Jaakko Vilander

BRIDGING THE KNOWING-DOING GAP: THE ROLE OF ATTITUDE IN INFORMATION SECURITY AWARENESS

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2021

ABSTRACT

Vilander, Jaakko
Bridging the knowing-doing gap:
The role of attitude in information security awareness
Jyväskylä: University of Jyväskylä, 2021, 110 pp.
Cyber Security, Master's Thesis
Supervisor: Woods, Naomi

As the contemporary workers and computers converge, modern information systems tend to become sociotechnical rather than solely technical. This development has caught the eye of attackers who are now exploiting the human aspect, the proverbial "weakest link", instead of the hardened technical aspects of information systems, causing organizations substantial loss despite investments in cyber security. Thus, many incidents today are either directly caused or indirectly facilitated by insiders who are either lacking in information security awareness or acting contrary to their knowledge. This has provoked the term *the knowing-doing gap*.

This study examined that gap between knowledge and behaviour, why employees wilfully omit, and the role of attitude in bridging that gap. The study was conducted as a web-administered survey using the Human Aspects of Information Security Questionnaire (HAIS-Q), to which 287 participants responded. The data was analysed using linear regression, Baron-Kenny mediation, and comparison of means.

The primary results indicated that attitude is a stronger determinant for behaviour than knowledge. In the mediation analysis, results suggested that most of the influence between knowledge and behaviour is mediated through attitude. However, although knowledge was weakly correlated with behaviour, the gap effect was inverse and did thus not support the existence of a knowing-doing gap. Nevertheless, the results provide an incentive for information security professionals to focus on fostering attitudes rather than only building knowledge. Furthermore, reasons to why employees omit secure behaviour and scientifically supported recommendations for improving information security awareness are presented, which may benefit professionals in their work.

Keywords: information security, compliance, awareness, knowing-doing gap

TIIVISTELMÄ

Vilander, Jaakko
Tietämisen ja tekemisen välistä kuilua ylittämässä:
Asenteen rooli tietoturvatietoisuudessa
Jyväskylä: Jyväskylän yliopisto, 2021, 110 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Woods, Naomi

Nykyaikaisten tietokoneiden ja työntekijöiden välisen konvergenssin yltyessä modernit tietojärjestelmät voidaan nähdä ennemmin sosioteknisinä kuin pelkästään teknisinä. Tämä kehitys ei ole jäänyt huomiotta hyökkääjiltä, jotka ovat alkaneet käyttää hyväkseen tietoturvallisuuden inhimillistä aspektia, sen vertauskuvallista ”heikointa lenkkiä”, kovennettujen teknisten järjestelmien sijaan, aiheuttaen samalla huomattavaa vahinkoa organisaatioille huolimatta mittavista investoinneista kyberturvallisuuteen. Näin ollen monet tämän päivän tietoturvapoikkeamista ovat joko puutteellisen tietoturvatietoisuuden omaavien tai vastoin parempaa tietoaan toimivien työntekijöiden suoraan aiheuttamia taikka välillisesti fasilitoimia. Tämä on synnyttänyt ajatuksen tietämisen ja tekemisen välisestä kuilusta (engl. *knowing-doing gap*).

Tämä tutkimus tarkasteli tuota kuilua tiedon ja käyttäytymisen välillä, miksi työntekijät tieten tahtoen jättävät tietoturvaohjeita noudattamatta sekä asenteen roolia tuon kuilun ylittämisessä. Tutkimus toteutettiin verkkovälitteisenä kyselytutkimuksena käyttäen *The Human Aspects of Information Security Questionnaire* -kyselykaavaketta (HAIS-Q). Kyselyyn vastasi 287 henkilöä. Data analysoitiin käyttäen lineaariregressiota, mediaatioanalyysiä ja varianssianalyysiä.

Tutkimuksen päätulokset indikoivat, että asenne on merkittävämpi tekijä käyttäytymisen kannalta kuin tieto. Mediaatioanalyysissä tulokset viittasivat siihen, että valtaosa tiedon vaikutuksesta käyttäytymiseen välittyy asenteen kautta. Siitä huolimatta, että tieto korreloi käyttäytymiseen, kuilua tiedon ja tekemisen välillä ei havaittu. Tästä huolimatta tulokset tarjoavat tietoturva-ammattilaisille yllykkeen keskittyä koulutuksessa ennemmin asenteiden vaalimiseen kuin tiedon karttuttamiseen. Tämän lisäksi tutkimusraportissa tarjotaan tieteellisesti perusteltuja selityksiä sille, miksi työntekijät poikkeavat ohjeista sekä suosituksia tietoturvatietoisuuden parantamiseksi, mitkä voivat niin ikään hyödyttää tietoturva-alan ammattilaisia heidän työssään.

Avainsanat: tietoturvallisuus, tietoturvatietoisuus, tietoturvaohjeiden noudattaminen, tietämisen ja tekemisen välinen kuilu

ACKNOWLEDGEMENTS

I thank my instructor, Assistant Professor Naomi Woods of the University of Jyväskylä, for patiently assisting my efforts during this extensive process, as well as my code reviewer, Postdoctoral Researcher Oleksiy Khriyenko. Furthermore, I extend my gratitude to Professor Michael R. Webb and the Human Aspects of Cyber Security research team of the University of Adelaide for sanctioning the use of the HAIS-Q for the purposes of this study.

FIGURES

FIGURE 1 Information security awareness model (Parsons et al., 2017, p. 48) 6
FIGURE 2 Referential frame and scope of the study 7
FIGURE 3 The security - usability - functionality triad (Rahalkar, 2016) 20
FIGURE 4 Policy and compliance research and relationships (Cram et al., 2017, p. 613) 28
FIGURE 5 A RCT model for explaining policy violations (Siponen & Vance, 2012, p. 25) 31
FIGURE 6 A model of PMT (Vance et al., 2012, p.191) 33
FIGURE 7 An adaptation of the KAB model 36
FIGURE 8 The information technology learning continuum (NIST, 2003, p. 8) 40
FIGURE 9 Organizational structure, units, and personnel groups (PG) 44
FIGURE 10 Research model. 52
FIGURE 11 Descriptive statistics of the respondents 58
FIGURE 12 Proportions of computer and sensitive information usage 59
FIGURE 13 Density distributions and scaled mean ISA scores per variable 63
FIGURE 14 Plotted knowledge and behaviour scores with regression line 64

TABLES

TABLE 1 Information security behaviour modes (Alfawaz et al., 2010, p. 53)..... 4
TABLE 2 The links between forms of extrinsic motivation, factors, and explaining theories 35
TABLE 3 Variables used to monitor compliance. Derived from Sommestad et al. (2014) 37
TABLE 4 Aspects (constructs), focus areas, and sub-areas of the study 49
TABLE 5 Development and use of the HAIS-Q (Parsons et al., 2017, p. 42)..... 50
TABLE 6 Demographic variables and their response alternatives..... 51
TABLE 7 Descriptive statistics of reliability of the constructs in the study 54
TABLE 8 Statistical tools in the data analysis per hypothesis..... 59
TABLE 9 Descriptive statistics of information security awareness by age 62
TABLE 10 Inferential statistics of demographic variables..... 62
TABLE 11 Inferential statistics of the aspects 64
TABLE 12 Regression and mediation model in three blocks (standardized coefficients) 65
TABLE 13 Reasons why respondents would leave information security incidents unreported 66
TABLE 14 Reasons why respondents would omit information security policy 66
TABLE 15 Elements of success in an ISAP..... 73
TABLE 16 Elements of success in awareness training 74

TABLE OF CONTENTS

ABSTRACT
TIIVISTELMÄ
ACKNOWLEDGEMENTS
FIGURES
TABLES

1 INTRODUCTION 1
1.1 Information security awareness 1
1.2 The knowing-doing gap and the KAB model 4
1.3 Research aim and scope 6
1.4 Thesis outlines 8

2 THE SOCIOTECHNICAL INFORMATION SYSTEM 9
2.1 Theoretical foundations of the sociotechnical information system 9
2.1.1 Differences between the social and the technical subsystems 11
2.2 The social subsystem and information security 12
2.2.1 Who? Threat landscape of the social subsystem 13
2.2.2 Why? Vulnerability landscape of the social subsystem 17
2.2.3 How? Risky behaviour and focus areas of the HAIS-Q 21

3 IMPROVING INFORMATION SECURITY COMPLIANCE 28
3.1 Deterrence Theory 29
3.2 Rational Choice Theory 31
3.3 Protection Motivation Theory 32
3.4 Self-Determination Theory 34
3.5 The Theory of Planned Behaviour: the KAB model 35
3.5.1 Raising awareness 38

4 DEMOGRAPHIC FACTORS IN INFORMATION SECURITY AWARENESS 43
4.1 Organizational factors 44
4.2 Individual factors 46

5 RESEARCH METHODOLOGY 48
5.1 Measures 48
5.1.1 The HAIS-Q 48
5.1.2 Demographic variables 51
5.1.3 Open items 52
5.1.4 Reliability and validity 53
5.2 Participants 57
5.3 Procedure 59

6 RESULTS 61
6.1 Effects of demographic variables on awareness 61
6.2 Effects of knowledge and attitude on behaviour 64
6.2.1 Quantitative content analysis: reasons for non-compliance 66

7 DISCUSSION 67
7.1 Comparison 67
7.2 Implications 69
7.2.1 Demographics 69
7.2.2 Reasons for non-compliance 70
7.3 Recommendations 72
7.4 Future research 76

8 CONCLUSION 78

1 INTRODUCTION

> "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" (Bruce Schneier)

At the dawn of the decade, economic leaders of the world gathered at the World Economic Forum to contemplate the potential hazards of the coming ten years. Perhaps to the surprise of few, the sphere of information and communication technology, or *cyber* in layman's terms, was anticipated to pose the greatest challenges for humanity, only after the extinction-level threat of global warming (Zwinggi, Pineda, Dobrygowski, & Lewis, 2020). To be specific, information security is the disruptive factor that few businesses can afford to overlook. Ultimately, information has the potential to supersede capital as the most important factor of production (Capgemini, 2012). Therefore, success in financial environment will require success in the cyber environment as well and the protection of the most irreplaceable asset of many companies: data (Van Niekerk & Von Solms, 2010). To safeguard their information assets in the coming decade, successful leadership will need to incorporate best practices in both management and strategy to cultivate information security awareness and culture to create a fully functioning, holistic information system (Zwinggi et al. 2020; Parsons et al., 2017). Fortunately, SANS (2019) foresees the third decade of the 21st century as the era of *information security awareness*.

1.1 Information security awareness

In the evolving information environment, widespread information security awareness (hereafter also awareness) is generally a key contributor to successful information security (Furnell & Clarke, 2012; D'arcy, Hovav, & Galletta, 2009; ISO/IEC, 2018). It has been proposed as an acknowledged fact that awareness is the most significant mitigating factor of security breaches in organizations (Safa, Von Solms, & Flutcher, 2016; see also Sherif, Furnell, & Clarke, 2015). In fact, it

has recently been shown that improving information security awareness is one of the most cost-effective ways of diminishing the information security risk associated with insiders within an organization (Ponemon, 2020). Information security awareness has two dimensions: knowledge and behaviour (Parsons et al., 2017). The first refers to the extent to which employees, or insiders, comprehend the guidance outlined in organizational policy and secure behaviour in general (Bulgurcu, Cavusoglu, & Benbasat, 2010) and the latter to the extent to which they comply in accordance with that comprehension (Kruger & Kearney, 2006, p. 289). Conversely, the lack of information security awareness is at the root of insiders' mistakes (Safa, Von Solms, & Furnell, 2015b).

Consequentially, the insider threat, the threat posed by individuals within an organization who either due to inadvertence or omission fail to comply to information security policies or engage in otherwise insecure behaviour, remains one of the most prominent threats today (ENISA, 2020b). Careless and non-compliant employees cause security incidents that bear substantial costs to organizations (Johnston, Warkentin, McBride, & Carter, 2016; Ponemon, 2020). In 2020, the average insider-caused incident cost 11.45 million in EUR to the organization (Ponemon, 2020). As such, deviant acts of employees represent a significant threat to organizations (PWC, 2012; ENISA, 2020b; Peltier, 2016; FireEye, 2020; Landman, 2019), which has earned humans the proverbial title of the "weakest link" of information security (see e.g. Schneier, 2015, p. 255; Furnell & Clarke, 2012; Guo, Yan, Archer, & Connelly, 2011; Vroom & Von Solms, 2004; Gonzales & Sawicka, 2002; Cox, 2012; Ifinedo, 2012; Andress, 2014, p. 120).

From another perspective, however, humans can be viewed as the unwilling first line of defence. In fact, while the cyber security industry has placed emphasis on hardening the technical aspects of information systems, the social aspect has become disproportionally weak in comparison and thus pushed humans to the frontline of information security (Ifinedo, 2012; SANS, 2018; Harris & Furnell, 2012; Gardner, 2014; Ponemon, 2020). This disparity is justified by the fact that human issues cannot be solved with product-based solutions and are harder to implement and evaluate (Furnell & Clarke, 2012), even though organizations ought to specifically prioritize countering people-based attacks (Bissell, Lasalle, & Dal Cin, 2019). Arguably, the disparity has encouraged attackers, ranging from opportunistic "script kiddies" to highly resourced state actors (Goodman, 2016; DCDC, 2016; Schneier, 2015; Laari, Flyktman, Härmä, Timonen, & Tuovinen, 2019), to leverage the human aspect to infiltrate the technical system, which can in turn be observed as increased social engineering (Bissell et al., 2019; Verizon, 2019). Moreover, by attacking the human person, other layers of protection, even encryption, can be bypassed – with merely one simple click (Kaspersky, 2020; Schneier, 2015; Andress, 2014).

However, the notion of the "weakest link" might be obsolete or counterproductive at worst. The human factor pervades most information systems and can never be exhaustively eliminated from the equation (Kaufman, Perlman, & Speciner, 2002). In addition, all people are susceptible to human error and coercion. At worst, remarks like "the weakest link" or "you can't patch stupid" build

a culture of indifference towards challenges that are likely solvable. Rather than adopt such a fatalistic stance, the root causes of non-compliance and the right steps to improve information security compliance (hereafter also compliance) can be uncovered. Previously, as a response to such neglect of the human aspect as a part of the overarching work environment, research in organizational work design introduced the notion of the sociotechnical system (Bostrom & Heinen, 1977).

Therefore, adopting a sociotechnical view of information systems might help understand underlying issues. A sociotechnical system is one that considers the social and technical aspects of a holistically (Trist & Bamforth, 1951). From this perspective, information security is neither, contrarily to how it might be intuitively viewed, solely a technological issue. When we speak of the information system, we often envisage the technical aspect: computers, routing devices, cabling, networks, and the Internet. Nevertheless, humans, the operators of the computers, can be perceived as processors of information as well (Norman, 1969), perhaps as much as computers and, consequentially, they remain central figures in maintaining information security (Kaufman et al., 2002). Moreover, while adopting the sociotechnical perspective, interest lies specifically in what occurs when the technical and the social interact (Lee, 2001). This interest was initially raised when the foundation of sociotechnical theory was laid by Trist & Bamforth (1951), who made a paradoxical observation within the coal-mining industry: despite enhanced technology and improved working incentives, productivity was on the decline. The conclusion was that the social and technical aspects of labour were incompatible in a way that had an adverse effect on work.

Similar paradoxical observations can be made within the field of information security. In fact, the paradoxes are many-fold. Firstly, on the macro level, although organizations in the private sector are steadily growing their investments in information security on a yearly basis (Gartner, 2020; Ponemon, 2020), information security is on the decline, both in terms of the amount of information security incidents and the cost of a single data breach (Bissell et al., 2019; IBM, 2019). On the meso level, despite organizations are taking different managerial initiatives to improve information security compliance, getting employees to comply remains one of the most strenuous tasks within information systems security (Warkentin & Willison, 2009; Hwang, Kim, Kim, & Kim, 2017; Hagen, Albrechtsen, & Hovden, 2008). Finally, on a micro level, people tend to seek ways to circumvent technical security measures to their personal convenience, which is incompatible with the fact that they are in general willing to pay to secure their information (Workman, Bommer, & Straub, 2008). Also, a dilemma known as the privacy paradox arises as users often report being wary regarding privacy although they act contrarily (Smith, Dinev, & Xu, 2011). These paradoxes bear similar features to the sociotechnical dilemma established by Trist & Bamforth (1951). However, the phenomenon also bears another name.

1.2 The knowing-doing gap and the KAB model

Today, the rift that divides knowledge and behaviour is also known as the *knowing-doing gap*, a term coined by Pfeffer and Sutton (2000) in their namesake book. Essentially, the knowing-doing gap posits that people possess the necessary knowledge to act but do not behave consistently with that knowledge (Alfawaz, Nelson, & Mohannak, 2010). The central idea is that knowledge of *what* to do does not automatically result in correct behaviour; *what* is not enough. The concept was initially linked to organizational performance, but it has since been adopted into information security as well (e.g., Gundu, 2019; Workman et al., 2008).

However, as (Alfawaz et al., 2010, p. 52) have formulated, *knowing* but *not doing* is not the only mode of behaviour that can be observed, mode meaning a "manner or way of acting, doing, or being". Following the knowing-doing analogy, they proposed three other information security modes of behaviour based on the information security awareness dimensions of knowledge and behaviour. The behaviour modes are illustrated in table 1.

TABLE 1 Information security behaviour modes (Alfawaz et al., 2010, p. 53)

Mode of behaviour	Description	Example of related information security behaviour
Mode 1: Not knowing-not doing	The subject does not know the organisation's policies and does not have general security knowledge. As a result, they are not complying	Information security policy is not in place or is not properly communicated. Users are: - sharing passwords - visiting harmful web contents
Mode 2: Not knowing-doing	The subject does not know the policies and does not have knowledge but is compliant	Users are voluntarily: - reporting violations. - sharing related knowledge
Mode 3: Knowing-not doing	The subject knows the policy or has the required knowledge, but is not compliant	There is a policy in place and well communicated but users intentionally violate rules and circumvent policy
Mode 4: Knowing-doing	The subject knows the policy and has the knowledge and they are compliant	Information security at place and well communicated and users are abiding by the rules.

Nevertheless, little research has been made based on the idea that organizations, or people in general, may have a general mode of behaviour in terms of information security, besides indirect evidence that the knowing-doing gap may be a relevant phenomenon information security (Workman et al., 2008). For instance, Aytes and Connolly (2004) discovered that university students exhibited risky behaviour even though being relatively familiar with safe practices. On the other hand, while development has been made to unravel why some act contrary to their better knowledge regarding information security, some studies suffer from a score of methodological weaknesses (Workman et al., 2008). Nevertheless, the question whether this is a universal phenomenon remains up to debate and a research gap prevails. In Gundu's (2019) study involving a South African

organization, workers who had good knowledge of secure behaviour possessed a negative attitude towards policy compliance. Therefore, their actions did not correspond with the level their knowledge would predetermine, causing a knowing-doing gap. Although Gundu's (2019) results are not generalizable beyond the studied population, they prompt another understudied topic: attitude as a mediator between knowledge and behaviour.

The knowledge-attitude-behaviour (KAB) model incorporates attitude as a mediator between knowledge and behaviour (Schrader & Lawless, 2004) and highlights the importance of attitude as an antecedent for compliance (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). The KAB model is also relevant in terms of information security awareness by limning its two dimensions, knowledge and behaviour, together. While some authors view information security awareness as solely intellectual, cognitive quality[1] (Siponen, 2000, p. 31; Bulgurcu et al., 2010; Albrechtsen & Hovden, 2010), it can also be viewed from a broader perspective, as both the knowledge *and* the behaviour, and seen to bridge the divide between cognition and action by including attitude to the formula (e.g., Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2014a; Sherif et al., 2015). Thus, uniform with the KAB model, information security awareness contains three interconnected components (Pattinson et al., 2019, p. 5):

1. What a person knows about secure behaviour (knowledge)
2. How a person feels about behaving securely (attitude)
3. What a person does when handling sensitive information (behaviour)

Pattinson et al. (2019, p. 5) envelops information security awareness into an introspective question "am I doing something that may jeopardize the confidentiality, integrity, or availability of the information I am now using?". The term conscious care behaviour (as opposed to careless behaviour) is also used to depict a situation where an individual willfully considers the consequences of their actions while working with information systems (Safa et al., 2016). Therefore, in addition to being a question of knowledge, secure behaviour and compliance is also a question of attitude.

By implementing attitude, the KAB model also postulates that merely increasing knowledge does not constitute desired behaviour, attitudes must be satisfied as well (Parsons et al., 2014a; Schrader & Lawless, 2004; Gundu, 2019). Thus, the KAB model encapsulates not only information security awareness, but the knowing-doing gap as well and provides a plausible framework for some of the sociotechnical paradoxes involved in information security. Hence, according to the KAB theory, it follows that compliance can be observed only if individual attitudes harboured towards information security dilemmas are favourable, and vice versa. On the organizational, meso level, this is to say that individual compliance cannot be achieved unless organizations successfully influence attitudes (Kruger & Kearney, 2008).

[1] Siponen (2000, p. 31) describes information security awareness as "a state where individuals in an organization are aware of… their security mission".

1.3 Research aim and scope

Thus, the purpose of this study was to address the understudied topic of the knowing-doing gap, determine whether such a phenomenon could be observed, and, specifically, investigate the role of attitude compared to and as a mediator between knowledge and compliant behaviour. Another key interest was to compile viable, scientifically founded means of improve information security awareness to the use of the organizations. In addition, to explain the causes of the knowing-doing gap, the study strived to pinpoint why omissive and inadvertent behaviours occur. Hence, the research questions were formulated as follows:

1) Is there a knowing-doing gap within the organization?
2) What causes the knowing-doing gap?[2]
3) What are the roles of attitude and knowledge for the gap?
    a. How can organizations build knowledge and foster attitudes to improve information security awareness and bridge the gap?

However, as figure 1 illustrates, information security awareness and its elementary parts, knowledge, attitude, and behaviour, can be influenced through individual factors (e.g., age, work experience, or formal education), organizational factors (e.g., organizational security culture and other social factors), and intervention factors (e.g., awareness training).

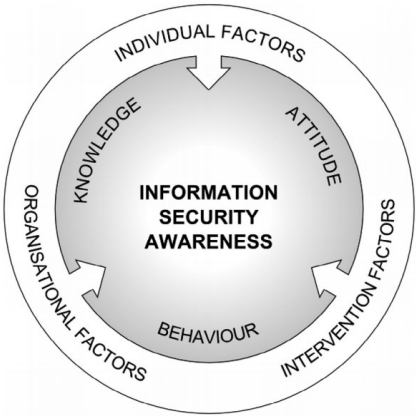

FIGURE 2 Information security awareness model (Parsons et al., 2017, p. 48)

In fact, when evaluating compliance and information security awareness, organizational factors such as demographics, nationalities, business types, and management styles must be acknowledged (Goel & Chengalur-Smith, 2010; Hovav & D'Arcy, 2012). This urges to consider variables that may influence information security awareness on a local scale, some of which may even be globally generalizable. Case research that acknowledges organizational

[2] i.e., what causes non-compliance and why do employees engage in risky behaviour.

demographics also provides the target organization with actionable information to, for instance, help the organization plan interventions (Chua, Wong, Low, & Chang, 2018). However, intervention factors (apart from the literature review in section 2) were not considered as a part of this study as it would have required a longitudinal study. Furthermore, through examining individual factors that are "global", i.e., common beyond the organization. There are multiple indications that individual factors influence information security awareness (see e.g., Chua et al., 2018). Thus, the study was influenced by the question:

4) Do demographic factors influence information security awareness?

Specifically, the demographic variables selected to represent the demographic variables were the unit and the personnel group of the respondents, which were both organizational factors, as well as age, level of formal education, and work experience (within the same employer), which represented the individual factors. The justifications and associated research gaps for these factors are discussed more thoroughly in section 4 along with a more detailed description of the target organization. Due to confidentiality issues, identifiable information regarding the organization will be left undisclosed.

Figure 2 integrates the concept of information security awareness and the relationships associated with its component parts to depict the scope of the study in its frame of reference. Furthermore, it highlights the potential knowing-doing gap and the role of attitude as a possible explanatory factor. As figure 1 showed, apart from intervention factors, the external factors that influence information security awareness are included.

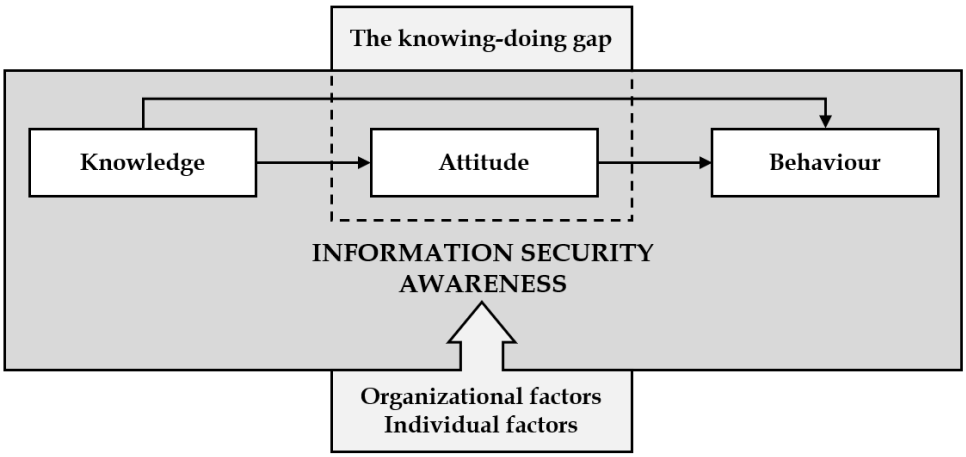

FIGURE 3 Referential frame and scope of the study

1.4 Thesis outlines

Excluding the introduction, the thesis consists of seven chapters. Chapters 2, 3, and 4 represent the literature review of the thesis. Specifically, chapter two builds on the theoretical fundaments and concepts hitherto presented. In addition, chapter 2 presents a literature review that pertains to research question 2 (reasons for non-compliance) and provides justifications for the primary measure used in the study, the Human Aspects of Information Security Questionnaire (HAIS-Q). The third chapter represents the literature review for research questions 1 (the knowing doing-gap) and 3 (attitude) and fourth chapter for research question 4 (demographics). The material for literature review was collected primarily using Google Scholar as well as using the JYKDOK database of the library of the University of Jyväskylä and the finna.fi article database. The material was chosen indiscriminately. However, during the collection process, sources evaluated at level 1 of the quality scale of the Finnish Publication Forum (2021) were emphasized, while some sources were evaluated at level 3. The literature review was supplemented with recent threat reports from information security organizations (e.g., ENISA, 2020b), standardization organizations (e.g., ISO/IEC, 2018), information security research institutes (e.g., Ponemon, 2020), and renowned threat intelligence (e.g., Crowdstrike, 2020) and other information technology companies (e.g., IBM, 2019; Verizon, 2018).

Chapter 5 aims to explain and justify the research methodology, the measures, participants, and procedures utilized in the study. It also covers limitations associated with the methodology. Furthermore, the sixth and the seventh chapter involve the presentation of results and discussion of the results, respectively, with respect to the previous findings presented in the literature review. Chapter 7 also infers the most significant implications and provides recommendations based on the findings in the literature review, specifically the fourth chapter. Finally, chapter 8 concludes and summarizes the thesis by reviewing the context, gap, findings, and the implications that follow.

2 THE SOCIOTECHNICAL INFORMATION SYSTEM

"First, we view the human as a processor of information" (Donald Norman)

Often, we lend colloquial terms from computer science to describe human nature (Gleick, 2011). Likely, such metaphors are used to make otherwise intangible concepts more intuitive and relatable to human beings. However, as the chasm between humans and computers in everyday life continues to narrow down, the understanding of the layman grows wider still from increasingly complex contemporary information and communication technology (ICT). This chasm gives rise to a lack of cyber know-how of the average worker (Clarke & Knake, 2019). Because such a divisive development likely entails problems in terms of information security in the long run, understanding the convergence of human beings and computing devices, the sociotechnical information system, is essential.

The following chapter approaches the information system from a sociotechnical perspective and demonstrates, from a psychological and historical perspective, how human beings are innate elements of information systems as well. In fact, for 300 years, until the mid-20th century, computers were humans who followed fixed rules without authority to deviate from them (Turing, 1950). In contrast, by unveiling some of the profound differences between humans and modern computing devices, this section outlines challenges that arise in terms of information security. Specifically, the section addresses the questions who deviate from the "fixed rules", why do they deviate from them, and how do these deviations constitute a risk for information security and the modern workplace.

2.1 Theoretical foundations of the sociotechnical information system

In this basic form, an information system is a system that monitors and retrieves data from the environment, specializes in the processing of the data, and presents it to generate required information (Curry, Flett, & Hollingsworth, 2006).

Information systems also include anterior metainformation to "know" how to process inputs, such as language in human memory or the scripts and programs in computers. Nevertheless, establishing a unified definition for the concept of the information system and an associated real-world entity has proven problematic (Boell & Cezec-Kecmanovic, 2015). Zachman (1987) argued over three decades ago that the notion of an information system was becoming detached from any theoretical construct or real-world phenomena and losing any semantic meaning. He noted that the definition of a particular system varies in sync with alterations in perspective: the system in the eyes of the planner is different to that of the end-user. Therefore, Zachman (1987) deduced that a single exhaustive description does not exist. Thus, the definition of an information system could best be understood as a tool that varies depending on how it is being used, as models and theories often do, being purposefully simplified versions of their respective, often unnecessarily complex real-world counterparts.

Regardless, definitions, or models, for information systems are plenty. In the arena of standardization organizations, NIST (2020, p. 405), the US National Institute of Standards and Technology, an information system is "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information", and therefore takes a functional and process-oriented approach. The ISO/IEC (2018, p. 5), the joint committee between the International Organization of Standardization and the International Electrotechnical Commission, on the other hand, view information systems more structurally and sees one as "the set of applications, services, information technology assets, or other information-handling components". These standardized definitions are important for what they include, but simultaneously, for what explicitly exclude: people – although it remains unclear whether people are implicitly included.

This is a notion that is taken into consideration by other system theorists since the idea of separating human beings and computing devices from a systems perspective has become unsustainable (Trist, 1981). While looking for contemporary information system definitions Boell and Cezec-Kecmanovic (2015) found four distinct views with which to observe the information system:

- *the technology view*,
- *the process view*,
- *the social view*, and
- *the sociotechnical view*.

Of these, the sociotechnical view provides a useful tool for the purposes of understanding the entirety of information security. Although the concept itself was conceived already in the 1950's (Trist & Bamforth; Trist, 1981, p. 7), to comprehend the magnitude of information systems in modern organizations, human-computer interaction, and its repercussions for security, adopting a sociotechnical view can help model and understand information systems security in a useful way. As it happens, the role of humans is often neglected when it comes

to controlling information systems (Ponemon, 2020; Harris & Furnell, 2012). When adopting sociotechnical standpoint, we concede that:

> "the information systems field examines more than just the technological system, or just the social system, or even the two side by side; in addition, it investigates the phenomena that emerge when the two interact" (Lee, 2001, p. iii)

Organizations exist to fulfil a certain function, which entails that people use technical artifacts to carry out certain tasks related to the organizational function (Trist, 1981). In fact, contemporary standards perceive (sociotechnical) information systems in organizations as a composition of three key features: technology, people, and management or organizational processes (NIST, 2020; VAHTI, 2014). Raggad (2010) extends the definition of the information system by stating that in addition to activities, technology, and the newly introduced people, networks and data are elementary parts of the information system. While all significantly contribute to information security, within the context of these features, people play a central role (Cheng, Li, Li, Holm, & Zhai, 2013). People are information handling components as much as computers (Raggad, 2010; Norman, 1969). However, the analogy has its limitations.

2.1.1 Differences between the social and the technical subsystems

While conceding to the fact that the social and technological subsystems are a part of the same aggregate system, it must be stressed that social (people) and technological components, in the case of information security computers, are fundamentally different. Whereas computers are complicated, difficult to comprehend but nevertheless comprehensible and predictable, humans tend to be complex. This is to say that while human beings adhere to certain regularities, logic, and rationality, they are fundamentally unpredictable and from a systematic perspective beyond the comprehension of contemporary science. As Karl Popper (1972) stated, human behaviour is highly irregular, disorderly, and reminiscent of clouds due to their innate difficulty to be predicted. To elaborate, humans do also not understand computers. The layman's understanding is often limited to the extent that they only perceive computers as "magical boxes that… get their jobs done" (Schneier, 2015, p. 255).

From a pedagogic perspective, humans and computers have vastly different ways of turning instructions into practice. The computer is a slave of its instructions; it can only comply to the instructions of its operating system, its programs, and its user, and it is impossible for it to violate them. A human being can also be instructed, with policies for example, and persuaded. However, due to freedom of choice, compliance is entirely up to the individual and a score of complex psychological behavioral patterns. People cannot simply be told to change their behaviour; "that's not how the brain works" (Zinatullin, 2016, p. 84). Moreover, computer instructions can be stacked nearly endlessly without suffering a decline in performance. On the contrary, humans have a much lower cognitive processing capacity and need clear and simple guidelines to retain a high level of

capability and compliance (Krol, Moroz, & Sasse, 2012; Gundu, 2019). Sharing cognitive resources across several tasks simultaneously is encumbering and stressful, whereas computers do so with diligence. Unlike computers, people need to be incentivized and motivated.

Other differences in terms of information processing between computers and humans include storage capacity, data transmission capability and speed, memory and data loss, scalability, connectivity, and updateability, to mention some (Harari, 2018, p. 38). Computers are also not singular in the same sense that people are. It is easy to connect computers into a dexterous network, control, and update when the need occurs, while humans, oppositely, are not as easily "connected" and are even harder to "update" (Leidner & Kayworth, 2006; Lacey, 2010). Still, the human factor pervades most information systems and can never be exhaustively eliminated from the equation (Kaufman et al., 2002).

Nevertheless, due to their pervasiveness and the inevitable collision, it is tempting to juxtapose human beings and computers. For instance, SANS (2018) speaks of the human "operating system", as opposed to the software installed on computers, which both store, process, and transmit data. Analogies between the human being and the modern computer architecture can be traced back to the cognitive revolution, also known as the informational turn, which, unsurprisingly, took place in sync with the development of the first transistor-based and circuit-integrated computers in 1950–1960 (Gleick, 2011; Säljö, 2004). This revolution laid the foundation to cognitive science, combining psychology, computer science, and philosophy in one discipline (Gleick, 2011; Säljö, 2004). Thus, it would seem only natural that cognitive science, and perhaps psychology as well, with their complex research subject, the brain, borrowed their concepts from the more tangible field of computer science. The brain was a "processor" and "storage" of information, people were described to "handle" information and "access" and "retrieve" it on demand from their "long-term" and "short-term" memory (Säljö, 2004, p. 53). As Donald Norman (1969, p. 3), one of the pioneers of American cognitivism, stated: "first, we view the human as a processor of information." Perhaps, since our technological solutions are engineered by our brains, it is only fitting that these technological innovations should be regarded as part *of* it, not apart *from* it – two sides of the same coin that is the sociotechnical system.

2.2 The social subsystem and information security

> "If you don't know the threat, how do you know what to protect" (Kurt Haas' first law)

Three fundamental concepts associated with information security are threats, vulnerabilities, and risks. In addition, an aggregate term commonly used to limn the arsenal of attacks and attackers in relation to a system's information security is the *threat landscape* (Schneier, 2015). Congruently, the *vulnerability landscape* depicts features of the system that an attacker can exploit to their benefit. *Risk* expresses the effect of uncertainty on security and, thereafter, the potential that

threats will exploit vulnerabilities in an information system (ISO/IEC, 2018). Since security is threat-oriented, understanding the threat landscape of a system, vulnerabilities, and risks, is a prerequisite for securing it (NIST, 2020).

This section examines part of the threat landscape, the attackers, or threat actors, of the social subsystem as well as the vulnerability landscape of the human aspect, risks associated with unsecure behaviour and attacks risky behaviour increases susceptibility to. Specifically, this section answers three critical questions relevant to the knowing-doing gap:

- *Who* the individuals are that constitute the inside threat and the knowing-doing gap,
- *Why* those individuals succumb to non-compliant behaviour, either inadvertently or through omission, and
- *How* such behaviour increases risk to the organization by exposing information systems to attacks by threat actors.

Importantly, the "why" question also reviews literature to answer research question 2, *why* individuals consciously omit secure behaviour or inadvertently fail to comply. In addition to outlining risky behaviour, the "how" question answers *how* information security awareness can be measured by justifying the measurement items used in this study. Namely, this part of the subsection lists user behaviour associated with the seven focus areas[3] of the HAIS-Q and exemplifies how such behaviour is relevant in terms of the contemporary threat landscape.

2.2.1 Who? Threat landscape of the social subsystem

> "Only amateurs attack machines; professionals target people." (Bruce Schneier)

The term threat is commonplace among information security-related discourse. NIST (2020, p. 424) defines a threat, very much like ISO/IEC (2018), as "any circumstance or event with the potential to adversely impact… [an organization] through a system via [various effects]". The Internet Engineering Task Force (IETF, 2007, p. 155) continues by adding that threats may be inadvertent or intelligent. Intelligent threats are essentially threat actors (sometimes also agents), beings that intentionally seek to exploit vulnerabilities due to a range of motives (NIST, 2020, p. 422). Threats and threat actors can be divided to either external, the outsider threat, or internal, the insider threat (IETF, 2007, p. 22; Loch, Carr, & Warkentin, 1992).

Outside threat actors include nation states, vandals, hacktivists, criminals, terrorists, and patriotic hackers – even businesses are today among the principal sources of threat (Laari et al., 2019; DCDC, 2016; Schneier, 2015). While outsiders are not within the scope of this study, they are noteworthy in the sense that they are the primary source of threat that can leverage unwary insiders for malicious

[3] These are password management, email use, Internet use, social media use, mobile devices, information handling, and incident reporting

purposes. Thus, people can also form an attack vector, an initial route for an attacker to form contact with the target, at the behest of the outside threat (DCDC, 2016). To circumvent solid organizational cyber defences, the attacker uses the unhardened insider as a "crowbar" to gain access to the system (Kaspersky, 2020). Each year threat actors refine their use of the human aspect rather than relying on technical activities and focus their efforts on people over the technical subsystem, simply because it generally requires less effort (Proofpoint, 2019). In fact, recent years has seen a surge in people-based attacks (Bissell et al., 2019). According to Verizon (2019), social engineering as a part of data breaches rose from 17% to 35% and the human person as an intermediary target from 19% to 39% between 2013 and 2018.

Attacks that leverage the human aspect are known as *social engineering*, a hacker term for deceit. In traditional terms, the social engineer is a con artist. It entails subtly persuading an unwitting target person to do the bidding of the hacker (Schneier, 2015). In short, social engineering is "the art of getting users to compromise information systems" (Krombholz, Hobel, Huber, & Weippl, 2015, p. 114). Social engineering includes the pretence of possessing legitimate access to the information (Security Committee, 2018). It is particularly precarious since it bypasses all technological forms of intrusion prevention: network security, host security, and even cryptography (Schneier, 2015; Proofpoint, 2019).

Krombholz et al. (2015) categorize social engineering attacks into five distinct approaches:

- *Physical approaches*, such as dumpster diving or shoulder surfing,
- *Social approaches*, such as phishing emails,
- *Reverse social engineering*, for instance, causing a technical problem and then calling from "tech support",
- *Technical approaches*, such as gathering data from open sources, and
- *Sociotechnical approaches*, that combine several of the above.

Social engineering is also often an enabler for technical forms of attack (DCDC, 2016). Combined with zero-day vulnerabilities, social engineering is a tactic favoured even by state-sponsored actors with formidable technical aptitudes (Krombholz et al., 2015; Kaspersky, 2020).

According to ENISA (2020b), the European Union Agency for Cybersecurity, the insider threat can be divided into five distinct categories:

- *Careless workers*, or inadvertent insiders, who violate policy,
- *Insider agents* who steal information at the behest of a third party,
- *Disgruntled employees* who want to damage their organizations,
- *Malicious insiders* who use their credentials for personal gain, and
- *Feckless third parties* who compromise information security via impostor accounts or stolen credentials.

Furthermore, ENISA (2020b) has three different subcategories for malicious insiders (agents, disgruntled employees, and those out for personal gain), includes credential thieves that merely utilize stolen credentials, and, most importantly, does not accommodate a category for omissive individuals. Therefore, on a higher level of abstraction, the insider threat can be thought to be comprised of three categories, namely:

- *Malicious insiders*,
- *Inadvertent insiders*, and
- *Omissive insiders*.

While the malicious insider poses a serious threat, inadvertent and omissive insider do not per se constitute a threat. Rather, they pose a risk that contributes to the manifestation of a threat. NIST (2020, p. 414) defines, in line with other common definitions, that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event" and typically determinable by the *impact* of the circumstance or event unfolding and the *probability* that it occurs. Therefore, one can also evaluate the insider threat from a risk perspective by assessing probability and impact.

In terms of probability, Proofpoint (2019) reports that all but 1% of attacks observed made use of technical system vulnerabilities; the rest targeted the social subsystem. However, though this remains unclear, these numbers might represent attempted attacks not successful security breaches. FireEye (2020) reports that only 1% of targeted attacks included a malicious insider, although this figure does not include inadvertence or omissive behaviour. Nevertheless, in the scientific community, researchers claim that most cyberattacks are progressed through human error (Khan, Sawhney, Das, & Pandey, 2020; Schultz, 2005; Wood & Banks, 1993). From a more local perspective, Silvers (2017) has estimated that a three out of four employees engage in risky behavior in the cyber domain.

There is also the question how much of the insider threat is caused by each threat category. IBM (2019, p. 30) concluded that the majority (51%) of data breaches in 2019 were due to malicious attacks, whereas human error accounted for 24%. Albeit the sample is small, it illustrates that disparities exist. According to Ponemon (2020), 23% of all insider-induced incidents were due to malicious insiders, i.e., persons seeking personal gain, agents, or disgruntled employees (ENISA, 2020b). Another 14% were due to credential thieves, imposters who had stolen credentials for illegitimate entry. The rest, some 62%, pertained to employee or contractor inadvertence (Ponemon, 2020). Some researchers agree that insider activity is seldom malicious in nature (Furnell & Clarke, 2012).

However, in terms of impact, the insider threat is more clearly quantified. The average insider-perpetrated data breach in 2020 cost 11.45 million in EUR, although costs resulting from inadvertence were not as steep as those resulting from the malicious insider (Ponemon, 2020; IBM, 2019; see also Harris & Furnell, 2012, p. 13), likely due to differences in intent. In fact, breaches due to malicious attacks were up to one-fourth more costly than those caused by human error or inadvertent insiders (IBM, pp. 6–7). When an insider incident occurs, up to a third

of costs are spent on containment alone (Ponemon, 2020). In addition to financial costs, reputational damage bore an even greater effect on organizations afflicted with an insider attack, the cumulative effect of both soaring to 65% (Egress, 2019).

With potentially high probability and high impact, the threat posed by insiders as whole is real. Polled business executives themselves stipulate that accidental leaks of confidential information and insider attacks bear the greatest impact on organizations (Bissell, Lasalle, Van Den Dool, & Kennedy-White, 2018; Bissell et al., 2019). The threat of insiders in business is widespread and has risen in recent times; all types of insider threats and risks are increasing, especially credential theft (FireEye, 2020). Large instances are especially affected as organization size positively correlates with insider incidents, being the most salient with the largest organizations (Ponemon, 2020; Bissell et al., 2019).

While cases might come rarely[4] (Peltier, 2016; FireEye, 2020), the scenario of the *malicious insider* bears grave destructive potential as insiders usually have clearances and knowledge of the system otherwise left unknown to outsiders, especially in organizations with open trust models (FireEye, 2020). The very definition of the attacker on the inside refers to an individual working in an organization who uses legitimate authority for illegitimate gain (Padayachee, 2012). Past employees and third-party contractors are also considered malicious insiders (FireEye, 2020). Malicious insiders are spurred by various motives: money, ideology, and revenge, but also coercion and ego (Watts, 2018; FireEye, 2020).

As such, with low probability but high impact, malicious acts of employees represent a significant threat to organizations (PWC, 2012). Of the fifteen most popular threats in 2020, insider attacks were ranked ninth by ENISA (2020c). Disgruntled past or current employees or third-party contractors might, for instance, delete data, plant malicious code, or purely sabotage hardware (Peltier, 2016; FireEye, 2020). Notorious examples from the arena of national security are plenty although cases are also ample in the private sector (Landman, 2019) but seem to rarely hit similar headlines. Trends that arise from recent insider events include:

- *Extortion*, the threat of compromising information security unless demands, often monetary, are met,
- *Espionage*, the theft of vital or valuable intellectual property,
- *Asset destruction*, by physically or logically influencing the information system, and
- *Workplace stalking,* where insiders illegitimately view sensitive data or steal co-worker credentials for malign purposes (FireEye, 2020)

Moreover, the *inadvertent insider* continues to pester organizations by causing undue risk, security incidents, and costs by carelessly violating information security policies (Johnston et al., 2016; Ponemon, 2020). Some argue that the key threat, no less, is the employee, who due to inadvertence fails to comply with organizational policy or standards and engage in secure behaviour (Siponen, Pahnila, & Mahmood, 2007). Inadvertently caused incidents are also known as

[4] FireEye (2020) reports that 1% of targeted attacks involved a malicious insider

behavioural information security incidents (Bauer & Bernroider, 2017), denoting the connection of the issue to behavioural psychology. Inadvertence can be perceived as a matter of accident but more commonly inadvertence is caused by lack of knowledge (Furnell & Clarke, 2012). However, the fact that inadvertent incidents are caused by carelessness or lack of knowledge does not eliminate that individuals have the potential to cause substantial harm to the organization since they possess broad and legitimate access (Gundu, 2019; Padayachee, 2012). Even a minor act of non-compliance can contribute to major consequences and thus even inadvertent insiders can pose substantial threat. It also appears that information security violations are very mundane: leaving computers unlocked and malpractice concerning passwords are among the most common risky behaviours, even amongst information security experts (Siponen & Vance, 2010). Moreover, employees have been found to under the assumption that anti-virus software is infallible and that pdf files are always trustworthy, opening them despite warnings (Krol et al., 2012). This highlights the reason why inadvertence constitutes such risk and why inadvertence is apt to inspire derogatory rhetoric towards the human aspect and the proclamation of the "weakest link".

Omissive insiders are of particular interest in terms of this study. The concept of omissive behaviour implies that the individual knows how to act but still decides to act otherwise, in other words, omits (Cox, 2012; Gundu, 2019). Even if omission may intuitively appear extremely culpable, there are ethical principles that easily endure a formal, normative transgression (Siponen & Iivari, 2006). Nevertheless, the dilemma of omission is at the nexus of the knowing-doing gap (Pfeffer & Sutton, 2000). As opposed to individuals who simply lack the knowledge to comply, workers that are aware of the risks and mitigations, but still act otherwise, pose a greater concern. The issue with these individuals is often deemed motivational but may prove many-fold and require further understanding of human psychology, being consequentially more difficult to tackle (Furnell & Clarke, 2012).

Therefore, the following subsection considers psychological peculiarities, or vulnerabilities in cyber security terms, that not only make humans susceptible to inadvertence but also cause omissive behaviour. Moreover, the subsection addresses possible ethical justifications and answers *why* people a willing to omit, as denoted in research question 2.

2.2.2 Why? Vulnerability landscape of the social subsystem

A vulnerability is a "weakness that can be exploited by one or more threat [actors]" (ISO/IEC, 2018, p. 11; see also NIST, 2020, p. 423). A vulnerability is not necessarily a negative quality; it might be an intentional, built-in feature that only becomes adverse upon exploitation. Any system, technical, social, or otherwise, possesses vulnerabilities that can be exploited to the disadvantage of the system. Vulnerabilities related to the social subsystem can be classified into vulnerabilities pertinent to *inadvertent behaviour*, aspects that threat actors may capitalize on,

and vulnerabilities associated with *omissive behaviour*, factors that enable the knowing-doing gap to arise.

Inadvertent behaviour

Perhaps the most logical causes for inadvertent violations are fundamentally human: unconsciousness and carelessness, i.e., not knowing or not being cautious enough (Safa et al., 2016). A lack of knowledge might manifest in insufficient knowledge of regulations, failure to understand the logic behind them, or failure to appraise the threat that is caused by ignoring them (Cox, 2012). Thus, security matters may feel unimportant (Junger, Montoya, & Overink, 2017).

Moreover, the human person contains peculiarities that place it susceptible to risky behaviour. The optimism bias, for one, causes people to presume that negative events are less likely to occur to them (Weinstein, 1980). This can lead individuals to willingly engage in insecure behaviour under a sense of false invulnerability. This is further exacerbated in the cyber domain, where consequences of detrimental actions easily pass unnoticed. In addition, although people are generally able at identifying threats in their physical environment, as they are hardwired to do so, they are also prone to underestimating risks (Weinstein, 1980). Underappreciating risks is also especially salient in the intangible cyber domain (Schneier 2015, p. 256). For instance, risk-taking propensity is a predeterminant for lower information security awareness (McCormac et al., 2017a; Weirich, 2005) and impulsivity, "the urge to act spontaneously without reflecting on an action or its consequences" (Coutlee, Politzer, Hoyle, & Huettel, 2014, p. 2), is associated with unsecure information security behaviour and risky behaviour online (Egelman & Peer, 2015). Impulsivity is likely to pose heightened risk in the abstract and complex digital environment, where conceiving the consequences the of illicit behaviour is difficult (Cox, 2012). In contrast, big five traits conscientiousness, agreeableness, and emotional stability positively influence variance in information security awareness to a significant degree (McCormac et al., 2017a; Parsons et al., 2014a; Shropshire et al., 2015).

Inadvertence might also be the result of successful social engineering (Cox, 2012): psychological manipulation of people to expose confidential information or act in a way that jeopardizes the confidentiality of information (Anderson, 2020, p. 84). Basically, social engineers succeed by exploiting specific "vulnerabilities" of the human person: emotions, such as curiosity, fear, laziness, greed, and the will to be helpful and trust (Schneier, 2015, p. 266). These emotions are vulnerabilities in the sense that they are entirely "intentional features" of human nature but exploitable at expense of the individual. For example, trust has been vital to humans from an evolutionary perspective, trusting and being trusted even releases oxytocin into the bloodstream (Hadnagy, 2018), and researchers agree upon the fact that people thus possess a proclivity to trusting others as a default mindset (Ostrom, 1998; Mills, 2013). However, this has potentially hazardous repercussion in the cyber domain, where human sensory authentication is bypassed (Schneier, 2015). Difficulty of human authentication is further exacerbated by the increase of digital platforms that replace physical interaction in

the workplace (Krombholz et al., 2015). Therefore, a victim of social engineering often acts on trust rather than hard methods of authentication that technical devices utilize (Cox, 2012; Proofpoint, 2020).

Although any information system, social, technical, or sociotechnical, is built upon trust, trust issues are also not exclusive to social engineering. In terms of access control, malicious insiders thrive in organizations with open trust models and a trusting organizational culture (FireEye, 2020). May (2017) aptly suggests that organizations and individuals alike should not be entirely trustless but should surely trust less. In fact, a rising trend is to advocate zero-trust models in information systems, especially due to the rapidly growing remote workforce (Drolet, 2020).

Omissive behaviour

While the former applies to inadvertent behaviour, there are other reasons to why people engage in non-compliant behaviour that contradicts with their better knowledge. The very nature of the malicious insider entails that some may decide to omit purely out of dissatisfaction and dissent (Weirich, 2005). However, there are additional factors that enable omission.

As moral beliefs and values influence compliance (Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; D'Arcy & Herath, 2011), *Neutralization theory* posits that the temporary neutralization of values enables acts that are normally perceived as wrong. Neutralization, by denying the existence of an information security problem, has been discovered to be a significant predictor of non-compliance (Siponen & Vance, 2010; Moody, Siponen, & Pahnila, 2018). However, workers may also not feel morally obliged to comply (Mohammadnazar, Ghanbari, & Siponen, 2019). This can be particularly salient among normal workers who may not perceive compliance as a matter of right and wrong, unlike security professionals (Moody et al., 2018). Furthermore, neutralization techniques may undermine the effects of peer pressure in a non-compliance situation as individuals are able to rationalize away feelings of guilt, self-blame, and blame from others (Siponen & Vance, 2010). Nevertheless, neutralization is not a motivator but an enabler and the mechanism, not the cause, why employees to divert from their values.

The lack of valuation altogether provides another explanation. Padayachee (2012) suggests, based on the theory of human motivation by Deci and Ryan (1985), that omissive behaviour stems from *amotivation*, which refers to a state of being where the individual lacks an intention to act due to not valuing an activity or not possessing sufficient competence to execute the activity. Therefore, an employee not only devoid of motivation but also inadequately resourced will fail to comply. Thus, an employee must be equipped with the necessary knowledge, skills, tools, and time before compliance can be anticipated (Padayachee, 2012). However, an employee can also be deprived of resources.

Security is a trade-off in the sense that increase in security comes at the expense of some other virtue, e.g., functionality or usability; the privilege of having a locked front door comes at the inconvenience of having to carry a key whilst out (Schneier, 2015). In essence, "workload generates contradictory interests

between functionality and information security" (Albrechtsen, 2007, p. 1). Beautement, Sasse, and Wonham (2008) propose that recurring compliance, trading security for usability or primary work tasks, leads to the depletion a "compliance budget". If compliance requires no or a minimal trade-off, most employees will comply. However, if extra effort is required, this effort will be juxtaposed against perceived benefits and personal goals. This comparison will lead to compliance whenever the compliance threshold has not been exceeded and the individual has enough of their budget remaining. When the compliance budget is entirely depleted, the compliance threshold collapses (Beautement et al., 2008). Some call the resulting state *security system anxiety* (Hwang et al., 2017) and others *security fatigue* (Bada, Sasse, & Nurse, 2015) or amotivation (Padayachee, 2012). While the definitions vary, the phenomenon is nevertheless the same: when strenuous compliance or a high level of vigilance is continuously required, employees will be deprived of energy, and they will begin to omit (Hwang et al, 2017; Bada et al., 2015; Beautement et al., 2008).

Unsurprisingly, employees have been found to circumvent security measures to ease their burden, e.g., by cancelling automated anti-virus software because of decreased computer performance or download dubious files from the Internet to help them in their work (Parsons et al., 2017). In fact, people trade security for usability to the extent that it becomes irrational and paradoxical (Workman et al., 2008; Smith et al., 2011). The willingness to trade security for usability is an issue that experts view as a common concern (Calic, Pattinson, Parsons, Butavicius, & McCormac, 2016). On the other hand, there are instances where employees create an unsanctioned but feasible alternative to an unviable security measure, thus retaining as much security as possible, a phenomenon dubbed *shadow security* due to its obscurity (Kirlappos, Parkin, & Sasse, 2014).

The security, usability, and functionality (SUF) triangle, depicted in figure 3, models the issue and how emphasizing one of the dimensions comes at the cost of the other two (Rahalkar, 2016); increments in system functionalities broaden the surface of attack and complicate its use.

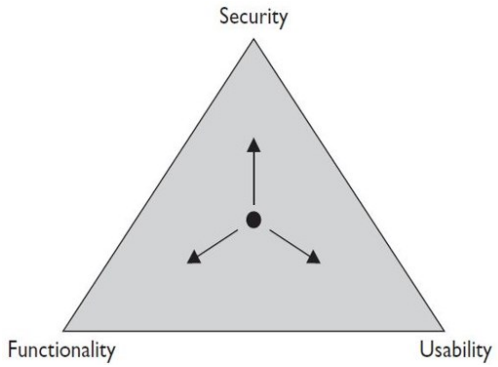

FIGURE 4 The security - usability - functionality triad (Rahalkar, 2016)

Passwords illustrate the dilemma between usability and security: traditionally, strong passwords are difficult to memorize while weak ones are easier to remember or, in other words, more usable (Sasse, Brostoff, & Weirich, 2001).

However, the trade-off between password memorability and user convenience is not proportionately affected when increasing password verification times to increase password memorability (Woods & Siponen, 2019). Thus, contrarily to the SUF model, improvements in usability can coincidentally improve security (Shropshire, Warkentin, & Sharma, 2015). If a certain utility in a technical system is perceived to be inconvenient to an employee's work, enhancing the ease-of-use of that utility would diminish the likelihood of the user circumventing any security features associated with the utility.

However, omission is not solely a result of perceived inconvenience. Security measures are honestly perceived as obstacles to one's work (Bada et al., 2015) and work impediment is a genuine reason for omission and non-compliance (Hwang et al., 2017). Thus, employees willingly ignore policy and practice as they are hindrances to their job tasks (Post & Kagan, 2007). Goal system theory posits that individual objectives are aligned in a hierarchical network. When "getting the job done" is juxtaposed against security, the former often prevails (Bada et al., 2015; Zinatullin, 2016, p. 83). In information systems in general, usability is often prioritized over security (Stevens, 2018). In terms of software development, security is a non-functional quality, which means it is traditionally not prioritized over functional qualities. Security is also the primary work objective of a select few and a mere secondary goal or even an additional inconvenience for others (Schneier, 2015). When attention is focused on a prioritized task, less focus will be placed on secondary obligations such as security concerns (Junger et al., 2017). Although it might even be ethically correct to, on occasion, prioritize other work-related aspects over security (Siponen & Iivari, 2006), the dilemma remains whether the consideration or the position of a given actor is adequate to make such prioritizations. Nevertheless, goal hierarchy provides another plausible explanation for omission and the knowing-doing gap.

Lastly, as we actively learn from our social environment, we are highly impacted behaviour by people, peers, and management, in our vicinity and the pressure they exert (Junger et al., 2017; Moody et al., 2018). However, this issue is discussed in further detail in section 4.

2.2.3 How? Risky behaviour and focus areas of the HAIS-Q

Risk signifies the extent of a threat as a function of the impact and likelihood of the threat occurring (NIST, 2020). Therefore, it follows that risky information security behaviour, or non-compliance, is such that increases the probability of the occurrence of a threat or the exploitation of a vulnerability (ISO/IEC, 2018). In contrast, behaviour change in terms of information security can be observed as reduced risk (Bada et al., 2015).

The following section charts risky and non-compliant behaviour as opposed to information security awareness. Moreover, the section completes the threat landscape by mapping some of the most relevant attack methods contemporary threat actors utilize to capitalize on risky employee behaviour. The following subsection is also topical because these methods and the behaviours also

represent the seven focus areas and the items (observable in appendix 1) of the HAIS-Q questionnaire used in the study.

Password management

Attackers often utilize stolen credentials to mimic legitimate users, but risk of substandard passwords is greater than that. As much as 81% of data breaches have included the use of weak or stolen credentials (Verizon, 2018, p. 28; Verizon, 2019, p. 10; FireEye, 2020). While threat actors predominantly steal credentials to enable their attacks, they use social engineering or info-stealing malware to obtain them (Proofpoint, 2019, p. 4). Descriptively, the most prevalent way[5] attackers gain initial access, escalate privileges, evade defences, and persist in systems is with the aid of valid accounts (Crowdstrike, 2020). While FireEye (2020) deflates this account by a margin, they nevertheless point that the problem with stolen credentials perseveres and is aggravated by the fact that stolen credentials are the costliest incidents to organizations (Ponemon, 2020). Although organizations can halt poor password behaviour by enforcing password policies with technical solutions, some may be circumvented, which leaves room for attackers to exploit weak credentials.

While inferior passwords continue to be a risk on their own, even lengthy or complex passwords are not sufficient in the contemporary threat landscape. Therefore, Verizon (2018, p. 28; see also Crowdstrike, 2020) suggests that access control management should be exercised on an organizational level and that users should endorse two-factor authentication (2FA) when available. Additionally, a robust access management process is needed to supplement 2FA in protecting identities. Lest organizations cease to rely on basic ID and password combinations for authentication, Crowdstrike (2020, p. 65) anticipates that valid credential theft will continue as a popular and effective method of infiltration.

Email use

Perhaps the most effective and thus also most popular form of social engineering is *phishing* (Crowdstrike, 2020; Ponemon, 2020; Dodge, Coronges, & Rovira, 2012; Khan et al., 2020). Phishing is an ICT-borne attempt to acquire sensitive or confidential information from an authorized owner, usually by masquerading the attempt as a legitimate inquiry or encouragement to act (Parsons et al., 2017, p. 43). Phishing is also an umbrella term for several more specific techniques. In *spear-phishing*, the attacker lures a targeted individual, organization, or business with often highly sophisticated and tailored communication (e.g., spoofed emails) that may include personally enticing material (Dodge et al., 2012). Descriptively, phishing attacks are often tailored to the industry: declaring "urgency" or "payment" for businesses and "greetings" or "requests" for education (Proofpoint, 2020; Symantec, 2019). Although email remains the most common vector, phishing can be conducted through several mediums, e.g., phone calls, SMS, or social

[5] Over 70 % of observed cases in 2019 (Crowdstrike, 2020).

media (ENISA, 2020a; Proofpoint, 2020). Email is also a large target; 25% of phishing attempts in 2018 sought to harvest email credentials (Proofpoint, 2019).

Of fifteen threat types assessed by ENISA (2020c) in their 2020 threat landscape report, phishing was the third most threatening type. For instance, the WannaCry ransomware and the Ukraine war power grid attacks were both initiated by way of phishing (Khan et al., 2020). Thus, despite being rudimentary, phishing is not solely a method for those who lack technical capacity. Of all spearphishing-initiated data breaches by advanced persistent threat (APT) actors in 2019, up to 20% were executed via links and 20–50% via attachments in emails (Crowdstrike, 2020, see also FireEye, 2020). In fact, up to 65% of APT groups have used email as an attack vector (Symantec, 2019).

Proofpoint (2019, pp. 8–10) has also noted that *impostor attacks* are specifically deceitful phishing attacks that trick users to act through spoofing, such as look-alike domain names or legitimate signatures. Tech giants, such as Google or Facebook, are especially popular spoofing aliases (IBM, 2020). Though organization size positively correlates with incoming impostor attack volume, it may be that smaller organizations are more susceptible due to absence of controls and awareness. Impostors also appear to seek to capitalize on Monday morning backlogs and social jetlag and, conversely, are inactive during weekends (Proofpoint, 2019).

Although ENISA (2020a; see also Proofpoint, 2019) expects mediums such as social media or messaging software to popularize and surpass emails in the long term, email also remains the most common medium to inject malware. In 2018, 94% of detected malware were delivered through emails or specifically their attachments (Proofpoint, 2019). Attachments are often Office files and popular attachment formats include .doc, .dot, .exe, and .rtf (Symantec, 2019). Fortunately, as 99% of email-borne malware requires human interaction (Proofpoint, 2019; ENISA, 2020a), there is an opportunity to block the email-borne threat with sufficient awareness. In fact, click rates are down to 3% in 2018 from 25 % in 2012 (Verizon, 2109, p. 14).

Internet use

Phishing attempts may also sometimes involve links to *watering holes*, websites that are specifically tacked to harvest sensitive information, such as login credentials (Watts, 2018). In a watering hole attack, an attacker compromises a legitimate website with malware and then waits for a user to input sensitive information. Watering holes can also be set up independently, without phishing, on often used websites (Krombholz et al., 2015). Advanced forms of domain fraud can include near-identical layouts, identical domain names (by using Unicode over ASCII), or legitimate secure certificates (Proofpoint, 2019) – or even the three combined (Krombholz et al., 2015). Moreover, in 2020, 74% of phishing sites have been found to use encrypted communication, HTTPS, compared to 32% just two years before (APWG, 2020). Using TLS or SSL over HTTP prompts the green lock icon on the address bar in many browsers creating the illusion that visiting the website is safe.

An attacker can also spoof an original website with a counterfeit version, a *contaminated website* that infects visitors with malware. Besides targeted attacks, contaminated websites may lay dormant on the web awaiting arbitrary visitors (Laari et al., 2019). Unfortunately, website-based attacks are difficult to monitor, unless organizations monitor all their external go-to sites (Krombholz et al., 2015).

Social media use

Though less favoured in relation to other online information sources, *social media* has also become a platform for attackers to administer social engineering techniques, both as an attack vector and as a means of conducting espionage (Proofpoint, 2019; Laari et al. 2019). As previously stated, phishing through social media is expected to rise in the foreseeable future (ENISA, 2020a). Thus, the tendency of individuals to post sensitive personal or work-related information online inconsiderately has repercussions. Hence, implementing sufficient security features on personal social media accounts and reviewing them regularly can provide extra coverage.

Whaling involves phishing for data that enables the attacker to target high-value individuals, for which social media is a cornucopia (DCDC, 2016). Counterintuitively, Proofpoint (2019) has found that the most targeted individuals are not the VIP's of organizations. The most frequently targeted people are those who have easily discoverable information on organizational websites, publicly available files, social media, traditional media, and other online sources. Overt digital identities can form considerable risk to organizations. However, people with privileges are the most lucrative targets (Proofpoint, 2019).

Mobile devices

Technological advancements and alterations in working practices are making the workforce increasingly remote. However, the increase in convenience is associated with a proneness to various threats. One hazard of mobile-driven, remote work is the use of public wireless networks and hotspots. There are numerous techniques an attacker may intercept wi-fi traffic, including ARP spoofing, sidejacking, via "evil twin" impostor access points, or WPA cracking (Shahin, 2017). Still, many connect to and send sensitive data over public wireless networks without taking any security precautions, such as using a VPN, thinking that paying for a hotspot makes it secure (Shahin, 2017).

Threats associated with working in a public environment are not, however, restricted to digitally borne vectors. Shoulder surfing, eavesdropping on an unsuspecting victim to observe confidential information, is widely recognized among both researchers and anecdotal accounts, making it more frequent "than we might think" (Bošnjak & Brumen, 2019, p. 1). In a global experiment by Ponemon (2016), shoulder surfing was successful in 91% of cases worldwide, with 27% of all leaked data being sensitive information. However, shoulder surfing is not only a remote work issue, but can take place at the workplace as well, as all employees should not have access to all information an organization holds.

A more ruthless physical threat is larceny. While physical access is invaluable for hackers, the high value and portable size of mobile devices make them opportune targets for common thieves as well (Prey, 2020). Up to 61% of U.S. businesses have experienced laptop or tablet misplacement or theft and one-in-ten of corporate laptops are lost before the end of their lifespan (Kensington, 2018). However, a mobile device is twice as likely to be inadvertently misplaced than stolen and many devices are lost at the workplace perimeter (Prey, 2020; Kensington, 2018). Nevertheless, the theft of a mobile device constitutes a serious data breach. While device replacement, consumption of IT resources, productivity loss, and loss of personally identifiable information are major concerns, loss of proprietary data constitutes the greatest factor associated with mobile device losses (Kensington, 2018). In fact, one-fourth of all data breaches in the financial industry could be traced to lost corporate mobile devices (Bitglass, 2016).

In conclusion, employees with inadequate knowledge on how to secure company and bring-your-own devices or how to properly transmit information are clear indicators that the organization is at risk (Ponemon, 2020).

Information handling

However, the notion of information security is not solely a digital or even a technological one. While information security and cyber security share tremendous overlap, they are not entirely analogous: storing and transmitting data as digital bits is only one way of processing, preserving, and communicating information (Von Solms & Van Niekerk, 2013). Cyber (or ICT) only refers to the technological means of communicating information.

Peltier (2016, p. 4) notes that the idea of the "paperless office", one that relies entirely on digital data and communication, manifested as early as 1965. However, much of organizational information is still in physical form, such as paper prints. Therefore, a clean desk policy is common practice in environments where sensitive data is handled: physical data are not to remain visible, unobserved, and they ought to be disposed of in accordance with the sensitivity of the data (Andress, 2014). Particularly in information-intensive organizations, information security is extensively influenced by how employees handle digital and conventional data, associated removable media, browsers, emails, paper documents, and the data they enclose (Sommestad, Karlzén, & Hallberg, 2017). Moreover, threat actors can utilize dumpster diving as well, which places emphasis on data disposal.

Baiting is the act of placing malware-planted removable media, external hard drives, USB sticks, or CD-ROMs, on premises that can cause an individual of an organization to collect them and insert them into an organizational host (Krombholz et al., 2015). While baiting in its simplest form seems like a crude approach, replication through removable media is nevertheless an effective means for attackers to access a protected system (Crowdstrike, 2020). For instance, one of the most secure networks in the world, the SIPRNET (Secret Internet Protocol Router Network) of the Pentagon, the headquarters of the United States department of defence, was initially infiltrated with USB sticks that had been

littered on a parking lot of a United States military base in the Middle East (Sanger, 2020). However, baiting is not restricted to digital removable media. Actors may also attempt to infiltrate a technical system with infected files, such as a fake invoice sent to accounting, a résumé sent to human resources, or a fake lawsuit (or the threat of) over a fabricated event (Proofpoint, 2019).

Incident reporting

Lastly, no matter what method of attack is suspected, user incident reporting is paramount. Simply put, the faster containment occurs, the lower the costs and therefore reporting of vigilant employees forms one of the most effective countermechanisms to data breaches (Albrechtsen & Hovden, 2014; Gardner, 2014; Verizon, 2018; Ponemon, 2020). Furthermore, people have been found to be more efficient at detecting internal incidents than technology (Verizon, 2018). For instance, although network intrusion detection systems utilize artificial intelligence to detect anomalies, these technologies have limitations that do not constrain human beings. Moreover, as stated, malicious insiders are a prominent threat to organizations (ENISA, 2020a). Therefore, colleagues can report suspicious behaviour by potential malicious insiders, who would otherwise go unobserved. Ponemon (2020; see also Verizon, 2019) suggests organizations should have an insider threat management program that implement incident reporting in effect to detect and mitigate insider-initiated incidents swiftly.

To summarize, the contemporary threat landscape consists of outsider and insider actors, both of which constitute serious threat. However, although malicious insiders are a threat source by themselves, the true threat source springs from the outside and the threat actors who expand the threat landscape by directing their exploits on the relatively weaker human subsystem and its vulnerabilities (Proofpoint, 2019). Hence, the inadvertent or omissive insider poses the risk, but the outsider poses the threat. Fortunately, in terms of risk, this also implies that there is potential for individuals to either increase or decrease the probability of a threat being realized (Bada et al., 2015).

Moreover, organizations can also implement technological (see e.g., Ponemon, 2020, Kaspersky, 2019; Proofpoint, 2019) or administrative (Hagen et al., 2008, ISO/IEC, 2018) solutions to mitigate these risks. However, as countering many of even the technological exploits require user interaction (or omission), organizations cannot solely rely on software or policy to ensure information security; even automated attacks often require human interaction. Therefore, whether incidents are inadvertently or maliciously incurred, the threat landscape necessitates a people-centred posture and ensuring compliance (Proofpoint, 2019; Bissell et al., 2019; Padayachee, 2012; Ponemon, 2020; Williams, 2008).

The vulnerability landscape, both in terms of inadvertence and omission, also seems expansive. Prominent vulnerabilities include lack of knowledge or resources, biases, human emotions, dissent, moral valuations, motivation, contradicting goals, fatigue, or social factors. However, while it is possible to gain an overview from literature as similar "landscapes" share similar features, a need for organization-specific research remains. Organizational circumstances cannot

be accurately deducted from a broader frame of reference, which motivates to conduct research on a local level. Consequentially, results on the local level also supplement the broader theoretical foundation and previous findings.

However, the question how compliance is to be achieved remains. Some deduct that the only known remedy for the social engineering (Gardner, 2014) and the most effective way to defend against information security threats (Safa et al., 2016) is information security awareness. To provide such defences, information security organizations recommend information security awareness programmes (SANS, 2018) or policies on insider threats based on user awareness (ENISA, 2020b), which are likewise believed to be the most effective way of countering insider threats. The following section outlines scientifically established success factors of ensuring compliance through awareness-focused efforts. In doing so, the section spans a comprehensive literature review into ways the scientific community has sought to divert individuals from threats and risky behaviour described in the past subsection and promote compliant behaviour.

3 IMPROVING INFORMATION SECURITY COMPLIANCE

"If you think compliance is expensive – try non-compliance." (Paul McNulty)

Information security compliance refers to the adherence of central activities documented in an organizational information security policy (Padayachee, 2012). Thus, the information security policy provides the context within which compliance takes place, but compliance determines the efficacy of the policy (Puhakainen & Siponen, 2010). Whereas compliance is an adaptive response, non-compliance is a maladaptive response, one that causes problematic behaviour and harmful outcomes (Vance, Siponen, & Pahnila, 2009). Hence, as the issue of compliance is fundamentally behavioural, academics have selected socio-cognitive theories to manage compliance (Harris & Furnell, 2012; Vance, Siponen, & Pahnila, 2012; Moody et al., 2018). Analysing 114 papers related to security policies, Cram, Proudfoot, and D'arcy (2017) modelled the theoretical discourse surrounding compliance and identified five distinct linkages, depicted in figure 4, in which this study is primarily associated with relationship 3.

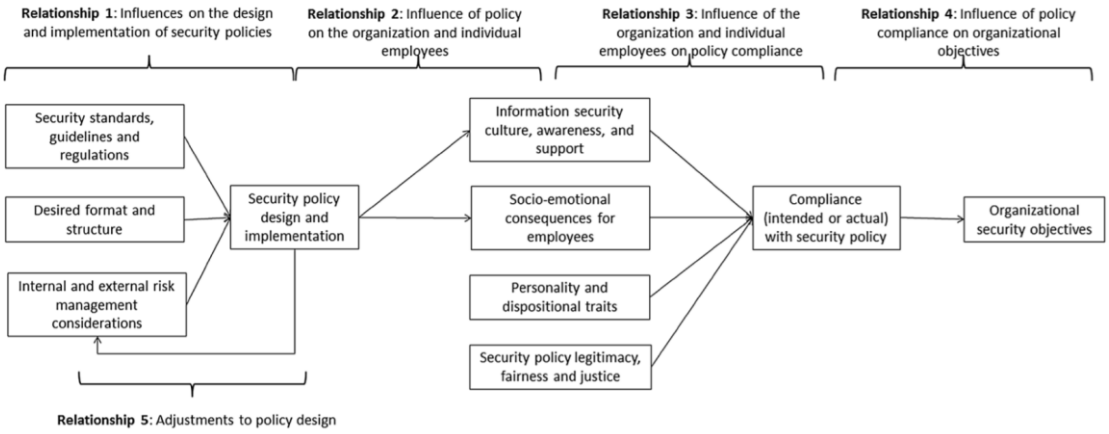

FIGURE 5 Policy and compliance research and relationships (Cram et al., 2017, p. 613)

However, although research around the topic has been plenty, achieving compliance has proven arduous (Sommestad et al., 2014; Puhakainen & Siponen, 2010). While up to 11 theoretical concepts have been applied to information security compliance (Moody et al., 2018), research is primarily fixated around four theories (Cram et al., 2017; Sommestad et al., 2014):

- *Deterrence Theory* (DT),
- *Rational Choice Theory* (RCT),
- *Protection Motivation Theory* (PMT), and
- *The Theory of Planned Behaviour* (TPB).

The literature review regarding this study came to the same conclusion. These four primary theories are presented in the following section to provide an overview of the current research in the area, demonstrate research gaps and highlight hypotheses, and, in addition, accumulate a stockpile of findings to reinforce the recommendations and conclusions of the study – which factors increase the probability of adaptive responses, or decrease risk, and which discourage and decrease the probability of maladaptive responses, or increase risk.

3.1 Deterrence Theory

Research concerned with information security policy compliance has leaned heavily on deterrence theory (Siponen & Vance, 2010; D'Arcy & Herath, 2011; Hu, Xu, Dinev, & Ling, 2011). Traditionally speaking, deterrence is the preventative effect of punishment or the threat of it has on potential violators (Ball, 1955). Thus, studies that investigate deterrence as a means of ensuring compliance approach information security management from a coercive stance (Kolkowska & Dhillon, 2013). Though deterrence tends to provoke negative connotations, the principle of DT is that "it is better to prevent than to punish" (Gundu, 2019, p. 95). *Specific deterrence* aims to prevent violators from renewing violations and general deterrence to encourage others to abstain from non-compliance via the example set by punishing violators. Deterrence is an extrinsic motivator, meaning that it makes certain activities desirable not due to their inherent value but a separable outcome (Ryan & Deci, 1985). Deterrence, thus, does not promote adaptive behaviour, but is intended to thwart maladaptive behaviour (Vance et al., 2009).

When looking at the issue of non-compliance from the perspective of the malicious insider, plausible deterring factors include certainty of detection, celerity of detection, and severity of punishment. These three factors combined are known as the *classical deterrence theory* (D'Arcy & Herath, 2011; Higgins, Wilson, & Fell, 2005). In the case of the inadvertent or omissive insider, however, variables that influence compliance via deterrence are an employee's (threat) appraisal of the severity of a security breach and the probability of a security breach; certainty of detection might be a factor only if some sort of monitoring is applied (Herath & Rao, 2009).

Cheng et al. (2013) explain that deterrents can either be formal or informal. Formal deterrents are mainly vertical and include organizational sanctions such as rebuke, reminders, demotion, and suspension and are expressed through explicit rules and regulations. Informal deterrents are commonly a result of social disapproval or peer-pressure such as shame, embarrassment, expectations, and norms, and may be more tacitly distributed. In addition, informal sanctions include self-disapproval and moral beliefs. Informal sanctions are fundamentally an extension to classical deterrence theory known as *contemporary deterrence theory*. Generally, both formal and informal sanctions, especially social pressures, affect intent to violate policies (Cheng et al., 2013). Social factors are more intricately examined within theories of social psychology, such as the Social Bond Theory (SBT) (see e.g., Safa et al., 2015b).

However, there appears to be some disparity regarding the effect of formal sanctions. While some have found perceived certainty and severity of punishment to significantly influence compliance (Li, Zhang, & Sarathy, 2010), other results validate certainty of punishment but contradict severity (Herath & Rao, 2009) or validate severity but contradict certainty (D'Arcy et al., 2009). D'Arcy and Herath (2011, p. 648; see also D'Arcy & Hovav, 2009; D'Arcy et al., 2009) concluded that the contradictions could be explained through contingency variables, which determine the effect of formal sanctions:

- *Self-control*: sanctions tend to have a lesser effect on individuals with lower self-control,
- *Computer self-efficacy*: individuals with higher self-efficacy with computers tend to hold formal sanctions in lesser regard,
- *Moral beliefs* moderate the deterrent effects of sanctions,
- *Virtual work* may reduce the effects of sanctions, and
- *Employee position* meaning that individuals with higher positions or stakes in the organization are more receptive toward sanctions.

Sanctions may also be ineffective if people have not been caught to provide an example (Moody et al., 2018).

In terms of informal sanctions, it has been discovered that embarrassment and shame can prove more efficient deterrents than formal sanctions (Grasmick & Bursik, 1990). While some have successfully applied shaming as a deterrent in information security (Harris & Furnell, 2012), other studies have failed to yield significant results (Siponen & Vance, 2010). Moreover, shaming can be hazardous due to various detrimental effects and thus may have its uses in circumstances where the cohesion in groups and the relationships employees foster are strong (people must care what peers think) and where other forms of incentives are employed as well (Harris & Furnell, 2012). For instance, by introducing rewards, a more comprehensive approach where both the stick and the carrot are implemented can effectively provide greater coverage for non-compliance controls (Chen, Ramamurthy, & Wen, 2014; Marcinkowski & Stanton, 2003; Stanton, Stam, Mastrangelo, & Jolton, 2005; Gundu, 2019). However, disparity associated with

DT applies to rewards as well; there are findings that suggest that rewards do not have a significant effect on compliance (Pahnila, Siponen, & Mahmood, 2007; Moody et al., 2018; Herath & Rao, 2009). Jai-Yeol (2011) concluded that rewards are effective, but only if they are not perceived as means to control behaviour.

Therefore, it is presumable that the evidence regarding the effect of deterrents is circumstantial and as such only partially commensurable. Despite the contradictions, information security experts estimate that disciplinary procedure has a very high impact on compliance (Furnell & Rajendran, 2012). Nevertheless, it is questionable whether deterrence can effectively enforce compliance. Can one expect, for instance, that someone would choose a stronger password in fear of repercussions from an organizational level? Therefore, other studies apply other behavioural theories to close in on the matter from a more personal standpoint (Herath & Rao, 2009) and reach for motivations in human behaviour beyond sanctions and rewards.

3.2 Rational Choice Theory

Rational Choice Theory (RCT) has overlap with deterrence theory as both take sanctions into account, although RCT includes the into the broader category of "costs" (Moody et al., 2018). The thought pattern of rational choice is reminiscent to the compliance budget and the trade-off analogy (Schneier, 2015, p. 261; Rahalkar, 2016): with security comes a respective amount of additional burden. Rational choice theory concludes that actors pursue gain and evaluate the costs and benefits in each situation to maximize gain (Paternoster & Simpson, 1996). Essentially, decision-making from this perspective is a matter of utilitarian calculations (Siponen & Vance, 2012). As figure 5 depicts, the consequences of non-compliance, such as sanctions, personal moral beliefs, and estimated benefits influence the intentions of individuals.

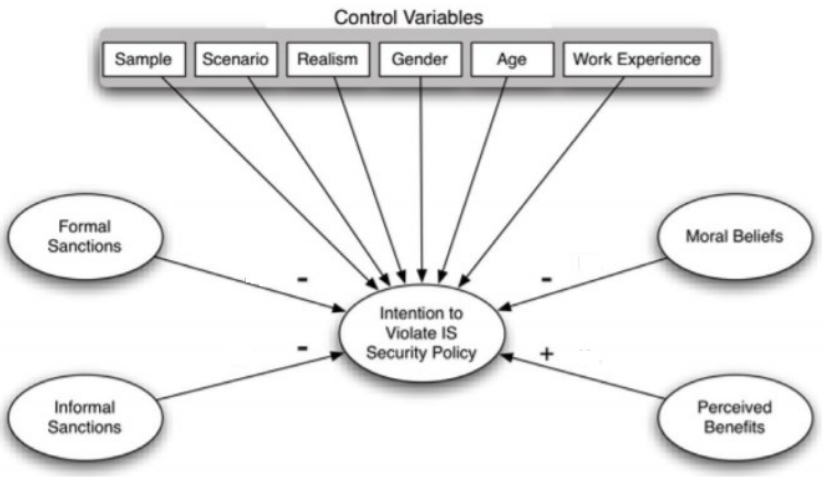

FIGURE 6 A RCT model for explaining policy violations (Siponen & Vance, 2012, p. 25)

Although humans undoubtfully tend to act in an irrational way that waives gain, hence the privacy paradox, the theory offers explanatory power to policy compliance. In addition to the results associated with sanctions previously discussed, perceived personal gain and moral beliefs are thought to influence intent to noncomply (Furnell & Rajendran, 2012; Siponen & Vance, 2012). Additional studies indicate that thee cost-benefit analysis is indeed a factor when an individual determines whether to or not to comply with information security policies (Hu et al., 2011; Li et al., 2010; Bulgurcu et al., 2010), although many assume a selfish disposition. In addition, individuals appraise the costs and benefits from the perspective of the organizations as well (Beautement & Sasse, 2009). This implies that the motives to adhering to policy are not solely egotistical; employees might also perceive that non-compliance is in the best interest of the organization. Organizations may also increase perceived benefits or, conversely, decrease perceived costs by improving usability and benefit of use related to the usage of information systems (Shropshire et al., 2015). As stated, this implies, in contrast to the SUF model, that usability affects the security of a system (Rahalkar, 2016). Thus, according to the RCT, usability can be regarded as a security feature.

3.3 Protection Motivation Theory

Protection Motivation Theory (PMT) proposes a more thorough model that incorporates cost-benefit (or cost-reward) assessment with a wider theoretical foundation. PMT was initially introduced by R. W. Rogers (1975) and founded on earlier work on threat, stress, and coping, predominantly built by Richard Lazarus in his lifework. PMT initially stems from health psychology, but has been adapted into many fields, including information security.

The theory suggests that the perceived severity of a threat, vulnerability (sometimes referred to as probability of occurence), efficacy of the recommended preventive behaviour, and self-efficacy of the individual define human reactions, intentions, and behaviour. The first two factors are categorized as threat appraisals and the latter two coping appraisals. Threat appraisal refers to the magnitude a person feels threatened and coping appraisal to whether that person's responses are adequate to overcome the threat. In spirit of Lazarus' coping mechanisms, a threatened individual's appraisals must result in a positive outcome: people must perceive that their resources, or coping appraisals, suffice to respond to the appraised threat (Workman et al., 2008). An appraised inability to cope results in amotivation as "nothing can be done" to prevent the threat. Maddux and Rogers (1983) later revised and extended Rogers' (1975) theory of protection motivation by including, following RCT, costs and rewards (or benefits) as factors, in addition the original four, a model of which is presented in figure 6. Furthermore, extending PMT with *locus of control*, an individual's beliefs about how strongly they can influence their life events, creates the threat control model (TCM) (Workman et al., 2008).

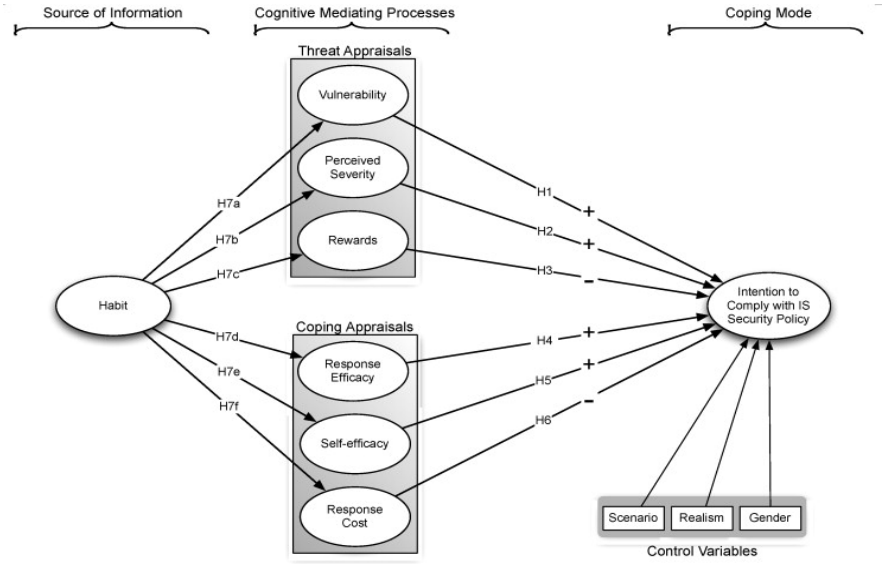

FIGURE 7 A model of PMT (Vance et al., 2012, p.191)

All four components of the traditional PMT have been found to influence compliance to organizational policy (Ifinedo, 2012; Siponen et al., 2007; Siponen, Mahmood, & Pahnila, 2014). However, some results suggest that coping appraisals do not influence attitudes towards compliance, though the evidence might be circumstantial (Siponen, Pahnila, & Mahmood, 2010). Further studies that have utilized the extended PMT have validated the role of both the original and the additional factors (Vance et al., 2012; Workman et al., 2008). These factors have had, partly through habit, a significant predictive effect on intention to comply (Vance et al., 2012). Especially perceived severity of a threat and perceived vulnerability greatly dictate motivation to comply (Workman et al., 2008).

PMT is also tightly linked to the concept of fear appeal, a strategy to manipulate threat appraisals to induce an air of threat and thus incite certain desirable behaviour, for example, to endorse an information security policy. By appealing to fear, individuals can be made feel threatened and thus motivated to act (protect) in a certain way. Results also show that fear appeal is a formidable predictor of intention to comply with information security policies (Johnston & Warkentin, 2010; Workman et al., 2008). Fear appeal rhetoric can also effectively be augmented with sanctioning rhetoric, thus incorporating a component from DT to add a dimension of personal relevance to PMT (Johnston, Warkentin, & Siponen, 2015). However, appealing to fear might become counter-productive if fear becomes a chronic state (Workman et al., 2008). This cultivates a fatalistic attitude where nothing can (presumably) be done to avoid security incidents. In a state of alarmism or with a distorted false-positive alert ratio, like the boy who cried "wolf", people may eventually start to succumb to amotivation. Also, it is debatable whether information security threats truly evoke fear, an emotional state in the traditional psychological sense, or merely some lesser sense of urgency (Moody et al., 2018).

Instead of appealing to fear, intrinsically oriented studies suggest that data- and individual-focused motivational appeals can yield greater intent to comply

(Menard, Bott, & Crossler, 2017). Factors such as the desire to perform well at work or to behave in a manner that is uniform with ones' self-identity bear significant influence on compliance (Guo et al., 2011). This illustrates a development where researchers have sought to develop coping and threat appraisals that can be considered as intrinsic motivators rather than extrinsic. Extrinsic and intrinsic motivation are associated with Self-Determination Theory (SDT) by Deci and Ryan (1985). While it is not a theory profoundly utilized in compliance research, it provides a theoretical taxonomy and a layout to classify and categorize different appeals as well as factors and theories that influence compliance.

3.4 Self-Determination Theory

SDT posits that motivation is either intrinsic or extrinsic (Deci & Ryan, 1985). *Intrinsic motivation*, the highest and most autonomous form of motivation stems from the inherent interest towards or satisfaction of performing a given task, including satisfying curiosity or through perceived self-worth (Deci & Ryan, 1985; Safa et al., 2015b; Zinatullin, 2016). *Extrinsic motivation* refers to performing an act because it leads to an external outcome, not due to its inherent interest. Extrinsic motivation is four-fold and related to:

- *External regulation* i.e., sanctions and rewards,
- *Introjection*, a person complies to maintain self-esteem in relation to the social environment,
- *Identification*, a person identifies social norms as one's own, and
- *Integration*, a person has fully assimilated identified norms (Deci & Ryan, 1985).

While SDT does not specifically propose how to improve compliance and is therefore not a central theory in explaining information security compliance, the taxonomy also provides insight on the various and varyingly internalized means of motivating compliance – intrinsic motivation being at the top tier. SDT serves to illustrate that not all theories are equal in their methods, and perhaps ability, to motivate and foster compliance among individuals. Thus, SDT provides a template with which to classify other theories associated with information security compliance. For instance, Padayachee (2012) constructed a taxonomy based on the Self-Determination Theory (SDT) that classifies factors relevant to information security compliance. In addition to being a tool to classify different compliance-influential factors, SDT can be utilized to classify entire theories.

To summarize the last three theories, it seems as though DT, RCT, and PMT are associated with the four aspects of extrinsic motivation, shown in table 2 (except Social Bond Theory, which was only discussed briefly in section 3.1). For instance, PMT could be regarded to be motivated by integration, the most autonomous form of extrinsic motivation (Padayachee, 2012). The influencing factors presented in table 2 are motivational factors that are associated with compliant

security behaviour (Padayachee, 2012), grouped with their respective extrinsic aspects and psychological theories.

TABLE 2 The links between forms of extrinsic motivation, factors, and explaining theories

Extrinsic aspect[6]	Compliance factors[7]		Explaining theory
External regulation	Sanctions	Monitoring	Deterrence Theory
	Rewards	Policies	
Introjection	Management	Peer behaviour	Social Bond Theory
	Social disapproval		
Identification	Resources	Visibility	Rational Choice Theory[8]
	Training	Info quality	
Integration	Threat appraisal		Protection Motivation Theory[9]
	Coping appraisal		

However, whereas the previous theories seek to influence compliance with an extrinsic approach, there appears to be a lack of theories and studies that emphasize intrinsic motivation. Specifically, by introducing the concept of attitudes, subjective emotional dispositions, compliance can be approached intrinsically albeit indirectly as well. One such theory, the Theory of Planned Behaviour (TPB), and one of its branches, the knowledge-attitude-behaviour (KAB) model, are presented in the following section. Further on, the section covers the contemporary scientific body regarding information security awareness and how to raise it on an organizational level.

3.5 The Theory of Planned Behaviour: the KAB model

> "One of the most enduring lessons of social psychology is that behaviour change often precedes changes in attitudes and feelings" (Timothy Wilson)

The TPB postulates that behaviour is motivated by intent, attitudes towards behaviour, subjective norms surrounding behavioural performance, and the perception of the individual of the facility with which behaviour can be met. The TPB was built upon the Theory of Reasoned Action (TRA), which was presented by Fishbein and Ajzen (1975) and later revised by Ajzen (1985) to produce the TPB by including perceived behavioural control, a construct that combines self-efficacy and locus of control, to the model. The KAB model can be viewed as a slight alteration of the TPB and the TRA, which both incorporate attitude is an important antecedent to explain behavioural intent, in this case compliance or non-compliance.

[6] Deci & Ryan, 1985
[7] Padayachee, 2012
[8] Paternoster & Simpson, 1966
[9] Rogers, 1975; Maddux & Rogers, 1983

The KAB model implements attitude as a mediating factor between knowledge and behaviour and therefore posits that knowledge gains alone are not enough to influence behaviour (Parsons et al., 2014a; Schrader & Lawless, 2004). Security in an organization necessitates that its employees' attitudes are aligned with the volition of security management (Kruger & Kearney, 2008). However, prior knowledge is in turn a critical antecedent for attitude formation: when encountering a problem, people determine their attitude to solve it and the decide upon the optimal course of action and finally take action (Lee, Lee, & Kim, 2016). Thus, compliance originates from knowledge but is mediated by changes in attitude, which result in positive outcomes in human performance (Parsons et al., 2014a; Schrader & Lawless, 2004).

Fishbein and Ajzen (1975) understand attitude as a subjective emotional responsive disposition an individual holds against oneself, another person, a thing, place, event, or act arising from the real-world that influences how one behaves. Knowledge, or beliefs, on the other hand, are cognitive representations of the world – subjective assessments that a thing will contain certain attributes, or an act will lead to a particular result. Therein behaviour can be viewed as the intentional response to the stimuli induced by knowledge- or attitude-related factors and an attempt to interact with the world to conform it in the image of said attitudes and beliefs, as illustrated in figure 7.

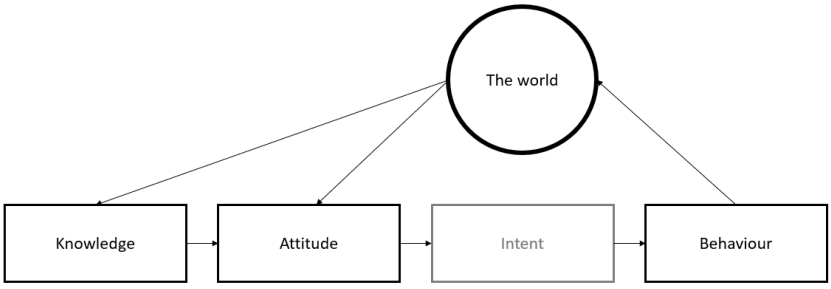

FIGURE 8 An adaptation of the KAB model

The scientific body around the KAB model is ample. In terms of knowledge, a systematic literature review covering 68 studies conducted between 2003 and 2016 indicated that knowledge had a significant positive effect on how employees subsequently behave (Mahfuth, Yussof, Abu Baker, & Ali, 2017). Furthermore, scholars largely agree on the fact that possession of necessary knowledge and associated competencies is key to achieving compliance and ensuring that employees have the means to meet the information security requirements placed upon them and a chance at internalizing policies – and it is the responsibility of the organization to achieve this (Harris & Furnell, 2012, p. 14; D'Arcy & Hovav, 2009; Padayachee, 2012; Marcinkowski & Stanton, 2003; Alfawaz et al., 2010; Knapp, Morris, Marshall, & Byrd, 2009).

Concerning attitude, another substantial systematic literature review spanning 111 peer-reviewed articles by Sommestad et al. (2014) found that attitude towards compliance was one of the two of the most studied and the most

influential dependent variables regarding perceived compliance. Table 3 demonstrates six of the most influential dependent variables in terms of compliance with their respective, most influential independent variable. Moreover, the table shows that there is a clear interconnectedness between attitudes, intentions, and actual compliance and an ascending causal link.

TABLE 3 Variables used to monitor compliance. Derived from Sommestad et al. (2014)

Dependent variable	Independent variable	Primary study	Effect size (β)
Att. towards compl.	Threat appraisal	Herath & Rao, 2009	0.39
Intention to comply	Att. towards compl.	Weighted mean[10]	0.35
Actual compliance	Intention to comply	Weighted mean[11]	0.50
Att. towards misuse	Perc. sev. of sanctions	Dugo, 2007	-0.47
Intention to misuse	Att. towards misuse	Weighted mean[12]	0.39
Actual misuse	Intention to misuse	Lee, Lee, & Yoo, 2004	0.29

Moreover, recent studies have concluded that attitude towards compliance is one of the most significant, if not the most significant, factors for compliant behaviour (Bauer & Bernroider, 2017; Siponen et al., 2014; Sommestad et al., 2014; Safa et al., 2015a). Conversely, it has also been shown that attitude towards non-compliance increases intention to not comply (Guo et al., 2011). Although other studies in the theoretical setting of TRA and TPB have concluded that there are other variables at play that have equal or even greater effects on behaviour than attitude (Bulgurcu et al., 2010; Herath & Rao, 2009), variation in results presumably appear due to dissimilarities in study populations (e.g., professionals and students) and because the attitude-behaviour linkage is more robust with working professionals, especially in fields where security is inherent to the organization, such as banking or national security (Bauer & Bernroider, 2017). Nevertheless, it appears that the TPB cannot by itself explain all the measurable variance associated with intended compliance, as variables such as anticipated regret and habit also supplement the theory (Sommestad et al., 2017). However, this does not by itself drain the usefulness of the model. Raising awareness and training users has proven effect (Ponemon, 2020; Gardner, 2014; Parsons, 2014a). The importance of raising information security awareness to mitigate breaches is highlighted not only in the scientific community (Safa et al., 2016; Knapp et al., 2009) but in standardization (ISO/IEC, 2018), among information security organizations (Ponemon, 2020, p. 24), and IT vendors (Verizon, 2018) as well. Unfortunately, there is also evidence that investments in awareness are insufficient (PWC, 2012; May, 2017), even if they are assessed to be more effective than other forms of controls (Hagen et al., 2008).

[10] Incl. Johnston & Warkentin (2010), Pahnila et al., (2007), Ifinedo (2012), Li, Zhang, & Sarathy (2010), Bulgurcu et al., (2010), Zhang, Reithel, & Li (2009), and Herath & Rao (2009)
[11] Incl. Pahnila et al., (2007) and Siponen, Pahnila, & Mahmood (2010)
[12] Incl. Guo et al. (2011) and Dugo (2007)

3.5.1 Raising awareness

Before advancing to conclusions, the following subsection will review some of the literature to examine what practical actions organizations can take to improve information security awareness, as outlined in research question 3a. The motivation for this is to be able to reinforce the conclusions of the study with practical tips based on scientific research and recommendations from security organizations to support investment decisions in information security awareness.

Traditional methods of improving information security awareness include sporadically disseminated, vertical measures such as presentations, emails, posters, or coffee mugs directed at large populations (Puhakainen & Siponen, 2010; Kruger & Kearney, 2008). In addition, small-scale activities, employee participation or group processes such as collective reflection, also improve awareness and behaviour in the short term (Albrechtsen & Hovav, 2010). However, a common recommendation is to compile activities longitudinally into a formal, structured information security awareness programme (ISAP, sometimes dubbed program or campaign) maintained as a part of organizational information security management to reduce risk and susceptibility to threats (Albrechtsen & Hovden, 2014; Gardner, 2014; Bauer, Bernroider, & Chudzikowski, 2017). An ISAP supports the development and enforcement of organizational policies by outlining acceptable behaviour and disseminating information to users (Albrechtsen & Hovden, 2014; Gardner, 2014; Gundu, 2019). ISAP's may also train users to be observant of threats, abstain from risky behaviour, cultivate attitudes, influence organizational security culture (Safa et al., 2015b), and mitigate cultural biases (Tsohou, Karyda, & Kokolakis, 2015). Awareness-raising interventions have a positive effect on knowledge of policies and that better knowledge results, on average, in better attitudes towards the policies (Williams, 2008; Parsons et al., 2014a).

As is customary to information security management, standardization organizations also provide standards and "best practices" for running an ISAP (see e.g., NIST, 2003). However, scientific literature covers the subject as well. Firstly, researchers and standards agree that ISAP's are not projects but ongoing processes; programmes and employees need to be updated regularly (Knapp et al., 2009; NIST, 2020; Bauer et al., 2017). Moreover, an efficient awareness regimen should not only include a continuous ISAP strategy (Bauer et al., 2017) but also a communication flow integrated to the regular communication of the organization, not only posters, emails, or coffee mugs (Puhakainen & Siponen, 2010). This is not only to accentuate the importance of information security but specifically to ensure that employees do perceive information security as a concrete issue that relates to their daily work. The relevance of regulation to one's work, i.e., role values, is central to compliance to said regulations (Moody et al., 2018).

Knowledge of existing threats also influence employee attitudes (Puhakainen & Siponen, 2010; Furnell & Rajendran, 2012), possibly due to threat appraisals (Workman et al., 2008) and fear appeals associated with PMT. Raising awareness of threats, risks, and vulnerabilities also increases benefits of compliance: 1) it improves performance, thus also reducing security costs, 2) builds

competence, thus increasing confidence, and 3) by increasing confidence, reduces fatigue associated with security (Beautement et al., 2008). Nevertheless, many studies recommend that awareness-raising initiatives should highlight the benefits of compliant behaviour rather than overly stressing the negative consequences of non-compliance (Bauer & Bernroider, 2017; Siponen & Vance, 2010; Parsons et al., 2014a; Bada et al., 2015).

As information security training, along with policies, is often perceived as technical and incomprehensible, educators should consider a soft, pedagogic approach and incorporate layman's terms rather than technocratic vocabulary (Bauer et al., 2017; Caldwell, 2016). Another problem is that training is often considered dull; workers do not generally need facilitating conditions to instigate simple forms of secure behaviour (Moody et al., 2018). Thus, efficient training also includes stimuli that encourage the trainee to conduct cognitive information processing (Puhakainen & Siponen, 2010) that pertains to contemporary threats (Proofpoint, 2019). Studies show knowledge of a threat also alters attitudes towards information security and influences intent to comply (Pahnila et al., 2007), coupling the KAB model with PMT and threat appraisals. The closer the training is to the real-world, the better the results (Proofpoint, 2019). Phishing exercises, for example, have proven to be effective in terms of results and cost (Dodge et al., 2012; Ponemon, 2020). As threat actors adopt new tactics, organizations can enlist users to combat them through awareness programs related to the various forms of social engineering (Crowdstrike, 2020, p. 66). Since people want to interact and perform, gamification may motivate open possibilities to enhance threat-oriented training further (Khan et al., 2020). However, to maximize effect, combined delivery methods of both online and onsite training and education can be applied (Kusumawati, 2018; Abawajy, 2014; Caldwell, 2016).

A user-tailored approach can also improve ISAP's (Furnell & Clarke, 2012). Matching individual learning styles in training improves information security awareness (Pattinson et al., 2019). Learner-controlled training, training that is tailored to the levels and learning styles of learners, can motivate and engage individuals in ways that significantly improve learning outcomes, including training performance, training satisfaction, and the ability to retain information, and precedes self-efficacy, threat severity, and threat vulnerability perceptions (Abraham & Chengalur-Smith, 2019). This means that learner-controlled training enhances users' sensitivity to observe threats *and* strengthens their confidence to act. Thus, awareness training has most potential when it is tailored and targeted at vulnerable groups (Dodge et al., 2012; Proofpoint, 2019). For instance, computer savvy individuals and employees working from home can be vulnerable as they are less influenced by security education, training, and ISAP's (D'Arcy & Hovav, 2009). NIST (2003) provides a framework for a tailored effort, illustrated in figure 8. It organizes learning into a continuum and divides into parts by participant levels and roles. It is up to management to determine vital and light-to-learn skills that are trained for most, high-cost skills that must be acquired for some, and baselines for the entire workforce (FireEye, 2020). For instance, secure handling of data can be foreign to many (Ponemon, 2020).

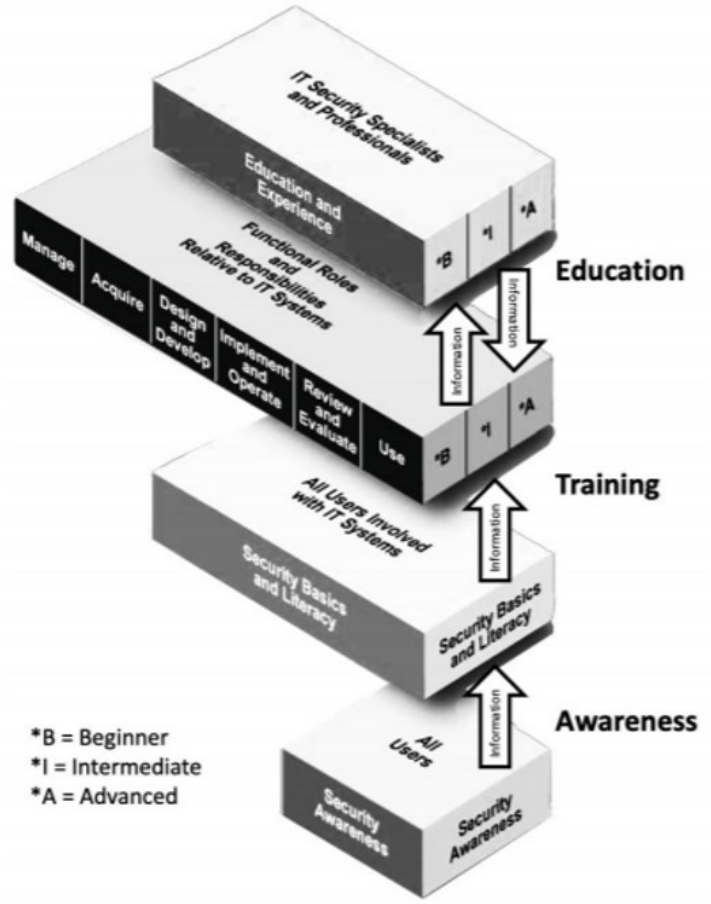

FIGURE 9 The information technology learning continuum (NIST, 2003, p. 8)

Prioritizing training objectives is also of the essence. There is always some pedagogic threshold, which means that trying to teach too much may result in zero learning effect (Krol et al., 2012). Awareness-raising efforts might even be counterproductive if they are perceived as a nuisance or too straining (Junger et al., 2017). Thus, not all increments on knowledge work towards good security behaviour: the quality of the training determines much of the outcome (Gundu, 2019). Choice or cognitive overload mean that the more information people are provided, the likelier they are to be encumbered into inaction. Thus, the fewer behaviours they are taught, the likelier they are to exhibit those behaviours.

In addition to restraint in fear appeals and user-tailored training, a study found that professional preparation, culture-awareness (see also Karjalainen, Siponen, Puhakainen, & Sarker, 2013), user feedback (see also Bauer et al., 2017), and, most importantly, sustainability once attitude shifts take place are factors that support the effectiveness of ISAP's (Bada et al., 2015).

Finally, SANS (2019) highlights that successful implementation requires sufficient investment. Firstly, the programme owner should be able to dedicate full-time to it, as part-time obligations are the primary limitation to programme maturity. In addition, data shows that successful implementation requires at least two full-time employees, while 3.9 employees correlated with optimal

programme maturity. Moreover, although information security is often perceived as a technical branch, awareness professionals should also possess soft skills, such as communication and marketing, to effectively educate and verbalize programme objectives (Bauer et al., 2017; Caldwell, 2016; SANS, 2019). Organizations can also utilize voluntary information security ambassadors for a few of hours monthly to further the agenda of information security management at high scale and low cost (Spitzner, 2017).

In conclusion, based on the literature review, organizations can effectively gain an advantage against information security threats by investing in the knowledge and awareness of their employees (Hwang et al., 2017; Safa et al., 2016; Gardner, 2014; Verizon, 2018; SANS, 2019; Ponemon, 2020; ISO/IEC, 2018). By increasing awareness, compliance will simultaneously increase (Workman et al., 2008). Simply put, when we know better, we also do better. Nevertheless, this has proven to be more complex as behavioural sciences seldom allow such linearity (Sommestad et al., 2014). As stated, human nature, inadvertence, and omission form a gap between knowledge and behaviour. Such a phenomena, the knowing-doing gap, has been theorized to exist in information security as well (Alfawaz et al., 2010; Workman et al., 2008) and initial proof of its existence has been demonstrated (Gundu, 2019), albeit narrowly. As the topic requires further validation, it can be hypothesized that:

> **H1A** There is a weak ($0.25 < r < 0.5$) or moderate ($0.5 < r < 0.75$) correlation between knowledge and behaviour (compliance) in the organization. Knowledge is, on average, higher than behaviour.

This means that the knowing-doing gap should be observable in irregularity and a lower correlative relationship between knowledge and behaviour as well as higher knowledge than perceived secure behaviour. The descriptive terms (weak, moderate) regarding correlation can be considered as a rule of thumb rather than entirely accurate or entirely arbitrary. However, they are useful in scaling the interaction between knowledge and behaviour – or lack thereof – in case correlation is far from absolute.

Moreover, despite that information systems security research carries a decades-long history, the academic community has yet to demonstrate which theories are best at explaining phenomena and solving dilemmas in the sphere of information security (Siponen & Baskerville, 2018). Nevertheless, all the examined theories have some merit in their ability to explain and provide a theoretical foundation for improving compliance (Workman et al., 2008). To some extent, shifts in attitude indicate the internalization of collective norms and the point where the individual is inherently not only compliant, but personally determined to engage in secure behaviour. If so, not only is compliance likely to improve, but may also result in the improvement of the information security culture of the organization as well, which in turn can revert to improved compliance, creating a virtuous cycle (Thomson, 2010; Ifinedo, 2014; Sherif et al., 2015). In this sense, shifts in attitude might represent the highest form of improvement regarding human

information security. However, apart from TPB, attitude is seldom taken into direct consideration, despite its evident relevance (Sommestad et al., 2014), which leaves intrinsically motivational potential unused. As opposed to deterrents and fear appeals, increasing knowledge and cultivating attitudes can potentially provide organizations less-rigid means to influence compliance (D'Arcy & Hovav, 2009). However, despite its apparent importance, the role of attitude compared to knowledge has not been established, apart from indirect results and suspicions (Bauer & Bernroider, 2017; Siponen et al., 2014; Sommestad et al., 2014; Safa et al., 2015a) and the implication that attitude is a mediator as embedded in the KAB model. Hence, two important hypotheses follow:

H1B The effect of attitude on perceived secure behaviour is greater than that of knowledge.

H1C Effects between knowledge and behaviour are mediated by attitude toward behaviour.

4 DEMOGRAPHIC FACTORS IN INFORMATION SECURITY AWARENESS

There is also a need to consider organizational factors, such as demographics, when assessing compliance and awareness (Goel & Chengalur-Smith, 2010). However, although demographic considerations are widely applied in other fields (Chua et al., 2018), there is a scarcity of studies that incorporate demographic factors into awareness research (Moody et al., 2018; Whitty, Doodson, Creese, & Hodges, 2015). Nevertheless, acknowledging demographic factors bears importance as it allows organizations to plan and manage their awareness interventions purposefully. Furthermore, compliance and awareness do not solely result from a function of individual factors but a function that includes factors that stem a situational, social environment (Alfawaz et al., 2010).

Hence, the following chapter presents a set of demographic factors, both individual *and* organizational, that potentially influence information security awareness. The section covers literature on each of these factors and supplements the justifications for examining these factors by reason where prior research is lacking. The first two of the following are organizational factors and the latter three individual ones:

- *unit*,
- *personnel group*,
- *age*,
- *work experience*, and
- *formal education*.

In distinction to organizational factors, individual factors can be considered global; results thereof are, in theory, generalizable into a broader population whereas organizational factors are constrained by the boundaries of the target organization. Thus, studying individual factors also introduces comparable results into an international framework, where variance in information security awareness between nationalities and ethnicities have been observed (Hovav & D'Arcy, 2012; Lubis, Fauzi, Liandani, & Lubis, 2020; Chua et al., 2018).

4.1 Organizational factors

The justifications for investigating the influence of the unit and personnel group of an individuals' information security awareness are embedded in the structure and nature of the organization. The target organization is a Finnish-based entity with broad international connections and delegates abroad. The organization provides employment to hundreds of professionals with diverse vocational backgrounds. The organization is longstanding and possesses, as many modern businesses and non-profit organizations alike, considerable interest in safeguarding the security of its information. The workforce in Finland alone consists of hundreds of employees distributed primarily across five units in physically separate locations and with their respective security departments. Therefore, as responsibility for information security is partially shared across the security departments of each unit, there is reason to suspect that variance in levels of information security awareness between different units presides. Simultaneously, measuring information security awareness unit-wise is in a sense an indicator of success for each security department.

Moreover, the workforce is comprised of six distinct personnel groups, such as executives or subject-matter experts. These personnel groups are represented in each unit (although not evenly), as depicted in the matrix-like perspective of the structure of the organization in figure 9. Employees can be clustered into personnel groups based on similarities in job roles, career paths, and vocational backgrounds. These distinctions are, with a sufficient degree of probability, significant enough to produce differences in information security awareness. There is also evidence that such differences may exist; studies have shown that there is variance among personnel groups (or statuses) in terms of secure behaviour (Lubis et al., 2020) and awareness (Mittal & Ilavarasan, 2019). However, the studies were conducted in an educational setting amongst different students and staff positions and are as such incommensurable.

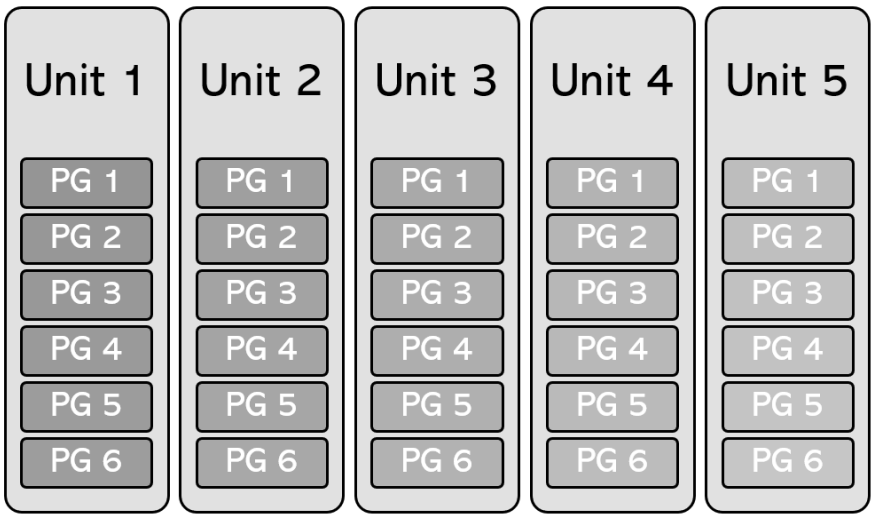

FIGURE 10 Organizational structure, units, and personnel groups (PG)

Moreover, a key factor for information security awareness, this study, and the primary backbone of the argument that information security awareness might vary between physically and structurally segregated parts of an organization is *organizational culture* (Wiley, McCormac & Calic, 2020; Knapp et al., 2009; Greene & D'Arcy, 2010). Like all social groups, the organizational setting has its own organizational culture, which Schein (1989, p. 278) describes as:

> "the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and, therefore to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."

Nel and Drevin (2019, p. 148) concisely describe the term as "the feel of the organization to its members that directs and motivates employee efforts". Within the larger concept of organizational culture is the integral security and information security culture of the organization (Thomson, Von Solms, & Louw, 2006), the collection of conventions that "encompass all sociocultural measures that support technical security measures" (Schlienger & Teufel, 2003, p. 47). However, information security culture may be contradictory to organizational policy. Thus, culture underlies that the immediate social climate can sometimes become a source for practical conventions that is preferred over official policy. Hence, different units or personnel groups within the same organization, especially in larger organizations such as the target organization, may possess different average levels of information security awareness, just as some individuals are more aware than others (Furnell & Rajendran, 2012). In fact, results have shown differences in subcultures regarding information security and associated beliefs, i.e., what constitutes secure behaviour and the probability of compliance under pressure to perform (Ramachandran, Rao, & Goles, 2008).

The reason behind subculture, or the compartmentalization of information security culture, lies in social phenomena that are applicable to the workplace (Cheng et al., 2013, p. 449). Although some models disregard the role of social factors, there is a consensus among studies that they are significant in terms of compliance to norms (Moody et al., 2018). Positive example set by top management, direct supervision, and peers all motivate individuals to comply with policy (Chan, Woon, & Kankanhalli, 2006; Furnell & Rajendran, 2012; Zinatullin, 2016). Social disapproval of peers also encourages to comply (Padayachee, 2012). Conversely, non-compliant behaviour of peers influences non-compliance as well (Junger et al., 2017; Hwang et al., 2017). People are also willing to be non-compliant due to peer pressure; people just want to "fit in" rather than arouse a conflict (Weirich & Sasse, 2001). Moreover, people are sensitive to their peers' behaviour not solely because of social approval, but to ease one's own decision-making process as well (Cialdini, Martin, & Goldstein, 2015) and look for cues on how to act (Junger et al., 2017), a form of social learning. For instance, in a study on Facebook encompassing some 50,000 people, displaying the number of "friends" who utilize security features on Facebook to users led to 37% more of

those users to utilize the same features, compared to users who were not displayed (Das, Kramer, Dabbish, & Hong, 2014). Furthermore, social norms are a source of influence for compliance (Siponen et al., 2014; Pahnila et al., 2007), attitudes towards compliance (Ifinedo, 2014) but also, oppositely, to whether individuals submit to conducting security violations (Guo et al., 2011) and unethical behaviour (Gino, Ayal, & Ariely, 2009). Thus, culture works both ways and can either be a "vaccine" or a "virus".

In summary, considering prior research, the structure of the target organization, and the potential that structure has in forming subcultures with varying values, assumptions, and conventions regarding both units and personnel groups, the following hypotheses are suggested:

H2A There are significant differences in information security awareness between units within the target organization.

H2B There are significant differences in information security awareness between personnel groups within the organization.

4.2 Individual factors

Explicitly organizational factors appear to be, at least to the extent of the literature review, an understudied aspect of information security awareness. However, although a certain dearth remains there as well (Whitty et al., 2015), individual factors have been more thoroughly covered. Perhaps the most examined individual factor is that of age.

There is a popular assumption that suggest the "digital natives", the younger generations that were born into a world where information technology and the Internet pre-existed, are more apt at functioning securely in the digital domain (Caldwell, 2016). Conversely, it is logically presumed that the "digital immigrants", who have encountered ICT only later in life, are oppositely more vulnerable due to having less technology-aware formal education and perhaps more reluctantly adopt technology into their daily lives (Hadlington & Chivers, 2018). Despite the logic, a substantial body of evidence suggest the contrary: that, in fact, older employees tend to have better information security awareness (Pattinson et al., 2019; McCormac et al., 2017a; Ögütçü et al., 2016; Hadlington & Chivers, 2018; see also Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). In a study conducted with Malaysian workers, age represented 55% of the predictability of the information security awareness mean score (Chua et al., 2018). However, these studies were conducted with Australian, Malaysian, or Turkish populations. As information security issues may vary on a national basis (Hovav & D'Arcy, 2012), a need for a broader international data remains. As far as the literature review covered, only Oksanen and Keipi (2013) have studied a similar topic in Finland: vulnerability to cybercrime. In line with the results previously mentioned, results indicated that the youngest age group was the most

vulnerable. However, this study did not examine information security awareness per se, which again leaves room for further validation. Thus, the following is proposed:

> **H2C** There is a significant difference in information security awareness between different age groups.

Two further factors, namely work experience or educational level, appear far less studied. Nevertheless, both seem intuitively appealing. Prior knowledge in the form of education or work experience helps individuals resolve problems (Lee et al., 2016). Therefore, it makes sense that higher educational level and work experience would predicate higher levels of information security awareness, the latter especially in terms of organizational policy. In essence, the broader and longer the experience with an organization or the higher the level of formal education, the wider the information security awareness of the individual. The proclivity to seek new information and the inadequate knowledge of normal organizational practices may place individuals with shorter tenures or employments susceptible to risky behaviour (Mittal & Ilavarasan, 2019).

However, for some reason, the role of work experience or formal education on information security compliance and awareness appears to be scarcely examined in previous research. An exception is Chua et al. (2018), who studied both and found that there was no observable correlation between work experience and information security awareness but that higher education levels correlated with information security awareness. The positive correlation between formal education and information security awareness (Ögütçü et al., 2016) and compliance (Vance et al., 2012) has been observed in other studies as well. Moreover, in a qualitative study with industry experts, education was thought to have a low to medium impact on compliance (Furnell & Rajendran, 2012). Nevertheless, as the coverage is somewhat slim, there is room to investigate and validate further. Hence, the following hypotheses are presented:

> **H2D** There is a significant difference between work experience (within the same employer) and information security awareness.

> **H2E** There is a significant difference between the level of formal education and information security awareness.

5 RESEARCH METHODOLOGY

The choices regarding research methodology and their justifications are covered in the following chapter. First, the choices associated with the measures are depicted followed by a presentation of the questionnaire and the supplementary measures used in the study. Thereafter, the limitations concerning reliability and validity are addressed, both regarding prior studies where the HAIS-Q has been utilized as well as this study. Next, the data collection and participants are described, including descriptive statistics of the sample. Lastly, in the procedural subsection, methods regarding data analysis are presented.

5.1 Measures

The study was conducted as a survey with a strong statistical backbone supported by a branch of quantitative content analysis. Firstly, the study leaned heavily on statistical methods to test the hypotheses proposed in chapters 3 and 4. Furthermore, by analysing the contents of the open answers given by the respondents, the study attempted to determine why individuals deviate from secure behaviour against their knowledge, in other words, to provide plausible explanations to the knowing-doing gap, as outlined in research question 2.

5.1.1 The HAIS-Q

Information security awareness in the survey was measured with the Human Aspects of Information Security Questionnaire (HAIS-Q). The HAIS-Q measures information security awareness through seven focus areas, or constructs, all relevant topics for information security awareness. While other focus areas could potentially be included, it was not done to retain the integrity of the questionnaire. Thus, the focus areas included the original focus areas that, nevertheless, envelop the concept of information security awareness well, as demonstrated in section

2.2.3: password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting.

However, the focus areas were not the constructs used for analysis. As observable in table 4, the focus areas were further divided into three sub-areas. These sub-areas were measured via separate knowledge, attitude, and behaviour items. The three aspects of knowledge, attitude, and behaviour were the constructs used in the analysis, each consisting of 21 items in total, or 63 for the entire questionnaire (Parsons et al., 2017). This is the first occasion the HAIS-Q has been utilized to measure aspects instead of focus areas (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2013; Parsons et al., 2014a, Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2014b; Parsons et al., 2015; Pattinson et al., 2015a; Pattinson et al., 2015b; Pattinson et al., 2016, Calic et al., 2016; McCormac et al., 2017a; McCormac et al., 2017b; Parsons et al., 2017; Hadlington & Chivers, 2018; Mittal & Ilavarasan, 2019; Pattinson et al., 2019). The setup of the entire questionnaire can be observed in appendix 1.

TABLE 4 Aspects (constructs), focus areas, and sub-areas of the study

Aspect	Focus area	Sub-area
Knowledge / Attitude / Behaviour	Password mgmt	Using the same password across multiple platforms
		Sharing passwords with colleagues
		Using strong passwords
	Email use	Clicking on links from unknown senders
		Clicking on links from known senders
		Opening attachments in emails from unknown senders
	Internet use	Downloading files from the Internet
		Accessing dubious websites
		Entering personal information online
	Social media use	Reviewing social media privacy settings
		Considering consequences of posts
		Posting about work on social media
	Mobile devices	Physically securing mobile devices
		Sending sensitive info over public wireless connections
		Shoulder surfing
	Information handling	Disposing of sensitive printouts
		Inserting removable media in work computers
		Leaving sensitive material on the work desk
	Incident reporting	Reporting suspicious behaviour or colleagues
		Ignoring colleagues' poor IS behaviour
		Reporting all incidents

Although there are other measurement constructs available to measure compliance, few incorporate knowledge, attitude, and behaviour aspects. Moreover, the HAIS-Q was chosen based on additional merits such as:

- Robust reliability and validity (see table 5; see also Hadlington & Chivers, 2018, p. 4),
- Broad set of consistent factors,
- Applicability to contemporary threats and TTP's (see section 2.2.3),

- Applicability to organizational policy (the HAIS-Q measures concepts that are relevant for the target organization).

The greatest benefit of the HAIS-Q is its engagement in a score of diverse research projects and samples (e.g., Hadlington & Chivers, 2018). As partly demonstrated in table 5, over 2 000 working professionals and governmental personnel has taken the questionnaire to date, vouching strongly for the use of the HAIS-Q in this study as well. While the Multiple Criteria Decision Analysis (MDCA) model exemplified by Kusumawati (2018) utilizes the same KAB framework as the HAIS-Q and is intuitively more versatile, the latter was preferred due to better comprehensiveness in terms of latent constructs.

TABLE 5 Development and use of the HAIS-Q (Parsons et al., 2017, p. 42)

Purpose	Sample	*n*	Reference
Initial content validity	Australian government employees	203	Parsons et al. 2013 Parsons et al. 2014a
Validation of KAB	Working Australians	113 500*	Parsons et al. 2014b
Assessment of ISC	Working Australians	500*	Parsons et al. 2015
Assessment of individual differences	Working Australians	500*	Pattinson et al. 2015a
Content validation	Australian university students	23	Pattinson et al. 2015b
Construct validation	Australian financial employees	198	Pattinson et al. 2016
Content validation	Information security experts	15	Calic et al. 2016
Assessment of individual differences	Working Australians	505**	McCormac et al. 2017a
Test-retest reliability, internal consistency	Working Australians	197	McCormac et al. 2017b
Construct validity	Australian university students and Working Australians	112 + 505**	Parsons et al. 2017

*) same dataset
**) same dataset

Moreover, it is worth noting that Moody et al. (2018) have devised a promising model that unifies 11 theoretical foundations and factors and their construct applications. Regardless of the apparent formidability, the proposed model, the Unified Model of Information Security Compliance (UMISPC), is too broad and specific to be reasonably administered to the target organization. In addition, although the UMISCP appears promising, it has yet to be proved compared to the HAIS-Q. Furthermore, though alternate measures exist, they address more specific fields such as password management (Stanton et al., 2005) or protection of mobile devices (Mylonas, Kastania, & Gritzalis, 2013), which renders them unsuitable to produce a comprehensive overview of the information security awareness of the target organization.

As stated, the HAIS-Q comprises of 63 items across 7 focus areas, or constructs. Thus, each construct comprises of nine items examined through three aspects of information security awareness: knowledge, attitude, and behaviour. While the seven focus areas represent central topics for information security

awareness, they were not utilized as variables in the study. Instead, variables representing knowledge, attitude, and behaviour were used. To generate these composite variables, all items under knowledge, attitude, and behaviour were summed to produce three scores, respectively. Thus, each score comprised of 21 items each, distributed across 7 focus areas each including three items.

In the survey, items that pertained to the HAIS-Q were coded on a five-level Likert scale, between "strongly agree" and "strongly disagree", which is customary to the questionnaire (Parsons et al., 2017, p. 46). Thus, the questionnaire remains simple and reasonable yet discrete enough to provide accurate, quantifiable data. Still, it must be noted that the metric and encoding utilized in this study can primarily indicate order between different values of a variable and intervals only with restrictions (Singleton & Straits, 2018, pp. 130–131). This means, for example, that the difference between a respondent's value 4 and 5 correspond, in the real-world, to an exact observable interval of 1 along a finite scale. Therefore, since this type of ordinal measurement perhaps mainly portray the rank order of cases, the efficacy of older statistical techniques, such as Pearson's correlation coefficient, are only suitable for use with due discretion.

5.1.2 Demographic variables

Moreover, the questionnaire was supplemented with items that measure demographic variables, which were primarily used to test hypotheses H2A–E. The introduction of demographic items enabled thorough analysis based on organizational demographics that can help to identify key areas of development and strengths within the target organization and validate or challenge existing scientific knowledge, as presented in the hypotheses. The variables are shown in table 6 along with the response alternatives. Age and work experience were grouped to ease analysis. To even the number of respondents in experience group, work experience was grouped more narrowly at short experience and broadened at longer since it was estimated that the population median age would be high.

In addition, the demographic variables were utilized as control variables to eliminate extraneous explanations and to improve the explanatory power of the regression model associated with H1A–C (Singleton & Straits, 2018, p. 89).

TABLE 6 Demographic variables and their response alternatives

Unit	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5	
Personnel group	PG 1	PG 2	PG 3	PG 4	PG 5	PG 6
Age group	18-29	30-39	40-49	50-		
Work experience	1-3	3-10	10-20	20-		
Educ. background	Prim. school	Second. school	Under-grad.	Grad.	Post-grad.	

The background variables were tested against a standardized composite information security awareness score that comprised of all the knowledge, attitude, and behaviour scores.

5.1.3 Open items

Finally, the respondents had the voluntary possibility to provide open responses with respect to research question 1, why individuals omit complying to security policy. The respondents were asked to complete the following phrases with one or more plausible causes:

- If I were to violate information security policy, it would be due to:
- If I were to leave an information security incident unreported, it would be due to:

Response alternatives were initially developed to ease analysis but were later replaced by enabling open answers. In this way the answers of the respondents were not unduly restricted and provided a broader spectrum of answers beyond what the author would possibly have anticipated. The answers were analysed and clustered beneath topics at the authors discretion but guided by the theory outlined by the literature review outlined in section 2.2.2.

To summarize, the independent (IV), dependent (DV), and mediation variables (MV) and their relationship to the hypotheses are illustrated graphically in the quantitative research model in figure 10. Squares in the model are measured variables and squares composite variables. The circles enveloping the focus areas are grey to highlight that they were not directly used in the study. Variables M, X, and Y represent the mediation relationship. The qualitative, open items are not represented in the model.

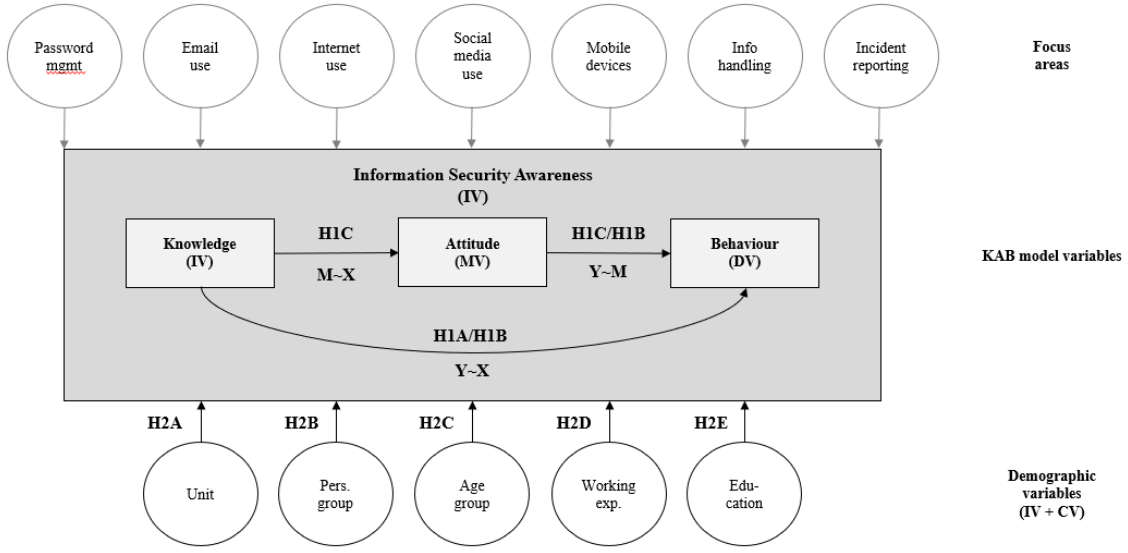

FIGURE 11 Research model

5.1.4 Reliability and validity

The validity of the HAIS-Q measure has previously been tested with solid results. Firstly, convergent validity, which demonstrates that the measure used produces reciprocal results with other, theoretical methods of measurement that investigate the same real-world phenomena, was tested by applying an empirical phishing study (Parsons et al., 2017, p. 43). Secondly, a thorough study to assess the internal reliability was conducted with a substantial sample (n=505) of the Australian working population. Internal reliability was demonstrated with Cronbachs's alpha. All scores landed between 0.75 and 0.82, which is above the arbitrary but recommended index of 0.70 (Parsons et al., 2017, p. 44). A study conducted by McCormac et al. (2017b, p. 6) yielded similar results: in a test-retest setting indexes varied between 0.75–0.83 in the first and 0.78–0.84 in the second test. The conclusion was that HAIS-Q was both externally reliable and internally consistent, although the HAIS-Q has also been found not to hold well on other occasions (Mittal & Ilavarasan, 2019), likely due to methodological weaknesses.

Since the questionnaire was originally in English but administered in two different languages (Finnish and Swedish), the possibility of encountering both translational issues and ambiguity were evident. Therefore, the questionnaire was administered to a pilot sample (n=19) and subjected to evaluation of two bilingual language experts. After gathering information from the pilot sample, results did not indicate that the survey contained issues that might dispute the reliability of the study. However, the feedback from the language experts prompted changes in the formulation of the items. By refining the questionnaire in this manner, the study was outlined so that the use of ambiguous language and the subsequent possibility of misinterpretation decreased (Singleton & Straits, 2018).

Reliability and construct validity were measured with Cronbach's alpha. Cronbach´s alpha can be understood as an index that indicates levels of reliability within a measurement construct according to the covariance of item-pairs (Singleton & Straits, 2018, p. 136). In this study, Cronbach´s alpha was calculated from the relationship and correlation of the items underlying each aspect, knowledge, attitude, and behaviour as well as each focus area. Nevertheless, there are at least two notable details worth highlighting with respect to using Cronbach's alpha.

Cronbach's alpha assumes unidimensionality within the constructs and cannot discern whether it is multidimensional. A unidimensional scale expects factor loadings to be equal within a latent construct. In practice, this means that a factor analysis should yield same values for all elementary variables (Cortina, 1993). However, the HAIS-Q is multidimensional. As proven in a study by Parsons et al. (2017), factor loadings within focus areas of the HAIS-Q vary from 0.04 in incident reporting and 0.27 in social media use, with the average variance being 0.14. In terms of this study, the composite scores of knowledge, attitude, and behaviour comprise of the "dimensions" provided by the seven focus areas,

which escalates multidimensionality even further but simultaneously increases the number of items in the construct.

Since the focus areas in this study were measured with nine items from three distinct perspectives, knowledge, attitude, and behaviour, and with the aim of observing discrepancy between the knowledge and behaviour scores (H1A), it was presumable that this would reflect upon construct reliability should the hypothesis hold. Therefore, multidimensionality combined with some inferior item intercorrelations influenced the Cronbach's alpha score (Cortina, 1993). In fact, the results thus suggest that respondents have truly answered differently to, for example, knowledge-related and behavioural items.

Cronbach's alpha also assumes that respondents answer *something* consistently, or *correctly*, to each item and does not tolerate non-conformity well. Therefore, each time a respondent answered contrarily to his or her peers, the response reflects negatively on alpha, even though the respondent has given an honest answer. Thus, alpha says nothing about the extent to which items measure what it is intended to measure, only about the homogeneity of the data (Cortina, 1993). What alpha does reveal, however, is the average interrelatedness of items while simultaneously accounting for the items in the measure (Sijtsma, 2009). In short, while the sample remains heterogenous, reliability measured by Cronbach's alpha will inevitably be affected. But that does not mean the data cannot be internally consistent.

Therefore, the alpha index of 0.67 concerning the knowledge variable was accepted, thus disregarding the 0.70 cut-off criterion often advocated as a satisfactory minimum among scientific customs. After all, what a satisfactory level of reliability is depends on how a measure is being used and neither are values strict cut-off points (Nunnally, 1978). The other composite constructs appeared reliable, as shown in table 7. Nevertheless, the focus area constructs undeniably suffered from issues of low reliability: four out of seven values were between 0.60–0.70 – even with extenuating circumstances accounted for and even though strongly contradictory items were discarded. These values were significantly lower than those presented by Parsons et al. (2017). However, the focus area constructs were not directly utilized in the analysis, as denoted in table 7.

TABLE 7 Descriptive statistics of reliability of the constructs in the study

Focus area	α	Mean	Std	Note
Knowledge	**0.67**	**96.77**	**10.77**	
Attitude	**0.80**	**99.63**	**7.10**	
Behaviour	**0.81**	**99.15**	**6.84**	
Password management	0.71	42.11	3.95	
Email use	0.64	35.89	5.33	Item K4 discarded
Internet use	0.75	43.11	2.18	
Social media use	0.66	42.22	2.66	
Mobile devices	0.69	38.81	1.87	Item K13 discarded
Information handling	0.60	43.87	1.86	
Incident reporting	0.83	41.86	3.50	

There are, however, two plausible explanation for low reliability within the focus areas. Certain possibly outdated items aroused controversy, which could be observed as increased irregularity and some feedback from respondents. Ambiguity was also caused by non-idiomatic translation. Non-idiomatic translation was initially chosen as a principle to help refrain from unintentionally altering the questionnaire. However, this caused misinterpretations among some of the items. Despite this, some conclusions were made on how to improve the questionnaire. The questions "I am allowed to click on any links in emails from people I know" and "when working in a public space, I have to keep my laptop with me at all times" caused the greatest variance among the HAIS-Q items and thus decreased reliability in Cronbach's alpha. In the first case, this was likely due to the translation to Finnish, which was done non-idiomatically. This led to ambiguity in the questionnaire. However, the "real answer" also depends on whether the authenticity of the sender has been established or not. In the latter case, some respondents may have thought that they always need to bring their computers when working in a public environment, which is of course untrue.

In addition, since length and complexity are determining factors for password entropy, and thus security, and memorability for usability from a human perspective (Woods & Siponen, 2019), the items regarding password management may require change. For example, to the form: "When choosing passwords, their length, complexity, and memorability should be considered". Lastly, when using the HAIS-Q, the author should include introductions to knowledge, attitude, and behaviour items to orientate the respondent into each theme and ensure that the respondent answers from the right perspective. While this has been done in previous studies (e.g., Parsons et al., 2017), it was not implemented during this survey.

Social desirability effect

The social desirability effect, in theory, suggests that there will be some inaccuracy in measurements that requires respondents to verbally report on behaviour that can be deemed as socially undesirable and contradictory to one's own self-image or established norms social environment (Singleton & Straits, 2018, p. 133; Cox, 2012). Social desirability might be a particularly concerning phenomena in a punitive working environment, where employees prefer socially desirable images over encountering issues in the workplace (McCormac, 2017b, p. 8). Therefore, measurements generally underestimate the prevalence of socially undesirable behaviour and attitudes. In the case of this study, this implies that answers were inevitably, but systematically, positively biased. Thus, the results might portray a more favourable yet distorted view of information security awareness within the studied sample.

This limitation was initially investigated by McCormac et al. (2017b) with a sample of 197 working Australians. The study found promising results for the HAIS-Q but also prompted need for further development: the constructs were neither internally consistent nor precise. Thereafter, Parsons et al. (2017, p. 44) performed Pearson correlations between HAIS-Q responses and an eight-item

version of the Crowne-Marlowe Social Desirability Scale, a measure that assesses the significance of the social desirability effect on a questionnaire. The conclusion was that only six items (out of 63), slightly less than 10%, had a correlation that imply a variance greater than 6%. Thus, a careful estimation could be made that accumulating inaccurate data is not a significant threat as the overall notion was that respondents generally provide truthful answers to the questionnaire. Moreover, bias in this study was further avoided by administering the survey online: participants who respond online feel less judged and therefore provide more truthful answers (Duffy, Smith, Terhanian, & Bremer, 2005).

Objective and perceived behaviour

A popular convention in information security research has been to survey compliance through the reports of employees and their perceived compliance (Cram et al., 2017). However, this raises an issue since there is always some discrepancy between *actual* behaviour and *perceived* behaviour. There is evidence, for instance, that studies that measure perceived and actual behaviour yield contradictory results (Workman et al., 2008; Guo et al., 2011). Arguably, measuring compliance as a survey is challenged since such a method measures perceived compliance or non-compliance (sometimes also misuse) through the individual's intention or attitudes instead of actual (sometimes also objective) compliance (Sommestad et al., 2014). In brief, perceived compliance, intent to comply, or attitude towards compliance is not equal to actual compliance.

While this poses a valid argument, a score of studies shows that intent to comply significantly influences and results in actual compliance (Pahnila et al., 2007; Siponen, Pahnila, & Mahmood, 2010; Siponen, Mahmood, & Pahnila, 2014; Ifinedo, 2014; Safa et al., 2015b). Furthermore, the systematic literature review by Sommestad et al. (2014) has showed with reasonable effect sizes (0.29–0.50) that actual compliance did follow from both attitudes towards compliance and intent towards compliance. The results strongly favour monitoring compliance through subjective perceptions and show that a survey is a plausible approach to gain insight on compliance. Lastly, the discrepancy regarding intent to comply and compliance has been demonstrated to be moderated by individual factors, such as personality traits, which may explain varying results in different samples (Shropshire et al., 2015).

Although some propose an ethnographic approach to measuring compliance (Workman et al., 2008), evaluating human performance longitudinally and across a large population entails other issues. Firstly, it is very difficult to produce a controlled environment and ascertain reliability and validity (Vroom & Von Solms, 2004). In addition, capturing actual omissive behaviour is difficult, since reporting clearly uncompliant behaviour can be detrimental to the individual (Cox, 2012). Moreover, conducting field research can lead to the observer's paradox, where the observer inadvertently impacts the phenomenon being observed. This does not suggest that studying compliance ethnographically is impossible, but problems concerning measures, methods, and situational and subjective factors cause random error, which must be considered (Vroom & Von Solms, 2004).

An ethnographical study would neither be able to take all possible information security behaviours into account due to the ideographic nature of behaviour (Workman et al., 2008). On the contrary, using a survey enables the collection of broad samples from large populations and, subsequently, the processing of even larger data sets quantitatively. This, in turn, eases the detection of statistical significances and reinforces inferences drawn from the data. In conclusion, despite its drawbacks, a survey is a scientifically viable approach to study information security awareness.

5.2 Participants

As described in section 4.1, the target organization was a large and longstanding Finnish organization. The sample was drawn from a population that comprised of the entire personnel of the organization. To obtain sufficient data from a broad spectrum of respondents, data collection was randomized, providing equal possibilities for the entire population participate and thus ensuring that the sample accurately represented the characteristics of the population (Elmes, Kantowitz & Roediger, 2006, p. 172). Randomization was achieved by disseminating the questionnaire to the entire organization via email and collecting responses over a period of six weeks, ensuring everyone had a chance to respond. During that period, two reminders were delivered, influencing response rates by roughly 20%.

However, this kind of randomization posed a slight risk of *non-response bias* or *participation bias*. The theory concerning these cognitive biases purports that only individuals affectively dispositioned towards the topic of a study are more likely to voluntarily participate in it. The difference stem from the fact that people who are most likely to partake in the survey are systematically different from those who do not (Fowler, 2009, pp. 51–56). To reverse these effects, participants were encouraged respond despite that they may not by person or profession hold information security issues personally relevant. However, due to the integral role of security in the organization, employees were be expected to harbour preoccupation towards taking the questionnaire, which might have prevented unilaterality. Ultimately a total of 287 respondents replied to the questionnaire, which represents a substantial amount of the population. As for the open items, A total of 114 responses were accumulated regarding incident reporting and 149 regarding omission of information security norms. Descriptive data on the sample by background variable are presented in figure 11. As shown, there was relatively high dispersion amongst the respondents in terms of unit, personnel group, and educational background, whilst the distributions were more even amidst age groups and work experiences. Thus, grouping within age and work experience may be considered successful. Overall, all variables received sufficient respondents in each category with the exception that participants pertaining to PG2 and the elementary school background were few. However, this was observed not to significantly influence the measurement of variance.

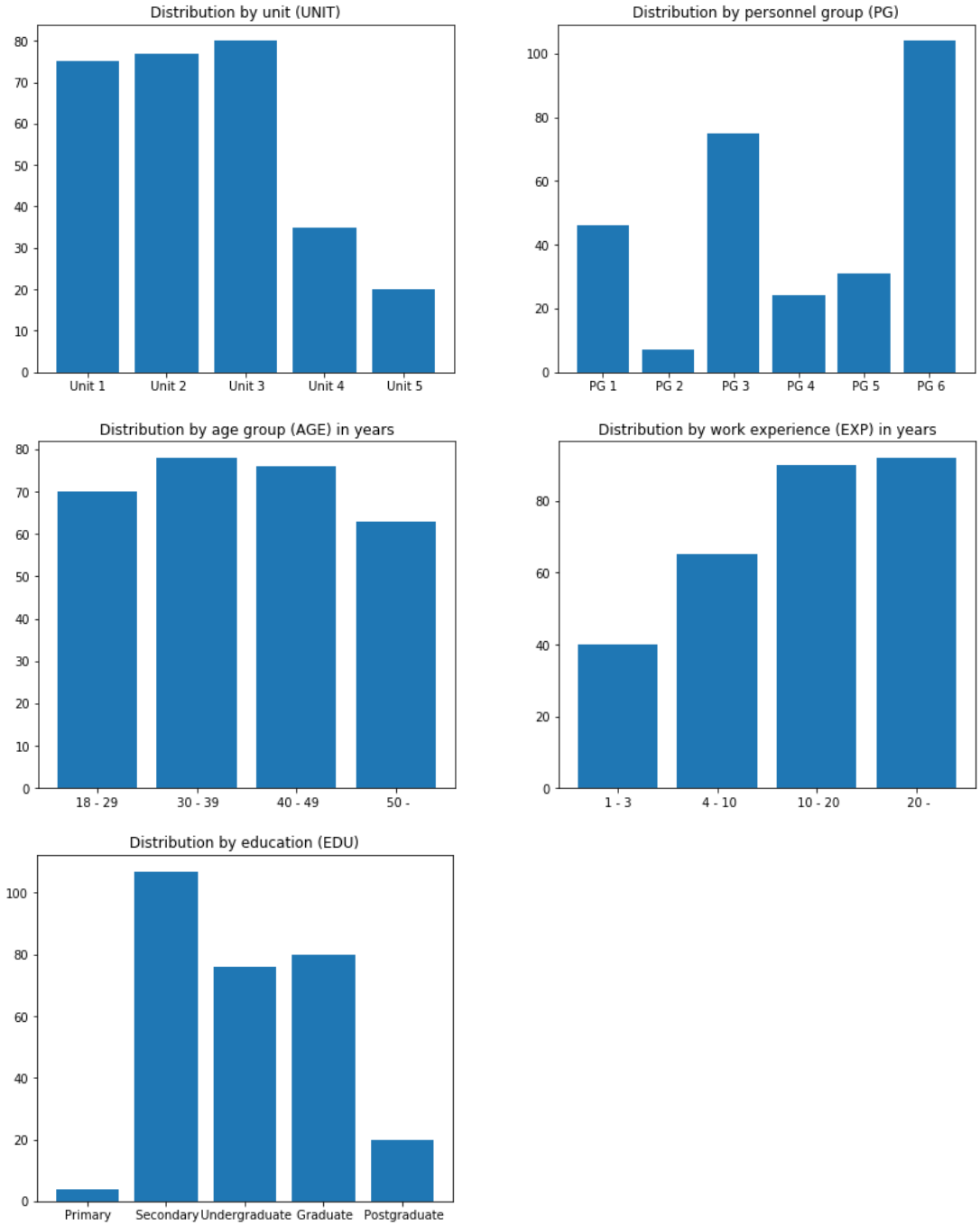

FIGURE 12 Descriptive statistics of the respondents

In addition, respondents were asked to report how often they handle sensitive information, such as personally identifiable information, or use computers to conduct their work. As figure 12 shows, computer usage (CU) and sensitive information usage (SIU) are extremely commonplace within the sample. 98.3% of employees use computers and 81.9% handle sensitive information at least weekly, while 76.7% and 37.3% do so daily, respectively. The substantial amount of work-related sensitive information and computer usage illustrates that information security is a relevant issue within the sample.

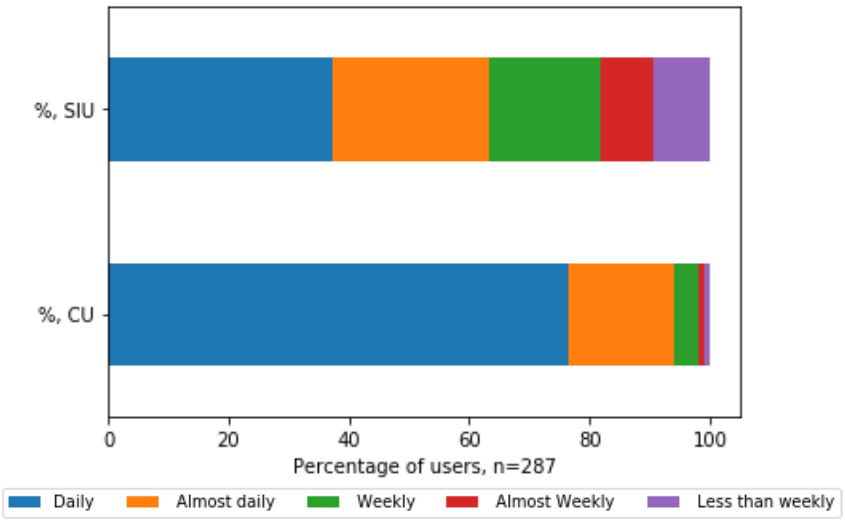

FIGURE 13 Proportions of computer and sensitive information usage

5.3 Procedure

Because of the bilingual and international nature of the target organization, the initially English HAIS-Q was translated into Finnish and Swedish by the author so that participants could choose to respond in their preferred language or native tongue. The supplementary items were formulated in Finnish and Swedish as well. The translations were given to two bilingual language experts and native speakers for inspection to decrease ambiguity. The questionnaire was administered as a through Webropol, a web-based survey service.

The analysis was conducted with two separate methods: purely statistical quantitative methods, Pearson's correlation, linear regression, and analysis of variance (one-way F-test), and quantitative content analysis, which was used to categorize responses to the open questions under key themes. The maximum number of response categories was not restricted. Mediation analysis was conducted using the Baron and Kenny (1987) method. The statistical significance of the mediation was determined using the bootstrapping method. The analysis methods are concisely illustrated in table 8.

TABLE 8 Statistical tools in the data analysis per hypothesis

Hypothesis	Measurement	Statistical significance
H1A	Pearson's r Regression coefficient	Two-tailed test
H1B	Linear regression	Student's t-test
H1C	Baron and Kenny (1987) method (mediation)	Bootstrapping (two-sided test)
H2A-E	Comparison of means Linear regression	F-test Student's t-test

In the regression analysis phase, the regression model was tested in two separate blocks for additional contrast: first with only the control variables and then with the knowledge and attitude scores included. The explanatory power of the construct, or the proportion of the variance in the dependent variables, was measured with the coefficient of determination (R^2) and subsequently adjusted (R_{adj}) to account for volatility when extraneous, latent variables were added to the model.

In the analysis phase, the maximum value for statistical significance, the alpha, was arbitrarily set to 0.05 at all stages, according to scientific conventions. Results with a statistical value above alpha were discarded. All variables were also standardized to achieve notional common scaling. The average score of each variable was subtracted from each individual score and divided by one standard deviation. The data was also scoped for anomalies (Singleton & Straits, 2018, p. 496), such as ambiguous responses to open questions, which were subsequently discarded in the quantitative content analysis phase.

The data analysis framework utilized throughout the study was the Python programming language and its libraries and modules. In addition to data handling libraries NumPy and Pandas, Scikit (sklearn) and Scipy libraries as well as statsmodels and pingouin modules were used for statistical analysis. Matplotlib and Seaborn were the libraries of choice for data visualization. Python was chosen mainly due to the authors learning purposes. However, McKinney (2017, p. 1) notes that Python has elevated its appeal as a data analysis tool in recent times and is well suited for handling multidimensional datasets and analysing multiple spreadsheet-like tables, such as .csv format also utilized in this study. All code was run as Jupyter notebooks on a web browser.

Python provided a multitude of built-in tools to draw measures of correlation and statistical significance from the data. Moreover, a string was written to assess reliability with Cronbach's alpha since there were no pre-existing modules for this purpose. The code was reviewed and approved by an expert from the University of Jyväskylä.

6 RESULTS

This chapter presents the obtained results. First, results gained from the statistical analyses are presented. This includes analysis regarding both the demographic variables' effects on information security awareness (H2A-E) and the relationships between knowledge, attitude, and behaviour (H1A-C). Finally, the answers to the open items are introduced in a separate subsection.

6.1 Effects of demographic variables on awareness

The results regarding demographic variables are illustrated with density distributions and scaled mean information security awareness scores. These are illustrated in figure 13 below. The results suggest that there is small, albeit observable differences between units within the organization (F=0.50), ranging from an average scaled information security awareness score of about -0.10 with the lowest to 0.21 with the highest scoring unit. This is to say that the best scoring unit scored, on average, 0.21 standard deviations better than the average respondent. Respondents representing unit 5 scored better than other respondents by a clear margin. In contrast, respondents that pertain to unit 2 scored clearly weaker than the average respondent. Similarly, results indicate that there were very mild differences between personnel groups (F=0.60), the range being roughly -0.13–0.15 standard deviations and personnel groups 1 and 5 having the overwhelmingly best scores. Conversely, personnel group 3 had clearly inferior average scores. However, values regarding both units and personnel groups were statistically insignificant (p>0.05). Therefore, the hypotheses associated with units (H2A) and personnel groups (H2B) could not be verified.

However, the results confirm the hypothesis (H2C) that there are statistically significant differences between age groups in terms of information security awareness (F=2.73, p<0.05). As the third row of figure 13 illustrates, the results suggest a positive correlative effect between age and information security awareness. Additionally, the oldest age group had a considerably higher mean level of

information security awareness. The scaled mean information security awareness scores are highlighted in the horizontal bar chart with a red colour to denote statistical significance. Descriptive statistics regarding age are shown in table 9.

TABLE 9 Descriptive statistics of information security awareness by age

Age	Count	Mean	Std	Min	25%	50%	75%	Max
18-29	70	-0.16	1.01	-4.32	-0.53	-0.04	0.52	1.41
30-39	78	-0.11	1.84	-4.48	-0.75	0.04	0.82	1.49
40-49	76	0.02	0.82	-2.14	-0.39	0.12	0.60	1.49
50-	63	0.29	0.89	-2.06	-0.21	0.52	1.00	1.41

The results regarding work experience share semblance with those of age, although the ratio of intra-group and extra-group variance was substantially lower (F=1.30). In addition, the result was also statistically insignificant (p>0.05). However, as shown in the fourth row of figure 13, work experience indicates a plausible correlative effect with information security awareness, with a range between -0.21–0.15, albeit being statistically substandard. Thus, hypothesis H2D was not supported.

The results did neither support the hypothesis that formal education is a significant factor in terms of information security (H2E). The differences between groups were rather low (F=0.47) and results were statistically insignificant (p>0.05). The uniformity of the distributions, as illustrated in the fifth row of figure 13, highlight the notion that all educational levels share substantial overlap. Mean information security scores show that the respondents that possessed postgraduate degrees scored the lowest, although this effect is likely to be caused by a few outliers at some 3 standard deviations below the mean. Density distributions also show that respondents were stacked normally around the scaled mean across all demographic variables. However, some respondents appeared to be underperforming, especially when grouped by unit and personnel group. This is illustrated in the small spike at around -2 and the lag down to -6 standard deviations. Inferential statistic concerning all demographic are compiled in table 10.

TABLE 10 Inferential statistics of demographic variables

Variable	F-statistic	Dispersion	P-value	Hypothesis
Unit	0.50	-0.10–0.21	>0.05	H2A, insignificant
Personnel group	0.60	-0.13–0.15	>0.05	H2B, insignificant
Age	2.73	-0.15–0.29	<0.05	H2C, supported
Work experience	1.30	-0.21–0.14	>0.05	H2D, insignificant
Education	0.47	-0.18–0.12	>0.05	H2E, insignificant

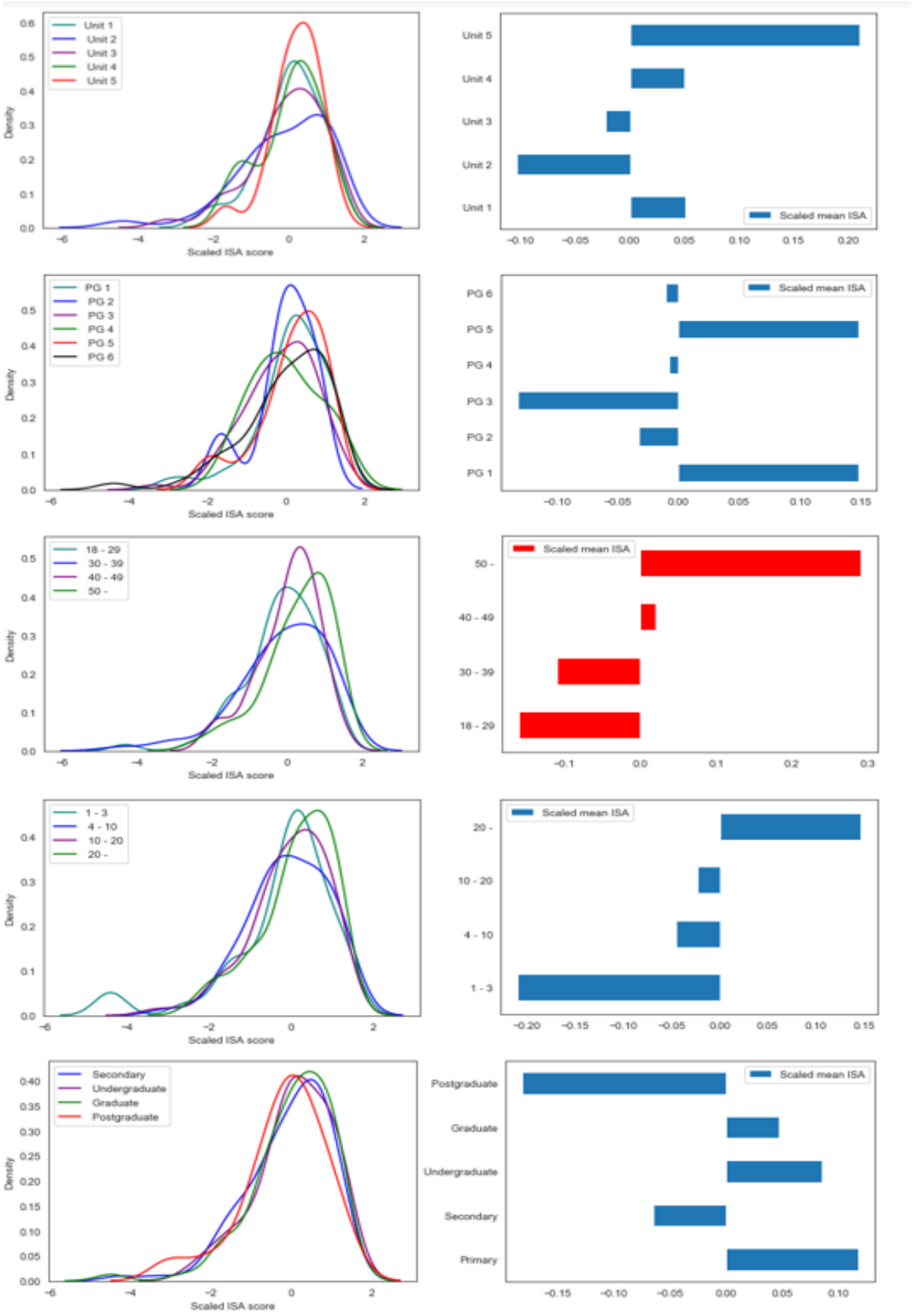

FIGURE 14 Density distributions and scaled mean ISA scores per variable

6.2 Effects of knowledge and attitude on behaviour

Hypothesis H1A expected there to be a weak ($0{,}25 < r < 0{,}5$) or moderate ($0{,}5 < r < 0{,}75$) correlation between knowledge and behaviour (compliance). These limits were met as analysis yielded a weak, statistically significant (r=0.496, p<0.005) correlation. Although the correlation coefficient fits in the expected bounds, hypothesis H1A was not confirmed: behaviour scores were generally higher than knowledge scores, except for very high knowledge scores (see figure 14) suggesting an inverse knowing-doing gap: respondents report to behave more securely than their knowledge would predetermine. This is effect is illustrated in figure 14 and the fact that the mean knowledge score was 96.77 whilst the mean behaviour score was 99.15, as shown in table 11. Moreover, in a linear regression model with only the knowledge and behaviour items included, the correlation was moderate and with modest explanatory power (r=0.55, R^2=0.25).

TABLE 11 Inferential statistics of the aspects

Aspect	Mean	Std	Min	Max
Knowledge	96.77	4.60	79	105
Attitude	99.63	4.90	73	105
Behaviour	99.15	5.13	77	105

Means of knowledge and behaviour score fit within one standard deviation of the scores, which shows that the scores share overlap. Roughly one quarter (n=76, 26.5%) of the sample had higher knowledge scores than behaviour scores. Figure 14 also shows strong heteroscedasticity.

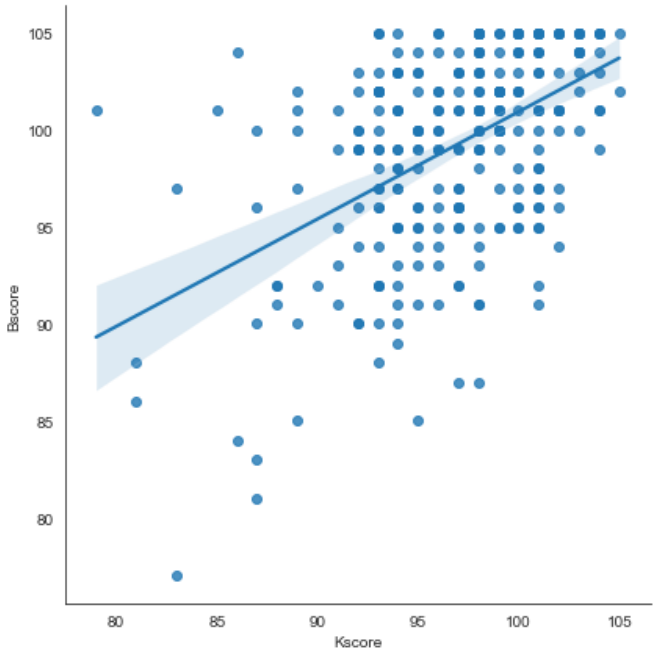

FIGURE 15 Plotted knowledge and behaviour scores with regression line

The regression model depicted in table 12 validates hypotheses H1B and H1C: that attitude has a greater effect on behaviour and that the effect of knowledge on behaviour is mediated through attitude. In the first block, the effect of solely the control (demographic) variables on behaviour were evaluated. This block confirmed what was measured priorly: of the background variables, age was the only statistically significant factor to influence behaviour, with a coefficient of 0.22, albeit the effect of age diminished when knowledge and attitude were introduced. Instead, formal education became a mildly negatively correlating factor in the second block. Moreover, the poor coefficient of determination (R^2) in the first block shows that the control variables only have miniscule explanatory power, accounting for some 1% of the adjusted effect.

The second block introduced knowledge and attitude as independent variables and revealed knowledge and attitude to be determining factors for behaviour with great statistical significance (p<0.01). Furthermore, attitude was shown to have a much greater effect on behaviour compared to knowledge, thus validating hypothesis H1B. The inclusion of knowledge and attitude also influenced the explanatory power of the model, increasing the R^2 to 0.503.

Lastly, the third block included attitude as a mediator between knowledge and behaviour, thus creating a mediation model. As the model in table 12 demonstrates, the indirect effect (or average causal mediation effects) exceeds that of the average direct effect with nearly twice as much effect, thus indicating partial mediation. The results conclude that 65% of the total effect was mediated through attitude, whereas the remaining 35% of the influence was directed between knowledge and behaviour. All results also yielded formidable statistical significance. Hence, hypothesis H1C was supported.

TABLE 12 Regression and mediation model in three blocks (standardized coefficients)

Variables	CV	CV+IV	IV+MV
Control variables			
Unit	0.006	-0.05	
Personnel group	-0.005	-0.007	
Age group	0.22*	0.115[i]	
Work experience	-0.098	-0.128	
Education	-0.067	-0.103*	
KAB model			
Knowledge		0.172**	
Attitude		0.603**	
Mediation model			
Att ~ Know			0.579***
Beh ~ Att			0.718***
Total			0.553***
Direct			0.196***
Indirect			0.358***
R^2	0.029	0.515	
R^2_{adj}	0.011	0.503	
$F\text{-}statistic_{prob}$	0.146	1.95e-40	

* $p < 0.05$; ** $p < 0.01$; [i] $p = 0.1$; t-test; *** $p < 0.01$; bootstrapping (two-sided)

6.2.1 Quantitative content analysis: reasons for non-compliance

Results from the open items are exhibited in tables 13 and 14 in descending frequential order along with the proportion of the topic of the total amount of responses. 39 respondents reported voluntarily that they would not omit and 23 that they would not leave an incident unreported. Altogether five answers were rejected due to their incomprehensibility.

TABLE 13 Reasons why respondents would leave information security incidents unreported

Cause	*f*	%
Lack of knowledge (on how to report or what an incident is)	25	21.9
The incident is insignificant	22	19.3
It is presumable that the incident has not caused any harm	13	11.4
The risk can be managed with local actions	12	10.5
Reporting endangers co-workers (physically or sanction-wise)	7	6.1
It is an established convention in the community	5	4.4
Reporting significantly impedes doing the job	5	4.4
Reporting has no practical effect	4	3.5
The cause of the incident is a superior	4	3.5
Lack of time or resources	4	3.5
Fear of repercussions	4	3.5
The incident has been discussed with the one responsible for the incident	3	2.6
A superior instructs to do so	3	2.6
The fault lies with the system and not the individual	1	0.9
Not regarded as one's responsibility	1	0.9
Indifferent attitude	1	0.9
Would never leave an incident unreported	39	
Rejected	2	

TABLE 14 Reasons why respondents would omit information security policy

Cause	*f*	%
They impede doing the job	37	24.8
Lack of knowledge (what risky behaviour is or what the norms are)	37	24.8
Accident or inadvertence	14	9.4
Instructions are complex or vague	13	8.7
Personal assessment that the benefits exceed the drawbacks	12	8.1
Lack of time or resources	7	4.7
A superior instructs to do so	7	4.7
Insignificance of the act	5	3.4
Mortal danger	5	3.4
The instructions do not truly enhance information security	4	2.7
The organization's other operations require to do so	4	2.7
Laziness	2	1.3
The organizations risk management can handle it	1	0.7
Others do it too	1	0.7
Would not omit	23	
Rejected	3	

7 DISCUSSION

The aim of the following chapter is to address the research questions; namely, is there a knowing-doing gap, what is the role of knowledge and attitude within it, what causes it, and what can be done to bridge it. In addition, the goal is to ascertain which demographic factors are associated with information security awareness. First, the results of the study are compared to previous findings. Second, implications for practice regarding the most remarkable discoveries are discussed. Then, recommendations derived from the implications are presented based on the results obtained from the literature review, especially section 3.5.1. Finally, implications and propositions regarding future research are presented along with the most significant constraints encountered.

7.1 Comparison

Poor information security behaviour, and the difficulties associated with raising awareness to improve it, continue to pester organizations (Bissell et al., 2019; Bissell et al., 2018; IBM, 2019; ENISA, 2020b; Warkentin & Willison, 2009), despite a consensus of its importance in preventing contemporary emergent threats (Safa et al., 2015a; Safa et al., 2016; Hwang et al., 2017; Hagen et al., 2008; Gardner, 2014; Verizon, 2018; SANS, 2019; Ponemon, 2020; ISO/IEC, 2018). This study assumed a part of the issue is that knowledge alone does not produce behaviour consistent with that knowledge, a phenomenon dubbed the knowing-doing gap (Pfeffer & Sutton, 2000). The primary objective of the study was to determine, whether such a gap existed in general and specifically within a target organization. Contrarily to previous studies (Gundu, 2019), propositions (Workman et al., 2008), and models (Cox, 2012), a knowing-doing gap could not be observed. Instead, in terms of the four-mode model devised by Alfawaz et al. (2010) and illustrated in table 1 in introduction, the organization was situated at mode 2, suggesting a lack of knowledge persists while employees remain compliant regardless.

In addition, the KAB model posits that effects between knowledge and behaviour are mediated through attitude (Parsons et al., 2014a; Schrader & Lawless, 2004) and multiple studies imply that attitude forms the cornerstone of compliance – or at least one among few (Bauer & Bernroider, 2017; Siponen et al., 2014; Sommestad et al., 2014; Safa et al., 2015a; Kruger & Kearney, 2008). Thus, attitude was proposed as a critical antecedent for compliant behaviour. The outcome of the study verified prior suspicions by showing that attitude had much greater effect on behaviour than mere knowledge. In fact, much of the effect between knowledge and behaviour was found to be mediated through attitude, just as the KAB model theorizes. This is to say that while building the knowledge base of employees is important (Sherif et al., 2015), fostering compliant attitudes is even more important.

The most notable finding concerning the demographics was that age influenced and appeared to be positively correlated with information security awareness based on data visualization. This verifies previous findings that suggest the same (Pattinson et al., 2019; McCormac et al., 2017a; Ögütçü et al., 2016; Hadlington & Chivers, 2018; Sheng et al., 2010). Moreover, knowledge in the form of work experience and formal education has similarly been associated with improved problem-solving (Lee et al., 2016). While visualizations of work experience prompted the impression that it might correlate with information security awareness, results were statistically insignificant. The results regarding work experience were thus partially consistent with previous studies (Chua et al., 2018). However, formal education showed no indication of being associated with information security awareness, which was inconsistent with previous findings (Ögütçü et al., 2016; Chua et al., 2018; Vance et al., 2012).

The influence of the immediate social milieu on human behaviour in general and information security in specific is a widely acknowledged dictum (Cheng et al., 2013; Chan et al., 2006; Zinatullin, 2016; Padayachee, 2012; Weirich & Sasse, 2001; Cialdini et al., 2015; Junger et al., 2017). Organizational culture combined with the segregated structure of the target organization gave reason to believe that variance among different units would persist. The cultural effect was also thought to influence vocationally clustered personnel groups, of which some evidence exists; studies among educational institutions have showed that variance among different personnel groups may occur (Lubis et al., 2020; Mittal & Ilavarasan, 2019). However, the study could not verify these effects. While there was minor variance in the information security awareness levels of different units and personnel groups, results were statistically insignificant. This does not, however, suggest that the units or personnel groups have similar levels of information security awareness or do not contain vulnerable individuals. Results only state that in terms of the variables used, results were not, on average, dissimilar enough to yield statistically significant variance.

7.2 Implications

The primary outcome of the study was determining the profound role of attitude as a critical antecedent and mediator for secure behaviour. Subsequently, this also validated the relationships between knowledge, attitude, and behaviour prescribed by the KAB model. In practice, while the open answers prompted a need for improvement in terms of knowledge, the results simultaneously highlight that, to truly influence behaviour, shifts in attitude are more important; attitude bears twice the impact of knowledge on behaviour. This gives information security educators a formidable incentive to emphasize fostering attitudes among the average employee rather than focusing on accumulating knowledge and technological skills. This also involves utilizing professionals that possess the necessary soft skills to inspire and cultivate intrinsic motivation (SANS, 2019). However, attitudes are not fostered solely through training but also within a comprehensive effort of the entire organization to build a security-conscious organizational culture (Nel & Drevin, 2019).

Although the knowing-doing gap was absent in terms of the population, it does not overrule the existence of the phenomenon, but rather the universality of it. The gap was merely not observable within the sample with the given measures. Instead, the relationship between knowledge and behaviour was inverse to what was initially expected. Thus, the results rather imply that employees either do not know or disagree on what constitutes secure behaviour. Despite this, they perceived to behave in accordance with secure principles outlined in the focus areas. Plausible explanations include successful organizational indoctrination or a strong organizational culture of obedience. However, one can argue whether this is a sufficient end-state or if the organization would rather have employees making well-informed omissive decisions in terms of information security.

7.2.1 Demographics

Previously, a logical assumption has been that digital natives, the younger generations that were born amidst the digital age, would possess a higher levels of information security awareness than digital immigrants, the older generations (Hadlington & Chivers, 2018; see also Caldwell, 2016). However, as previous studies have found (Pattinson et al., 2019; McCormac et al., 2017a; Ögütçü et al., 2016; Hadlington & Chivers, 2018) and this study verified, the youngest age groups are, on the contrary, the most vulnerable. The *maturity principle*, the psychological tendency to become more conscientious and agreeable while aging (Lüdtke, Trautwein, & Husemann, 2009), might provide a plausible explanation for this; both personality traits are associated with higher information security awareness (McCormac et al., 2017a; Parsons et al., 2014a; Shropshire et al., 2015) and the lack of them is linked to deviant workplace behaviour (Farhadi, Fatimah, Nasir, & Wan Shahrazad, 2012). Information security is also not solely a matter of digital communication and ICT (Von Solms & Van Niekerk, 2013), which

mitigates the relationship between information security and ICT. Perhaps, information security is more about attitude, being circumspect and harbouring a cautious mindset than having high Internet and computer skills and self-efficacy. In addition, the fact that the relationship between information security awareness and age was confirmed with a Finnish population for the first time implies that the phenomenon generalizable beyond nationalities.

Moreover, although information security awareness across all demographic factors were evenly distributed around the mean, there were considerable spikes and lag in density within personnel groups and units at low levels of information security awareness. This may hint that there are vulnerable groups and individuals within the personnel groups and units that could not be specified with the current demographic variables. The identification of these vulnerable groups, in addition to age, would allow organizations to target awareness efforts with precision for increased effectiveness (Dodge et al., 2012).

7.2.2 Reasons for non-compliance

The reasons for non-compliance and omission could be further categorized under four distinct labels: lack of knowledge, goal hierarchy and cost-benefit, organizational culture, and amotivation.

Lack of knowledge

The most popular topic in both items, omission and leaving incidents unreported, was lack of knowledge, populating one-fourth of all answers in each item and indicating a clear need for improving knowledge. For example, lack of knowledge could mean that the respondent felt that they did not clearly comprehend what the policies are or what behaviour constitutes information security risks. In terms of reporting, respondents saw that they did not have the capacity to identify an incident or how to appropriately report it if they did. Moreover, one-tenth reported that policies were vague or ineffective, difficult to comprehend or comply to, ambiguous, or volatile. Displaying goal hierarchy, the vast amount of documentation not related to information security contributed to that were not enough time to internalize those that do. Simultaneously, however, some claimed that instructions were insufficient or outdated; they did not cover exceptions or provide useful tools to solve common issues to get the job done.

Goal hierarchy and cost-benefit

Demonstrating the mechanics of RCT and PMT, one-third of answers highlight that individuals reported to conduct some form of appraisal of threat. They might leave an incident unreported due to the (appraised) insignificance of the incident or the presumption that it has not caused any harm. In addition, cost-benefit assessments regarding omission were observed. Furthermore, the most common category in terms of omission was impediment to doing the job, which supports

previous insights (Bada et al., 2015; Hwang et al., 2017; Post & Kagan, 2007) and goal hierarchy (Junger et al., 2017) – even reporting in some cases was perceived impeding. In multiple answers, respondents fatalistically expressed that fully complying with guidelines is impossible. For instance, one respondent had not been provided a means of moving work-vital software from one environment to another despite waiting for months. However, some displayed appraisal of organizational benefits as well (Beautement & Sasse, 2009), by expressing they would omit only if the organization's other operations required to do so.

Hence, much of the omission pertain to perceived benefits, perceived insignificance of risks and threats, or impediment to the job. However, although omission may in some cases even be in the best interest of the organization, employees deviating from guidelines at their own discretion further denotes the need for training and awareness: if omissive behaviour and practices cannot be entirely expelled, it is better to have employees make educated than uneducated appraisals. The employees should also be aware of where and how to find the mandate to deviate from guidelines.

Organizational culture

A notable proportion stated that they would omit guidelines due to established conventions in the workplace, indicating that smaller collectives may actively develop methods to circumvent guidelines, as estimated (Cheng et al., 2013; Chan et al. 2006; Furnell & Rajendran, 2012; Zinatullin, 2016; Junger et al., 2017; Hwang et al., 2017). Thus, some are willing to justify their behaviour on that basis even though observable differences in terms of personnel group or unit were not met.

Some punitive qualities also manifested since some respondents would leave incidents unreported due to possible sanctions to oneself or colleagues. Interestingly, some were under the assumption that incidents need not be reported if the issue could be addressed between the one responsible for the incident and a superior. One-tenth also presumed that incidents could be solved locally. This insinuates an enduring presumption is that the purpose of incident reporting is locating the perpetrator and imposing repercussions rather than preventing security breaches or their escalation.

Moreover, some would not report an incident if a superior or a colleague had caused it. Although reluctancy to inform on co-workers might be perceived as a display of loyalty or the fear of being left out, such practice may have an adverse effect as hazardous behaviour becomes suppressed. Some would also leave an incident unreported if a superior demanded it and one-in-twenty would infringe norms should a superior instruct to do so. One respondent with subordinates stated that they had the authority to do so. However, omission at the behest of management does not release the actor of responsibility as management cannot sanction illegitimate acts. This also implies that superiors possess a distorted immunity, and that the organization does not sufficiently disable informal retaliation or the perceived possibility of it. In few cases, respondents also felt that management did not comply and thus provided poor example and deprived subordinates of motivation, which is culturally detrimental (Nel & Drevin, 2019).

Amotivation

Amotivation refers to a lack of intention to act either due to not valuing or not possessing sufficient resources to execute an activity (Deci & Ryan, 1985). Lack of time or resources prominent in the open items suggests that an imbalance between work tasks and available resources occurs, which may constitute a security risk as well. To illustrate, workstations did not have the necessary shredders to dispose of sensitive printouts, which meant extensively looking for one on a regular basis, and some felt that hurry or cumbersome security measures hindered them from adequately appreciating security, proposing a deteriorating compliance budget (Beautement et al., 2008). A few answers also indicated some security fatigue (Bada et al., 2015). This indicates that an imbalance between resources, such as working hours, and work tasks can constitute risk in terms of information security. Singular respondents also displayed amotivation due to lack of valuation, admitted to being lazy and thus omitting security norms or harbouring indifferent or irresponsible attitudes toward reporting.

On the contrary, answers in both items also showed great obedience and perceived compliance: altogether denying the possibility of leaving an incident unreported was the most popular answer in incident reporting and the reluctance to omit the third-most popular in terms of omission, showing not only dispersion among respondents, but also great commitment to information security. The significance of these answers is further exacerbated by the fact that the respondents provided this answer entirely voluntarily. Results in terms of information security awareness scores were also auspicious compared to baseline metrics provided previous studies (Parsons et al., 2017), suggesting that awareness is generally on a decent level.

7.3 Recommendations

As the outright lack of knowledge is a profound shortcoming, the recommended approach is straightforward: sharing it. For instance, the population apparently has difficulty comprehending what constitutes insecure behaviour, what the relevant policies are, and how or why to report information security incidents. As the lack of knowledge persist despite a reported multitude of, reportedly ambiguous, policies, the organization has somehow failed at disseminating information. As the failure to raise awareness beyond documentation has eluded organizations now and before (PWC, 2012; Hagen et al., 2008; Bauer et al., 2017), other ways of distributing knowledge must be introduced. On such possibility is either reviewing the or instating an information security awareness programme (ISAP). However, the objective of the ISAP should not be constrained to building knowledge, but also fostering attitudes and raising information security awareness comprehensively.

Awareness programme

Properly communicating information security objectives (Goel & Chengalur-Smith, 2010; Von Solms, 2005; Flowerday & Tuyikeze, 2016; Knapp et al., 2009) as well as the ISAP itself (e.g., Hagen et al., 2008; Gardner, 2014; NIST, 2003; SANS, 2018; ISO/IEC, 2018) are widely covered topics in information security literature. Although ISAP's are not infallible (Bada et al., 2015), the efficacy of ISAP's as an intervention method has proven effect (Parsons et al., 2014a) and is a preferred method of raising awareness (Hagen et al., 2008; Bauer et al., 2017). As organizations cannot solely rely on disseminating information through written documentation that will likely not influence attitudes. They will also have to incorporate methods that will shift the attitudes of the employees by utilizing inspiring elements that nurture intrinsic motivation. Table 15 proposes elements that have been found to increase the likelihood of success in ISAP's.

TABLE 15 Elements of success in an ISAP

Proposition
Utilize a mix of intermittent interventions and long-term security education[13]
Integrate awareness efforts into daily communication flows[14]
Be mindful of the surrounding organizational culture and customize accordingly[15]
Appeal to fear but practice restraint in applying it[16]
Incorporate dialogue and provide and collect feedback[17]
Pertain to an iterative long-term strategy[18] that is sustainable once attitude shift occur[19]
Allocate sufficient resources, full-time personnel (2.4–3.9) and possible volunteers [20]

Moreover, information security officers can outsource their workload (SANS, 2019), e.g., by utilizing companies that provide awareness measurement, onsite education, or training platforms. Thus, the remaining responsibility of information security management would be to run the awareness programme: monitor awareness levels, implement controls and interventions in accordance, evaluate the effect of said measures, review, report, and repeat the process.

Training

Awareness training forms the basis for not only information security awareness programmes, but also policies (Bissell et al., 2019; ENISA, 2020b), information security culture (Sherif et al., 2015; Cybsafe, 2020), management (ISO/IEC, 2018), and governance (Knapp et al., 2009) and is one of the most cost-effective ways of

[13] Puhakainen & Siponen, 2010; Hwang et al., 2017; Bauer et al., 2017
[14] Puhakainen & Siponen, 2010
[15] Tsohou et al., 2015; Bada et al., 2015; Karjalainen et al., 2013
[16] Bauer & Bernroider, 2017; Siponen & Vance, 2010; Parsons et al., 2014a; Zinatullin, 2016
[17] Bauer et al., 2017; Bada et al., 2015
[18] Bauer et al., 2017; NIST 2003
[19] Bada et al., 2015
[20] SANS, 2019; Spitzner, 2017

reducing insider-induced risks (Ponemon, 2020, p. 24; Verizon, 2018). Whether training is outsourced or locally conducted, further recommendations are made regarding training in practice, expressed in table 16.

TABLE 16 Elements of success in awareness training

Proposition
Consider the cognitive threshold of learners[21]
Include general and targeted, either role-specific[22] or learner-controlled[23], training
Utilize rich and diverse media, i.e., both onsite and online training[24]
Enhance exercise engagement and performance, e.g., by gamification[25]
Pertain to contemporary risks and threats, e.g., social engineering[26]
Emphasize soft skills in education and educators[27]

Design

Although the equilibrium between security and usability is sometimes perceived as a zero-sum game (Rahalkar, 2016), one of the most central revelations of information security is that they can be improved concurrently (Shropshire et al., 2015; Workman et al., 2008; Woods & Siponen, 2019). Developing means of unloading employees is crucial since cognitive overload may cause susceptibility to risk-taking. Even situations with low costs induce hierarchization of goals (Junger et al., 2017) and cost-benefit assessments that expend the compliance budget in the long-term (Beautement et al., 2008) may lead to security fatigue when prolonged (Hwang et al., 2017; Bada et al., 2015). Instead, organizations should design policies, working conditions, technology, and associated choice architectures, and most of all security in general, in a way that preserves the compliance budget. As Beautement et al. (2008, p. 52) pertinently describe:

> "The most direct way to influence cost-benefit perception is to reduce the actual mental and physical workload that individuals have to expend on compliance… Well-designed security seeks to minimize friction between security and business processes and avoids putting individuals in situations where they have to choose between security goals and production goals."

Moreover, people tend to circumvent security measures that impede personal working goals (Krol et al., 2012) and develop alternative, preferred, and intuitively secure ways of "getting the job done", i.e., shadow security (Kirlappos et al., 2014). Organizations can seek to capitalize on the spontaneous design by employees to develop approved *and* feasible means of working securely. Employees

[21] Krol et al., 2012; SANS, 2019
[22] NIST, 2003; Bada et al., 2015; Bauer et al., 2017; Moody et al., 2018
[23] Abraham & Chengalur-Smith, 2019
[24] Kusumawati, 2018; Abawajy, 2012; Bauer et al., 2017; Caldwell, 2016
[25] apply game-design elements into an information security context; Khan et al., 2020
[26] Dodge et al., 2012; Johnston & Warkentin, 2010; Workman et al., 2008; Furnell & Rajendran, 2012; Beautement et al., 2008; Proofpoint, 2020
[27] Bauer et al., 2017; Caldwell, 2016; SANS, 2019

are often dedicated to the security interests of the organization (Beautement & Sasse, 2009) and thus inclusion in policy development and workplace design should be encouraged (Kirlappos et al., 2014; Tuyikeze & Flowerday, 2012) instead of unduly demonizing omission.

Despite thoroughly harmful attitudes are rare (Peltier, 2016; FireEye, 2020), to counter the potential malicious insider or the occasional insider who omits out of dissent or laziness, insider threat countermeasures plan can also be devised, deploying a range of physical, technical, and administrative controls (ENISA, 2020b; Ponemon, 2020; Kaspersky, 2019), including reporting on suspicious behaviour. In addition to technological detection mechanisms, technological solutions and workplace design can be used to unload strain or improve awareness, e.g., by providing employees with password managers (ENISA, 2020a), embedding security tips into screensavers, or by providing sufficient shredders to ease disposal of sensitive printouts.

Deterrents

Although deliberate or even careless behaviour may be subject to penalization (Herath & Rao, 2009; D'Arcy et al., 2009), organizations should avoid exaggerating the role of punishment and sanction with great discretion in terms of information security, especially organizations that already bear an organizational culture with punitive features. Instead, organizations may find sanctioning rewards useful to reinforce desirable behaviour (Chen et al., 2014; Pahnila et al., 2007), although being cautious not to market rewards as means to control behaviour (Jai-Yeol, 2011). Utilizing both sanctions and rewards with prudence may ultimately yield broader coverage (Marcinkowski & Stanton, 2003; Stanton et al., 2005). However, promoting a security-conscious organizational culture that holds employees accountable without supervision (Nel & Drevin, 2019) and features social disapproval of non-compliance from peers (Cheng et al., 2013; Chan et al., 2006; Furnell & Rajendran, 2012; Zinatullin, 2016; Padayachee, 2012) represents the most effective ways of issuing deterrents.

The punitive aspects were predominantly illustrated in the reluctance to report on oneself, colleagues, or superiors and the willingness to omit at the orders of a superior. Hence, organizations that involve such qualities must find means to interfere with informal reprimand or reprisals and clarify that the purpose incident reporting is 1) to initiate an adequate response to contain the escalation of the incident and 2) to provide information with respect to risk and control effectiveness assessments, as well as selection criteria and acquisition security requirements (NIST, 2020), not to instantiate an investigation. Incident reporting is vital and should thus be effectively promoted (Ponemon, 2020; Verizon, 2018).

7.4 Future research

The study elevated the role of attitude in achieving compliant behaviour. However, how to best foster attitudes was yet up to estimations based on previous literature. Thus, a possible strain of research would be to determine which educational or other factors are best at fostering attitudes. Moreover, in this study, some of the reasons for omission and associated frequencies were unveiled. However, to determine the generalizability of the frequencies and the most effective ways to mitigate them remains to be disclosed.

Furthermore, the study continued a recently initiated investigation (Chua et al., 2018) on the effect of work experience on information security awareness. Although statistical significance was not met, the results generated a suspicion that it might still be a relevant factor. This study was also constrained by combining nominal (unit, personnel group), ordinal (formal education) and interval variables (age, work experience) to measure variance with a comparison on means. Instead, future studies could utilize correlation measures to assess the correlation of interval data with information security awareness. Moreover, further studies could incorporate real values for interval variables and not cluster age or work experience into groups and look to define a saturation point where experience no longer significantly improves awareness.

Since the question regarding the knowing-doing gap remains contested, there might be room for additional studies for further verification. However, although the HAIS-Q offers some face validity, there may be underlying constraints that contest the use of the questionnaire in this form. Nevertheless, a measure explicitly designed for addressing the knowing-doing gap has not yet been established as far as the author is concerned. Such a measure would also support HAIS-Q by providing validity through multiple measurement tools. The UMISCP by (Moody et al., 2018) is also a promising model to be considered, by incorporating many of the psychological theories associated with information security compliance and awareness.

Siponen and Baskerville (2018) postulate that despite 30 years of research, the academic field has yet to demonstrate that research outcomes can beat industry practice. Thus, a longitudinal intervention and postintervention study should arguably be a priority. The HAIS-Q offers a framework for such a purpose. However, there are a multitude of measurement tools for information security awareness in the field and pinpointing the optimal ones to use in such an endeavour is a topic by itself. On the organizational level, the effectiveness of interventions could be measured by applying intervention measures, such as training, to a certain unit and controlling for the effect with one or two groups, or with a placebo group when applicable. The HAIS-Q instrument can also be used to measure the effectiveness of interventions in a test-retest format (Parsons et al., 2017).

In addition, organization could benefit from specifically examining the effects of their policies, the level of their distribution through tailored testing, and the information security policy awareness of individuals, instead of general

information security awareness. However, rather than sporadically measuring policies, awareness, or compliance, organizations should have a robust awareness programme with standardized measurements consistently conducted and incorporated into the information security lifecycle and the information security management system. Organizations could also supplement their information security awareness programmes by conducting a study to investigate the preferences of employees regarding awareness training (see e.g., Abawajy, 2012). Thus, organizations may develop training and intervention methods that are tailored to the needs and expectations of the employees.

To summarize, while a knowing-doing gap was unobserved, the study managed to ascertain the significance of attitude in achieving compliance, both individually and as a mediator between knowledge and behaviour, which dictates educators to focus on fostering attitudes as well. In addition, the study extended the breadth of the previously established results that information security is associated with higher age and thus significantly built on a growing body of research. Due to a substantial literature review, broad and well-informed implications and recommendations could be proposed along with possible development paths in terms of future research.

8 CONCLUSION

Threats associated with information security across all industries have risen to prominence in the past decade and likely continue to do so into the foreseeable future (Zwinggi et al. 2020). By investing in cyber security, organizations have tried to match the development (Gartner, 2020; Ponemon, 2020). Nevertheless, incidents continue to soar both in terms of cost and frequency (IBM, 2019; Bissell et al., 2019). One plausible explanation is that although organizations increase investments and harden their technical aspects of information security, investments in the human aspects of information security are disproportionate (Ifinedo, 2012; SANS, 2018; Harris & Furnell, 2012; Gardner, 2014; Ponemon, 2020), despite that organizational security should be based on the human aspect (Sherif et al., 2015; ENISA, 2020b; Bissell et al., 2019). This illustrates that information systems supersede the purely technical and includes the social (Boell & Cezec-Kecmanovic, 2015). The emergent sociotechnical system is central in terms of information security as well as threat actors focus increasingly on the social subsystem (Proofpoint, 2019), evident in the rise of social engineering (Bissell et al., 2019; Verizon, 2019). Thus, the lack of information security awareness represents a crucial information security threat (Safa et al., 2015b; D'arcy et al., 2009).

Due to this threat assessment, it is widely understood that humans represent the "weakest link" of information security (Furnell & Clarke, 2012; Guo et al., 2011; Vroom & Von Solms, 2004; Gonzales & Sawicka, 2002; Cox, 2012; Ifinedo, 2012; Schneier, 2015; Andress, 2014). This is exacerbated by the knowing-doing gap, the proclivity of humans to act inconsistently with their better knowledge (Pfeffer & Sutton, 2000, Gundu, 2019; Aytes & Connolly; Smith et al., 2011). However, when Kaufman et al. (2002, p. 237) aptly describe the sociotechnical system, they formulate that humans are:

> "incapable of securely storing high-quality cryptographic keys, and… have unacceptable speed and accuracy when performing cryptographic operations… [They] are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations."

Therefore, despite humans are inferior when it comes to computing capabilities, the human aspect inescapably pervades information systems. Because the human aspect cannot be excluded from the sociotechnical information system, the remark of "the weakest link" is obsolete and detrimental from a pedagogic viewpoint. Of course, this is not to suggest that human behaviour is trivial in terms of information security, but rather that the human factor is an indispensable component of the information system and thus requires valuation and consideration. However, although the criticality of the human aspect is acknowledged, appreciating the fine discerning connotations between the social and the technological has proven problematic (Bauer et al., 2017; Caldwell, 2016). Humans must be "operated" and "updated" as humans, by abiding to the laws of psychology rather than those of computer science (Zinatullin, 2016). The reasons why humans fail to exhibit compliant behaviour must be understood (Kirlappos et al., 2014).

Therefore, the goal of this study was to determine why employees fail to comply. While reasons for non-compliance is a previously well-studied topic (e.g., Junger et al., 2017; Cox, 2012; McCormac et al., 2017a; Parsons et al., 2014a; Myyry et al., 2009; D'Arcy & Herath, 2011), the study sought to quantify these reasons from the target organization's point of view and broaden the discourse by introducing less-studied topics. Specifically, the main objective was to further ascertain whether a knowing-doing gap in information security exists, as some suggest (Gundu, 2019). As the KAB model proposes that attitude mediates effects between knowledge and behaviour (Parsons et al., 2014; Schrader & Lawless, 2004), specific interest was placed upon comparing the influence of knowledge and attitude on subsequent behaviour, which had not previously been done with these measures (Parsons et al., 2013; Parsons et al., 2014a, Parsons et al., 2014b; Parsons et al., 2015; Pattinson et al., 2015a; Pattinson et al., 2015b; Pattinson et al., 2016, Calic et al., 2016; McCormac et al., 2017a; McCormac et al., 2017b; Parsons et al., 2017; Hadlington & Chivers, 2018; Mittal & Ilavarasan, 2019; Pattinson et al., 2019). Another fundamental ambition was to determine practical ways of improving information security awareness, as proposed in research question 3a. The fourth and final question was whether demographic factors are associated with information security awareness, which, in terms of various factors, appear scantly covered (Chua et al., 2018; Whitty et al., 2015).

As a result, the study yielded promising results regarding the role of attitude as an essential antecedent of secure behaviour and a mediator between information security related knowledge and behaviour. While the role of attitude was previously suspected to contain significance (Bauer & Bernroider, 2017; Siponen et al., 2014; Sommestad et al., 2014; Safa et al., 2015a; Kruger & Kearney, 2008), the study managed to quantify the effects in relation to knowledge acquisition and conclude that the effects mediated through attitude on behaviour are far greater. This provides information security educators with novel results regarding the role of attitude and a powerful incentive to emphasize fostering attitudes instead of building knowledge. To meet these ends, the study compiled a substantial amount of literature into recommendations in the form of simple but scientifically backed propositions. The recommendations pertained specifically to

information security awareness programmes, information security awareness training, and elements of design and deterrence that may offer organizations means improve information security awareness.

With reference to why employees omit secure behaviour, the study quantified and presented reasons for omission and non-compliance that were strongly linked to the current scientific discourse and a broad representation of related theories. First, the fundamental discovery was that much of the perceived non-compliant behaviour was related to a pure lack of knowledge, which denotes that a considerable amount of the insider threat is related to inadvertence rather than omission. Second, another essential finding was that as much as one-third of perceived non-compliance was related to goal hierarchies and cost-benefit assessments. Specifically, perceived benefits, perceived insignificance of risks and threats, or impediment to the job were viewed as factors that cause employees to omit. Third, cultural factors such as informal conventions and the influence of superiors and colleagues were significant causes for omission. Lastly, amotivation, stemming primarily from a lack of resources and only in a few cases from lack of valuation, proved a prominent risk for omissive behaviour.

In addition, the results also showed that demographic factors are associated with information security awareness: age was associated and positively correlated with information security awareness, which affirms previous results (Pattinson et al., 2019; McCormac et al., 2017a; Ögütçü et al., 2016; Hadlington & Chivers, 2018; Sheng et al., 2010) and expands the phenomena into a new population with a different national background (see also Oksanen & Keipi, 2013), thus extrapolating the phenomena. Such discoveries are significant in their ability to identify vulnerable groups and to concentrate targeted, more effective awareness efforts on these groups (Dodge et al., 2012).

The originality and value of this study can thus be condensed in its ability to providing novel results regarding the role of attitude in information security and by further validating prior research with respect to reasons for non-compliance and demographic factors associated with information security awareness.

Ultimately, the human aspect represents a core component for information security and can improve security in ways that, at the brink of the new decade, computers cannot. Depending on the perspective, people can either be viewed as the last line of defence or the first barrier of information security. In either case, both likely prove a more constructive pedagogic approach than that of the weakest link.

REFERENCES

Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 3(33), 237–248.* https://doi.org/10.1080/0144929X.2012.708787

Abraham, S. & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers & Security, 87*. https://doi.org/10.1016/j.cose.2019.101586

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26(4)*, 276–289. https://doi.org/10.1016/j.cose.2006.11.004

Albrechtsen, E. & Hovden, J. (2010). Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. *Computers & Security, 29(4),* 432–445. https://doi.org/10.1016/j.cose.2009.12.005

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A behaviour compliance conceptual framework. In C. Boyd & W. Susilo (eds.), *Information Security 2010: AISC '10 Proceedings of the Eighth Australasian Conference on Information Security Australian Computer Society*, Brisbane, Australia, 2010. Retrieved 24.5.2020 from http://eprints.qut.edu.au/29221/

Ajzen, I. (1985). *From Intentions to Actions: A Theory of Planned Behavior*. Heidelberg, Germany: Springer. DOI:10.1007/978-3-642-69746-3_2

Anderson, R. J. (2020). *Security engineering: a guide to building dependable distributed systems* (3rd ed.). Indianapolis: Wiley. ISBN: 978-1-119-64283-1

Andress, J. (2014). *Basics of Information Security*: *Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.). Elsevier: Waltham, MA. ISBN: 978-0-12-800744-0

APWG, 2020. *Phishing Activity Trends Report.* Anti-Phishing Working Group. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

Aytes, K. & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational End User Computing, 16(2)*, 22–40. DOI:10.4018/joeuc.2004070102

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In *International*

Conference on Cyber Security for Sustainable Society, January, 2015. ISSN: 2052-8604

Ball, J. C. (1955). The deterrence concept of in criminology and law. *The Journal of Criminal Law, Criminology, and Police Science, 46(3),* 347–354. Retrieved 23.5.2020 from https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=4387&context=jclc

Baron, R. M. & Kenny, D. A. (1987). The Moderator-Mediator Variable Distinction in Social Psychological Research. *Journal of Personality and Social Psychology, 51(5)*, 1173–1182. DOI: 10.1037/0022-3514.51.6.1173

Bauer, S. & Bernroider, E. W. N. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48(3)*. https://doi-org./10.1145/3130515.3130519

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145–159. http://dx.doi.org/10.1016/j.cose.2017.04.009

Beautement, A. & Sasse, M. A. (2009). The economics of user effort in information security. *Computer Fraud & Security, 10*, 8–12. https://doi.org/10.1016/S1361-3723(09)70127-7

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. In *NSPW '08: 2008 New Security Paradigms Workshop*, Lake Tahoe, CA, USA, September, 2008. https://doi.org/10.1145/1595676.1595684

Bissell, K., Lasalle, R. M., & Dal Cin, P. (2019). *The Cost of Cybercrime (Ninth Annual Cost of Cybercrime Study): Unlocking the Value of Improved Cybersecurity Protection*. Accenture Security. Retrieved 15.7.2020 from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

Bissell, K., Lasalle, R. M., Van Den Dool, F., & Kennedy-White, J. (2018, April 10). *Gaining ground on the cyber attacker: 2018 State of Cyber Resilience*. Accenture. Retrieved from https://www.accenture.com/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf

Bitglass (2016). *Financial Services Breach Report 2016*. Bitglass Inc. Retrieved 26.3.2021 from https://pages.bitglass.com/Report-Financial-Services-Breach-Report-2016-LP.html

Boell, S. K. & Cezec-Kecmanovic, D. (2015). What is an Information System? In *HICSS '15: Proceedings of the 2015 48th Hawaii International Conference on System Sciences*, Hawaii, USA, January, 2015. https://doi.org/10.1109/HICSS.2015.587

Bošnjak, L. & Brumen, B. (2019). Shoulder surfing: From an experimental study to a comparative framework. *International Journal of Human-Computer Studies, 130,* 1–20. https://doi.org/10.1016/j.ijhcs.2019.04.003

Bostrom, R. P. & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective Part I: The Causes. *MIS Quarterly, 3*, 17–32. https://doi.org/10.2307/248710

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34(3),* 523–548. DOI: 10.2307/25750690

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security, 6,* 8–14. https://doi.org/10.1016/S1361-3723(15)30046-4

Calic, D., Pattinson, M., Parsons, K., Butavicius, M., & McCormac, A. (2016). Naïve and accidental beahviours that compromise information security: what the experts think. In S. M. Furnell & N. L. Clarke (eds.), *Proceedings of the 10th Internation Symposium on Human Aspects of Information Security and Assurance, HAISA 2016 (12–21).* United Kingdom: Plymouth University.

Capgemini (2012). The Deciding Factor: Big Data & Decision Making. Capgemini Economist Intelligence Unit. Retrieved from https://www.capgemini.com/wp-content/uploads/2017/07/The_Deciding_Factor__Big_Data___Decision_Making.pdf

Chan, M., Woon, I., & Kankanhalli, A. (2006). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *International Journal of Information Security and Privacy, 1(3),* 18–41. DOI: 10.1080/15536548.2005.10855772

Chen, Y., Ramamurthy, K, & Wen, K. (2014). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems, 29(3),* 157–188. https://doi-org/10.2753/MIS0742-1222290305

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39,* 447–459. http://dx.doi.org/10.1016/j.cose.2013.09.009

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics, 35(6)*, 1770–1780. https://doi.org/10.1016/j.tele.2018.05.005

Cialdini, R. B., Martin, S. J., & Goldstein, N. J. (2015). Small behavioral science-informed changes can produce large policy-relevant effects. *Behavioral Science & Policy, 1(1)*, 27–35. Retrieved 4.10.2020 from https://behavioralpolicy.org

Clarke, R. A. & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York, NY: Penguin Press. ISBN 9780525561972

Cortina, J. M. (1993). What is Coefficient Alpha? An Examination of Theory and Applications. *Journal of Applied Psychology, 78(1)*, 98–104. https://doi.org/10.1037/0021-9010.78.1.98

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., & Huettel, S. (2014). An Abbreviated Impulsiveness Scale (ABIS) Constructed through Confirmatory Factor Analysis of the BIS-11. *Archives of Scientific Psychology, 2(1)*, 1–12. DOI: 10.1037/arc0000005

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behaviour, 28,* 1849–1858. http://dx.doi.org/10.1016/j.chb.2012.05.003

Curry, A., Flett, P., & Hollingsworth, I. (2006). *Managing Information and Systems: the business perspective*. New York, NY: Routledge. ISBN 0–415–35586–9

Cram, A., Proudfoot, J., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26(1),* 605–641. doi:10.1057/s41303-017-0059-9

Crowdstrike (2020). *Global Threat Report 2020*. Retrieved 15.5.2020 from www.crowdstrike.com

Cybsafe (2020, January 4). The 'ABC' guide to improving information security. Retrieved 4.1.2021 from https://www.cybsafe.com/community/blog/the-abc-guide-to-improving-information-security/

D'Arcy, J. & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20(6),* 643–658. https://doi-org/10.1057/ejis.2011.23

D'Arcy, J. & Hovav, A. (2009). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. *Journal of Business Ethics, 89,* 59–71. DOI 10.1007/s10551-008-9909-7

D'Arcy, J., Hovav, A., & 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

Das, S., Kramer, A. D. I., Dabbish, L. A., & Hong, J. I. (2014). Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 739–749. doi:10.1145/2660267.2660271

DCDC (2016). *Cyber Primer* (2nd ed.). The Development, Concepts and Doctrine Center. United Kingdom Ministry of Defence. Retrieved 2.9.2020 from www.gov.uk/mod/dcdc

Deci, E. L. & Ryan, R. M. (1985*). Intrinsic motivation and self-determination in human behavior.* New York, NY: Plenum. ISBN 978-1-4899-2271-7

Dodge, R., Coronges, K., & Rovira, E. (2012). Empirical Benefits of Training to Phishing Susceptibility. In D. Gritzalis, S. Furnell, & M. Theoharidou (eds.), *Proceedings of the 27th IFIP TC 11 Information Security and Privacy Conference*, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. https://doi.org/10.1007/978-3-642-30436-1

Drolet, M. (2020, Dec 30). Five Key Cybersecurity Trends For 2021. Forbes. Technology Council. Retrieved 27.3.2021 from https://www.forbes.com/sites/forbestechcouncil/2021/12/30/five-key-cybersecurity-trends-for-2021/

Duffy, B., Smith, K., Terhanian, G., & Bremer, J. (2005). Comparing data from online and face-to-face surveys. *International Journal of Market Research*, *47(6)*, 615. DOI: 10.1177/147078530504700602

Dugo, T. (2007). *The Insider Threat to Organizational Information Security: A Structural Model and Empirical Test* (Dissertation). Auburn University. Retrieved 17.10.2020 from https://etd.auburn.edu/handle/10415/1345.

Egelman, S. & Peer, E. (2015). Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS). *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems 1*, Seoul, Republic of Korea, April 18–23, 2014. http://dx.doi.org/10.1145/2702123.2702249

Egress (2019). *Insider Data Breach survey 2019*. Retrieved from https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

Elmes, D. G., Kantowitz, B. H. & Roediger III, H. L. (2006). *Research Methods in Psychology* (8th renewed ed.). USA: Thomson Wadsworth. ISBN 978-1119330448

ENISA (2020a). *ENISA ETL Report 2020 - Phishing*. European Union Agency for Cybersecurity. Retrieved 15.11.2020 from https://www.enisa.europa.eu/publications/phishing

ENISA (2020b). *ENISA ETL Report 2020 – Insider Threat*. European Union Agency for Cybersecurity. Retrieved 15.11.2020 from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat

Farhadi, H., Fatimah, O., Nasir, R., & Wan Shahrazad, W. S. (2012). Agreeableness and Conscientiousness as Antecedents of Deviant Behavior in Workplace. *Asian Social Science, 8(9),* 2–7. http://dx.doi.org/10.5539/ass.v8n9p2

FireEye (2020). *M-trends 2020*. FireEye Mandiant Services Special Report. Retrieved 7.10.2020 from https://content.fireeye.com/m-trends/rpt-m-trends-2020

Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention and behavior: an introduction to theory and research*. Reading, MA: Addison-Wesley. ISBN 978-0201020892

Fowler, F. J. (2009). *Survey Research Methods* (4th ed.). Thousand Oaks: SAGE Publications USA. ISBN 978-1412958417

Furnell, S. & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31,* 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Furnell, S. & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security, 3(2012),* 12–15. https://doi.org/10.1016/S1361-3723(12)70053-2

Gardner, B. (2014). What Is a Security Awareness Program? In B. Gardner & V. Thomas (eds.), *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats*. Elsevier: Waltham, MA. ISBN: 978-0-12-419967-5

Gartner (2020, June 17). Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020. Gartner Inc. Retrieved 9.3.2021 from https://www.gartner.com/en

/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem

Gino, F., Ayal, S., & Ariely, D. (2009). Contagion and Differentiation in Unethical Behavior The Effect of One Bad Apple on the Barrel. *Psychological Science, 20(3)*, 393–398. DOI: 10.1111/j.1467-9280.2009.02306.x

Gleick, J. (2011). *The information: a theory, a history, a flood*. Toronto: Random House. eISBN 978-0-307-37957-3

Goel, S. & Chengalur-Smith, I. (2010). Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems, 19*, 281–295. doi:10.1016/j.jsis.2010.10.002

Gonzales, J. & Sawicka, A. (2002). A Framework for Human Factors in Information Security. In *WSEAS International Conference on Information Security*, Rio de Janeiro, Brazil, 2002. Retrieved 3.7.2020 from http://ikt.hia.no/josejg/

Goodman, M. (2016). *Future Crimes: Inside the Digital Underground and the Battle for our Connected World* (1st Anchor Books ed.). New York: Anchor Books. ISBN 978-0385539005

Gundu, T. (2019). Ackowledging and Reducing the Knowing and Doing gap in Employee Cybersecurity Compliance. In N. van der Waag-Cowling & L. Leenen (eds.), *Proceedings of the 14th International Conference on Cyber Warfare and Security,* Stellenbosch University, South Africa, February 28 –March 1, 2019.

Guo, K., Yuan, Y., Archer, N., & Connelly, C. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems, 28(2)*, 203–236. DOI: 10.2753/MIS0742-1222280208

Grasmick, H. G. & Bursik, R. J. Jr (1990). Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model. *Law & Society Review, 3(1990),* 837–862. DOI: 10.2307/3053861

Greene, G. & D'Arcy, J. (2010). Assessing the Impact of Security Culture and the Employee-Organization Relationship in IS Security Compliance. In *Proceedings of the 5th Annual Symposium on Information Assurance*, Albany, NY, United States, June 16-17, 2010. https://doi.org/10.1.1.295.8181

Hadlington, L. & Chivers, S. (2018). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. *Policing: A Journal of Policy and Practice, 14(2)*, 479–492. https://doi.org/10.1093/police/pay027

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (2nd ed.). Indianapolis, IN: John Wiley & Sons. ISBN 978-1-119-43373-6

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16(4)*, 377–397. https://doi.org/10.1108/09685220810908796

Harari, Y. N. (2018). *21 Lessons of the 21st Century*. Lithuania: Scandbook UAB.

Harris, M. & Furnell, S. (2012). Routes to security compliance: be good or be shamed? *Computer Fraud & Security, 12(2012),* 12–20. https://doi.org/10.1016/S1361-3723(12)70122-7

Herath, T. & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18(2)*, 106–125. https://doi.org/10.1057/ejis.2009.6

Higgins, G.E., Wilson, A. L., & Fell, B. D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture, 12,* 166–184. doi: 10.1.1.463.8233

Hovav, A. & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea. *Information & Management, 49(2),* 54–60. https://doi.org/10.1016/j.im.2011.12.005

Hu, Q., Xu, Z., Dinev, T. & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 6(54)*, 54–60. https://doi.org/10.1145/1953122.1953142

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review, 41(1)*, 2–18. https://doi.org/10.1108/OIR-11-2015-0358

IBM (2019). *Cost of a Data Breach Report 2019*. IBM Security. Retrieved 25.4.2020 from https://www.ibm.com/downloads/cas/ZBZLY7KL

IBM (2020). *X-Force Threat Intelligence Index 2020*. IBM Security. Retrieved 8.10.2020 from https://www.ibm.com/downloads/cas/DEDOLR3W

IETF (2007). *Internet Security Glossary, Version 2.* Internet Engineering Task Force. Network Working Group. Retrieved 7.1.2021 from https://tools.ietf.org/html/rfc4949

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the

Protection Motivation Theory. *Computers & Security, 31(1)*, 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51(1)*, 69–79. https://doi.org /10.1016/j.im. 2013.10.001

ISO/IEC (2018). International standard ISO/IEC 27000 (fifth edition). Geneva: ISO.

Jai-Yeol, S. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48(7),* 296–302. https://doi.org/10.1016/j.im.2011.07.002

Johnston, A. C. & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34(3)*, 549–566. DOI: 10.2307/25750691

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems 25(3)*, 231–251. https://doi.org/10.1057/ejis.2015.15

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39(1)*, 113–134. https://doi.org /10.25300/MISQ/2015/39.1.06

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66*, 75–87. http://dx.doi.org/10.1016/j.chb.2016.09.012

Karjalainen, M., Siponen, M., Puhakainen, P., & Sarker, S. (2013). One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. In *Proceedings of The Pacific Asia Conference on Information Systems (PACIS 2013), 98*. http://aisel.aisnet.org/pacis2013

Kaspersky (2019). *Kaspersky Industrial Cybersecurity: solution overview 2019*. Retrieved from https://ics.kaspersky.com/media/KICS-Solution-overview-2019-EN.pdf

Kaspersky (2020). What Is an Advanced Persistent Threat (APT)? Retrieved 6.10.2020 from https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security: Private Communication in a Public World* (2nd ed.). New Jersey: Prentice Hall PTR. ISBN 0-13-046019-2

Kensington (2018). *Locking Down Mobile Devices to Keep Business Data Safe*. Kensington. Retrieved from https://www.kensington.com/siteassets /documents/kensington-lockingWP-277450-june2018-FINAL.pdf

Khan, A. H., Sawhney, P. B., Das, S., & Pandey, D. (2020). SartCyber Security Awareness Measurement Model (APAT). In *2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, Mathura, Uttar Pradesh, India, February 28–29, 2020. DOI: 10.1109/PARC49193.2020.236614

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliant behaviors provides the basis for effective security. In *Proceedings of the 2014 Conference of Usable Security (USEC '14)*, San Diego, CA, USA, February 23, 2014. http://dx.doi.org/10.14722/usec.2014.23%3C007

Knapp, K. J., Morris, R. F. Jr., Marshall, T. E., & Byrd, T. Y. (2009). Information security policy: an organizational level process model. *Computers & Security, 28,* 493–508. https://doi.org/10.1016/j.cose.2009.07.001

Kolkowska, E. & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computer & Security, 33*, 3–11. http://dx.doi.org/10.1016/j.cose.2012.07.001

Kusumawati, A. (2018). Information Security Awareness: Study on a Government Agency. In *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*, Malang, Indonesia, November 10–12, 2018. DOI: 10.1109/SIET.2018.8693168

Krol, K., Moroz, M., Sasse, M. A. (2012). Don't work. Can't work? Why it's time to rethink security warnings. In *7th Conference on Risk and Security of Internet and Systems (CRiSIS)*, October, 2012. DOI: 10.1109/CRISIS.2012.6378951

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122. doi:10.1016/j. jisa.2014.09.005.

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25(4)*, 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Kruger, H. A. & Kearney, W. D. (2008). Consensus ranking – An ICT security awareness case study. *Computers & Security, 27(7-8)*, 254–259. https://doi.org/10.1016/j.cose.2008.07.001

Laari, T., Flyktman, J., Härmä, K., Timonen, J., & Tuovinen, J. (2019). #uhka. In T. Laari (eds.), #*kyberpuolustus: Kyberkäsikirja Puolustusvoimien henkilöstölle*.

Series 3: working papers no. 12. National Defence University, Department of Warfare. ISBN 978-951-25-3120-2

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management Computer Security, 18(1),* 4–13. DOI: 10.1108/09685221011035223

Landman, T. (2019, September 5). Famous Insider Threat Cases | Insider Threat Awareness Month. Security Boulevard. Retrieved 10.1.2021 from https://securityboulevard.com/2019/09/famous-insider-threat-cases-insider-threat-awareness-month/

Lee, A. S. (2001) Editor's Comments. *MIS Quarterly, 25(1)*, iii–vii. DOI: 10.5555/2017130.2017131

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security, 59*, 60–70. https://doi.org/10.1016/j.cose.2016.02.004

Lee, S. M., Lee, S., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 6(41)*, 707 – 718. https://doi.org/10.1016/j.im.2003.08.008

Leidner, D. & Kayworth, T. (2006). A review of culture in information systems research: toward a theory of information theory culture conflict. *Managemement Information Security Quarterly, 30(2),* 357–399. DOI: 10.2307/25148735

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 4(48)*, 635–645. https://doi.org/10.1016/j.dss.2009.12.005

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly, 16(2)*, 173–186. https://doi.org/10.2307/249574

Lubis, M., Fauzi, R., Liandani, P., & Lubis, A. R. (2020). Information Security Awareness (ISA) towards the Intention to Comply and Demographic Factors: Statistical Correspondence Analysis. In *Proceedings of the 8th International Conference on Computer and Communications Management (ICCCM´20)*, Singapore, Singapore, July 17–19, 2020. https://doi.org/10.1145/3411174.3411196

Lüdtke, O., Trautwein, U., & Husemann, N. (2009). Goal and Personality Trait Development in a Transitional Period: Assessing Change and Stability in Personality Development. *Personality and Social Psychology Bulletin, 35(4),* 428–441. doi:10.1177/0146167208329215

Maddux, J. E. & Rogers, R. W. (1983). Protection motivation theory and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 5(19)*, 469–479. doi:10.1016/0022-1031(83)90023-9.

Mahfuth, A., Yussof, S., Abu Baker, A., & Ali, N. (2017). A systematic literature review: Information security culture. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, Langkawi, Malaysia, July 16–17, 2017. DOI: 10.1109/ICRIIS.2017.8002442

Marcinkowski, S. J. & Stanton, J. M. (2003). Motivational aspects of information security policies. In *SMC '03 Conference Proceedings: IEEE internal conference on systems, man and cybernetics*, Washington, DC, USA, October 8, 2003. DOI: 10.1109/ICSMC.2003.1245623

May, R. (2017, November). Your Human Firewall – The Answer to the Cyber Security Problem. TEDxWoking. Retrieved 12.11.2019 from ted.com/talks

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017a). Individual Differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017b). A Reliable Measure of Information Security Awareness and the Identification of Bias in Response. *Australasian Journal of Information Systems*, *21*, 1–12. DOI: 10.3127/ajis.v21i0.1697

McKinney, W. (2017). *Python for Data Analysis* (2nd ed.). Sebastopol: O'Reilly Media, Inc.

Menard, P., Bott, G., & Crossler, R. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems, 34(4)*, 1203–1230. DOI: 10.1080/07421222.2017.1394083

Mills, C. M. (2013). Knowing When to Doubt: Developing a Critical Stance When Learning From Others. *Developmental Psychology,* 49(3), 404–418. DOI: 10.1037/a0029500

Mittal S., & Ilavarasan P.V. (2019). Demographic Factors in Cyber Security: An Empirical Study. In: I. Pappas, P. Mikalef, Y. Dwivedi, L. Jaccheri, J. Krogstie, M. Mäntymäki (eds.), *Digital Transformation for a Sustainable Society in the 21st Century*. I3E 2019. Lecture Notes in Computer Science, vol 11701. Springer, Cham. https://doi.org/10.1007/978-3-030-29374-1_54

Mohammadnazar, H., Ghanbari, H., & Siponen, M. (2019). Moral sensitivity in informationsecurity dilemmas. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden, June 8–14, 2019. Retrieved 14.11.2020 from https://aisel.aisnet.org/ecis2019_rip/44

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42,* 1–28. DOI: 10.25300/MISQ/2018/13853

Mylonas, A., Kastania, A. & Gritzalis, D. (2013). Delegate the Smartphone User? Security Awareness in Smartphone Platforms. *Computers & Security, 34*, 47–66. https://doi.org/10.1016/j.cose.2012.11.004

Myyry, L. , Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18(2)*, 126–139. https://doi.org/10.1057/ejis.2009.10

Nel, F. & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security, 27(2)*, 146–164. https://doi-org./10.1108/ICS-12-2016-0095

NIST (2003). *NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program*. M. Wilson & J. Hash. National Institute of Standards and Technology. Joint Task Force Transformation Initiative. Retrieved 4.10.2020 from https://csrc.nist.gov/publications/detail/sp/800-50/final

NIST (2020). *NIST Special Publication 800-53 (Revision 5): Security and Privacy Controls for Information Systems and Organizations.* Joint Task Force. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Norman, D. A. (1969). *Memory and Attention: An Introduction to Human Information Processing*. New York, NY: John Wiley & Sons Inc.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill Book Company. Retrieved from http://125.22.75.155:8080/view/web/viewer.html?file=/bitstream/123456789/11061/1/Psychometric%20Theory%20Second%20Edition.pdf

Oksanen, A. & Keipi, T. (2013). Young People as Victims of Crime on the Internet: A Population-based Study in Finland. *Vulnerable Children and Youth Studies, 8(4)*, 298–309. DOI: 10.1080/17450128.2012.752119

Ostrom, E. (1998). A Behavioral Approach to the Rational Choice Theory of Collective Action: Presidential Address, American Political Science

Association, 1997. *The American Political Science Review, 92(1)*, 1–22. DOI: 10.2307/2585925

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31(5)*, 673–680. https://doi.org/10.1016/j.cose.2012.04.004

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. In *40th Annual Hawaii International Conference on System Sciences*, Hawaii, United States, January, 2007. DOI: 10.1109/HICSS.2007.206

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). An analysis of information security vulnerabilities at three Australian government organizations. In *Proceedings of the European Information Security Multi-Conference, EISMC 2013 (34–44)*, Lisbon, Portugal, 2013. DOI: 10.1.1.663.2951

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014a). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computer Security, 42,* 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014b). A study of information security awareness in Australian government organizations. *Information management and Computer Security, 22(4)*, 334–345. DOI: 10.1108/IMCS-10-2013-0078

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., & Jerram, C. (2015). The influence of organizational security culture on cybersecurity decision making. *Journal of Cognitive Engineering and Decision Making, 9(2)*, 117–129. DOI: 10.1177/1555343415575152

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66,* 40–51. DOI: 10.1016/j.cose.2017.01.004

Paternoster, R. & Simpson, S. (1996). Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. *Law & Society Review, 30(3),* 549–584. Retrieved 26.5.2020 from https://heinonline.org/HOL/LandingPage?handle=hein.journals/lwsocrw30&div=35

Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, K., & McCormac, A. (2019). Matching training to individual learning styles improves information security awareness. *Information & Computer Security, 28(1)*. https://doi.org/10.1108/ICS-01-2019-0022

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015a). Factors that influence information security behavior: an Australian web-based study. In T. Tryfonas & I. Askoxylakis (eds.), *Proceedings of human aspects of information security, privacy, & trust, HCI 2015 (231 – 241)*. Los Angeles: Springer International.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Jerram, C. (2015b). Examining attitudes toward information security behaviour using mixed methods. In S. Furnell & Clarke, N. (eds.), *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance, HAISA 2015,* 57–70. United Kingdom: Plymouth University.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The information security awareness of bank employees. In S. M. Furnell & N. L. Clarke (eds.), *Proceedings of the 10th Internation Symposium on Human Aspects of Information Security and Assurance, HAISA 2016,* 12–21. United Kingdom: Plymouth University.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Boca Raton, FL: CRC Press. ISBN 084939032X

Pfeffer, J. & Sutton, R. I. (2000). *The Knowing-Doing Gap: How Smart Companies Turn Knowledge into Action*. Boston, MA: Harvard Business School Publishing. ISBN 1-57851-124-0

Ponemon (2016). *Global Visual Hacking Experimental Study: Analysis.* Ponemon Institute, 3M. Retrieved from https://multimedia.3m.com/mws/media/1254232O/global-visual-hacking-experiment-study-summary.pdf

Ponemon (2020). *2020 cost of insider threats global report*. Ponemon Institute Research Report. Retrieved from https://www.proofpoint.com/sites/default/files/2020-04/gtd-pfpt-us-tr-ponemon-institute-2020-cost-of-insider-threats.pdf

Popper, K. (1972). *Objective knowledge: an evolutionary approach*. London: Oxford University Press. ISBN 0-19-824370-7

Post, G. V. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26(3)*, 229–237. https://doi.org/10.1016/j.cose.2006.10.004

Prey (2020). *Mobile Theft Loss Report 2020*. Prey Inc. Retrieved from https://preyproject.com/uploads/2020/03/Mobile-Theft-Loss-Report_2020.pdf

Proofpoint (2019). *Human Factor Report 2019*. Retrieved from https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

Proofpoint (2020). *2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike*. Retrieved 23.5.2020 from https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

Publication Forum (2021). Evaluation. Finnish Publication Forum. Retrieved 20.1.2021 from https://julkaisufoorumi.fi/en/evaluations

Puhakainen, P. & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34(4)*, 757–778. DOI: 10.2307/25750704

PWC (2012). *Information security breaches survey 2012*. Technical report. PricewaterhouseCoopers. Retrieved from https://www.pwc.co.uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf

Raggad, B. G. (2010). *Information Security Managament: Concepts and Practice*. Taylor & Francis Group: Boca Raton, FL. ISBN: 978-1-4398-8263-4

Rahalkar, S. A. (2016). *Certified Ethical Hacker (CEH) Foundation Guide.* Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-2325-3_6

Ramachandran, S., Rao, S. V., & Goles, T. (2008). Information Security Cultures of Four Professions: A Comparative Study. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, Waikoloa, Hawaii, USA, January 7–10, 2008. ISBN: 978-0-7695-3075-8

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 1(91)*, 93–114. doi:10.1080/00223980.1975.9915803.

Safa, N. S., Von Solms, R., & Flutcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security, 2*, 15–18. https://doi.org/10.1016/S1361-3723(16)30017-3

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015a). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., Von Solms, R., & Furnell, S. (2015b). Information security policy compliance model in organizations. *Computers & Security, 56,* 70–82. https://doi.org/10.1016/j.cose.2015.10.006

SANS (2018). *Creating Environments for Successful Awareness Programs: Security Awareness for Executives.* Executive Security Awareness Report. SANS Security Awareness. Retrieved from https://www.sans.org/sites/default/files/2018-12/Executive-Security-Awareness-Report-2018_1.pdf

SANS (2019). *SANS Security Awareness Report: The Rising Era of Awareness Training*. SANS Security Awareness. Retrieved 23.12.2020 from https://www.sans.org/security-awareness-training/reports/2019-security-awareness-report

Sasse, M. A., Brostoff, S. & Weirich, D. (2001). Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security, *BT Technology Journal*, *19(3)*, 122–131. DOI: 10.1023/A:1011902718709

Schein, E. H. (1989). The Role of the Founder in Creating Organizational Culture. In H. J. Leavitt, L. R. Pondy, & D. M. Boje (eds.). *Readings in Managerial Psychology (4th ed.)*. Chicago, IL: University of Chicago Press. ISBN 0-226-46991-3

Schlienger, T. & Teufel, S. (2003). Information security culture – from analysis to change. In J. Eloff, H. Venter, L. Labuschagne & M. Eloff (eds.), *Proceedings of 2003 Information Security South Africa (ISSA)*, Sandton Convention Center, Johannesburg, South Africa, 9-11 July, 2003.

Schneier, B. (2015). *Secrets and Lies: Digital Security in a Networked World* (15th ed.). Indianapolis: John Wiley & Sons. ISBN 978 111 909 2438

Schrader, P. G. & Lawless, K. A. (2004). The Knowledge, Attitudes, & Behaviors Approach: How to Evaluate Performance and Learning in Complex Environments. *Performance Improvement, 43(9),* 8–15. Retrieved 4.4.2020 from https://eric.ed.gov

Schultz, E. (2005). The human factor in security. *Computers & Security, 24(6),* 425–426.

Security Committee (2018). *Vocabulary of Cyber Security*. The Finnish Security Committee. Helsinki: Sanastokeskus TSK. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Shahin, E. (2017). Is WiFi Worth It: The Hidden Dangers of Public WiFi. *Catholic University Journal of Law and Technology, 25(1)*, 205–230. Retrieved 26.3.2021 from https://scholarship.law.edu/jlt/vol25/iss1/7

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & 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)*, Atlanta, Georgia, USA, April, 2010. https://doi.org/10.1145/1753326.1753383

Sherif, E., Furnell, S., & Clarke, N. (2015). Awareness, Behaviour, and Culture: The ABC in Cultivating Security Compliance. In *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, United Kingdom, December 14–16, 2015. DOI: 10.1109/ICITST.2015.7412064

Sijtsma, K. (2009). On the Use, the Misuse, and the Very Limited Usefulness of Cronbach's Alpha. *Psychometrika, 74(1)*, 107–120. DOI: 10.1007/S11336-008-9101-0

Silvers, C. (2017). The Cyber Skills Gap. TED talk at TEDxElonUniversity. Retrieved 9.12.2020 from https://www.youtube.com/watch?v=AvPsukNLENc.

Singleton, R. A. & Straits, B. C. (2018). *Approaches to Social Research* (6th ed.). Oxford: Oxford University Press. ISBN 978-0195372984

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8(1)*, 31–41. DOI: 10.1108/09685220010371394

Siponen, M. & Baskerville, R. L. (2018). Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example. *Journal of the Association for Information Systems, 19(4)*. DOI: 10.17705/1jais.00491

Siponen, M. & Iivari, J. (2006). IS Security Design Theory Framework and Six Approaches to the Application of IS Security Policies and Guidelines. *Journal of the Association for Information Systems, 7(7)*, 445–472. DOI: 10.17705/1jais.00095

Siponen, M., Mahmood, A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51(2)*, 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' Adherence to Information Security Policies: An Empirical Study. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. Von Solms (eds.), *New Approaches for Security, Privacy and Trust in Complex Environments. Proceedings of the IFIP TC-11 22nd International Information Security Conference*, SEC 2007, Sandton, South Africa, May 14–16, 2007. DOI: 10.1007/978-0-387-72367-9_12

Siponen, M., Pahnila, S., & Mahmood, A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43(2)*, 64–71. DOI: 10.1109/MC.2010.35

Siponen, M. & Vance, A. O. (2010). Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations. *Management Information Systems Quarterly, 34(3),* 487–502. Retrieved 24.2.2021 from https://aisel.aisnet.org/misq/vol34/iss3/7/

Siponen, M. & Vance, A. O. (2012). IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing, 24(1)*, 21–41. doi.org/10.4018/joeuc.2012010102

Smith, J. H., Dinev, T. & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35(4)*, 989–1015. DOI: 10.2307/41409970

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security, 22(1),* 42–75. DOI 10.1108/IMCS-08-2012-0045

Sommestad, T., Karlzén, H., & Hallberg, J. (2017). The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems, 59(4)*, 344–353. https://doi-org/10.1080/08874417.2017.1368421

Spitzner, L. (2017, November 8). The Power of a Security Ambassador Program. SANS Security Awareness. Retrieved 9.1.2021 from https://www.sans.org/security-awareness-training/blog/power-security-ambassador-program

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Journal of Computers and Security, 24(2),* 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance, 6(2),* 1–4. DOI: 10.17645/pag.v6i2.1569

Symantec (2019). *Internet Security Threat Report 2019*, *Volume 24*. Retrieved 11.3.2021 from https://docs.broadcom.com/doc/istr-24-2019-en

Säljö, R. (2004). *Oppimiskäytännöt: sosiokulttuurinen näkökulma*. Juva: WSOY.

Thomson, K-L. (2010). Information Security Conscience: a precondition to an Information Security Culture? *Journal of Information System Security, 6(4)*, 5–19.

Thomson, K-L., von Solms, R. & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud Security, 10*, 7–11. https://doi.org/10.1016/S1361-3723(06)70430-4

Trist, E. L. & Bamforth, K. W. (1951). Some Social and Psychological Consequences of the Longwall Method of Coal-Getting: An Examination of the Psychological Situation and Defences of a Work Group in Relation to the Social Structure and Technological Content of the Work System. *Human relations, 4(1)*, 3–38. https://doi.org/10.1177/001872675100400101

Trist, E. L. (1981). *The evolution of socio-technical systems: a conceptual framework and an action research program*. Toronto: Ontario Ministry of Labour. Retrieved from https://www.lmmiller.com/blog/wp-content/uploads/2013/06/The-Evolution-of-Socio-Technical-Systems-Trist.pdf

Tsohou, A., Karyda, M. & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs, *Computers & Security, 52,* 128–141. https://doi.org/10.1016/j.cose.2015.04.006

Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind, 236(59)*, 433–460. https://doi.org/10.1093%2Fmind%2FLIX.236.433

VAHTI (2014). Tietoturvallisuuden arviointiohje. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. Finnish Ministry of the Treasury. https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2014_pdf_0.pdf

Vance, A., Siponen, M., & Pahnila, S. (2009). How personality and habit affect protection motivation. In *Workshop on Information Security and Privacy, 2009*, 14–21. Retrieved 24.5.2020 from https://www.researchgate.net/publication/266042081_How_Personality_and_Habit_Affect_Protection_Motivation

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49,* 190–198. http://dx.doi.org/10.1016/j.im.2012.04.002

Van Niekerk, J. F. & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29(4)*, 476–486. https://doi.org/10.1016/j.cose.2009.10.005

Verizon (2018). *2018 Data Breach Investigation Report (VDBIR)*. Retrieved from http://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

Verizon (2019). *2019 Insider Threat Report.* Retrieved from https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

Von Solms, S. H. (2005). Information Security Governance – Compliance management vs operational management. *Computers & Security, 24(6)*, 443–447. https://doi.org/10.1016/j.cose.2005.07.003

Von Solms, R. & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security, 38(0),* 97–102. http://dx.doi.org/10.1016/j.cose.2013.04.004.

Vroom, C. & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23(3)*, 191–198. https://doi.org /10.1016/j.cose.2004.01.012

Warkentin, M. & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18(2)*, 101–105. DOI: 10.1057/ejis.2009.12

Watts, C. (2018). *Messing with the Enemy - Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News.* New York, NY: Harper. ISBN 9788832551600

Weirich, D. & Sasse, M. A. (2001). Pretty Good Persuasion: A first step towards effective password security for the Real World. In *Proceedings of the New Security Paradigms Workshop*, Cloudcroft, New Mexico, USA, September 10 – 13, 2001. DOI: 10.1145/508171.508195

Weirich, D. (2005). Persuasive Password Security. Doctoral Dissertation, Department of Computer Science, University College London, UK. Retrieved from http://sec.cs.ucl.ac.uk/fileadmin/sec/publications/ Weirich_Thesis_final.pdf

Whitty, M. T., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking, 18(1),* 772–778. DOI: 10.1089/cyber.2014.0179

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security, 88*. https://doi.org/10.1016/j.cose.2019.101640

Williams, P. (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report, 13*, 207–215. http://dx.doi.org/10.1016/j.istr.2008.10.009.

Wood, C. C. & Banks, W. W. (1993). Human error: an overlooked but significant information security problem. *Computers & Security, 12(1)*, 51–60. https://doi.org/10.1016/0167-4048(93)90012-T

Woods, N. & Siponen, M. (2019). Improving password memorability, without inconveniencing the user. *International Journal of Human-Computer Studies, 128(2019),* 61–71. https://doi-org/10.1016/j.ijhcs.2019.02.003

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24,* 2799–2816. https://doi-org/10.1016/j.chb.2008.04.005

Zachman, J. A. (1987). A Framework for Information Systems Architecture. *IBM Systems Journal, 26*. Retrieved from http://www.zachman.com/images /ZI_PIcs/ibmsj2603e.pdf

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17(4)*, 330–340. DOI: 10.1108/09685220910993980

Zinatullin, L. (2016). *The Psychology of Information Security: Resolving conflicts between security compliance and human behaviour.* United Kingdom: IT Governance Publishing. ISBN 978-1-84928-790-6

Zwinggi, A., Pineda, M., Dobrygowski, D., & Lewis, R. (2020, January 23). Why 2020 is a turning point for cybersecurity. World Economic Forum Annual Meeting. Retrieved 16.3.2020 from www.weforum.org

Ögütçü, C., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

APPENDIX 1 - THE HAIS-Q

	Knowledge	Attitude	Behaviour
Focus area: Password management			
Using the same password	It's acceptable to use my social media passwords on my work accounts. ^	It's safe to use the same password for social media and work accounts. ^	I use a different password for my social media and work accounts.
Sharing passwords	I am allowed to share my work passwords with colleagues. ^	It's a bad idea to share my work passwords, even if a colleague asks for it.	I share my work passwords with colleagues. ^
Using a strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters. ^	I use a combination of letters, numbers and symbols in my work passwords.
Focus area: Email use			
Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know. ^	It's always safe to click on links in emails from people I know. ^	I don't always click on links in emails just because they come from someone I know.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender. ^	If an email from an unknown sender looks interesting, I click on a link within it. ^
Opening attachments in emails from unknown senders	I am allowed to open email attachments from unknown senders. ^	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.
Focus area: Internet use			
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job. ^	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. ^
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to. ^
Entering information online	I am allowed to enter any information on any website if it helps me do my job. ^	If it helps me to do my job, it doesn't matter what information I put on a website. ^	I assess the safety of websites before entering information.
Focus area: Social media use			
SM privacy settings	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings. ^
Considering consequences	I can't be fired for something I post on social media. ^	It doesn't matter if I post things on social media that I wouldn't normally say in public. ^	I don't post anything on social media before considering any negative consequences.
Posting about work	I can post what I want about work on social media. ^	It's risky to post certain information about my work on social media.	I post whatever I want about my work on social media. ^
Focus area: Mobile devices			
Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute. ^	When working in a public place, I leave my laptop unattended. ^
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work files via a public Wi-Fi network. ^	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network. ^
Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Focus area: Information handling			
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones.^	Disposing of sensitive print-outs by putting them in the rubbish bin is safe. ^	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. ^	I wouldn't plug a USB stick found in a public place into my work computer.
Leaving sensitive material	I am allowed to leave print-outs containing sensitive information on my desk overnight. ^	It's risky to leave print-outs that contain sensitive information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there. ^
Focus area: Incident reporting			
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen. ^	If I saw someone acting suspiciously in my workplace, I would do something about it.
Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague. ^	If I noticed my colleague ignoring security rules, I wouldn't take any action. ^
Reporting all incidents	It's optional to report security incidents. ^	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security incident, I would report it.