	*[Usually agreeing to what other people say without question]*
Neuroticism	*[Tending to be nervous, anxious or worried]*

Can you explain how/why each personal trait can lead someone to act in ways that risk exposing them to cyber engineering attacks? Can you think of any internal or environmental factors which encourage or make easier a mistaken judgement about a modern cyberthreat?

How, and to what extent, does employees' perception of risk play a role in influencing their exposure to cyber-social engineering when engaging with LinkedIn from their workplace?

Precisely, I would like to identify what factors (cognitive and contextual), in your opinion, can influence their perception of potential deceptive attacks carried out on professional social networking sites.

For instance, do you think nationality and culture could influence susceptibility and how a possible threat is perceived by individuals using career-oriented social networking sites (CSNS)?

[If factors are identified by the informant] How can these factors affect employees' perception of deceptive attacks or scams, such as phishing emails and fake profiles or job posts?

In your opinion, how, and to what extent, does employees' propensity or willingness to take risk impact their exposure to cyber-social engineering when using LinkedIn from their workplace? Do you think the employees' nationality could promote risk taking? For instance, do you think citizens of country X are of equally willing to take risk as citizens of country Y? Are there any factors that facilitate that type of behaviour? Do you think a risk-taker in the real world necessarily continues such behaviour online?

"Individuals who have a high level of engagement in using the internet tend to believe that they can bypass potential scams they might encounter on social media, without needing to comply with information security policies in the organisation" Do you agree with this statement? Why?

Do you think junior and senior employees are equally exposed to cyber-social engineering threats, or could the magnitude of responsibility in the work environment impact their level of computer self-efficacy and risk perception? Does such a difference which affect the level of risk for each employee? Does it affect the consequences of possible security breaches resulting from their activities?

In the era of job-seeking through online networking sites, with highly competitive credentials needed to market oneself, how do you think employees should handle their privacy settings on LinkedIn? Should they expose detailed personal and career information to attract the attention of recruiters? What criteria, do you think, should they follow prior to posting anything to protect themselves from those who exploit such information? In your opinion, what criteria should an individual consider when deciding to connect with someone on LinkedIn? To what extent do you think your colleagues look for these criteria?

What kind of information do you look for in posts on LinkedIn? What kind of information do you look for in someone's profile?
What do you look for to judge whether it's safe to give information to a person on

LinkedIn? Do you think your colleagues use LinkedIn in the same way?

From your observation, what do you think your colleagues use LinkedIn for? What type of information do you think your colleagues post on LinkedIn? Do you think they limit who can see this information, or do they leave it open to everyone?

Some studies show that men are more susceptible to CSE attacks than women. Do you think this finding is accurate and why? If you don't agree, why? Could nationality and culture play a role at some point?
Could age group have an impact?

APPENDIX I

Additional Interview questions emanated from interview pilot-stud/post statistical findings reviewed by an expert:
Q. From your point of view, how can employees' personality trait impact on their behaviors of social media/CSNS, and how their traits are rooted (i.e., environment) [ask about nationality/gender/age/work level] Q. Can these traits be the same, Online/offline? [Ask about culture differences and any possible impacting factors]. Q. Do you believe employees [can/cannot] imagine themselves to be in control of their information (privacy risk)? Why? Do people read policy and terms of SNS platforms (i.e., LinkedIn)? [based on the findings] Q. Have you had something bad happen to you in the past of what you become later to discover it was due to either not aware of the terms or responding to a malicious message? What happened? Q. What makes Saudi/Non-Saudi LinkedIn users [a job seeker] to decide how to 1) increase their network connection, 2) follow others, 3) participate or refrain to like, comment. Endorse, reshare a post, etc.? why?

APPENDIX J

Study Hypothesis	Findings (Bivirate)	Significance Level	Findings (Multivirate)	Significance Level	Factors Removed	Factors Remaining
Personality Characteristics						
Employees who express ***high levels of conscientiousness*** *are* ***less*** *susceptible* to CSE victimisation on LinkedIn than are those who express **low levels of conscientiousness.**	A 1-unit increase, decreases the odds of being susceptible to CSE victimisation by **39.7%**	(*p* = .00)	A 1-unit increase, decreases the odds of being susceptible to CSE victimisation by **56.7%**	(*p*= .00)		**Conscientiousness**
Employees who express ***high levels of extraversion*** *are* ***more*** *susceptible* to CSE victimisation on LinkedIn than are those who express l**ow levels of extraversion.**	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **51.4%**	(*p* = .00)	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **80.6%**	(*p*= .00)		**Extraversion**
Employees who express ***high levels of agreeableness*** *are* ***more*** *susceptible* to CSE victimisation on LinkedIn than are those who express **low levels of agreeableness.**	A 1-unit increase Increases the odds of being susceptible to CSE victimisation by **142.7%**	(*p* = .00)	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **151.5%**	(*p*= .00)		**Agreeableness**
Employees who express ***high levels of openness to experience*** *are* ***more*** *susceptible* to CSE victimisation on LinkedIn than are those who express **low levels of openness to experience.**	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **31.5%**	(*p* = .002)	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **42.7%**	(*p*= .006)		**Openness to Experience**
Employees who express ***high levels of neuroticism*** *are* ***less*** *susceptible* to CSE victimisation on LinkedIn than are those who express **low levels of neuroticism.**	Insignificant	(*p* = .786)	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **34.2%**	(*p*= .025)		**Neuroticism**
Disposition to Risk Factors						
Employees who express **high levels of risk perception** are **less** susceptible to CSE victimisation on LinkedIn than are employees with **low levels of risk perception.**	A 1-unit increase, decreases the odds of being susceptible to CSE victimisation by **12.9%**	(*p* = .09)			**Risk Perception**	
Employees who express **high levels of willingness to assume risk** are **more** susceptible to CSE victimisation on LinkedIn than are employees with **low levels of willingness to assume risk.**	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **21%**	(*p* = .02)			**Willingess to Assume Risk**	
Employees who ***perceive they have control over information*** **(privacy risk)** are ***less*** *susceptible* to CSE victimisation on LinkedIn than are employees who **perceive they have little control over their information.**	A 1-unit increase, decreases the odds of being susceptible to CSE victimisation by **18%**	(*p* = .03)			**Perceived Control Over Information (Privacy Risk)**	
Employees who express ***high levels of IT self-efficacy*** *are* ***less*** *susceptible* to CSE victimisation on LinkedIn than are employees who express **low levels of IT self-efficacy.**	A 1-unit increase, decreases the odds of being susceptible to CSE victimisation by **12.9%**	(*p* = .02)	A 1-unit increase, decreases the odds of being susceptible to CSE victimisation by **34.8%**	(*p* = .00)		**IT Self-Efficacy**
Habitual Behaviour Factors						
Employees with ***low levels of information security habitual behaviour*** on LinkedIn (low RHBIS score) are ***more*** *susceptible* to CSE victimisation than are those with **lower levels of information security habitual behaviour** on LinkedIn.	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **17%**	(*p* = .09)	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **27.7%**	(*p* = .056)		**Information Security Habitual Behaviour**
Employees with *high levels of engagement* on LinkedIn (RHBLE) are *more susceptible* to CSE victimisation of CSE than are those with lower levels of engagement on LinkedIn.	A 1-unit increase, increases the odds of being susceptible to CSE victimisation by **18%**	(*p* = .03)			**Level of Engagement**	
Employees with *high frequency of SNS use* on LinkedIn are *more susceptible* to CSE victimisation than are those with lower frequency of SNS use on LinkedIn.	Insignificant	(*p* = .52)			**Frequency of SNS Use**	
Demographic Factors						
Older employees are less susceptible to CSE victimisation on LinkedIn than are younger employees.	Odds of being susceptible to CSE attacks on LinkedIn are **82% lower for those aged 62 and over** compared to those **aged 18-28**, while other age groups are insignificantly different from the baseline group (reference category 18-28 years old).	(*p* = .01)	Odds of being susceptible to CSE attacks on LinkedIn are **95.5% lower for those aged 62 and over** compared to those **aged 51-61 were lower by 84.1%**, while those **aged 40-61 were lower by 76.6%**. And those **aged 29-39 were lower by 73.8%,** (compared to reference group 18-28)	(*p*=.00), (*p*=.06), (*p*=.07), (*p*=.03)		**Age**
Female employees are less susceptible to CSE victimisation on LinkedIn than are male employees.	Odds of being susceptible to CSE attacks on LinkedIn are **3.15** times higher for **males** than **females** (reference category)	(*p* = .001)	Odds of being susceptible to CSE attacks on LinkedIn are **6.158** times higher for **males** than **females** (reference category)	(*p*=.00)		**Gender**
Employees in senior positions in the organisation *are less susceptible* to CSE victimisation on LinkedIn than are employees in a junior position.	Odds of being susceptible to CSE attacks on LinkedIn are **73% lower for department management/Section supervisors (level 2)** and **86% lower for top-level managers (level 3)** compared to the reference category of **the lowest-level employees (level 1**).	(*p*= .05), (*p*= .00)	Odds of being susceptible to CSE attacks on LinkedIn are **67.8% lower for department management/Section supervisors (level 2)** and **89% lower for top-level managers (level 3)** compared to the reference category for **the lowest-level employees (level 1**).	(*p*=.01), (*p*=.08)		**Structural Power / Level of Work**
The *nationality* of an employee *can increase their susceptibility* to CSE victimisation.	Odds of being susceptible to CSE attacks on LinkedIn are **75%** lower for **non-Saudis** when compared to **Saudis** (reference category	(*p*= .00)			**Nationality**	
Motivational Factors						
Users who are *motivated by career advancement* on LinkedIn *are more susceptible* to CSE victimisation than are those who are less motivated in this way.	A 1-unit increase, increases the odds of being susceptible to CSE attacks on LinkedIn by **1.048 times**	(*p*=.00)	A 1-unit increase, increases the odds of being susceptible to CSE attacks on LinkedIn by **1.031 times**	(*p*=.08)		**Professional Advancement**
Users who are *more inclined* than others *to present themselves and their credentials* on LinkedIn *are more* susceptible to CSE victimisation.	Insignificant	(*p*=.19)			**Self-Presentation**	