ASSESSING INFORMATION SECURITY COMPLIANT BEHAVIOUR USING THE SELF-DETERMINATION THEORY

by

YOTAMU GANGIRE

submitted in accordance with the requirements
for the degree of

Magister Technologiae

in the subject

Information Technology

at the

UNIVERSITY OF SOUTH AFRICA

PROMOTOR: Prof Adéle da Veiga
CO-PROMOTOR: Prof Marlien Herselman

February 2021

DECLARATION

I hereby declare that this document: **Assessing information security compliant behaviour using the self-determination theory**, submitted for evaluation towards the requirements of the subject: Information Technology, as part of the Magister Technologiae qualification at the University of South Africa, is my own original work and has not previously been submitted to any other institution of higher learning or subject for evaluation. All sources used or quoted in this document are indicated and acknowledged by means of a comprehensive list of references.

Surname, Initials: Gangire Y

Student Number: 50801627

Signature: ____________ Date: 22 February 2021

ACKNOWLEDGEMENTS

I would like to thank the Almighty God whose grace sufficiently saw me through this journey, which was not easy at all. I am forever grateful for His provision throughout this study.

Many people were involved along the way, in various capacities as I conducted this study. I would like to thank everyone who was involved with this work for their support, help, guidance and encouragement.

I am deeply indebted to my promoter, Prof. Da Veiga, for her guidance and encouragement, for being consistently a source of reassurance and support, and for encouraging me to keep on. My supervisor also made sure to contact the right people, at every point of this study for input, guidance and financial support. I learnt quite a lot and this work would not be possible without your guidance. Thank you so much!

Professor Herselman, my co-promoter, for the time afforded to this research project. She provided invaluable advice and helped shape this study's direction. Thank you!

To my promotor and co-promotor, you are the best I could ever have in this journey. I would not hesitate to work with you again if an opportunity presented itself to do so.

To all those who participated in the expert panel review and the pilot study, I am grateful. You helped to provide new insights and perspectives to this study, without which this study would not be what it came out to be. Thank you!

Special thanks to Dr Korf, for the assistance with data analysis and interpretation.

To my family and friends who encouraged me along the way, thank you so much.

The University of South Africa's Women in Research Grant, and the College of Science Engineering and Technology (CSET), School of Computing (SoC) for supporting this project.

ABSTRACT

Information security research shows that employees are a source of some of the security incidents in the organisation. This often results from failure to comply with the Information Security Policies (ISPs). The question is, therefore, how to improve information security behaviour of employees so that it complies with the ISPs. This study aims to contribute to the understanding of information security behaviour, especially how it can be improved, from an intrinsic motivation perspective.

A review of the literature suggested that research in information security behaviour is still predominantly based on the extrinsic perspective, while the intrinsic perspective has not received as much attention. This resulted in the study being carried out from the perspective of the self-determination theory (SDT) since this theory has also not received as much attention in the study of information security behaviour. The study then proposed an information security compliant behaviour conceptual model based on the self-determination theory, (ISCBM$^{SDT)}$. Based on this model, a questionnaire, the ISCBM^{SDT} questionnaire, was developed using the Human Aspects of Information Security Questionnaire and SDT. Using this questionnaire, a survey (n = 263) was carried out at a South African university and responses were received from the academic, administrative and operational staff. The following statistical analysis of the data was carried out: exploratory factor analysis, reliability analysis, analysis of variance (ANOVA), independent samples test (t-tests) and Pearson correlation analysis. The responses to the survey questions suggest that autonomy questions received positive perception followed by competence questions and relatedness questions. The correlation analysis results show the existence of a statistically significant relationship between competence and autonomy factors. Also, a partial significant relationship between autonomy and relatedness factors as well as between competence and relatedness factors was observed.

The exploratory factor analysis that was performed on the questionnaire produced 11 factors. Cronbach alpha was then computed for the eleven factors and all were found to be above 0.7, thus suggesting that the questionnaire is valid and reliable. The results of the research study also suggest that competence and autonomy could be more important than relatedness in directing information security behaviour among employees.

KEY TERMS

Information security policies (ISP), information security compliance behaviour, information security policy compliance, self-determination theory, intrinsic motivation

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

PUBLICATIONS

Gangire, Y., Da Veiga, A., & Herselman, M. (2019). A conceptual model of information security compliant behaviour based on the self-determination theory. *Proceedings of the 2019 Conference on Information Communications Technology and Society, ICTAS 2019*, 1–6. Durban, South Africa: IEEE Computer Society.

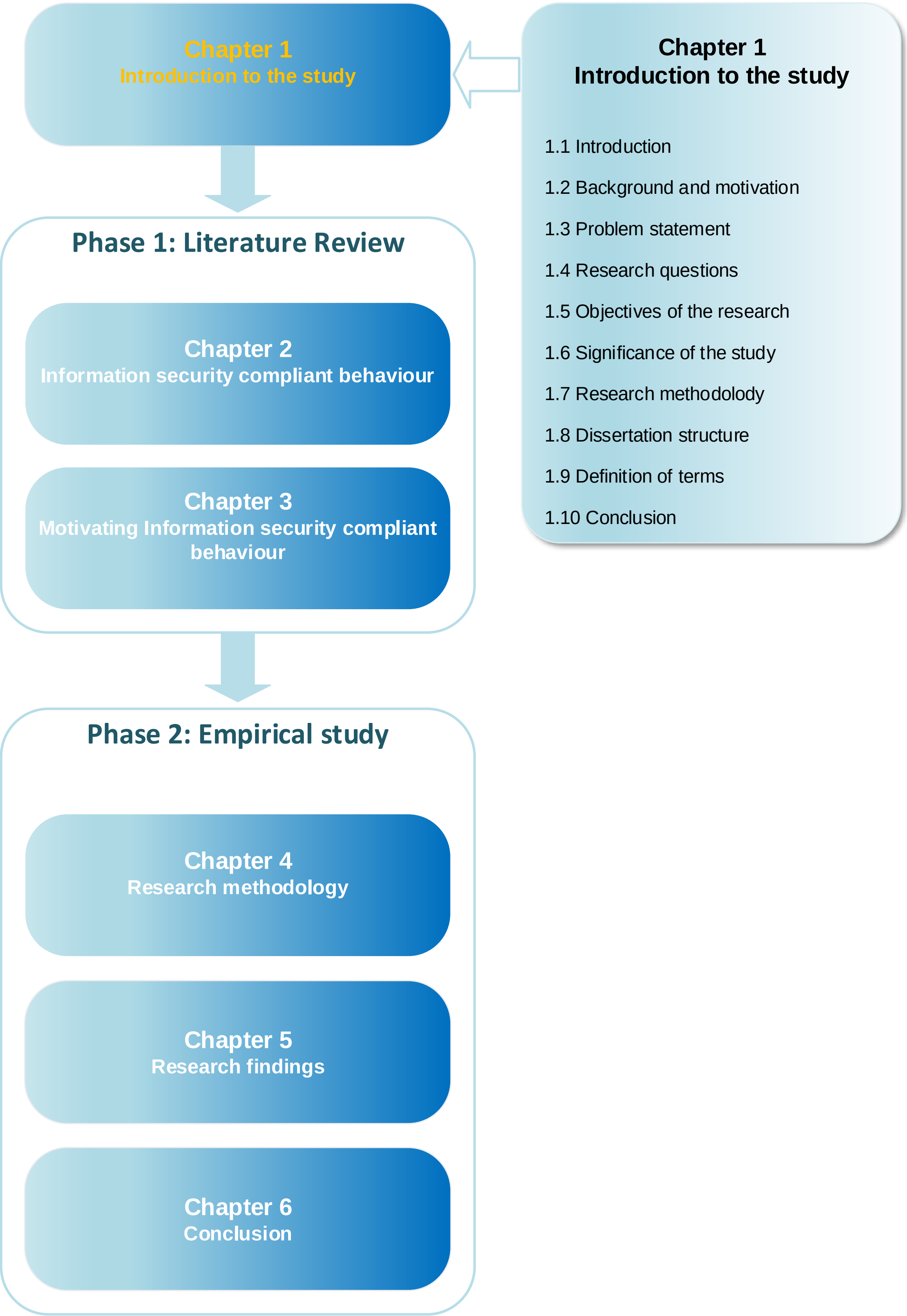
Gangire, Y., Da Veiga, A., & Herselman, M. (2020). Information Security Behavior: Development of a measurement instrument based on the self-determination theory. In N. Clarke & S. Furnell (Eds.), *Proceedings of the 14th IFIP WG 11.12 International Symposium, HAISA 2020* (593rd ed., pp. 144–157). Mytilene, Lesbos, Greece: Springer International Publishing.

Gangire, Y., Da Veiga, A., & Herselman, M. (2021). Assessing information security behaviour: A self-determination theory perspective. Information and Computer Security. **[Accepted for publication 14 December 2020]**

LIST OF ABBREVIATIONS

Abbreviation	Term in full
PMT	Protection Motivation Theory
TRA	Theory of Reasoned Action
CET	Cognitive Evaluation Theory
TPB	Theory of Planned Behaviour
HT	Habit Theory
GDT	General Deterrence Theory
NT	Neutralisation Theory
SDT	Self-Determination Theory
IM	Intrinsic Motivation
EM	Extrinsic Motivation
SCT	Social cognitive theory
SBT	Social Bond Theory
SLT	Social Learning Theory
RCT	Rational Choice Theory
SET	Social Exchange Theory
OT	Organisation Theory
SE	Self Efficacy
TCMD	Theory of Cognitive Moral Development
TMTV	Theory of Motivational Types of Values
CT	Coping theory
MDT	Moral Disengagement Theory
CBM	Composite Behaviour Model
PAP	Principal agent paradigm
DTPB	Decomposed Theory of Planned Behaviour
CDT	Cognitive Dissonance Theory
ISP	Information Security Policy
UMISPC	Unified model of information security policy compliance

CHAPTER 1



Chapter 1
Introduction to the study

Phase 1: Literature Review

Chapter 2
Information security compliant behaviour

Chapter 3
Motivating Information security compliant behaviour

Phase 2: Empirical study

Chapter 4
Research methodology

Chapter 5
Research findings

Chapter 6
Conclusion

Chapter 1
Introduction to the study

1.1 Introduction

1.2 Background and motivation

1.3 Problem statement

1.4 Research questions

1.5 Objectives of the research

1.6 Significance of the study

1.7 Research methodolody

1.8 Dissertation structure

1.9 Definition of terms

1.10 Conclusion

1 INTRODUCTION TO THE STUDY

1.1 Introduction

This study investigates information security compliant behaviour amongst employees in organisations. Through the conceptualisation of a model, factors will be identified for the assessment of information security compliant behaviour. The model will be conceptualised using the self-determination theory (SDT) as the theoretical lens or perspective. Not only will the outcome(s) (i.e. the model) of this study provide an understanding of the intrinsic motivators of information security compliant behaviour, but the model will also assist the practitioner to develop methods for promoting information security compliant behaviour.

This chapter discusses the background to this study as well as the motivation, problem statement, research questions and the objectives for this research study. The paradigm that guides this study and the overview of the research methodology are also discussed. Lastly the chapter outlines the structure of the dissertation, and also highlights the summary of each chapter.

1.2 Background and motivation

The context of this study is information systems focussing on the human aspects of information security. The study specifically focuses on investigating, based on the SDT, the intrinsic motivation factors for information security compliant behaviour.

Information plays a significant role in the running of organisations. However, it is vulnerable to both internal and external threats and attacks (Alfawaz, Nelson & Mohannak, 2010; Doherty & Tajuddin, 2018). Figure 1-1 illustrates the sources of threats to an organisation’s information systems. The diagram shows that the perpetrators of threats can be human or non-human, and could also be internal or external to the organisation (Willison & Merrill, 2013). Despite organisations taking various measures to protect information assets, information security breaches still occur (Ifinedo, 2018; Kolkowska, Karlsson & Hedström, 2017; Snyman & Kruger, 2020a). Security incidents result in loss of revenue and sensitive data, breach of personal data, damage to equipment, denial-of-service attacks, network outages (Karyda, 2017), disruption of business processes (Kadir, Norman, Rahman & Ahmad, 2016), interruption of services, and loss of market value and reputation (Correia, Gonçalves & Teodoro, 2017). Security incidents also result in attackers stealing sensitive information such as customer and employee records (Bhaharin, Sulaiman, Mokhtar & Yusof, 2019). In some studies, as much as 35% of customer records and 30% of employee records were compromised, attesting to the impact of security incidents (PriceWaterhouseCoopers, 2018).

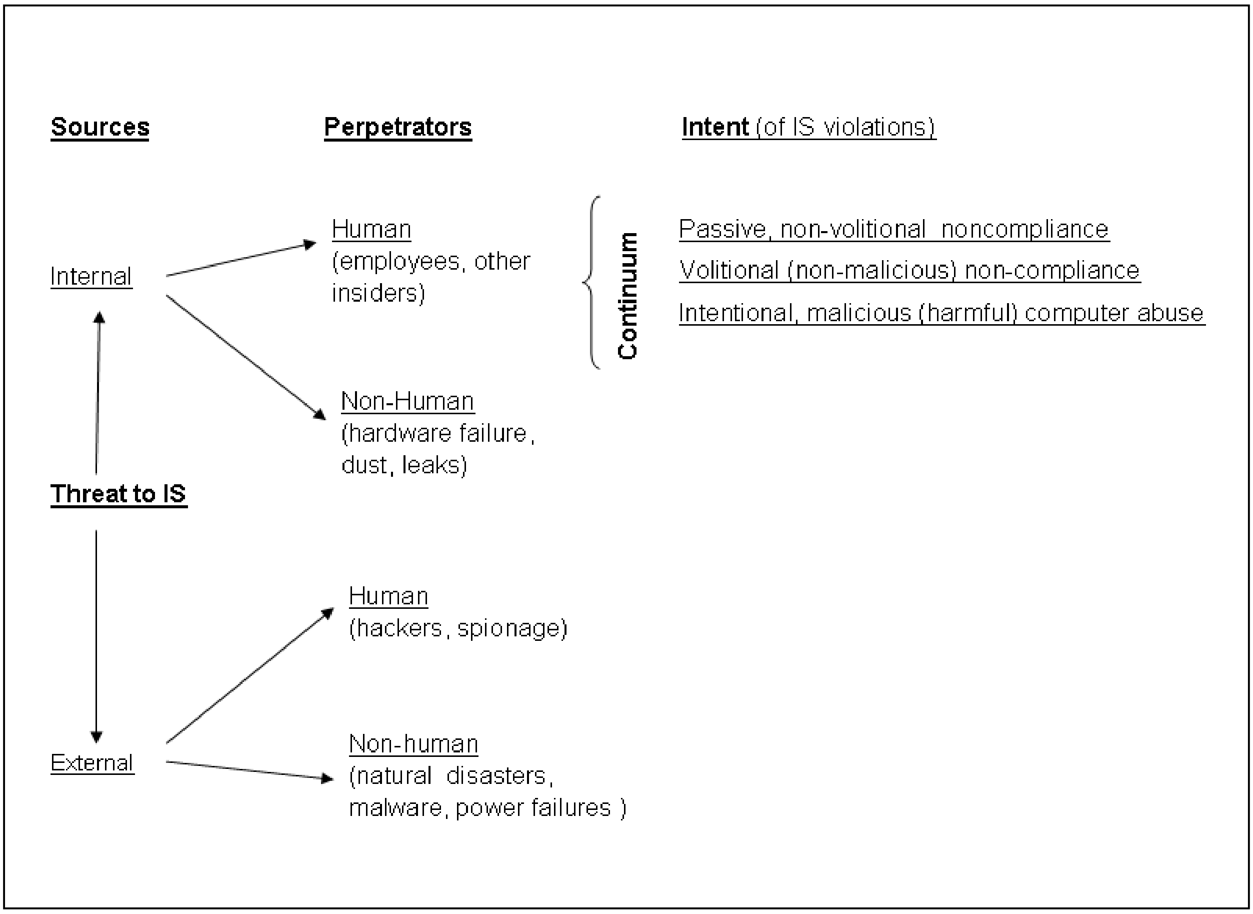

Sources
Perpetrators
Intent (of IS violations)
Internal
Human (employees, other insiders)
Continuum
Passive, non-volitional noncompliance
Volitional (non-malicious) non-compliance
Intentional, malicious (harmful) computer abuse
Non-Human (hardware failure, dust, leaks)
Threat to IS
Human (hackers, spionage)
External
Non-human (natural disasters, malware, power failures)

Figure 1-1: Sources of information security threats (Willison & Merrill, 2013)

Employees can exhibit risky behaviour which often threatens the security of information and information systems (Bélanger, Collignon, Enget & Negangard, 2017; Ifinedo, 2018; Mayer, Kunz & Volkamer, 2017). Employee behaviour has been cited as the cause of most of the security breaches experienced by organisations (Alshare, Lane & Lane, 2018; Ofori et al., 2020) and this poses major security risks (Agyekum Addae, Simpson & Oppong Appiagyei Ampong, 2019; Cram, Proudfoot & D’Arcy, 2017). Many of the security breaches result from employees’ careless actions, attempts to circumvent rules (Alfawaz et al., 2010), ignoring the information security policy (ISP) or failure to understand the ISP

(Bauer, Bernroider & Chudzikowski, 2017). Industry surveys have also confirmed the threat posed by the human element to information in the organisations. PriceWaterhouseCoopers (2018) reports that insiders such as employees, third parties such as suppliers, consultants and contractors caused 30% of the reported security incidents. Since 2018, the number of security breach incidents by insiders and third parties is on the increase (Ponemon Institute, 2020). Hence, in addition to the technical solutions, organisations must develop policies to safeguard their information and information systems from a human perspective.

To safeguard information and information systems, organisations implement security technologies to mitigate threats to the security of their information (Connolly, Lang, Gathegi & Tygar, 2016; Faizi & Rahman, 2020; Hwang & Cha, 2018). These technologies include the use of hardware and software technologies such as anti-virus software, firewalls (Herath & Rao, 2009a; Rhee, Kim & Ryu, 2009), network monitoring technologies, document security technologies and security management technologies (Hwang & Cha, 2018). However, these security technologies are subject to human failure, and do not guarantee the safety of information and information technology resources when the proper information security behaviour of employees is not taken into account (Bhaharin et al., 2019; Rhee et al., 2009). There is consensus among researchers that the security of information will not be achieved solely through the use of technological tools, but by combining people, processes and technological tools (Herath & Rao, 2009a; Ifinedo, 2018; Kolkowska et al., 2017; Da Veiga, 2016). Therefore, information security must also take into account employee behaviour (Ifinedo, 2013; Karyda, 2017), which is also important for the security of information (Bhaharin et al., 2019; Safa et al., 2015).

Employees are referred to as the insider threats (Faizi & Rahman, 2020; Ifinedo, 2012; Siponen, Adam Mahmood & Pahnila, 2014), the weakest link (Son, 2011; Tsohou, Karyda & Kokolakis, 2015) and a major threat to the organisational information systems (Bulgurcu, Cavusoglu & Benbasat, 2010; Cheng, Li, Li, Holm & Zhai, 2013). Outsiders can gain access to an organisation's information system through the organisation's employees (Son, 2011). For example, an outsider trying to access an organisation's information systems may get information such as passwords from an employee through social engineering. Another example is an employee using their access card to open the door for an unauthorised person or sharing their password with a co-worker. Such actions place the organisation’s information and information systems in danger since people who are not authorised to access the information end up accessing it.

Many threats to information and information systems assets in organisations are attributed to ISP violations by employees (Ifinedo, 2012; Kolkowska et al., 2017; Siponen et al., 2014; Son, 2011). As a result, organisations put in place ISPs to regulate the information security behaviour of employees (Alaskar et al. 2015; Ifinedo et al. 2018). It is anticipated that when employees follow the requirements of the ISPs the threats to the organisation’s information are reduced (Faizi & Rahman, 2020; Sommestad, Karlzén & Hallberg, 2017). However, organisational compliance with ISPs has proven difficult to achieve (Ifinedo, 2018; Niemimaa, Laaksonen & Harnesk, 2013; Torres & Crossler, 2019) since employees do not always act as set out in the ISPs (Moody, Siponen & Pahnila, 2018). Some of the reasons employees fail to comply with the ISPs include ignorance (Willison & Merrill, 2013), complacency, negligence, apathy, mischief, and resistance (Ifinedo, 2018). To inform employees about information security, organisations often use awareness programs (Bauer et al., 2017). These awareness and training programs are designed to reduce security breaches resulting from lack of information security awareness by employees (Woo, Sanders & Cerveny, 2018). Awareness programs also aid employees to become aware of security issues and how to behave in a secure manner (Curry, Marshall, Crossler & Correia, 2018; Han, Jung & Kim, 2017; Pfleeger, Sasse & Furnham, 2014; Tsohou et al., 2015). Therefore, awareness training programs, aim to influence positive information security behaviour among employees (Snyman & Kruger, 2020b).

Furnell & Rajendran (2012) assert that information security behaviour ranges from an established and recognized security culture on the one hand to total disobedience on the other hand, as shown in Figure 1-2. Therefore, the compliance levels of end users can progress from, for example, ignorance, which can lead to disobedience on the one hand, to awareness that can aid in establishing obedience and commitment thus leading to an establishment of a culture of compliance behaviour. Information security behaviours have also been categorised as: security-assurance behaviour, security-compliant behaviour, security risk-taking behaviour and security-damaging behaviour (Guo, 2013). According to Guo (2013), security-compliant behaviour complies with the ISP and avoids prohibited behaviour. According to Furnell & Rajendran (2012), employees are not always in the same category of compliance or non-compliance.

Commitment to compliance with ISPs depends on the motivation of employees (Connolly et al., 2016). Therefore, employees have to be motivated so that they are fully committed to compliance, which is in line with the expected information security behaviour in the organisation.

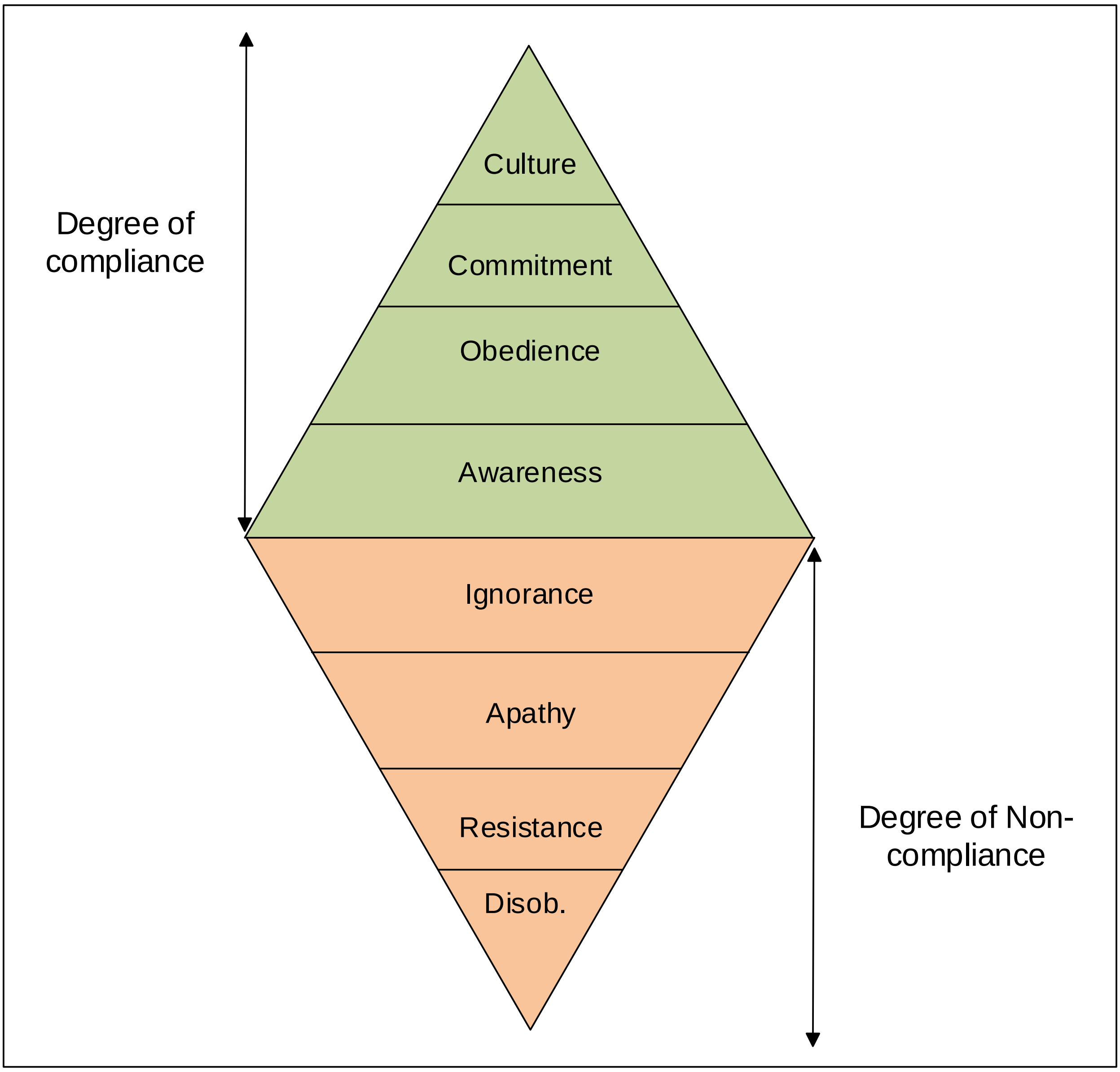


Figure 1-2: Security compliance levels in an organisation (Furnell & Rajendran, 2012)

Motivation influences compliance with ISPs, since it provides the impetus for one to behave in a particular manner (Vallerand, 2012). Researchers agree that both intrinsic and extrinsic factors affect the motivation of an individual (Padayachee, 2012; Son, 2011; Vallerand, 2012). Padayachee (2012) describes intrinsic factors as the inherent behaviour of an individual and extrinsic factors as the influence of the external environment. While motivation might be based on two extremes, that is, intrinsic and extrinsic, Ryan & Deci (2000) states that it can be of varying levels and orientations for any particular individual. An individual could be influenced by both intrinsic and extrinsic factors to comply with ISPs (Aurigemma & Mattson, 2017; Padayachee, 2012). Organisations are, therefore, faced with the challenge of motivating employees to comply with ISPs (Hina & Dominic, 2018; Torres & Crossler, 2019).

ISP compliance by employees in organisations has been studied by many researchers (Crossler et al., 2013) as they seek to understand employees' motivation to follow or violate ISPs (Son, 2011). To this end, researchers have offered different approaches to studying and achieving compliance. Some researchers have postulated that the extrinsic model (which is based on deterrence) is effective in discouraging employees from misusing the information assets of their organisations. However, some have questioned the effectiveness of this approach because inconsistent results have been reported on the effects of the deterrence model (Son, 2011). Kranz & Haeussinger (2014) have also found the deterrence model to be important but not adequate enough to motivate compliance with ISPs. Literature on the role of intrinsic motivation is scant (Alzahrani, Johnson & Altamimi, 2018; Sikolia & Biros, 2016). Therefore, there is a need for an approach that focuses on intrinsic factors to be investigated (Herath & Rao, 2009a; Padayachee, 2012; Son, 2011). For this reason, this study will attempt to define the intrinsic motivational factors that influence information security behaviour that are based on the SDT.

1.2.1 Self-determination theory (SDT)

SDT is a motivation theory, which states that humans are motivated by the need to satisfy three basic psychological needs, namely:

- The need for competence: The desire to feel capable to bring about desired outcomes (Ryan & Deci, 2000). The satisfaction of this need assists individuals to develop their skills and adapt to changing environments (Broeck, Vansteenkiste & Witte, 2008).
- The need for relatedness: This is the desire to be associated with others as a member of a group (Ryan & Deci 2000).
- The need for autonomy: This is the desire to act out of an individual's choice and will, resulting in entirely self-determined behaviour (Ryan & Deci 2000).

According to the SDT, the fulfilment of these three basic psychological needs yields intrinsic motivation (Ryan & Deci 2000; Deci & Ryan 2015). Intrinsic motivation is assumed to be the most autonomous type of motivation since it is supposed to stimulate the realisation of one's inborn potential (Broeck et al., 2008), leading to self-determined behaviour (Ryan & Deci 2000). Self-determination increases intrinsic motivation, resourcefulness, perseverance, and psychological well-being eventually leading to positive effects on behaviour (Ryan & Deci 2000). This study will, therefore, be based on the SDT.

1.3 Problem statement

It is the desire of management in organisations that employees should follow laid-down rules at all times (Myyry, Siponen, Pahnila, Vartiainen & Vance, 2009; Siponen & Puhakainen, 2010). The time and resources invested in establishing plans to ensure information is secure could be in vain if employees do not to comply with the ISPs (Humaidi & Balakrishnan, 2017). Since most information security incidents result from the failure by employees to comply with ISPs (Hwang, Wakefield, Kim & Kim, 2019), organisations need to ensure that employees follow policies and regulations to mitigate information security risks (Bulgurcu, Cavusoglu & Benbasat, 2011). Therefore, it is important to study and understand what motivates the information security behaviour of employees because this could lead to:

- Clarity on how information security behaviour of employees could be improved from being an information security threat to being ISP compliant (Crossler et al., 2013) and
- Understanding factors that motivate employees to follow ISPs (Crossler et al., 2013).

In the past, several studies have mostly focused on the extrinsic factors as drivers of compliance or non-compliance with ISPs (Bulgurcu et al., 2010; Yazdanmehr & Wang, 2015). The extrinsic-based model assumes that sanctions will discourage non-compliance (Vance & Siponen, 2010) and is, therefore, based on the deterrence theory (Siponen et al., 2014; Son, 2011). Extrinsic factors include rewards, punishments (Hayenga & Corpus, 2010; Yazdanmehr & Wang, 2015) or sanctions (Bulgurcu et al., 2010). However, some studies have pointed out the importance of the intrinsic model in fostering adherence to ISPs (Herath & Rao, 2009a; Son, 2011). Intrinsic motivation refers to the drive from within an individual to perform a given task (Wang, 2015) thus resulting in the task being performed for the challenge and interest associated with performing the task (Zohar, Huang, Lee & Robertson, 2015). Further research is apparently necessary on how intrinsic motivation promotes ISP compliance (Herath & Rao, 2009a; Padayachee, 2012; Son, 2011).

Understanding what motivates the security behaviour of employees assists policymakers and managers to manage the behavioural issues regarding ISP compliance. Hence, this study aims to contribute to the knowledge of the intrinsic motivation factors that foster ISP compliance. A review of the current literature on information security compliance indicated the following research problems (Herath & Rao, 2009a; Son, 2011):

- Research problem one: Employees are still considered as one of the main sources of information security incidents,
- Research problem two: Employees do not always comply with the ISP and
- Research problem three: Research on how intrinsic motivation promotes ISP compliance is limited.

1.4 Research questions

The main aim of this study is to assess information security compliant behaviour from the perspective of the competence, relatedness and autonomy. This will be done by developing a validated information security compliant behaviour model derived from the self-determination theory (ISCBM^{SDT}) questionnaire.

Based on the research problem statements listed in the preceding section, the above-mentioned aim of the research study and the purpose of this study, the following research questions will apply:

Research question 1: What would a model and assessment instrument for information security compliant behaviour comprise of?
Research question 2: What significant relationship exists amongst competence, relatedness and autonomy?

1.5 Objectives of the research

The following objectives were formulated:

1. To investigate what factors influence information security compliant behaviour of employees.
2. To explore the existing research with a view to establish theories that have been used for studying information security behaviour.
3. To provide a working definition of information security compliant behaviour.
4. To develop an information security compliant behaviour conceptual model that is based on the SDT.
5. To develop an information security compliant behaviour questionnaire that is based on the conceptual model, for assessing information security compliant behaviour from a competence, relatedness and autonomy perspective.
6. To conduct a survey in an organisation with a view to collect data to statistically validate the questionnaire.
7. To determine the validity and reliability of the questionnaire.
8. To determine the existence of a significant relationship amongst competence, relatedness and autonomy.

Table 1-1 links and aligns the research questions and objectives to their respective deliverables in this study. The table also shows the respective chapters in which the research questions and objectives are addressed.

Table 1-1: Summary table showing the research questions, objectives, chapter and their deliverables

Research Question	Objectives	Chapter	Deliverable
1. What would a model and assessment instrument for information security compliant behaviour comprise of?	1. To investigate what factors influence information security compliant behaviour of employees.	3	List of factors that influence information security compliant behaviour.
	2. To explore the existing research with a view to establish theories that have been used for studying information security behaviour.	3	Overview of existing research. Research gap. Theories used in previous studies.
	3. To provide a working definition of	2	Information security compliant behaviour defined.

Research Question	Objectives	Chapter	Deliverable
	information security compliant behaviour.		
	4. To develop an information security compliant behaviour conceptual model that is based on the SDT.	3	The conceptual model for information security compliant behaviour based on the SDT, SCBM^{SDT}.
	5. To develop an information security compliant behaviour questionnaire that is based on the conceptual model, for assessing information security compliant behaviour from a competence, relatedness and autonomy perspective.	4	Draft questionnaire.
	6. To conduct a survey in an organisation with a view to collect data to statistically validate the questionnaire.	4	Survey data.
	7. To determine the validity and reliability of the questionnaire.	5	Statistical analysis of results. Valid and reliable questionnaire (ISCBM^{SDT} questionnaire).
2. What significant relationship exists amongst competence, relatedness and autonomy?	8. To determine the existence of a significant relationship between competence, relatedness and autonomy.	5	Correlation between competence, relatedness and autonomy.

1.6 Significance of the study

This study seeks to apply the SDT in information security research, particularly information security behaviour. It is envisaged that this study will contribute to the expansion of an existing body of knowledge by developing a conceptual model based on the SDT and corresponding questionnaire. By developing a conceptual model based on the SDT and the corresponding questionnaire, this research is intended to make a contribution to the expansion of an existing body of information. By producing a model based on intrinsic motivation factors, this study will also improve our understanding of information security behaviour of employees. Lastly, the questionnaire produced by this study will be valuable for assessing the information security behaviour of employees.

1.7 Research methodology

The research methodology is based on the research onion model of Saunders et al. (2016), and will take the structure shown in Table 1-2. This section briefly describes the individual stages depicted in Table 1-2 that were applied in this study.

Table 1-2: Methodology summary

Research onion layer	Selection for this study
Philosophy	Positivist
Approach	Deductive
Strategy	Survey
Methodological Choice	Mono method – Quantitative
Time horizon	Cross-sectional
Data Collection	Questionnaire
Data Analysis	Descriptive and inferential statistics

1.7.1 Research paradigm/philosophy

The research philosophy refers to shared assumptions or ways of thinking about how knowledge is developed (Jonker & Pennink, 2010; Oates, 2006; Saunders et al., 2016). For this study the paradigm is based on the positivist research philosophy. Adopting a positivist philosophy implies measuring the characteristics of the social world using quantifiable data that can be analysed statistically (Creswell, 2014; Kothari, 2004).

1.7.2 Research design

A research design is a outline of methods and procedures that will be used for data collection and analysis in ways that maximise the internal and external validity of the results (Kothari, 2004; Oates, 2006). The research design is discussed below in terms of research strategy, reliability, validity, variables, research unit, correlation analysis and sampling.

1.7.2.1 Research strategy

The study will employ a cross-sectional survey strategy. The survey strategy allows the researcher to gather data from a large sample in a standardised manner (Oates, 2006). The study will use a questionnaire as the data collection instrument. The web-based questionnaire consisting of closed questions will be administered over the internet (Bhattacherjee, 2012).

1.7.2.2 Validity

Validity is the capability of a research design to yield valid conclusions (Marczyk, Fertinger & DeMatteo, 2005). The following were used to determine questionnaire validity: face validity, content validity and construct validity.

Face validity is used to determine if the questionnaire constructs make sense (Saunders et al., 2016). A panel of experts will be convened and a pilot test conducted to determine the face validity of the questionnaire.

Content validity is used to determine whether the questions address the aims and objectives of the research (Saunders et al., 2016). For this study, the questionnaire items covered the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al., 2017) from the perspective of the SDT discussed in the literature review chapter.

Construct validity is used to determine whether the questionnaire assesses the constructs that it was designed to assess (Creswell & Creswell, 2018). Construct validity can be determined using the exploratory factor analysis (EFA) (Gerber & Hall, 2017). The validity of the questionnaire will also be determined statistically by conducting the EFA.

1.7.2.3 Reliability

Reliability refers to whether the repeated use of the research instrument produces consistent results (Kothari, 2004; Marczyk et al., 2005). The questionnaire reliability will be determined statistically by computing Cronbach alpha coefficients.

1.7.2.4 Unit of analysis

This is the target of the investigation and is important for shaping the kind of data that should be gathered for the study and from whom it should be collected (Bhattacherjee, 2012). The targeted minimum responses are 125 since data will be produced per SDT category, that is, competence, relatedness and autonomy. Each of the SDT categories will have 25 questions. The minimum number of responses should be 5 times the total number of questions in the data collection instrument or per construct for statistical validation of the questionnaire (O'Rourke & Hatcher, 2013). The participants will be drawn from academic, administrative and operational staff from a university in South Africa. Both academic and administrative staff use information systems to support the students. This, therefore, requires staff members to familiarise themselves with the institution's ISPs to reduce security incidents.

1.7.2.5 Data analysis

The study will employ descriptive and inferential statistics for analysing the data. Descriptive statistics will be used to summarise, group and sort data collected from the sample, which can then be presented graphically. Inferential statistics will be used to estimate population parameters from the sample, that is, make generalisations about a population. SPSS software will be used to carry out statistical data analysis. The following will be carried out on the data: ANOVA, t-test, Pearson correlation analysis, exploratory factor analysis and reliability analysis. The next section outlines some of the statistical analysis that will be carried out on the collected data.

1.7.2.5.1 Factor analysis

Exploratory factor analysis will be conducted on the questionnaire. Factor analysis is conducted by examining the correlation among variables to establish common themes within the data (Leedy & Ormrod, 2015).

1.7.2.5.2 Reliability analysis

Creswell (2014) states that reliability analysis assesses the internal consistency of a set of scales or test items using Cronbach alpha. A Cronbach alpha value that is reliable indicates that items that make up a construct measure the same construct in the same way (Roberts & Priest, 2006).

1.7.2.5.3 Correlation analysis

This is used to determine and describe associations among variables and provide information on the direction (whether positive or negative) and strength of the relationship. Variables that have a positive correlation move in the same direction and those that have a negative correlation move in opposite directions (Marczyk et al., 2005). This study seeks to determine the correlation among competence, relatedness and autonomy.

1.7.2.6 Sampling

Sampling is a statistical procedure for choosing a subset of a population for purposes of studying and making statistical inferences about that population (Bhattacherjee, 2012; Oates, 2006). Sampling can either be probabilistic or non-probabilistic (Kothari, 2004; Oates, 2006). Probability sampling is used so that the sample typically represents the population being studied, and non-probability sampling is used when the sample does not need to be representative. This research will use the non-probability convenience sampling method. This entails the researcher selecting participants because they are available (Oates, 2006).

1.7.3 Research ethics

The ethical considerations in this study include: informed consent of the participants, anonymity and confidentiality of participants and protection of participants (Creswell, 2014; Oates, 2006). The study complied with the directives of UNISA Policy on Research Ethics. Appendices A and B include the respective research permission and ethics certificates issued for this study.

1.7.4 Flow diagram of the stages of this research study

Figure 1-3 shows the two stages involved in conducting this research study: phase 1 - literature review and phase 2 - empirical study.

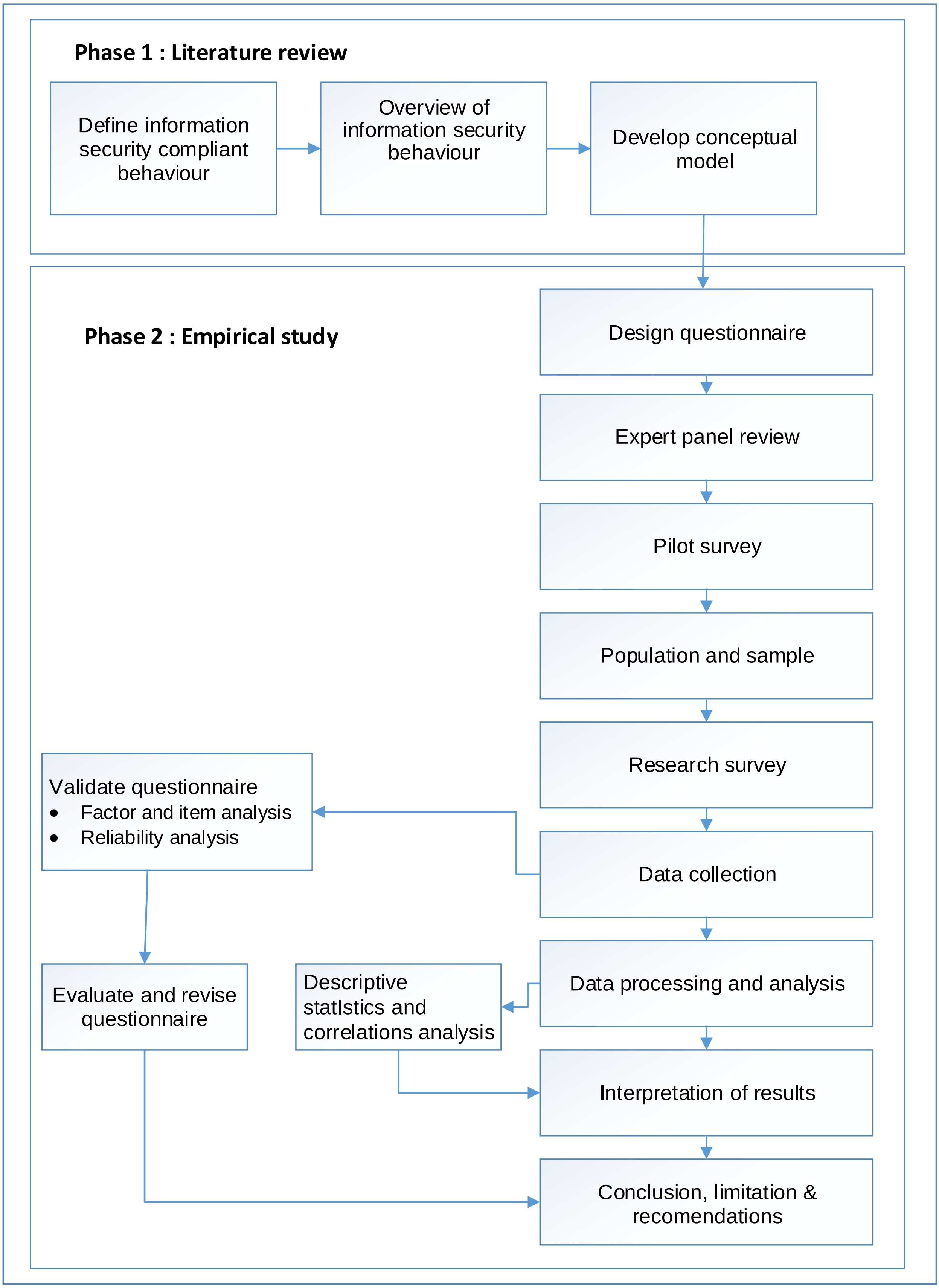

Phase 1 : Literature review
Define information security compliant behaviour
Overview of information security behaviour
Develop conceptual model
Phase 2 : Empirical study
Design questionnaire
Expert panel review
Pilot survey
Population and sample
Research survey
Data collection
Validate questionnaire
• Factor and item analysis
• Reliability analysis
Evaluate and revise questionnaire
Descriptive statIstics and correlations analysis
Data processing and analysis
Interpretation of results
Conclusion, limitation & recomendations

Figure 1-3: Flow diagram depicting the stages of this research study

1.8 Dissertation structure

As mentioned in the preceding section, this dissertation is divided into two phases: phase 1 - literature review and phase 2 - the empirical study. Details of the two phases are outlined below.

Literature review

Chapters 1 to 3 comprise the literature review phase and are summarised as follows:

- **Chapter 1: Introduction to the Study**

  The chapter provides the introduction, background and motivation of the study, research questions, objectives, and the significance of the study.
- **Chapter 2: Information Security Compliant Behaviour**

  This chapter proposes a definition of information security compliant behaviour, which will assist in setting the context for the research study and a common understanding of the term as used in the study.
- **Chapter 3: Motivating Information Security Compliant Behaviour**

  This chapter covers the following material.
  - An overview of information security compliance studies, that is, focussed on what was done in the past regarding information security compliance. Such an overview will assist in identifying the gap(s) that this study will aim to address.
  - An outline of the intrinsic factors influencing information security compliant behaviour, which motivates employees to comply with the ISP. Similar to the overview mentioned above, this outline will also contribute to establishing an existing gap.
  - A conceptual model is proposed depicting intrinsic motivational factors that affect ISP compliance, based on the self-determination theory. This model establishes the base upon which the development of the questionnaire is done.
  - Questionnaire themes are identified based on the “Human Aspects of Information Security Questionnaire (HAIS-Q)” (Parsons et al., 2017; Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014)

Empirical study

Similar to the literature review phase discussed above, the empirical study phase is made up of 3 three chapters, that is, chapters 4 to 6. A short description of these chapters is outlined below.

- **Chapter 4: Research Methodology**

  The chapter discusses how the empirical study was carried out. The sampling method used - non-probability convenience sampling method was used for the survey. The development of the questionnaire for this research study will include: literature review, convening an expert panel of reviewers for the questionnaire, pilot testing the revised instrument, finally, revisions made from the expert panel of reviewers and pilot test are included in the instrument and the main study is carried out. Data will be collected using a questionnaire which will be administered electronically via the internet. The data will be collected at a university in South Africa.
- **Chapter 5: Research Findings**

  Data analysis - descriptive and inferential statistics will be used to present the data. Descriptive statistics will be used to summarise, group and sort the collected data. Data will be presented graphically as well as a description of the most significant sample characteristics. Statistical analysis will be used to validate the questionnaire and to identify correlations.
- **Chapter 6: Conclusion**

  The chapter covers the following:
  - Evaluation of the research findings based on the study’s goals and objectives.
  - Answer the research questions using survey results to determine whether the objectives of this study have been fulfilled.
  - The chapter will also report on the limitations of this study, recommendations for further study and making conclusions from the results of the empirical study.

1.9 Definition of terms

This section provides some definitions as they are used in this research study.

1.9.1 Information security

It is the safeguarding of the confidentiality, integrity and availability of information (ISO/IEC 27001, 2005).

1.9.2 Information security policy

An ISP defines roles and obligations of employees in an organisation concerning information systems and information security (Bulgurcu et al., 2011; Son, 2011;

Yazdanmehr & Wang, 2016). It specifies what users can do and cannot do, as well as the consequences for failure to comply (Guo, Yuan, Archer & Connelly, 2011).

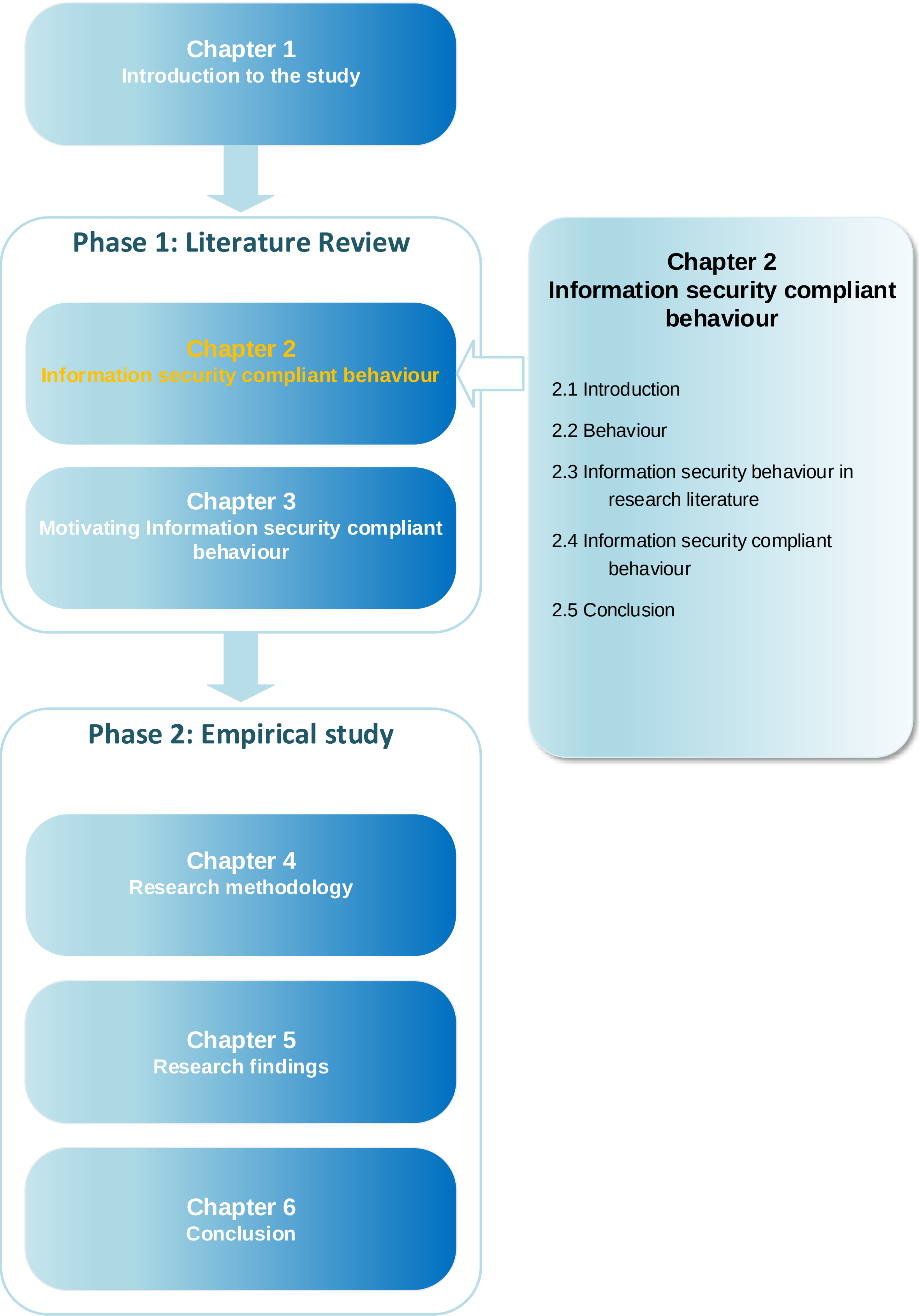
1.9.3 Compliance

Conformity with the ISP (Padayachee, 2012) and this behaviour minimise the risks to information and technology resources (Guo, 2013).

1.10 Conclusion

In this chapter, the study was contextualised with specific reference to the dependency of information security success on appropriate employee information security behaviour. The rationale of the study, the research problem and research questions were discussed. An overview of the research methodology was presented as well as the structure of the dissertation. The next chapter will discuss information security compliant behaviour.

CHAPTER 2


Chapter 1
Introduction to the study
Phase 1: Literature Review
Chapter 2
Information security compliant behaviour
Chapter 3
Motivating Information security compliant behaviour
Phase 2: Empirical study
Chapter 4
Research methodology
Chapter 5
Research findings
Chapter 6
Conclusion
Chapter 2
Information security compliant behaviour
2.1 Introduction
2.2 Behaviour
2.3 Information security behaviour in research literature
2.4 Information security compliant behaviour
2.5 Conclusion

2 INFORMATION SECURITY COMPLIANT BEHAVIOUR

2.1 Introduction

Chapter 2 proposes a working definition of information security compliant behaviour for the study. This definition will provide the context in which information security compliant behaviour occurs. In so doing, the chapter will answer the third research objective, which is: To propose a working definition of information security compliant behaviour.

Also, the chapter aims to achieve these objectives:

- Discuss the meaning of behaviour drawn from other fields of study, and thereafter deduce the characteristics and factors that promote information security behaviour.
- Discuss how other studies define information security behaviour or other equivalent terms.
- Propose a definition of information security complaint behaviour for this research study.

The chapter is organised as follows: Section 2.2 - Definitions of behaviour, Section 2.3 - Information security behaviour in literature and Section 2.4 - Information security complaint behaviour as defined in this study.

2.2 Definitions of behaviour

The current study focuses on behaviour that is compliant with information security requirements as stipulated in the organisation's ISPs and related regulations. Figure 2-1 shows the linkages between compliance, behaviour and information security; in summary, behaviour must conform to ISP requirements. The behaviour of employees determines the success of any information security program (Humaidi & Balakrishnan, 2017; Hwang et al., 2019). Therefore, understanding information security behaviour of users is necessary for assessing and improving information security behaviour (Alaskar et al., 2015). To further our understanding of information security compliant behaviour, this section will start by explaining behaviour, then a discussion of secure behaviour in the context of information security follows. The section will conclude by proposing a definition of information security compliant behaviour.

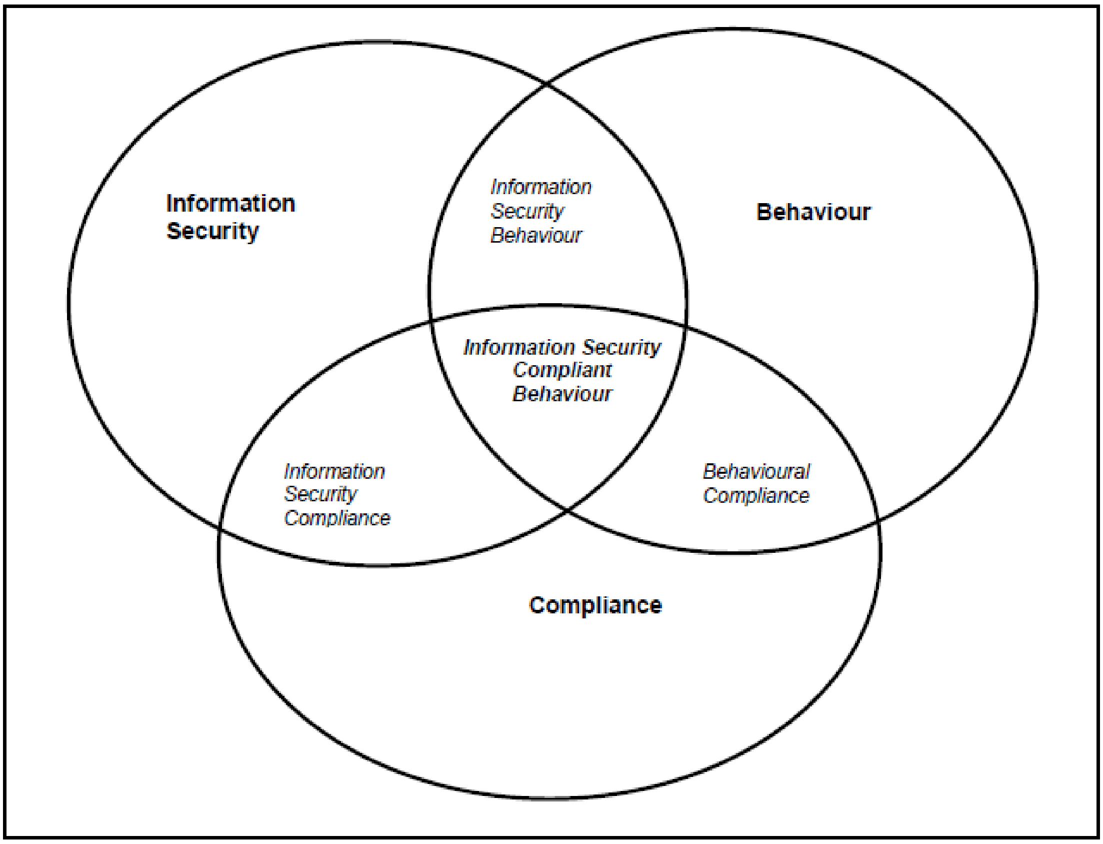

Information Security
Information Security Behaviour
Behaviour
Information Security Compliant Behaviour
Information Security Compliance
Behavioural Compliance
Compliance

Figure 2-1: Linkage between information security, behaviour and compliance in this study

Figure 2-1 shows some terms that are important to this chapter and that act as context and assumptions for this chapter. Behaviour generally refers to how organisms act in a given environment (Davis, Campbell, Hildon, Hobbs & Michie, 2015; Kwasnicka, Dombrowski, White & Sniehotta, 2016; Matsumoto, 2012; Tileubayeva, Massalimova, Kaufman & Fernandez, 2017). Compliance refers to the act of following rules (Padayachee, 2012). Information security is concerned with safeguarding the, integrity availability and confidentiality of information (Pfleeger & Pfleeger, 2015). Behavioural compliance refers to behaviour that complies with rules regardless of the environment. It is assumed that such people will comply with rules regardless of whether they understand the rules or not (Ahmad, Norhashim, Song & Hui, 2016; Alfawaz et al., 2010). Information security compliance refers to behaviour that complies with information security rules because the employee has knowledge of the rules and is willing to comply. Knowledge results from information security training (Guo, 2013). Information security behaviour is the behaviour of employees as they perform their work duties and it can be either in compliance or violation of the ISPs (Connolly et al., 2016).

Behaviour is ubiquitous, and this is shown by the proliferation of terms to describe it, such as consumer behaviour, human behaviour, animal behaviour and organisational behaviour (Cao, 2014). As a result, many writers on the subject of behaviour tend to assume that their readers understand its meaning and do not therefore define it (Levitis, Lidicker & Freund, 2009). A need exists for an operational definition to avoid ambiguities. The definition must specify what is to be included or excluded in the definition since no one-size-fits-all definition of behaviour exists (Levitis et al., 2009). A definition is also important for the measurement process of behaviour because, without a clear definition, a reliable and valid measurement to assess the behaviour may be difficult to produce (Conner & Norman, 2017). To provide context to formulate a definition for this study, the next section discusses some definitions of behaviour derived from other fields, the characteristics of behaviour and factors influencing behaviour in general.

2.2.1 Some definitions of behaviour

This section briefly looks at some definitions of behaviour which are drawn from other fields of study. The various definitions are listed below:

Table 2-1: Various definitions of behaviour

Definition	Reference
The way organisms respond to internal and or external stimuli and this excludes the organism's changes due to growth.	(Levitis et al., 2009)
An attempt by an individual to change its state of being, this is presented as a formula as follows: "Behaviour = Identity of the person, Want (motivational parameter), Know (cognitive parameter), Know-How (skill or competency), Performance (procedural aspects such as bodily postures, movements), Achievement (outcome), Personal Characteristics (individual difference), Significance".	(Bergner, 2011, p.148)
Actions of living organisms.	(Matsumoto, 2012)
The action or reaction by an organism. Reactions could be a result of past interactions with the environment. Actions could involve change or movement of the organism.	(Lazzeri, 2014)
People's responses to internal or external events. The type of action determines whether it can be assessed directly or indirectly.	(Davis et al., 2015)
A person's actions in response to events (internal or external) and can be assessed.	(Kwasnicka et al., 2016)
Action or response by a person that can be assessed, for example, the blinking of the eye or rise of the heart rate.	(Tileubayeva et al., 2017)

From the definitions listed in Table 2-1, behaviour could be the actions that a person performs or the responses or reactions to the environment. Thus, to behave appropriately, Schein (1971) states that an individual constructs a self-image to deal with their surroundings that makes it possible for the individual to fulfil various role expectations in their environment.

2.2.2 Behaviour and its attributes

The various attributes of behaviour are list in Table 2-2, these are taken from other fields of study.

Table 2-2: Some attributes of behaviour

Attribute	Reference
It can be motivated from within the organism or by its surroundings.	(Kwasnicka et al., 2016)
It involves the performance of the particular behaviour.	(Gozli, 2017)
It can be a group or a single entity performing a behaviour.	(Gozli, 2017; Lazzeri, 2014; Levitis et al., 2009)
It could result in changes in the environment.	(Bergner, 2011).
It occurs within an environmental and social context and can have meaning within a particular social context.	(Kwasnicka et al., 2016; Gozli, 2017)
It could be a result of past interactions with the environment.	(Kwasnicka et al., 2016; Lazzeri, 2014)
It could be volitional and have a motive.	(Baum, 2013; Gozli, 2017)
It takes time to enact.	(Baum, 2013).

It can be observed and measured, directly or indirectly.	(Davis et al., 2015);
	Kwasnicka et al., 2016;
	Tileubayeva et al. 2017)

It can be repeated and thus can become habitual.	(Kwasnicka et al., 2016)
It can be learned.	(Carden & Wood, 2018)

2.2.3 Factors influencing behaviour

Behaviour is influenced by motivation. Some motivational factors include the joy resulting from one's actions, results of the actions and behaviour that aligns with one's beliefs or values (Kwasnicka et al., 2016).

Behaviour is re-enforced by repeated performance (Kwasnicka et al., 2016) and repeated learning (Carden & Wood, 2018). Habit, therefore, plays an essential role in generating behaviour (Gardner, 2015). An individual learns through socialisation, that is, the various norms, rules of conduct, values and attitudes, and desirable behaviours through which one fulfils their expected roles (Schein, 1971). As behaviour becomes habitual, the chances that it will be maintained increase (Kwasnicka et al., 2016).

A habit can be changed by changing beliefs, opinions as well as the environmental context (Carden & Wood, 2018). The environment and social context can either facilitate or hinder behavioural change. Whereas stable environments make behaviour and habits easier to sustain (Kwasnicka et al., 2016), a change in the environment could disrupt a habit (Carden & Wood, 2018). The culture in which the individual finds themselves in and the roles they are expected to fulfil could also determine how an individual behaves (Schein, 1971).

Human behaviour is also affected by experiences, the longer some behaviour continues, the less likely one would want to change. For example, if a person stays in a job, owns a house, or belongs to a certain political group, for a long time they may not see the need to change (Stage & Fedotov, 2018). Immediate behaviour changes often result from extrinsic motivation factors. However, intrinsic factors are understood to have stronger and lasting effects on behaviour compared to extrinsic motivation (Kwasnicka et al., 2016).

From the above discussion, behaviour is motivated by either external or internal factors or both, and can be learned. Individuals exhibit certain behaviour as they react or adapt to the various influences, and as they do so, they affect their immediate surroundings. When continuously performed, behaviour becomes habitual. In information security, it is notable that employees can and must learn proper information security behaviours. This might mean breaking old habits that employees were used to and teaching them the correct information security behaviours. The employees must be made aware of information security compliant behaviour to be able to comply with the ISPs. The next section discusses information security behaviour derived from information security studies.

2.3 Information security behaviour in the research literature

ISP compliance leads to secure behaviour among employees (Sommestad, Hallberg, Lundholm & Bengtsson, 2014). In this study, secure behaviour concerning information systems refers to actions by employees to protect data or information and information technology resources of the organisation. For example, secure behaviour with regards to passwords could include the following: the user selecting strong passwords (Blythe, Coventry & Little, 2015; Rhee et al., 2009; Siponen, Pahnila & Adam Mahmood, 2010), the user not using the default security password (Blythe et al., 2015; Hwang et al., 2019) and the user not sharing passwords with other system users (Blythe et al., 2015; Cheng et al., 2013; Herath & Rao, 2009a). Researchers have used various terms to refer to secure behaviour by employees, some of which are:

- Security-related behaviour (Guo, 2013),
- Security compliant behaviour (Guo, 2013),
- Security assurance behaviour (Guo, 2013),
- Security behaviour (Blythe et al., 2015),
- Conscious care behaviour (Safa et al., 2015),
- Information security behaviour modes (Alfawaz et al., 2010),
- A typology of employees' information security behaviour (Ahmad et al., 2016)
- Protection-motivated behaviour (Posey, Roberts, Lowry, Bennett & Lowry, 2013)
- Information security behaviour (Pattinson, Butavicius, Parsons, Mccormac & Jerram, 2015),
- Compliant behaviour (Connolly et al., 2016) and
- Information security policy compliance (Bulgurcu et al., 2011; Guo, 2013; Li, Stafford, Fuller & Ellis, 2017; Padayachee, 2012).

The next section discusses these terms.

2.3.1 Security-related behaviour

Guo (2013) uses the term "security-related behaviour" to define employee behaviour as employees use information systems, which either protect or reduce risks to organisational information systems. Security-related behaviour can be appropriate or inappropriate, where appropriate behaviour is ISP compliant and the inappropriate behaviour is not. The two types of security-related behaviour can further be differentiated based on whether action is required or not and also whether there is a motive for the behaviour. The undesirable behaviours might require a motive to initiate it, whereas some of the desirable behaviours may not need strong motives. Regarding action or inaction on the part of the employee, one might comply without actively doing anything or vice-versa (Guo, 2013).

2.3.2 Security-compliant behaviour

These are the intentional or unintentional behaviours that are compliant with organisational ISPs. Employees may intentionally try to comply with security policy or they may not be doing anything, but still, be in line with the organisation's policy. One of the key characteristics of security-compliant behaviour is that it may not involve any action (Guo, 2013).

2.3.3 Security-assurance behaviour

These are intentional behaviours of employees carried out to safeguard the organisation's information systems. Security assurance behaviour include taking measures to safeguard information and to report information security breaches. It requires deliberate action and some expertise on the part of the employee (Guo, 2013).

2.3.4 Security behaviour

Blythe et al. (2015) use the term security behaviour to refer to an employee's ability to carry out proper and effective security activities. Security behaviour has three aspects; these are:

- Security hygiene – this refers to the efficacy of the security activities by employees.
- Prevention strategies – these are behaviours that protect information systems resources and prevent security breaches. Employees with high security hygiene take right actions and are less prone to security risks. Employees with low security hygiene, lack security awareness and engage in bad security behaviours. Some examples of low security hygiene behaviours include failure to change the default password and depending on the computer to auto-lock when they leaving their work-station.
- Security citizenship – this refers to actions that aid in business continuity and recovery. For example, employees in the high security hygiene category will back up their data and notify co-workers of security issues (Blythe et al., 2015).

2.3.5 Conscious-care behaviour

Conscious-care behaviour means that employees actively think about the effects of their actions with regards to information security as they use information systems. Information security knowledge, awareness and experience are important in fostering conscious-care behaviour (Safa et al., 2015).

2.3.6 Information security behaviour modes

Alfawaz et al. (2010) put forward security-behaviour modes as “knowing-doing mode, knowing-not doing mode, not knowing-doing mode and not knowing-not doing mode”. These are summarized below.

2.3.6.1 Not knowing-not doing

This refers to employees or system users who violate information security rules but do not have any knowledge of the organisation's ISP requirements (Alfawaz et al., 2010). Therefore, their failure to comply with ISPs could be attributed to their ignorance of the ISPs.

2.3.6.2 Not knowing-doing

This mode refers to employees who do not have any knowledge of the ISP requirements and security knowledge but exhibit the right information security behaviour. While such users are not aware of the organisation’s ISPs, they will ask superiors or colleagues before carrying out certain activities (Alfawaz et al., 2010).

2.3.6.3 Knowing-not doing

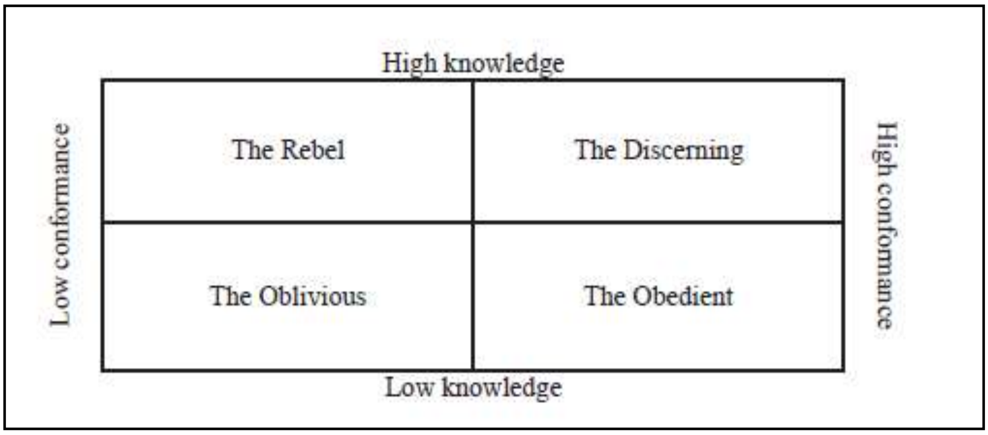
This refers to employees who have the required ISP knowledge and information security skills, but still violate the rules (Alfawaz et al., 2010).

2.3.6.4 Knowing-doing

This refers to employees who have knowledge of the ISPs and the information security knowledge/skills and thus comply with the ISPs (Alfawaz et al., 2010).

2.3.7 A typology of information security behaviour of employees

Ahmad et al. (2016) group employees into four categories, based on whether they are knowledgeable about security guidelines and whether or not they conform with the information security guidelines as shown in Figure 2-2. Discerning individuals will conform to the information security rules since they have information security knowledge. Obedient employees will follow information security rules, not because they have the knowledge, but merely follow rules for the sake of it. Rebel employees do not conform to information security guidelines despite having information security knowledge. Oblivious employees do not follow information security rules because they do not have the necessary information security knowledge (Ahmad et al., 2016).



High knowledge

Low conformance

The Rebel	The Discerning
The Oblivious	The Obedient

High confomance

Low knowledge

Figure 2-2: A typology of' information security behaviour of employees (Ahmad et al., 2016).

2.3.8 Protection-motivated behaviour

Protection-motivated behaviour refers to, "volitional behaviours enacted by organisational insiders to protect (1) organisationally relevant information and (2) the computer-based information systems in which the information is stored, collected, disseminated, and/or manipulated from information-security threat" (Posey, Roberts, Lowry, Bennett & Lowry, 2013, p.6). This suggests deliberate information security behaviour that protects an organisation's information and information systems.

2.3.9 Information security behaviour

Pattinson et al. (2015) use the term information security behaviour to refer to all the behaviours of computers users as part of doing their job and these behaviours can be deliberate risky or not.

2.3.10 Compliant behaviour

Connolly et al. (2016) refer to compliant behaviour as following the policies, procedures, and norms regarding information security within the organisation.

2.3.11 Information security policy compliance

Compliance is expressed as the adherence by employees to the ISPs (Bulgurcu et al., 2010; Guo, 2013; Padayachee, 2012). Li et al. (2017) define ISP compliance as employee compliance with information security guidelines as employees perform their jobs. Employees are expected to align their actions to the expected behaviours as written in organisational ISPs.

2.3.12 Review of the various definitions

From the various terms described above, some aspects of the behaviours are common. The most common theme being that secure behaviour concerning information security protects information system resources or results in the avoidances of security breaches and compliance with ISPs (Blythe et al., 2015; Guo, 2013; Safa et al., 2015). With regards to security assurance behaviour, the employee takes precautions (Guo, 2013); this aligns with Safa et al. (2015)'s definition of conscious care behaviour where the employee has to always think about the effect of their behaviour. Secure behaviour also results in business continuity and recovery (Blythe et al., 2015). It is the employee's intention to comply with the ISP (Guo, 2013; Safa et al., 2015), although Guo (2013) also states that the employee may unintentionally comply with the ISP. Alfawaz et al. (2010) also mention that in the not doing mode, the employee has knowledge of the rules and has the information security skills but chooses not to comply. Soomro, Shah & Ahmed (2016) propose a typology of information security behaviour of employees that has similarities with the behaviour modes of Alfawaz et al. (2010). Both studies state that an employee can comply with ISPs even when they are not knowledgeable about information security rules. The employees do not know about the existence of the ISPs but still act in secure ways with regards to information security. In summary, all the definitions have in common compliance with ISPs.

Table 2-3 summarises the attributes of behaviour and those of the information security behaviour sections. It should be noted that the respective summaries are listed side-by-side in the table but not for comparative purposes. These summaries from sections 2.2 and 2.3 are then built into the definition of information security compliant behaviour. The definition for information security compliant behaviour proposed in this study is, therefore, a result of the general behaviour definition from the various fields of study as shown section 2.2 as well as the definitions of secure behaviour from the behavioural information security literature.

Table 2-3: Summary of behaviour and attributes of information security behaviour

Behaviour	Information security behaviour
Behaviour is influenced by both intrinsic and extrinsic factors.	Involves protecting information and information system resources.
Behaviour has impact and meaning in a given environment.	Aims to prevent security breaches.
Behaviour can be learned.	Aids in business recovery and continuity.
Behaviour is observable and measurable.	To behave appropriately, employees must be knowledgeable about the ISPs.
Behaviour can be a reaction to environmental factors	Compliance is adherence to ISPs.

The next section describes information security compliant behaviour - the definition proposed in this study.

2.4 Information security compliant behaviour

Below is the proposed definition of information security complaint behaviour:

Users perform actions to protect the information and technology resources of their organisation from malicious others to maintain the confidentiality, availability, integrity and privacy of data/information. These actions could be reactions to attacks on the data or information and information systems resources, for example, restoring a database after a system crash. The actions could also be learned procedures performed regularly to protect data or information and information systems resources, for example, making a backup or changing a password.

These actions may not necessarily be part of the job specification of the user, and the user may have to learn and perform these actions. These actions must conform to the ISPs of the organisation. These actions result in:

- prevention of security breaches,
- business continuity, recovery and availability,
- protection of confidentiality of information (non-disclosure),
- protection of hardware, software, integrity and quality of information and
- maintenance of trust and reputation of both the employee and the organisation.

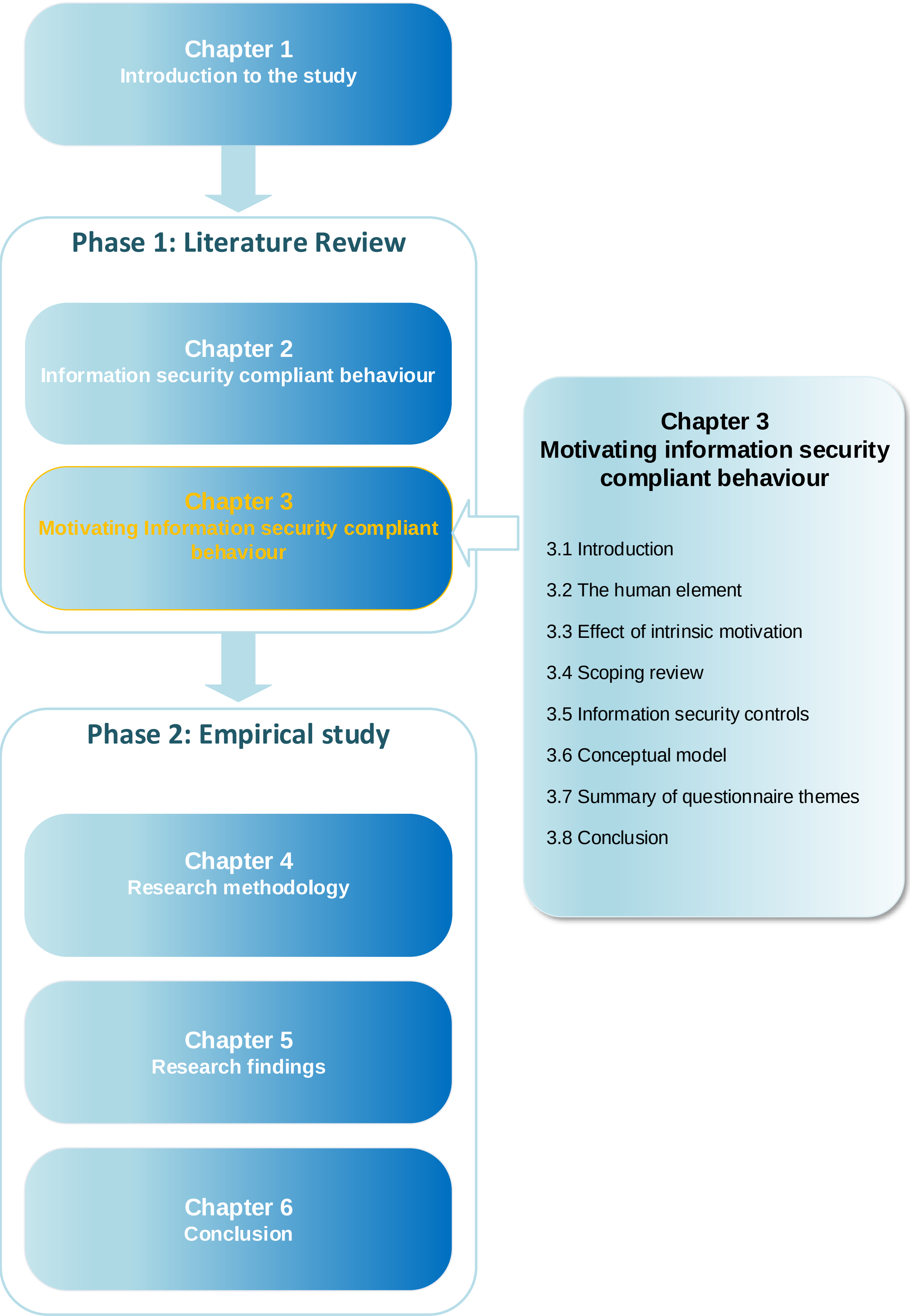
In the current study, information security compliant behaviour refers to the action of the employee in the context of a formal organisation and excludes the home user.

2.5 Conclusion

This chapter discussed behaviour in general and the meaning of secure behaviour concerning information security before proposing a definition of information security compliant behaviour. The objective of the chapter was to propose a definition of information security compliant behaviour for this study and this was achieved.

Chapter 3 comprises a literature review of information security compliant behaviour. The theoretical perspective of this study is also described. The results of the chapter include identification of the research gap for this study as well as identification of the conceptual model and questionnaire themes.

CHAPTER 3


Chapter 1
Introduction to the study
Phase 1: Literature Review
Chapter 2
Information security compliant behaviour
Chapter 3
Motivating Information security compliant behaviour
Phase 2: Empirical study
Chapter 4
Research methodology
Chapter 5
Research findings
Chapter 6
Conclusion
Chapter 3
Motivating information security compliant behaviour
3.1 Introduction
3.2 The human element
3.3 Effect of intrinsic motivation
3.4 Scoping review
3.5 Information security controls
3.6 Conceptual model
3.7 Summary of questionnaire themes
3.8 Conclusion

3 MOTIVATING INFORMATION SECURITY COMPLIANT BEHAVIOUR

3.1 Introduction

This chapter reviews the current body of literature regarding information security compliant behaviour. The outcome of this chapter is an information security compliant behaviour (ISCB) conceptual model from the perspective of the SDT. It is envisaged that the model will contribute to an improvement in our understanding of the significance of intrinsic motivation concerning information security behaviour.

This chapter will address objectives 1, 2 and 4 of the research, which are:

- To investigate what factors influence information security compliant behaviour of employees.
- To explore the existing research with a view to establish theories that have been used for studying information security behaviour.
- To develop an information security compliant behaviour conceptual model that is based on the SDT.

The chapter discusses intrinsic factors influencing information security compliant behaviour in section 3.3. A scoping review to explore the theories applied in studying information security complaint behaviour is outlined in section 3.4, information security controls in section 3.5, the theoretical perspective of this study and the conceptual model which is derived from the self-determination theory (SDT) in section 3.6. Before concluding the chapter in section 3.8, the chapter summarises the questionnaire focus areas in section 3.7. The next section is meant to provide a brief background on the human element, an important subject of this study. Thereafter, the discussion focuses on some of the intrinsic factors influencing the behaviour of the employees to comply with ISPs in the organisation.

3.2 The human element

It is said that technological solutions do not provide sufficient protection against information security threats (Bhaharin et al., 2019; Faizi & Rahman, 2020; Mani, Mubarak, Heravi & Choo, 2015; Safa et al., 2015) because they guard against technical attacks

(Flores & Ekstedt, 2012). The information security behaviour of employees is also important in reducing information security threats (Alohali, Clarke, Furnell & Albakri, 2017; Faizi & Rahman, 2020). The importance of both technology and the human element cannot, therefore, be overemphasised since both are important in ensuring that information security threats are reduced and information assets are protected (Bhaharin et al., 2019).

While employees can aid in reducing information security threats, it should be noted that they may also cause security breaches. The information security behaviour of employees has continued to impact both information security research and practice (Pahnila, Karjalainen & Mikko, 2013). Hence, it is important to find ways of reducing security breaches that result from employee behaviour. To that end, organisations usually put in place ISPs to reduce information security risks (Sommestad et al., 2017). It has been argued that compliance with ISPs, by employees, minimises security incidents (Humaidi & Balakrishnan, 2017; Nasir, Rashid & Hamid, 2017). Therefore, a need exists to understand what motivates compliance with ISPs (Bhaharin et al., 2019; Curry et al., 2018; Huang, Parolia & Cheng, 2016) since the human element is also responsible for security breaches (Ofori et al., 2020).

It is the argument of this study that the behaviour of employees is important in protecting information and should thus be managed to prevent information security threats. Therefore, the next section discusses the effect of intrinsic motivation on compliance with ISPs in organisations. The section will attempt to demonstrate the need for intrinsic motivation on ISP compliance among employees as well as the significance of intrinsic motivation in studying employee compliance with ISPs.

3.3 Effect of intrinsic motivation on compliance

Motivation is often described as either intrinsic or extrinsic. Behaviour resulting from intrinsic motivation is performed for the gratification of performing the task (Vallerand, 2012; Wang, 2015) as well as challenge and interest associated with the task (Zohar et al., 2015). On the other hand, extrinsic motivation is associated with behaviour that is influenced by the desire to get a reward or the fear of punishment (Hayenga & Corpus, 2010; Vallerand, 2012; Wang, 2015). According to Padayachee (2012), ISP compliance is a function of both intrinsic and extrinsic factors. In the information security context, it has been argued that deterrence mechanisms (a form of extrinsic motivation) are not enough to motivate the lasting commitment of employees to ISP compliance (Kranz & Haeussinger, 2014). A need, therefore, exists for an approach that focuses on the role of intrinsic motivational factors (Padayachee, 2012; Son, 2011), since few studies have been undertaken on this subject (Alzahrani et al., 2018; Sikolia & Biros, 2016).

This section discusses perceived effectiveness; legitimacy and perceived value congruency; and perceived fairness. It is aimed at demonstrating that intrinsic motivation is important in motivating compliance with ISPs.

3.3.1 Perceived effectiveness

Herath & Rao (2009) examined how extrinsic and intrinsic motivation promotes ISP compliance. On one hand, the study findings show that perceived effectiveness (an intrinsic motivation factor) positively affected ISP compliance of employees. On the other hand, extrinsic motivational factors (severity of the penalty, the certainty of detection, peer behaviour, and normative beliefs) were found to partially affect compliance intentions. The findings by Herath & Rao (2009) suggest that both intrinsic and extrinsic factors have an effect on the information security behaviour of employees. However, it can be argued that the intrinsic factors were found to be much more impactful since the extrinsic motivational factors only had a partial effect on compliance intention.

It is therefore concluded that, when employees perceive that their information security actions could successfully help deter security breaches, they will comply with the ISPs (Herath & Rao, 2009a).

3.3.2 Perceived legitimacy and perceived value congruence

Son (2011) studied the effect of perceived certainty and severity of sanctions as extrinsic factors as well as perceived legitimacy and perceived value congruence of information security policy compliance as intrinsic factors. The study showed that intrinsic motivation factors (perceived legitimacy and perceived value congruence of the ISP) promoted ISP compliance whereas the extrinsic factors did not. The results by Son (2011) suggest that the role of the intrinsic factors surpassed the role of the extrinsic motivation factors. Thus, Son (2011) suggested that intrinsic factors could improve our understanding and provide alternative solutions for ISP compliance; in addition to those provided by the extrinsic motivation factors. Perceived legitimacy of the ISP is defined as the extent employees regard the ISP as applicable, necessary and impartial. It is also argued that if the significance of the ISP is effectively communicated, employees will accept it as legitimate (Alzahrani et al., 2018; Son, 2011).

Perceived value congruence is the perception of employees regarding how much they share the same values with their organisations. People generally tend to interact with those with whom they share similar beliefs as this tends to verify and reinforce their own beliefs (Son, 2011). The employee will likely follow the ISP if the organisation's values align with their beliefs or personal norms.

The study by Son (2011) shows that the effect of the intrinsic factors was more significant than that of the extrinsic factors with regards to influencing ISP compliance intentions of employees.

3.3.3 Perceived fairness

Bulgurcu et al. (2011) assert that employees are intrinsically motivated towards ISP compliance if they perceive that the ISP is fair. ISP fairness refers to an employee's perception that the requirements contained in the ISPs are reasonable. In the study by Bulgurcu et al. (2011), ISP fairness was studied as a moderator to Perceived Organisational Cost of Non-Compliance (CNC) and Perceived Organisational Cost of Compliance (CC) and was found to impact perceived organisational cost of non-compliance. The research by Bulgurcu et al. (2011) also suggested that intrinsic motivation is important. Therefore, if employees perceive the ISP to be fair they will comply with its requirements.

The preceding discussion highlights that employees are affected by intrinsic and extrinsic factors to comply with ISPs and that intrinsic motivation impacts the ISP compliance intention of employees. Padayachee (2012) states that intrinsic motivation leads to stronger internalisation of behaviour that is compliant with ISPs than extrinsic motivation. However, given the importance of intrinsic motivation factors, there are few studies that have investigated information security behaviour of employees from the perspective of intrinsic motivation (Sikolia & Biros, 2016). This section has identified intrinsic motivation as being important; therefore, this study will proceed from the intrinsic motivation perspective.

The next section will discuss what has been done in the field and this was accomplished through a scoping review.

3.4 Scoping review

The previous section presented the significance of intrinsic motivation in the study of factors that motivate compliance with ISPs. This section, therefore, seeks to identify a theoretical perspective that can be used to study employee ISP compliance from an intrinsic perspective.

A scoping review was carried out and was guided by the Arksey and O'Malley methodology (Arksey & O'Malley, 2005; K, Heather & Danielle, 2010). A scoping review is an initial assessment of the literature to determine the main ideas and concepts available in a research area. It can be used to point out research gaps in a specific research area (Arksey & O'Malley, 2005). In this study, the scoping review was applied to identify the research gap and to provide a summary of theories used in information security compliance studies.

The scoping review of this research study aims to address the following:

- To gain a broad overview of studies on information security compliant behaviour for the period 2009 to 2020 as well as theories used and
- To establish the research gap for the current study.

The review process follows the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) method and the information is presented using the PRISMA flow diagram (Moher, Liberati, Tetzlaff & Altman, 2009). PRISMA comprises items used in presenting results of systematic reviews and meta-analyses and it can also be used for reporting scoping reviews (PRISMA, 2015). In this research study, PRISMA is used to illustrate the steps that were followed in carrying out the scoping review.

3.4.1 Search strategy

With academic databases containing hundreds of millions of entries that are available for search, a literature search often unearths a large number of studies with only a few studies being actually relevant to the research question and the majority is irrelevant. Devising a search strategy is therefore important because it avoids wasting valuable resources and time and it eliminates biases. To this end, careful selection of terms, inclusion and exclusion criteria and bibliographic databases is important to ensure that accurate, high quality and relevant data is collected for a comprehensive literature review.

3.4.1.1 Keywords

Conducting a literature review involves the use of web-based search engines or using various electronic research databases to search for data and identify materials that best describe the research topic of interest. A good set of keywords is important and will ensure that the search is as comprehensive as possible and assist the researcher to retrieve relevant information and minimises the number of irrelevant returns. For this reason, the following key words were used to search for relevant publications relating to this research: information security behaviour; information security policy compliance; and information security compliance behaviour.

3.4.1.2 Inclusion and exclusion criteria

The criteria for inclusion and exclusion are the conditions that were used to determine the papers to include or exclude from the scoping review. These conditions were set before the scoping review was conducted to ensure that all articles were treated without bias.

Publications were selected for inclusion to this research study on the basis that they:

- Were published between 2009 and 2020,
- Deal primarily with the topics of compliant information security behaviour or compliance to ISPs and
- In instances where several papers have referenced the same study, only the most recent paper was considered for this research study.

Publications were excluded on the basis that they:

- Were not written in English,
- The full text was unavailable,
- Were non-academic white papers,

- Were letters, editorials and position papers,
- Were papers related to health and safety in an engineering context,
- Were of health-related contexts such as hospitals governed by other legislation and
- Were papers related to health and compliance with medication.

3.4.1.3 Databases

The following databases were searched with the intention to retrieve the relevant articles that meet the search criteria: Web of Science, Scopus, Scholar Google, ACM Digital Library, IEEE as well as the conference papers of the International Symposium on Human Aspects of Information Security & Assurance (HAISA) which focuses specifically on information security aspects related to people.

3.4.1.4 Data collection and analysis

The initial literature search yielded 330 potentially relevant publications (171 from the academic databases and 159 from Scholar Google and HAISA). After removing duplicates, the number of publications was reduced to 192. After going through the abstracts, the number of publications was reduced to 48; this number was reduced further to 22 following a full-text scan. The information is shown in Figure 3-1 as a PRISMA flow diagram showing the statistics of the literature search, screening and selection up to the analysis of the selected studies.

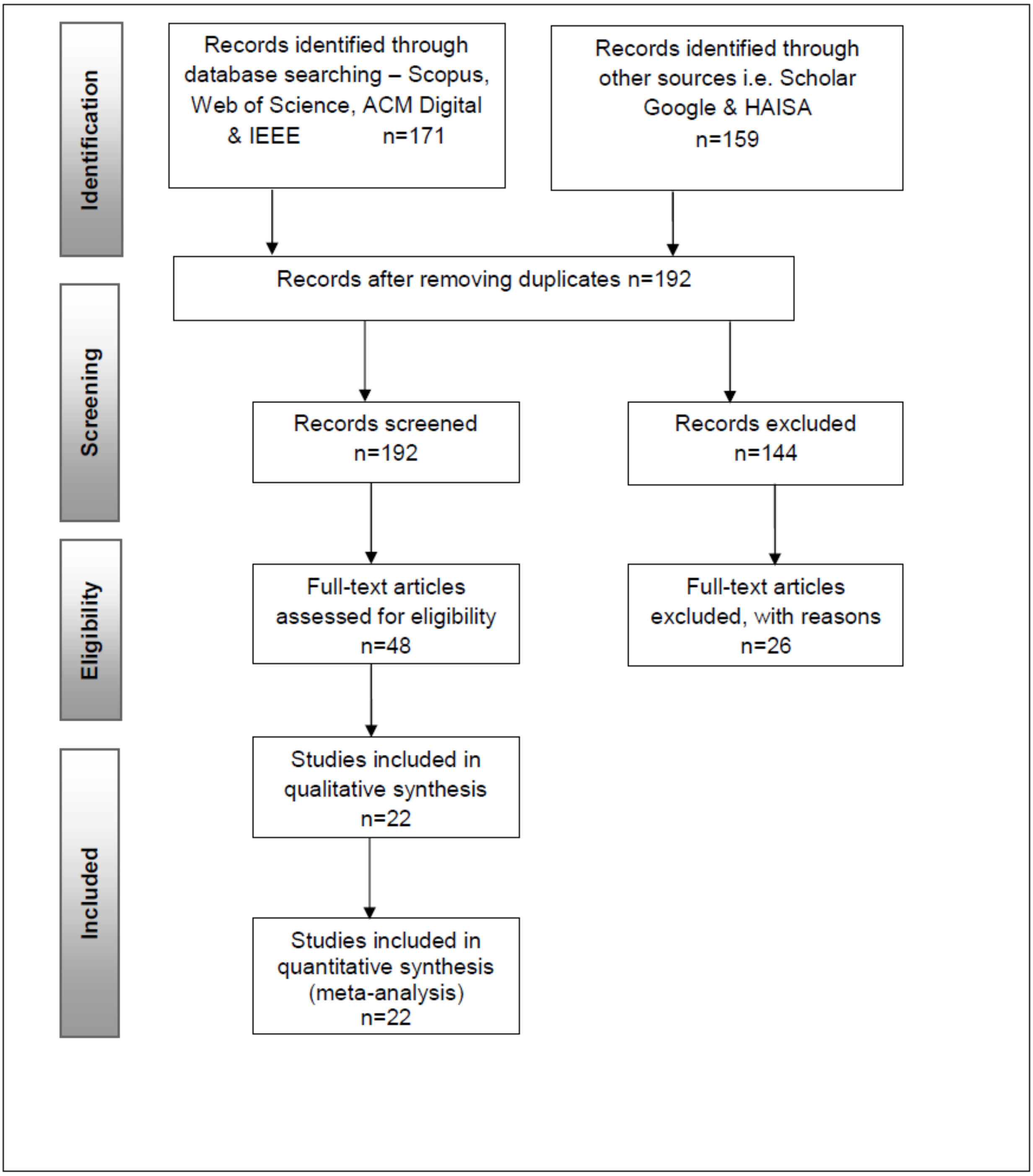

Identification
Screening
Eligibility
Included
Records identified through database searching – Scopus, Web of Science, ACM Digital & IEEE n=171
Records identified through other sources i.e. Scholar Google & HAISA n=159
Records after removing duplicates n=192
Records screened n=192
Records excluded n=144
Full-text articles assessed for eligibility n=48
Full-text articles excluded, with reasons n=26
Studies included in qualitative synthesis n=22
Studies included in quantitative synthesis (meta-analysis) n=22

Figure 3-1: PRISMA flow diagram

Table 3-1 summarises the final 22 papers. The table is organized as follows:

- YEAR in which the paper was published,
- AUTHOR(S) of the publication,
- FACTORS – variables or construct that the study evaluates,
- THEORIES that informed the study,
- CONTRIBUTIONS that the study makes or results of the study,
- OUTPUT/ARTIFACT – the additional product of the study and
- GAPS – areas that the respective studies have not addressed or have suggested for future research.

Creswell (2012) refers to a research gap as an area or topic that has not yet been researched or discussed in the current literature. In this study, this research gap emanates from various calls by researchers to: (i) conduct further research by expanding the scope of currently existing research; and/or (ii) conduct new research in areas that have not been covered by currently existing research. To this end, it is on the basis of the information presented in Table 3-1 that the research gaps that need to be addressed by this study were identified.

Table 3-1: Publications included in the scoping review

No.	Year	Author	Theories	Factors	Contributions	Output/Artefact	Gaps/Future research
1	2009	Herath & Rao	PAP GDT	"Severity of penalty, certainty of detection, normative beliefs and peer behaviour".	The study reports that: intrinsic and extrinsic factors influence information security behaviour; How an employee perceives their co-workers' compliance with the ISPs influences the employee's ISPs intentions. The certainty of detection was also reported to influence compliance intention.	Developed a model which is built using constructs from the deterrence theory and the principal-agent theory to assess factors that influence information security behaviours.	Research to evaluate positive extrinsic factors such as rewards and negative intrinsic factors such as perception of loss.
2	2009	Rhee et al.	SCT	"Self-efficacy, self-efficacy in information security (SEIS)".	The study found that users with high SEIS positively influence information security behaviour.	Model using the social cognitive theory to understand users' SEIS.	• Explore other variables that influence SEIS for example "vicarious learning" and "social persuasion" • Investigate how computer self-efficacy (CSE) i.e. self-efficacy regarding the general use of computers could lead to SEIS i.e. self-efficacy relating to information security skills. • Investigation of whether there is a correlation between CSE and SEIS.
3	2010	Bulgurcu et al.	TPB RCT	"Intrinsic benefit, safety, rewards, work impediment, intrinsic cost, vulnerability, and sanctions".	The study found that attitude, normative beliefs, and self-efficacy influence ISP compliance intentions of employees. The study also reports that information security awareness affects employees' information security behaviour.	A model integrating the TPB and the RCT to study the antecedents of ISP compliance.	• Identification of factors that foster information security awareness (ISA) • Investigation of the types of ISA that exist at different levels of the organisation as it is assumed that different aspects of ISA may be required at different levels of the organisation. • Identify other intrinsic factors influencing compliance, besides intrinsic cost and intrinsic benefit identified in this study.
4	2011	Abraham	No particular theory	"Security policies, communication practices, the content of awareness efforts, management influences, peer influences, deterrence efforts, rewards, employee participation, user's knowledge, self-efficacy, attitudes, beliefs, psychological ownership, organisational commitment,	Summary of factors affecting information security behaviour	A literature review which brings out 18 themes applicable to both security practitioners and researchers when implementing information security programs.	• A need exists for research that will analyse specific behaviours to particular ISPs. • A need exists for research that examines the changing aspects of security behaviour within groups in organisations since most studies focus on individual user security behaviour.

No.	Year	Author	Theories	Factors	Contributions	Output/Artefact	Gaps/Future research
				trust, procedural justice, ease of use and effectiveness of security technology".			
5	2011	Son	GDT	"Perceived deterrent certainty, perceived deterrent severity, perceived legitimacy, and perceived value congruence".	The study states that intrinsic motivation variables made a significant contribution by explaining better employees' compliance than the extrinsic motivation variables.	A model that integrated the general deterrence theory and the variables rooted in intrinsic motivation to explain employees' compliance behaviour.	A need exists to investigate more intrinsic motivation variables and how they influence compliance behaviour.
6	2011	Bulgurcu, Cavusoglu & Benbasat	TPB SBT	"ISP fairness, organisational commitment and organisation-based beliefs about the consequences of compliance and non-compliance".	The study found that beliefs about the effects of compliance or violation of ISP influence attitude towards ISP compliance.	A model built using the TPB and the SCT to study the effects of beliefs by employees on the results of ISP compliance or violation.	Investigation of the environments in which employees consider the ISPs to be fair.
7	2011	Aurigemma	TPB GDT PMT	"Habit, self-efficacy, perceived controllability, sanction severity, probability of sanction, perceived vulnerability, threat severity, response efficacy, consequence assessment, belief outcomes, perceived benefit and perceived cost of compliance".	A model that brings together common core constructs from several studies, building on the strengths of these studies.	A theoretical framework to help in understanding behavioural compliance with ISPs.	• A need exists to investigate the gap between behavioural intention and the actual behaviour. • Investigation of the cost-benefit analysis of the attitude to ISP compliance.
8	2012	Padayachee	SDT	"Apathy, resistance, disobedience, low self-control, opportunistic, incompetence, past deviant behaviour, external regulation, introjection, identification, integration, competence, etiquette, commitment, obedience, ethical and self-disapproval".	The paper produced a "Taxonomy of compliant information security behaviour", which was designed to help in understanding how motivation (intrinsic and extrinsic) , influences information security behaviour from the perspective of SDT.	The "Classification of Security Compliant Behaviour based on the Self-Determination Theory" model	• A need exists to examine factors that promote intrinsic motivation, compared to those that weaken it. • Application of the model from this study into a tool that can be used for the detection of insider threats by assessing employee motivations. • Investigate more intrinsic motivation factors that influence security compliant behaviour.
9	2012	Hu	TPB OT	"Top management, organisational culture, and employee cognitive beliefs".	The study found that the participation of top management in the information security functions of the organisation influences the attitudes of employees towards ISP compliance and the employees' perceived behavioural control over ISP compliance. The study also found that organisational culture influences employee attitudes towards ISP compliance.	A model that integrates top management, organisational culture, and TPB to study how management, organisational culture, and employee cognitive beliefs affect ISP compliance.	• An investigation of how the different methods and modes of communication that top management use to shape the beliefs of employees and the culture of the organisation, can influence compliance towards ISPs.

No.	Year	Author	Theories	Factors	Contributions	Output/Artefact	Gaps/Future research
10	2012	Ifinedo	PMT TPB	"Perceived vulnerability, perceived severity, response efficacy, response cost, self-efficacy, attitude toward compliance with ISPs, and subjective norms".	The study reports that "self-efficacy, response efficacy, attitude, perceived vulnerability and subjective norms" influence compliance with ISPs.	A model integrating the TPB and the PMT to understand employee ISP compliance.	Investigate compliance to ISP by contractors.
11	2013	Ifinedo	TPB SBT SCT	Attachment, commitment, involvement, and personal norm.	The study found that socio-organisational factors influenced employees' attitudes towards compliance with ISPs. Social influence and employees' competence perceptions concerning information security positively influence compliance with ISPs.	A model that utilises the TPB, SBT and SCT to explain ISP compliance.	Investigation of the effects of organisational citizenship behaviours on ISP compliance.
12	2013	Wall, Palvia, Lowry & Benjamin	SDT Psychological reactance theory	"Self-efficacy, response efficacy, self-determination and reactance to compliance".	The study reports that self-determination fosters how employees perceive self-efficacy and response efficacy and that psychological reactance decreases how employees perceive their response efficacy. It was also reported that response efficacy predicts security behaviour.	Conceptual model developed by integrating SDT and psychological reactance theory which was tested in an online survey.	• Investigate intrinsic motivation factors, since they could have greater effect on information security behaviour than extrinsic factors. • Development of an ISP compliance measurement instrument from the perspective self-determination theory.
13	2014	Kranz & Haeussinger	TPB SDT-OIT	Internal perceived locus of control (PLOC), external PLOC, self-efficacy, attitude and normative beliefs.	The study results show that alignment of employees' personal values with the organisation's information security goals influences the employees' intention to comply ISPs. The study also found that deterrence methods did not have any influence on ISP compliance intention.	A model integrating TPB and OIT, a sub-theory of SDT which was used to test employees' motivations to comply with organisational ISPs	• Investigate the role of employees' endogenous motivations and beliefs on information systems security behaviour • Employ longitudinal research designs to investigate the same constructs as in this study, in order to consider the changing user perceptions over time.
14	2015	Humaidi & Balakrishnan	Leadership style theory and & HBM	"Management support, information security awareness, security barrier, information system skills and trust, and self-efficacy".	Results of the study show that support from management has influence on security awareness, competence (self-efficacy) and ISP compliance. However, perceived susceptibility and perceived security barrier did not influence ISP compliance for low experience user groups.	Research model that integrated leadership style theory and HBM to study employee compliance with ISPs.	Investigate factors that mediate the relationship between leadership styles and user's information security compliance behaviour.
15	2015	Safa, Sookhak, Von Solms, Furnell, Ghani & Herawan	PMT TPB	"Information security awareness, information security organisation policy, information security experience, Involvement,	The study found that "information security awareness, information security organisation policy, experience and involvement, attitude towards information security,	Model integrating PMT and TPB to study how to foster "information security-conscious care behaviour" in employees.	Investigate how knowledge sharing and training techniques in information security can influence compliance with ISPs.

No.	Year	Author	Theories	Factors	Contributions	Output/Artefact	Gaps/Future research
				threat appraisal, and information security self-efficacy".	subjective norms, threat appraisal, and information security self-efficacy" have a positive effect on users' information security behaviour. However, the study found that the perception of behavioural control has no influence on information security behaviour.		
16	2016	Huang, Parolia & Cheng	Psychological ownership	Self-efficacy, psychological ownership, control right, self-investment, knowledge, training, background, and experience.	The study confirmed that self-efficacy positively influences ISP compliance and also found that psychological ownership does not influence ISP compliance	Model-based on psychological ownership to verify the impact of psychological ownership & self-efficacy of individuals concerning information security compliance behaviour.	Investigate the influence of organisation-based and information-based psychological ownership on information security behaviour.
17	2017	Humaidi & Balakrishnan	TPB Trust factor	Self-efficacy, perceived trust and management support.	Management support was found to influence health professionals' trust in ISP. Perceived trust was also found to influence health professionals' attitudes towards ISPs.	A model integrating the TPB and the trust factor to study the influence of management support on employee compliance with ISPs among health professionals.	Investigation of factors that mediate the relationship between leadership styles and employee's information security behaviour.
18	2018	Guhr, Lebek & Breitner	Full-range leadership theory	"Employees' security compliance intention, employees' security participation intention, transactional leadership, transformational leadership and passive/avoidant leadership".	The study found that transactional leadership does not influence employees' compliance intention with ISPs. The study also found that passive/avoidant leadership does not influence compliance with ISPs.	Model that can be used to study the effect of full-range leadership on employees' information security behaviour.	• Impact of adding moral reasoning to the current model for this study. • Investigate how leadership (management) impacts various information security behaviours.
19	2018	Alzahrani, Johnson & Altamimi	SDT	"Perceived competence, perceived relatedness, perceived autonomy, perceived legitimacy and perceived value congruency".	The study outlines the role of intrinsic motivation concerning the behaviour of employees towards ISP compliance.	A model integrating SDT with constructs "perceived legitimacy and perceived value congruency" to study the role of intrinsic motivation.	• Test the same research model using qualitative approaches. • Investigate the perception of legitimacy and value congruence using qualitative methods.
20	2019	Inho Hwanga, Robin Wakefield, Sanghyun Kimc, and Taeha Kimd	SLT	"Security education, security policy, physical security system, security visibility, management participation, information security awareness".	The study reports that security education, security policy, security visibility, management participation influences security awareness. However, physical security systems do not influence security awareness in the study. The study identifies the antecedents of information security awareness	Model based on the SLT that explains variables that influence security awareness. Where information security awareness influences intention to comply.	Identification of more factors, if any that influence information security awareness.
21	2020	Faizi & Rahman	UMISPC	Response efficacy, threat, fear, intention to comply with ISP	The study assessed the influence of fear on intention and found no significant relationship between fear	The study evaluated a model built using the UMISPC to study	• The study used a single scenario. The same study model could be used with

No.	Year	Author	Theories	Factors	Contributions	Output/Artefact	Gaps/Future research
					and intention to comply. However, the study found that there was a significant relationship between threat and fear as well as between response efficacy and threat	the effect of fear on intention to comply	more scenarios to investigate the influence of fear on intention.
22	2020	Snyman & Kruger	TPB	Physical milieu, Social milieu	The study investigated the role of “external contextual factors of information security behaviour”. These were conceptualised into the TPB. The study model shows that extrinsic factors have an effect on intrinsic factors.	Model showing how the external contextual factors interact with the TPB.	• The study investigated two factors only, more could be considered. • The study applied behavioural context analysis on external factors. Behavioural context analysis could be applied on the intrinsic factors as well.

From Table 3-1, the theories that appear most frequently in the studies considered are:

- Theory of Planned Behaviour (TPB) - 10 times,
- Self-determination Theory (SDT) - 4 times,
- Protection Motivational Theory (PMT) - 3 times,
- General Deterrence Theory – 3 times,
- Social Bond Theory(SBT) - 2 times and
- Social control theory (SCT) - 2 times.

Each of the remaining theories appears only once in the studies considered for the scoping review. A study by Lebek, Jörg, Neumann, Hohler & Breitner (2014) for identifying theories that were used most frequently in information security behaviour studies identified 54 theories, with the most frequently studied theories being: Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), General Deterrence Theory (GDT) and Technology Acceptance Model (TAM). The results of Lebek et al. (2014) were corroborated by Angraini, Alias & Okfalisa (2019) who found that TPB, GDT & PMT are some of the most frequently studied theories in information systems security behaviour for the period 2014 to 2018. A systematic review by Kuppusamy, Narayana & Maarop (2020) established that the SDT was one of the less used theories in information security behaviour studies and the Theory of Reasoned Action (TRA)/TPB and PMT was dominant; the study covered the period 2014 to 2019.

Table 3.1 shows that the models used in most of the studies were dominated by the extrinsic model where the motivation of employee to comply with ISP was largely affected by external factors. However, only 3 studies referred to the deterrence theory directly (Aurigemma & Panko, 2012; Herath & Rao, 2009a; Ofori et al., 2020; Son, 2011). The rest of the studies referred mostly to the effect of external factors that motivate employees. Examples of external motivation that were covered include: the effect of the external perceived locus of causality of employees on ISP compliance (Kranz & Haeussinger, 2014), organisation-based beliefs of employees on the consequences of compliance or violation of the ISPs (Bulgurcu et al., 2011) and the influence of management on compliance of employees to ISPs (Abraham, 2011; Hu, Dinev, Hart & Cooke, 2012; Humaidi & Balakrishnan, 2017).

The studies that addressed intrinsic motivational factors did so in addition to extrinsic motivational factors. However, the study by Alzahrani et al.(2018) used a model based solely on intrinsic motivation and the study by Rhee et al. (2009) only considered self-efficacy. The rest of the studies covered the intrinsic motivation factors and extrinsic factors (Herath & Rao, 2009; Son, 2011; Padayachee, 2012).

Therefore, this study takes the intrinsic motivational perspective and is based on the SDT, which postulates that the fulfilment of the three basic psychological needs (i.e. competence, relatedness, and autonomy) increases intrinsic motivation in individuals (Ryan & Deci, 2000). The SDT has not received as much attention as the other theories. While Padayachee (2012) used the SDT, the study did not test the theory empirically. Wall et al. (2013) integrated the SDT with Psychological Reactance theory and their study only considered competence and autonomy but excluded relatedness. Kranz & Haeussinger (2014) integrated the Theory of Planned Behaviour and the Organismic Integration Theory (a sub-theory of SDT), the authors did not consider the SDT the same way it is viewed in this current study. Alzahrani et al. (2018) integrated the SDT with the intrinsic motivation constructs of perceived value congruence and perceived legitimacy. The SDT has been used, in other studies, in conjunction with other theories. Therefore, this study seeks to study the SDT without integrating it with other theories or constructs from other theories.

The theories listed in Table 3-1 were applied in the studies considered for this review. Some studies considered a single theory and others a combination of and extensions of the theories. The theories formed the basis of the models that were developed in these studies.

The factors that were considered in Table 3-1 are the constructs or variables that were drawn from the theories. These factors were studied in relation to attitude to compliance, information security behaviour or compliance intention for the respective studies. Of all the factors considered, self-efficacy was the most investigated because it appears in 9 studies. All 9 studies investigated self-efficacy from different theories. Self-efficacy is similar to competence, which is being considered in this study.

The contributions listed in Table 3-1 refer to the findings reported in the respective studies. The studies reported the factors influencing the intention to conform with ISPs (Alzahrani et al., 2018; Faizi & Rahman, 2020; Guhr, Lebek & Breitner, 2019; Huang et al., 2016; Humaidi & Balakrishnan, 2015; Ifinedo, 2012; Kranz & Haeussinger, 2014) or information security behaviour (Bulgurcu et al., 2010; Herath & Rao, 2009a; Safa et al., 2015; Wall et al., 2013) or attitude concerning compliance (Bulgurcu et al., 2011; Hu et al., 2012; Humaidi & Balakrishnan, 2017; Ifinedo, 2013).

Table 3-1 shows outputs or artefacts in the form of models that were developed in the respective studies. The models, which were developed using the various theories, were adapted to demonstrate the relationship between factors and information security behaviour, intention to comply or attitude towards compliance. The factors were assessed on the basis of the developed models by, for example, testing the relationships depicted in the models.

The research gaps or future research in Table 3-1 relates to areas that authors of the studies consider were not covered by their studies or suggestions for extending their studies. This also includes research areas that were identified by the researcher as possible research areas that could be extended.

When considered as a whole, the information presented in Table 3-1 (i.e., theories, factors, contributions, output/artefact and gaps/future research) provide a summary and understanding of the research in information security behaviour or compliance with ISPs. Such an overview is important for this study because it allows the existing research gap to be identified and addressed. Table 3-1 shows that a need exists to study how the behaviour of employees could be motivated to conform to ISPs. This study contributes to addressing this need by assessing information security compliant behaviour from the perspective of the SDT.

In the following section the SDT, from which the conceptual model for this study will be derived, is discussed. A brief description of the theory is provided.

3.4.2 The self-determination theory (SDT)

The SDT explains the role of the basic psychological needs (the need for competence, relatedness and autonomy) in the development of self-determined behaviour (Legault, 2017). The SDT has been applied in other information security studies (Alzahrani et al., 2018; Kranz & Haeussinger, 2014; Padayachee, 2012; Wall et al., 2013) and states that the fulfilment of the basic psychological needs results in intrinsic motivation (Ryan & Deci, 2000). SDT assumes that the realization of the basic psychological needs is a requirement for the optimal psychological functioning of a human being (Broeck et al., 2008). From the SDT perspective, intrinsic motivation is associated with an increased sense of competence and self-determination. According to Ryan & Deci (2000), a perception of competence and autonomy enhances intrinsic motivation. Intrinsic motivation is claimed to be closely associated with self-determined behaviour (Deci & Ryan, 2015). The theory also states that people's relationships and their social environments should support the need for competence, relatedness and autonomy (Legault, 2017). Deci et al. (2017) state that the environment affects either positively or negatively the employees' need for competence, relatedness, and autonomy. According to Broeck et al. (2008) employees are best motivated when their innate potential is supported rather than when the work environment is over-controlling.

3.4.3 The need for competence

Competence, which is the belief that one is capable and can effectively carry out a task (Legault, 2017; Ryan & Deci, 2000), is linked to the self-efficacy concept of Bandura (1994). Self-efficacy is a person's belief in successfully carrying out task (Bandura, 1994). Bandura(1977) proposed that self-efficacy can determine how long one can persist when given a difficult task. The self-efficacy theory suggests that a person with low self-efficacy regarding a skill, will avoid such a task when that particular skill is required for the task (Bandura, 1977). In the domain of information security, self-efficacy refers to the perception that one has the information security skills to safeguard information and information systems from threats (Rhee et al., 2009; Safa et al., 2015), and by extension the ability to comply with ISPs (Ifinedo, 2012; Pahnila, Siponen & Mahmood, 2007; Safa et al., 2015). It is, therefore, assumed that individuals with high competence in information security will comply with the ISPs (Herath & Rao, 2009b; Ifinedo, 2013; Son, 2011). Self-efficacy was found to positively impact employee compliance with ISPs (Huang et al., 2016; Humaidi & Balakrishnan, 2017).

3.4.4 The need for relatedness

The need for relatedness refers to the desire to be meaningfully attached to others in a group (Legault, 2017). The need to belong and be connected with others is important for internalisation (Ryan & Deci, 2000). Satisfying the need for relatedness leads to the internalisation of the values and rules of the environment in which one is part of (Gagne & Deci, 2005; Ryan & Deci, 2000). When work is organized so that it allows employees to interdepend with colleagues, feel connected and respected by colleagues, they are likely to internalise the rules and develop intrinsic motivation (Gagne & Deci, 2005). If employees identify with the organisation they will feel attached to it and hence they will comply with rules (Li, Zhang & Sarathy, 2010). Therefore fulfilling the need for relatedness leads to attachment with the organisation and this has a positive impact on compliance with ISPs (Cheng et al., 2013; Ifinedo, 2012).

3.4.5 The need for autonomy

Autonomy is the perception that a person's behaviour is out of their own will, resulting in self-determined behaviour (Legault, 2017; Ryan & Deci, 2000). Autonomy is also described as the experience of internally perceived locus of causality, where an individual perceives that they determine their behaviour (Reeve, 2006). Therefore, when an employee is given a task, they act out of their own desire if the need for autonomy is satisfied (Broeck et al., 2008). It is stated that fulfilling the need for autonomy also increases the employees' effectiveness and their connection to the organisation (Deci et al., 2017). Employees whose behaviour is self-determined have a higher probability of complying with ISPs (Kranz & Haeussinger, 2014).

The next section discusses the information security controls that are put in place to protect information and information systems resources. This study assumes that when employees are intrinsically motivated, they will comply with ISPs. The information security controls will be used together with the SDT theory to develop the conceptual model.

3.5 Information security controls

Various standards define information security controls that must be put in place to protect information and information system resources in an organisation. This section will discuss the Centre for Internet Security Critical Security Controls Version 7 (CIS CSC) (Security

Centre for Internet, 2017), the NIST: Security and Privacy Controls for Information Systems and Organizations (SP800-53r5) (NIST, 2017) and the HAIS-Q questionnaire (Butavicius et al., 2020; Parsons et al., 2017), which were used to identify the key information security controls that end-users should be aware of. The two standards were selected because CIS CSC is meant for private organisations and the NIST standards are for the public sector, which suggests that the outcome should represent both the public and private sectors thus ensuring that the information security controls identified for this study map to key standards. HAIS-Q was selected because it is focused on areas of an ISP that are most prone to non-compliance (Parsons et al., 2014) and it has been validated on different samples of users (Butavicius et al., 2020; Parsons et al., 2017).

End-users must demonstrate compliance with the ISPs including information security controls that must be implemented to safeguard information and information system assets. Security controls focus on the necessary actions to safeguard information and the privacy of individuals (NIST, 2017). These are activities, processes or technologies that are implemented to decrease the risk of security breaches, that is, to prevent, mitigate and detect attacks (Pfleeger & Pfleeger, 2015). NIST defines families of controls with each family comprising a set of controls that address some security goals. These security and privacy controls must effectively and adequately decrease information security risks while complying with applicable laws and regulations (NIST, 2011). Therefore, users must demonstrate behaviour that is compliant with ISPs - behaviour that safeguards information and information systems. By so doing, users comply with the ISPs. A short description of CIS CSC, the NIST 800-53 R5 standard, a mapping of the two standards and HAIS-Q questionnaire is provided below.

- **NIST: Security and Privacy Controls for Information Systems and Organizations (SP 800-53 R5)**

NIST: Security and Privacy Controls for Information Systems and Organizations (SP 800-53 R5) defines a set of controls for federal information systems and organisations and is intended to help organisations fulfil the security and privacy requirements of FISMA, the United States Privacy Act of 1974. The controls can be applied in organisations or information systems involved in processing, storage, or disseminating of information (NIST, 2017).

- **Centre for Internet Security Critical Security Controls Version 7 (CIS CSC)**

Centre for Internet Security Critical Controls for effective cyber defence consists of 20 key actions, which are referred to as the Critical Security Controls (CSC). They are actionable recommendations that organisations implement to block or mitigate known attacks (Security Centre for Internet, 2017).

- **Mapping of NIST 800-53 R5 to CIS CSC 7**

Table 3-2 shows the mapping of the CIS controls to the NIST SP800-53 R5 controls. The table shows the control name in the first column with ticks in the second and the third columns to indicate the framework from which the control is derived. Ticks in both columns indicate a control exists in both standards. A single tick indicates that the control is found in one of the two frameworks. While Table 3-2 gives a list of the information security controls that organisations should implement, it is important to note that some controls apply to IT staff and others to end-users. Since the focus of this study is the information security behaviour of the end-user, therefore controls focussing on the end-user only will be included in the scope.

Table 3-2: Controls mapping of the CIS CSC 7 to the NIST SP800-53 R5 compiled from (NIST, 2017; Security Centre for Internet, 2017)

Control	**CIS CSC 7**	**NIST 800-53 R5**
Access Control	√	√
Awareness And Training	√	√
Audit And Accountability		√
Assessment, Authorization, And Monitoring	√	√
Configuration Management	√	√
Contingency Planning	√	√
Identification And Authentication	√	√
Individual Participation		√
Incident Response	√	√
Maintenance	√	√
Media Protection	√	√
Privacy Authorization		√
Physical And Environmental Protection		√
Planning		√
Program Management		√
Personnel Security		√
Risk Assessment	√	√
System And Services Acquisition		√
System And Communications Protection	√	√
System And Information Integrity	√	√

Control	**CIS CSC 7**	**NIST 800-53 R5**
Inventory and Control of Hardware Assets	√	
Inventory and Control of Software Assets	√	
Email and Web Browser Protections	√	
Limitation and Control of Network Ports, Protocols, and Services	√	
Penetration Tests and Red Team Exercises	√	

- **Human Aspect of Information Security Questionnaire (HAIS-Q)**

HAIS-Q is a questionnaire that was developed to study the relationships among the user's knowledge of ISP, attitude towards ISP and behaviour when using computers at work (Butavicius et al., 2020; Parsons et al., 2017). The instrument consists of 7 information security areas that are also referred to as focus areas. The focus areas are password management, email use, internet use, social media use, mobile devices, information handling and incident reporting (Parsons et al., 2017). Each of the focus areas is split into sub-areas, with each sub-area having a separate item for each of knowledge, attitude, and behaviour (KAB), which result in a total of 63 specific statements that make up the HAIS-Q. HAIS-Q uses a five-point Likert scale, which is rated from Strongly Agree to Strongly Disagree, for all the items in the questionnaire. The instrument uses the knowledge, attitude and behaviour model since it is assumed that the improvement in users' knowledge of the ISP and their attitude towards the ISP, positively impacts their information security behaviour (Parsons et al., 2017)

- **Selected information security controls for this study**

Table 3-3 shows the selected end-user information security controls for inclusion in this study. The controls have been selected based on the HAIS-Q focus areas, with an additional focus area of privacy. These controls are mapped to the CIS CSC and NIST 800-53 R5 standards to illustrate that they are correlated to the standards. The HAIS-Q questionnaire focus areas are listed in the second column, and references supporting the controls are also added. The controls are carried out by the end-users to protect the organisation's information as they carry out their work. These controls must be carried out by non-IS/IT staff, that is, they do not require IT expertise to perform.

Table 3-3 is organised as follows: the first column shows the focus area; the second column has the sub-areas as well as additional literature references for each sub-area.

The last three columns show the HAIS-Q, CIS CSC and NIST 800-53R5 alignment of the focus areas.

Table 3-3: Information security controls adapted from HAIS-Q and mapped to CIS CSC and NIST 800-53R5 (NIST, 2017; Pattinson et al., 2015; Security Centre for Internet, 2017)

Control/ Focus area	**HAIS-Q concepts with additional literature references for the controls**	**HAIS-Q**	**CIS CSC**	**Security & Privacy Controls (800-53R5)**
Password management	• Using the same password (Blythe et al., 2015; Curry et al., 2018; Shropshire, Warkentin & Sharma, 2015), • Sharing passwords (Bélanger et al., 2017; Blythe et al., 2015; Cheng et al., 2013; Herath & Rao, 2009a), • Using a strong password (Alohali et al., 2017)	√	√	√
Email use	• Clicking on links within emails sent by known senders (Blythe et al., 2015) • Clicking on links within emails sent by unknown senders (Alohali et al., 2017; Blythe et al., 2015) • Opening attachments in emails sent by unknown senders (Alohali et al., 2017; Blythe et al., 2015)	√	√	√
Internet use	• Downloading files (Bélanger et al., 2017; Blythe et al., 2015; Pattinson et al., 2015; Safa et al., 2015; Shropshire et al., 2015). • Accessing dubious websites (Bauer et al., 2017; Bélanger et al., 2017; Klein & Luciano, 2016; Pattinson et al., 2015) • Entering information online (Alohali et al., 2017; Öłütçü, Testik & Chouseinoglou, 2016)	√	√	√
Social media use	• Social media privacy settings (Bauer et al., 2017), • Considering consequences (Bauer et al., 2017) • Posting about work (Bauer et al., 2017)	√	√	√
Mobile devices	• Physically securing mobile devices (Bauer et al., 2017; Curry et al., 2018; Rhee et al., 2009) • Securing sensitive information via Wi-Fi (Bauer et al., 2017) • Shoulder surfing (Bauer et al., 2017)	√	√	√
Information handling	• Disposing of sensitive print-outs (Workman, Bommer & Straub, 2008), • Inserting removable media (Aurigemma & Mattson, 2017; Blythe et al., 2015), • Leaving sensitive material (Bauer et al., 2017)	√	√	√
Incident reporting	• Reporting suspicious behaviour (Pattinson et al., 2015), • Reporting all incidents (Pattinson et al., 2015), • Ignoring poor security behaviour by colleagues (Pattinson et al., 2015)	√	√	√
Privacy	• Non-disclosure of sensitive information (Blythe et al., 2015; Safa et al., 2015). • Processing client information in a lawful manner (Swartz, Da Veiga & Martins, 2019). • Process client information only for the purpose it was collected (NIST, 2017; Swartz et al., 2019). • Compliance with the organisation’s privacy policy (Dennedy, Fox & Finneran, 2014).			√

This section discussed the information security controls as defined in the framework CIS CSC and NIST 800-53R5, and these were mapped to the focus areas from the HAIS-Q. The resulting table is a list of controls that users should implement to exhibit information security compliant behaviour. These information security controls will be used as some of the building blocks for the conceptual Information Security Compliant Behaviour Model, which will serve as the basis for the development of the questionnaire. The theoretical model of this study is discussed in the next section.

3.6 Information Security Compliant Behaviour Model derived from the Self-determination theory (ISCBM^{SDT})

The preceding section considered some of the information security controls that employees should execute to protect the information in the organisation. These controls map to standards and will also have to be specified in the ISPs. In short, the employee is expected to comply with ISPs to protect the information and information resources in the organisation.

This section outlines the development of the conceptual model for this study. The model is built from the three concepts of the SDT, that is, the need for competence, the need for relatedness and the need for autonomy. When these needs are satisfied the employee should be intrinsically motivated to execute the information security controls. This study will assess a person’s perceived competence, perceived relatedness and perceived autonomy with respect to these information security controls.

A theoretical model in information security studies assists in the identification of factors that promote compliance with ISPs or the reasons employees engage in specific information security behaviours (Blythe et al., 2015). The conceptual Information Security Compliant Behaviour Model has been developed based on the following:

- The SDT’s concept of intrinsic motivation that was used in previous studies; for example, Classification of Security Compliant Behaviour by Padayachee (2012) that was not tested empirically, Wall et al. (2013) focused solely on autonomy, Kranz et al. (2014) used the meta-theory of the self-determination OIT in combination with GDT and Alzahrani et al.(2018) combined the SDT with the constructs perceived value congruence and perceived legitimacy.
- The SDT, which includes competence, relatedness and autonomy. This study will apply the three concepts of the SDT and will not combine them with other theories.

- Information security controls that must be implemented by end users as defined in the HAIS-Q and mapped to standards and other literature.

Figure 3-2 shows the Information Security Compliant Behaviour Model that is based on the self-determination theory (ISCBM^{SDT}). The security aspects (controls) that end users must implement are placed at the centre of the model. Perceived competence, relatedness, and autonomy could be important in understanding the intrinsic motivation of end users to implement the information security controls and are thus depicted on the sides with arrows pointing towards the security aspects. The model illustrates that intrinsic motivation of employees could, as suggested by the SDT theory, lead to information security compliant behaviour (ISCB). This is indicated by cumulative contribution of the three needs (i.e., perceived competence, perceived relatedness and perceived autonomy) and the security aspects (i.e., controls), which are indicated by arrows that are ultimately pointing towards and by extension influence the ISCB circle.

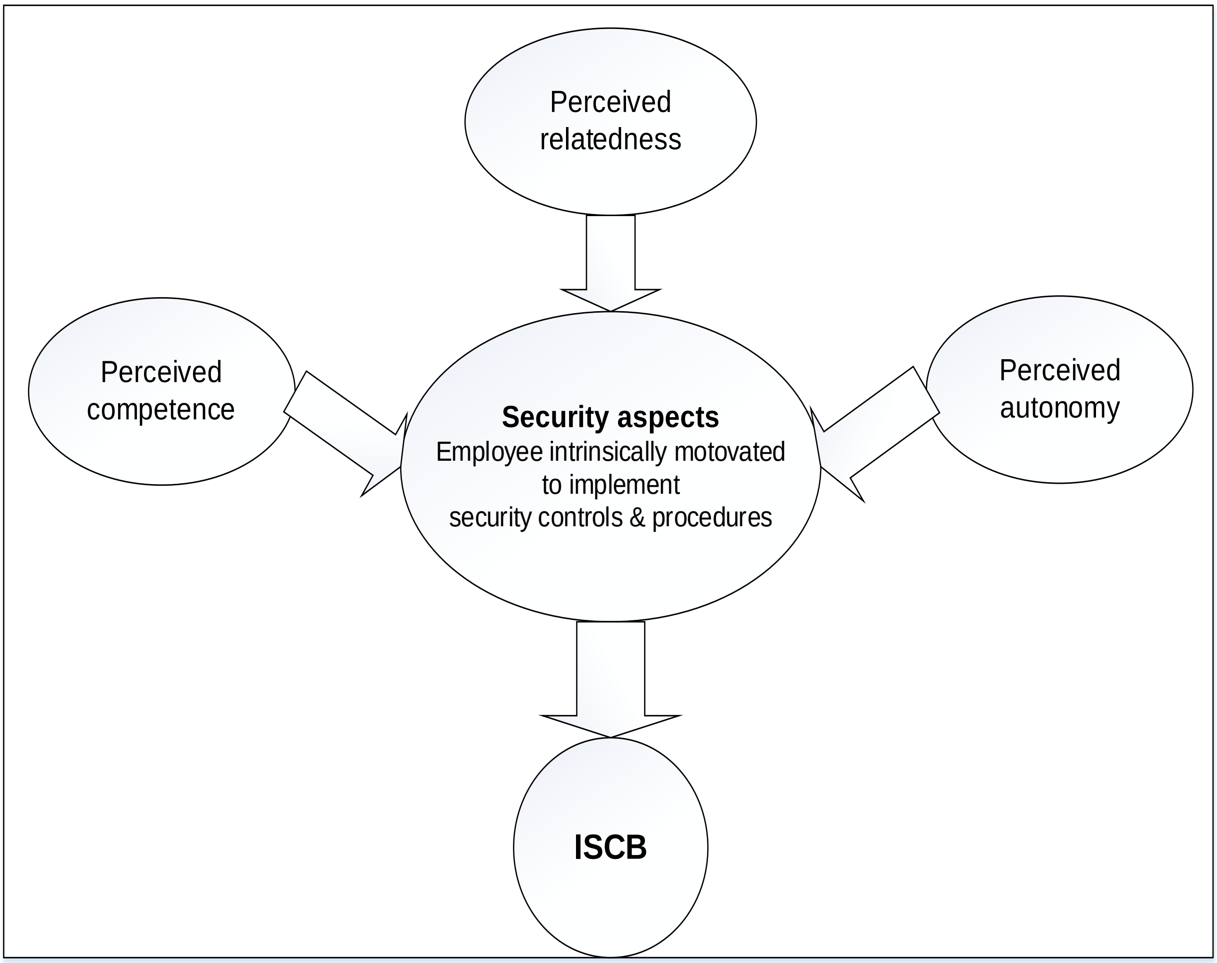


Figure 3-2: Information Security Compliant Behaviour Model derived from the Self-determination theory (ISCBM^{SDT})

The constructs that make up the ISCBM^{SDT} are discussed in the next section.

3.6.1 Perceived competence

The employee perceives that they have the relevant skills to carry out the information security actions, and they can adhere to the ISPs. The employees, also, perceive that they are capable of learning and mastering new skills of protecting information and information system assets. Therefore, the employees perceive that they can confidently comply with the ISPs and in cases where they encounter new or unfamiliar security aspects they are confident that they can learn and master them. Therefore, this study posits that when the need for competence is fulfilled the employees will comply with the ISPs.

3.6.2 Perceived relatedness

The employees feel they are part of the organisation and that they are valued. The employees believe that they can share their knowledge and in return be assisted by co-workers and superiors within the workplace. The employees believe that the support from colleagues motivates them to comply with the ISPs because they can also learn from fellow employees. The employees also perceive that they can successfully help other employees comply with ISPs. Therefore, this study posits that when the need for relatedness is fulfilled the employees will comply with ISPs.

3.6.3 Perceived autonomy

The employees believe it is their choice to follow the rules and the decision is based on their willingness to do so. The employees believe that they can comply with the ISPs because it is their choice to do so. They are motivated to do so, and for this study, it is assumed their perceived autonomy leads to intrinsic motivation. Therefore, this study postulates that when the need for autonomy is satisfied, the employees will comply with the ISPs.

3.6.4 Information security controls

From this study's perspective, information security controls refer to the security requirements that employees must adhere to, as stipulated in the ISPs. The security aspects discussed in this study were derived from literature, the HAIS-Q focus areas and the respective industry standards or frameworks.

The ISCBM^{SDT} proposes that the fulfilment of perceived competence, perceived relatedness, and perceived autonomy will lead to employees who are intrinsically motivated and result in:

- Increased internalisation of the ISPs,
- Compliance because their internal values align with the ISPs,
- Employee information security behaviour that is self-determined, as well as intentional compliance with ISPs and
- Employees who comply with the ISPs because of the innate satisfaction and enjoyment of doing so.

Therefore, when the need for competence, relatedness, and autonomy are fulfilled the employee conforms with the ISPs because the employee will be intrinsically motivated, thus contributing to information security compliant behaviour.

3.7 Summary of questionnaire themes

The questionnaire is based on the focus areas of the HAIS-Q (Butavicius et al., 2020; Parsons et al., 2017) and an additional focus area, privacy. The privacy dimension has been included since Parsons et al. (2017) suggest that there is a need to explore the relationship between privacy and information security awareness. Privacy was also included based on the mapping in Table 3-3; NIST includes privacy and it was, therefore, considered important to include it in the questionnaire. In this study, information privacy refers to how the organisation administers the collection, storage, processing and dissemination of personal information (Kokolakis, 2017).

The focus areas were adapted to the three concepts of the SDT, resulting in each section of the questionnaire focusing on each of competence relatedness and autonomy. By combining the HAIS-Q and the SDT, this study fills a research gap, which, as pointed out by Wall et al.(2013), suggests the existence of a possible need to develop an instrument to study information security that is based on the SDT. The questionnaire focus areas are discussed below.

3.7.1 Passwords management

Passwords enable users to access information systems. Only a person with a username and password for a given system will have access to that system. Passwords enable only authorised users to access a resource. Users are expected to keep their password(s) secure. The following sub-areas are considered under password management.

- Users must change the password and not use the default password (Blythe et al., 2015; Shropshire et al., 2015).
- The user must choose strong passwords (Bélanger et al., 2017; Blythe et al., 2015; Calic, Pattinson, Parsons, Butavicius & McCormac, 2016; Cheng et al., 2013; Herath & Rao, 2009a).
- Users must not share passwords with co-workers (Blythe et al., 2015; Cheng et al., 2013; Herath & Rao, 2009a).

3.7.2 Email use

Employees must understand their information security roles and responsibilities, even when they browse the internet and open their emails. Users should not open or download suspicious email attachments. The focus area includes the following sub-areas:

- Users must not download unsafe attachments (Bélanger et al., 2017; Blythe et al., 2015; Pattinson et al., 2015; Safa et al., 2015; Shropshire et al., 2015).
- Users must avoid clicking on links in emails whose sender they do not know (Alohali et al., 2017; Blythe et al., 2015).
- User must able to recognize when it is risky to open attachments in emails from unknown senders (Alohali et al., 2017; Bélanger et al., 2017; Blythe et al., 2015).

3.7.3 Internet use

Employees must understand their information security roles and responsibilities, even when they browse the internet. This focus area includes the following sub-areas:

- Users must be able to identify when it is risky to download files (Bélanger et al., 2017; Blythe et al., 2015; Pattinson et al., 2015; Safa et al., 2015; Shropshire et al., 2015).
- Users must avoid accessing dubious websites (Bauer et al., 2017; Bélanger et al., 2017; Klein & Luciano, 2016; Pattinson et al., 2015).

- Users should be able to determine the safety of the website before entering information online (Alohali et al., 2017; Ölütçü et al., 2016).

3.7.4 Social media use

This pertains to the responsible conduct of employees when on social media. The following sub-areas are considered:

- Employees should be able to review and adjust their social media privacy settings to protect their privacy (Bauer et al., 2017)
- Considering the consequences (Bauer et al., 2017). Employees have to understand the consequences of posting information online before doing so.
- Employees should act responsibly with regard to posting about work on social media (Bauer et al., 2017).

3.7.5 Mobile devices use

This involves the responsible use of mobile devices which store work information, when working in public areas. Employees should ensure the safety of these devices and the information stored on these devices as well as the safety of the information transmitted using these devices. Areas covered are:

- Employees must not leave their mobile devices unsecured or unattended when in public places (Bauer et al., 2017; Curry et al., 2018; Rhee et al., 2009).
- Employees must determine when it is safe to send confidential work information on public Wi-Fi (Bauer et al., 2017).
- Users should be able to shield their mobile devices from strangers when entering sensitive information on the device to guard against shoulder surfing (Bauer et al., 2017).

3.7.6 Information handling

This refers to how the employees handle confidential information on print or removable media; for example, printouts and USB drives. The following sub-areas are considered under this focus area:

- Users should be able to securely dispose of sensitive print-outs (Workman et al., 2008).
- Users should be able to avoid inserting removable media (Aurigemma & Mattson, 2017; Blythe et al., 2015).

- Users should be able to identify when it is risky to leave sensitive material when leaving their desk (Bauer et al., 2017).

3.7.7 Incident reporting

This focus area refers to how employees react when security incidents happen in the workplace. This includes the following themes:

- Users should report suspicious behaviour (Pattinson et al., 2015),
- Users should report all incidents (Pattinson et al., 2015),
- Users should not ignore poor security behaviour by colleagues (Pattinson et al., 2015).

3.7.8 Privacy

In this context, this applies to information that is restricted, for example, contract-sensitive information, proprietary information, classified information, privileged medical information and personally identifiable information. How personal data is gathered, stored, processed and disseminated are very important privacy issues (Kokolakis, 2017; S. Lee, Park & Suk, 2019). Users should be able to keep the confidentiality of such information, and this includes the following themes:

- Processing limitation - this involves processing client information within the boundaries of the law (Swartz et al., 2019).
- Purpose specification - process client information only for the purpose it was collected (NIST, 2017; Swartz et al., 2019).
- Policy specification - this involves adherence to the organisation's privacy policy (Dennedy et al., 2014).

Table 3-4 outlines the proposed statements that will form the basis for the construction of the questionnaire on information security compliant behaviour. The table also includes the questions from HAIS-Q all the questions under the headings knowledge, attitude and behaviour are the original HAIS-Q items and those for this study are under the headings competence, relatedness, and autonomy.

Table 3-4: Proposed questionnaire items adapted from (Pattinson et al., 2015; Parsons et al., 2017)

	Original HAIS-Q ITEMS			Proposed questionnaire item for this study		
Focus area	**Knowledge**	**Attitude**	**Behaviour**	**Competence**	**Relatedness**	**Autonomy**
Password management						
Using the same password (Blythe et al., 2015; Curry et al., 2018; Shropshire et al., 2015)	“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”.	I am capable of using different passwords for social media and work accounts.	I am influenced by my work colleagues to use different passwords for social media and work accounts because I get along with them.	I choose to use different passwords for social media and work accounts because the actions are congruent with who I am.
Sharing passwords (Bélanger et al., 2017; Blythe et al., 2015; Cheng et al., 2013; Herath & Rao, 2009a)	“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 passwords with colleagues”.	I feel able to meet the challenge of never sharing my work passwords with colleagues.	I am influenced by my work colleagues to never sharing my work passwords with colleagues.	I never share my work passwords with my colleagues because I have to follow instructions
Using a strong password (Alohali et al., 2017)	“A mixture of letters, numbers, and symbols is necessary for work passwords”.	“It’s safe to have a working password with just letters”.	“I use a combination of letters, numbers, and symbols in my work passwords”.	I am confident in my ability to mix letters number and symbols in work passwords.	I am encouraged by work colleagues to use a mixture of letters number and symbols in work passwords.	I choose to mix letters number and symbols in work passwords.
Email use						
Clicking on links in emails from known senders (Blythe et al., 2015)	“I am allowed to click on 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”.	I am confident in my ability to only click on links in emails from people I know.	I am influenced by work colleagues to only click on links in emails from people I know.	I choose to only click on links in email from people I know.
Users must avoid clicking on links in emails whose sender they do not know (Alohali et al., 2017; Blythe et al., 2015)	“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”.	I am confident in my ability to avoid clicking on links in emails from people I do not know.	I am influenced by work colleagues to avoid clicking on links in emails from people I do not know.	I do not feel pressured to avoid clicking on links in emails from people I do not know.
User must able to recognize when it is risky to open attachments in emails from unknown senders (Alohali et al., 2017; Bélanger et al., 2017; Blythe et al., 2015)	“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”.	I am confident in my ability to avoid opening attachments in emails from people I do not know.	I am influenced by work colleagues to avoid opening attachments in emails from people I do not know.	I do not feel pressured to avoid opening attachments in emails from people I do not know.
Internet use						
Downloading files (Bélanger et al., 2017; Blythe et al., 2015; Pattinson et al., 2015; Safa et al., 2015; Shropshire et al., 2015)	“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 ay file onto my work computer that will help me get the job done”.	I am able to identify when it is risky to download files onto my computer.	I am influenced by work colleagues to understand that it can be risky to download files on a work computer.	I choose not to download risky files onto my computer.
Accessing dubious websites(Bauer et al., 2017; Bélanger et al., 2017; Klein & Luciano, 2016; Pattinson et al., 2015)	“While I am at work, I shouldn’t access a certain website”.	“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”.	I am confident in my ability to avoid accessing dubious websites.	I am influenced by work colleagues to avoid accessing dubious websites.	I freely avoid accessing dubious websites.

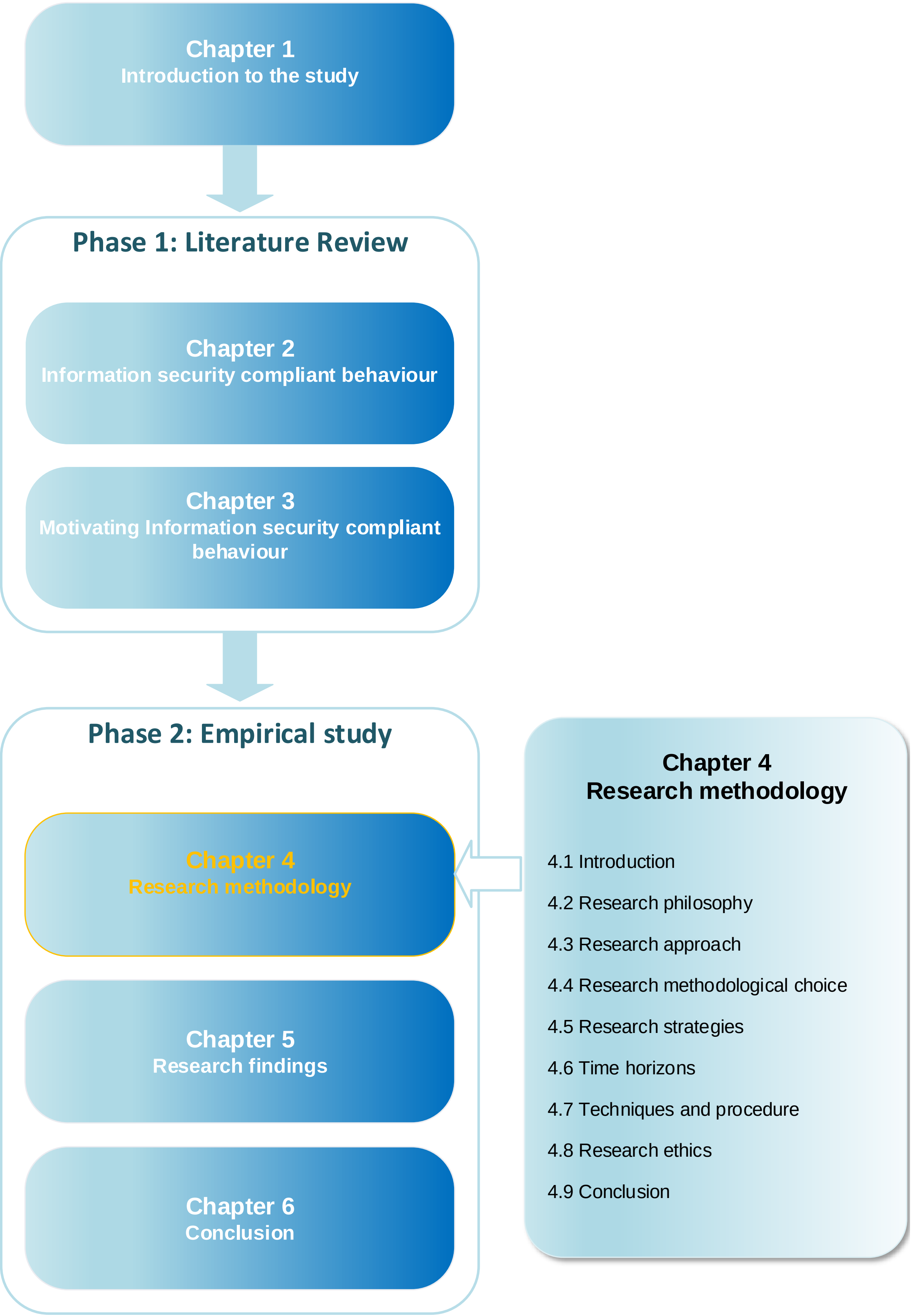
	Original HAIS-Q ITEMS			**Proposed questionnaire item for this study**		
Focus area	**Knowledge**	**Attitude**	**Behaviour**	**Competence**	**Relatedness**	**Autonomy**
Users should be able to determine the safety of the website before entering information online (Alohali et al., 2017; Öłütçü et al., 2016)	“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”.	I am confident of my ability to assess the safety of a website before entering information online.	I am influenced by my work colleagues to assess the safety of a website before entering information online.	It is my choice to assess the safety of a website before entering information
Social media use						
Social media privacy settings (Bauer et al., 2017)	“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”.	I am confident in my ability to review the privacy settings of my social media accounts.	I am influenced by my work colleagues to review the privacy settings of my social media accounts.	I choose to review the privacy settings of my social media accounts.
Considering consequences (Bauer et al., 2017)	“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”.	I am capable of considering the negative consequences before posting anything on social media.	I am influenced by my work colleagues to consider the negative consequences before posting anything on social media.	I consider the negative consequences before posting anything on social media because it is congruent with who I am.
Posting about work (Bauer et al., 2017)	“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”.	I am confident in my ability to avoid posting risky information about work on social media.	I am influenced by my work colleagues to avoid posting risky information about work on social media.	It is my choice to avoid posting risky information about work on social media.
Mobile devices						
Employees must not leave their mobile devices unsecured or unattended when in public places (Bauer et al., 2017; Curry et al., 2018; Rhee et al., 2009)	“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”.	I feel confident in my ability to keep my laptop with me all the time when working in a public place.	I am influenced by my work colleagues to keep my laptop with me all the time when working in a public place	I choose to keep my laptop with me all the time when working in a public place.
Securing sensitive information via Wi-Fi (Bauer et al., 2017)	“I am allowed to send sensitive work file 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 WIFI network”.	I am confident of how not to send sensitive work files over a public Wi-Fi network.	I am influenced by my work colleagues to avoid sending sensitive work files over a public Wi-Fi network.	It is my choice not to send sensitive work files using a public Wi-Fi network.
Users should be able to shield their mobile devices from strangers to avoid shoulder surfing (Bauer et al., 2017)	“When working on a sensitive document, I must ensure that strangers can’t see my laptop screen”.	“It’s a risk 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”.	I am capable of shielding, from strangers, my computer screen when working on a sensitive document.	I am influenced by my work colleagues to shield my computer screen from strangers when working on a sensitive document.	I choose to shield, from strangers, my computer screen when working on a sensitive document.
Information handling						
Users should be able to securely dispose of sensitive print-outs (Workman et al., 2008)	“Sensitive print-outs can be disposed of in the same 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”.	I am confident in my ability to dispose of sensitive printout by shredding or destroying them.	I am influenced by my work colleagues to dispose of sensitive printout by shredding or destroying them.	I choose to dispose of sensitive printout by shredding or destroying them.
Inserting removable media (Aurigemma & Mattson, 2017; Blythe et al., 2015)	“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	“I wouldn’t plug a USB stick found in public places into my work computer”.	I am confident in my ability to avoid inserting a USB stick I found in a public	I am influenced by my work colleagues to avoid inserting a USB stick I	I choose not to insert a USB stick I found in a public place into a work computer.

	Original HAIS-Q ITEMS			**Proposed questionnaire item for this study**		
Focus area	**Knowledge**	**Attitude**	**Behaviour**	**Competence**	**Relatedness**	**Autonomy**
		happen if I plug it into my work computer”.		place into my work computer.	found in a public place into a work computer.	
Users should be able to identify when it is risky to leave sensitive material when leaving their desk (Bauer et al., 2017)	“I am allowed to leave print-outs containing sensitive information on my desk”.	“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”.	I am confident in my ability to remove printouts with sensitive information on my desk when leaving.	I am influenced by my work colleagues to remove printouts with sensitive information on my desk when leaving.	I choose not to leave printouts with sensitive information on my desk overnight.
Incident reporting						
Reporting suspicious behaviour (Pattinson et al., 2015)	“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”.	I am confident in my ability to report any suspicious behaviour if noticed it.	I am influenced by my work colleagues to report any suspicious behaviour if noticed it.	I choose to report any suspicious behaviour if noticed it.
Ignoring poor security behaviour by colleagues (Pattinson et al., 2015)	“I must not ignore poor security behaviour from my colleagues”.	Nothing bad can happen if I ignore poor security behaviour by a colleague.	“If I noticed my colleagues ignoring security rules, I wouldn’t take any action”.	I am confident about my ability to notice poor security behaviour by colleagues.	I am influenced by my work colleagues to notice poor security behaviour by colleagues.	I choose to notice poor security behaviour by colleagues.
Reporting all incidents (Pattinson et al., 2015)	“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”.	I am confident in my ability to report any security incidents if noticed it.	I am influenced by my work colleagues to report any security incidents if noticed it.	I choose to report any security incidents if noticed it.
Privacy						
Processing limitation (Swartz et al., 2019)				I am confident in my ability to process client information legally.	I am influenced by my work colleagues to process client information legally.	I choose to process client information in a lawful manner.
Purpose specification (NIST, 2017; Swartz et al., 2019)				I am confident in my ability to only process client information for the intended purpose it was collected.	I am influenced by my work colleagues to only process client information for the intended purpose it was collected.	I choose to only process client information for the intended purpose it was collected.
Policy specification (Dennedy et al., 2014)				I am confident in my ability to adhere to the privacy policy of my organisation.	I am influenced by my work colleagues to adhere to the privacy policy of my organisation.	I choose to adhere to the privacy policy of my organisation.

3.8 Conclusion

This chapter discussed the intrinsic factors that impact the information security behaviour of employees and found that intrinsic motivational factors are as important as extrinsic motivational factors in information security. The chapter also, through a scoping review, explored existing literature to identify the theories used in the study of information security. As a result, the SDT was selected for developing the conceptual model for this study. It was demonstrated that intrinsic motivation is important. The relevant information security controls for this study were established by mapping the HAIS-Q to the CIS CSC and NIST 800-53R5 frameworks. Lastly, questionnaire focus areas were also established from the mapping of the HAIS-Q to the CIS CSC and NIST 800-53R5, and items for each focus area were phrased from a competence, relatedness and autonomy perspective.

CHAPTER 4


Chapter 1
Introduction to the study
Phase 1: Literature Review
Chapter 2
Information security compliant behaviour
Chapter 3
Motivating Information security compliant behaviour
Phase 2: Empirical study
Chapter 4
Research methodology
Chapter 5
Research findings
Chapter 6
Conclusion
Chapter 4
Research methodology
4.1 Introduction
4.2 Research philosophy
4.3 Research approach
4.4 Research methodological choice
4.5 Research strategies
4.6 Time horizons
4.7 Techniques and procedure
4.8 Research ethics
4.9 Conclusion

4 RESEARCH METHODOLOGY

4.1 Introduction

Previous chapters introduced the research study and the supporting literature review. This research is divided into two stages namely phase 1 (literature review) and phase 2 (an empirical study). Phase 1 presented the theoretical background of this research, which resulted in the research model and a questionnaire. The proposed research model, the ISCBM^{SDT}, was designed to provide a basis for the assessment of compliance with ISPs from a competence, relatedness and autonomy perspective. This chapter outlines the methodology for this study. The research onion, as defined by Saunders et al. (2016), was used as a logical framework for outlining the research methodology.

The chapter discusses the following: research philosophy, research approach, research methodological choice, time horizons, techniques and procedures, research ethics and conclusion.

4.1.1 Research onion

Saunders et al. (2016) outline the phases of the research process as layers, which consist of research philosophy, research approach, research strategy, choices, research time horizon, and data collection methods. The chapter discusses the selected philosophy, strategy and research method for this study. The research onion is shown in Figure 4-1, where each layer of the research onion describes in detail the respective stage of the research process. These are presented in the sections that follow.

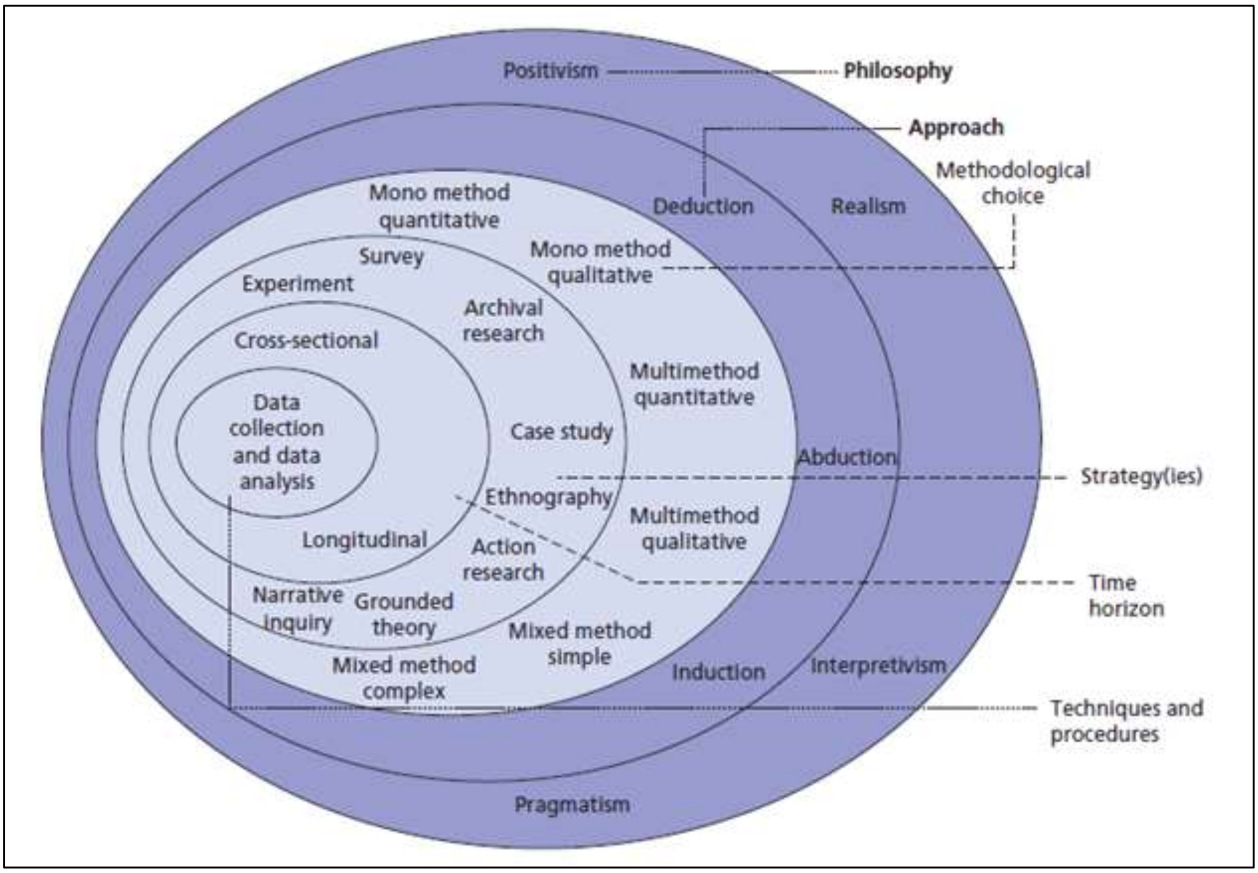


Figure 4-1: Research Onion (Saunders et al., 2016)

4.2 Research philosophy

Research philosophy refers to the way researchers view knowledge development. It defines the nature of knowledge. The research philosophy justifies and directs how a research project is carried out (Jonker & Pennink, 2010; Oates, 2006; Saunders et al., 2016). Four main research philosophies that are discussed in the works of many authors are known, namely: positivism, realism, interpretivism and pragmatism. Saunders et al. (2016) has identified three major philosophical assumptions and these apply to all the philosophical paradigms. Table 4-1 describes these philosophical assumptions and how they will be achieved in this study. The positivist philosophical paradigm was chosen for this study.

Table 4-1: Philosophical assumptions as applied in this study

Philosophical Assumption	Description	How it will be achieved in this study
Ontology	This is the researcher's understanding of reality. For example, positivists consider organisations to be independent of the individuals functioning under them.	This study will focus on the information security behaviour of individual members of staff, of the academic institution. Views expressed by respondents during the survey are their own and will not be interpreted as that of the institution.
Epistemology	This refers to the researcher's perspective of what knowledge is acceptable. The researcher must be independent of what is being researched.	The researcher will concentrate on what is observable and measurable, which is aimed at producing reliable data and results from the study. The researcher will not influence the views of the study participants.
Axiology	This refers to the role of the values held by the researcher when carrying out the research.	The researcher will carry out the study in a way that will ensure that the study is independent of the researcher's personal values in order to preserve objectivity. The questionnaire items will be based purely on the HAIS-Q and SDT and therefore the researcher's beliefs values should not affect the study.

4.2.1 Positivism

When studying problems using the positivist philosophy, the researcher identifies and evaluates factors that influence outcomes. In this philosophical paradigm, the researcher initially identifies a theory to work with, then gathers data to test the theory (Creswell, 2014). Positivism is the philosophical paradigm widely adopted by natural scientists (Oates, 2006). With regard to ontology, positivists consider social entities to be independent of the social actors within those entities. The epistemological position of a positivist is that only observable and measurable phenomena provide reliable data. Concerning axiology, positivists assume that for research to be objective, it must be undertaken in a way that ensures that the researcher’s personal values do not influence research outcomes (Saunders et al., 2016). Positivists predominantly adopt a quantitative approach and are more likely to use theories as the foundation of their research studies (Creswell, 2014; Saunders et al., 2016).

4.2.2 Realism

Realism assumes that reality is free from human thoughts, values or knowledge (Saunders et al., 2016). The ontological position of realism is that objects exist independent of the social actors. The epistemological position of realism is that observable and measurable phenomena provide reliable data. Contrary to the positivist view, in terms of axiology, realists are not objective they believe that the values and beliefs of the researcher influence the research. The research approach can be either quantitative or qualitative (Saunders et al., 2016).

4.2.3 Interpretivism

Interpretivists believe that people’s perceptions constitute reality. They recognise that people’s various backgrounds and experiences contribute to the creation of reality through social interaction (Wahyuni, 2012). Therefore, there can be many perspectives and interpretation of reality (Nicholas, 2010). From an ontology point of view, the interpretivists believe that reality results from how social actors interpret it. Therefore, there can be multiple realities that may change from time to time. Epistemologically, an interpretivist focuses on the personal meanings of the reality from the perspective of the various social actors. In terms of axiology, the researcher is subjective and is not independent of the research (Saunders et al., 2016). Interpretivists prefer to interact with the subjects of their study. They prefer qualitative data which provides them with rich explanations of the social concepts (Wahyuni, 2012) and prefer small samples (Saunders et al., 2016).

4.2.4 Pragmatism

In the pragmatism paradigm, the type of research problem determines the research approach and a mixed method research approach is preferred (Wahyuni, 2012). From an ontological perspective, pragmatism adopts the assumptions that are most suitable for a particular stage of the research process. Epistemologically, pragmatists maintain that either what is observed or the subjective meanings or both can result in credible research outcomes (Saunders et al., 2016). The axiological position is that the researcher adopts both subjective and objective points of views. It uses mixed or multiple research approaches as well as methods from both the quantitative and qualitative paradigms (Saunders et al., 2016; Wahyuni, 2012).

4.2.5 Chosen research paradigm

This study adopted the positivist research paradigm. The study adopted the self-determination theory to develop ISCBM^{SDT}, as stated in chapter 3. This study started with a theory which was used as the basis for the research.

4.3 Research approach

Since positivism has been adopted for this study, the deductive approach will also be applied in the study. Since this study used a survey questionnaire to collect data of a quantitative type. The inductive approach is more suitable to qualitative studies where the researcher interprets the views of the participants in a study to build general themes or theories from the ideas shared by the participants (Creswell, 2014). Instead, the deductive approach, which is discussed in more detail in the section that follows, was adopted for this research study.

4.3.1 Deductive approach

Using the deductive approach the researcher develops a hypothesis from a theory and develops a research approach to assess it (Creswell, 2014). The researcher reviews the relevant literature and uses this information as a basis for testing the hypotheses (Kothari, 2004). In the deductive approach, the researcher starts with a question and sets out to answer it (Creswell, 2014); for this reason, the deductive research is referred to as theory-testing research (Bhattacherjee, 2012). Figure 4-2 shows the deductive approach and it illustrates that the researcher starts with a theory, then formulates hypotheses or research questions and derives variables from the theory before assessing them using an appropriate research instrument.

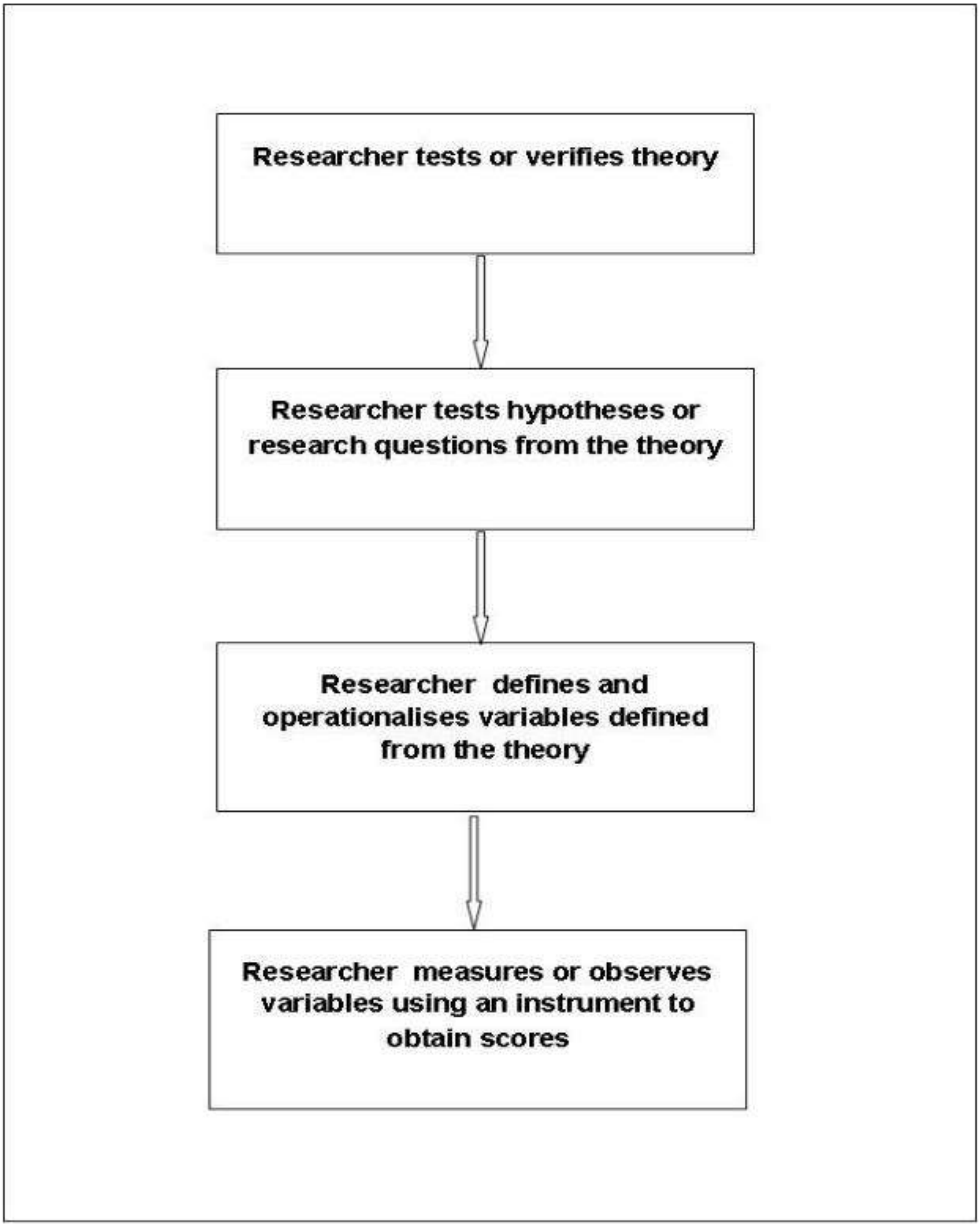

Researcher tests or verifies theory
Researcher tests hypotheses or research questions from the theory
Researcher defines and operationalises variables defined from the theory
Researcher measures or observes variables using an instrument to obtain scores

Figure 4-2: The deductive approach (Creswell, 2014)

The reason why the deductive approach was adopted for this research study was that this approach aligns well with the positivist philosophical paradigm chosen for this study. Also, this study builds on a theory (i.e. the SDT) and is also set to answer research questions; this means it aligns with the deductive approach as illustrated in Figure 4-2.

The rest of the chapter discusses the remaining layers of the research onion focusing predominantly on the choices that apply to the chosen positivist philosophy and the deductive approach.

4.4 Research methodological choice

The research onion includes these research approaches: mono-method, multi-method and mixed methods. In the case of mono-method, which is applied in this research study, a research study uses a single method for data collection and a corresponding data analysis technique, that is, either qualitative or quantitative (Saunders et al., 2016). For this study, the qualitative approach is not suitable because it involves the identification of themes and patterns in the collected data without using statistical procedures.

4.4.1 The quantitative approach

In the quantitative approach, the relationships between variables derived from the theory are examined. The measured variables produce data that can be analysed using statistical techniques (Creswell, 2014; Kothari, 2004), and the findings can be generalised across the respective population (Creswell, 2014). However, in contrast to the quantitative approach, the qualitative approach predominantly uses non-numeric data. This study uses the quantitative approach as it seeks to gather data and analyse it statistically.

4.5 Research strategies

The research strategy refers to how the researcher sets to execute the research study using any of the following approaches: action research, experimental research, case study, surveys, interviews, or systematic literature review (Oates, 2006; Saunders et al., 2016). This study will use the survey strategy as is discussed below.

4.5.1 Survey

The survey strategy enables the researcher to obtain data from a very large sample in a standardised, systematic and economic way (Oates, 2006). Using the survey strategy, when data is collected it is analysed by means of descriptive and inferential statistics (Saunders et al., 2016). For this study, the survey strategy was chosen because it is easy to collect large amounts of data from a large population at a single point in time (Creswell, 2014; Oates, 2006). Also, results from a survey sample can be generailised to the population (Creswell, 2014).

This study used the questionnaire as an instrument for data collection. The questionnaire is web-based and was administered over the internet. A questionnaire is made up of a list of questions (Kothari, 2004; Oates, 2006), and is suitable for collecting data from large samples (Saunders et al., 2016). A questionnaire can be made up of closed or open items or both, and these items/questions are formulated guided by the research questions or hypotheses of the study (Oates, 2006). The questionnaire was chosen for this study because it facilitates data collection in a standardised way, and the data can be processed using quantitative techniques. The questionnaire for this study consisted of closed questions.

To maximise the response rate, validity and reliability of the collected data, the questionnaire layout and purpose must be clear to the respondents (Saunders et al., 2016). The design and administration of the questionnaire for this study are discussed in section 4.7.3.

Advantages of using surveys are as follows:

1. It is inexpensive even when the population is large (Kothari, 2004; Oates, 2006).
2. There is no interviewer bias since the respondents fill out the survey in the absence of the researcher (Kothari, 2004).
3. Respondents have sufficient time to complete the questionnaire (Kothari, 2004).
4. Due to large samples that are normally used, the results are reliable (Kothari, 2004).

Disadvantages of using surveys are as follows:

1. It has a low rate of return of completed questionnaires (Kothari, 2004). In this study, this was addressed by sending reminders.
2. It can have ambiguous questions or omission of replies (Oates, 2006). In this study, this was addressed by carrying out a pilot study first then addressing any issues that arose from the pilot study.
3. Respondents who are willing to participate might not be the best representation of the population (Kothari, 2004). In this study, the questionnaire invitation and reminder emails were only sent to employees of the institution using a mailbox that

the institution set up for internal communication. Such an approach aided in ensuring that external parties or students did not receive the survey invitation.

4. People could be biased where they answer strongly agree for all questionnaire items so that they are not implicated or look bad. The researcher aimed to address this by reviewing the data to remove questions where respondents only selected one option for all the questions and by communicating to respondents that the survey is anonymous.

4.6 Time horizons

Time horizon refers to the period during which the study takes place, that is, the time between the start and completion of the research. The research onion presents two time horizons, the longitudinal and cross-sectional time horizons (Saunders et al., 2016). This study adopted a cross-sectional time horizon to study information security behaviour at a particular point in time. This time horizon (cross-sectional) was chosen because of the time constraints of this study.

4.6.1 Cross-sectional studies

Cross-sectional studies gather data from a population at a single point in time. This differs from longitudinal studies, which gather data over a period of time (Creswell, 2014).

4.7 Techniques and procedures

This section presents: sampling, data gathering and data analysis methods that are going to be used in the study.

4.7.1 Sampling technique

Sampling refers to the selection of study participants from the population. It is meant to guarantee that every member of the population is afforded an equal opportunity of being chosen (Bhattacherjee, 2012; Krauss & Putra, 2005; Signh, 2006). Sampling is useful when it is not practical and economical to gather data from the whole population (Saunders et al., 2016). The two general sampling categories are: probability (random) and non-probability sampling (Kothari, 2004; Saunders et al., 2016). Random sampling is used to ensure that each prospective respondent has an equal opportunity of being included in the sample (Bhattacherjee, 2012; Creswell, 2014). In qualitative research, purposeful sampling (a form of non-probability sampling) is used so that respondents' experience determines whether they are selected or not (Creswell, 2014).

4.7.1.1 Sampling method

This study employed the non-probability sampling using the following methods for each phase of the research:

- The institution: this was selected using the convenience method by selecting one of the universities in South Africa.
- The expert panel: the convenience sampling method was used to select the panel as follows: all of them had done work in information security research and some of them had developed the HAIS-Q, which was adapted to the SDT in this study.
- The pilot group: the convenience sampling was used to select the pilot sample in one of the academic departments of the institution because of their availability to participate in the study.
- The survey: the convenience sampling method was used for the survey. The survey was sent to all of the administrative, academic and operational staff members, and voluntary responses were received from those who chose to participate at their convenience.

4.7.2 Sample

The process of collecting quantitative data starts with the identification of the people and places to be studied (Creswell, 2012). This section discusses the sample, population and location of the study.

4.7.2.1 Unit of analysis

This refers to those participants who will provide the information that will be used to answer the research questions or hypotheses (Creswell, 2012). For this study, the unit of analysis is the individual employee since the study seeks to assess information security compliant behaviour of the employees from the perspective of competence, relatedness and autonomy.

4.7.2.2 Target population

This is the population from which the sample will be drawn (Saunders et al., 2016) and will ideally have shared features that the researcher wants to study (Creswell, 2012). Saunders et al. (2016) state that a sampling frame implies the population about which the study results can be generalised (Saunders et al., 2016). The study participants comprised the academic, administrative and operational staff from an academic institution in South Africa. Table 4-2 summarises the sampling requirements for the study.

Table 4-2: Sampling requirements for the study

	Minimum number required	**Years of experience (minimum)**	**Expertise and criteria**	**Level of education (minimum)**	**Country**
Institution	1	-	-	-	South Africa
Expert Panel	5	3	Information security research experience	Bachelors	Any Country
Pilot	10	3	Information security research experience	Bachelors	South Africa
Survey	125	1	Ability to use a computer. An employee of the university	N/A	South Africa

4.7.2.3 Sample size

A sample is a smaller group drawn from the target population that the researcher selects for the study. The researcher must determine the size of the sample from the population (Creswell, 2012). To enable statistical testing of both reliability and validity, the minimum number of responses has to be 5 times the total number of questions in the data collection instrument (O'Rourke & Hatcher, 2013). For this study statistical testing for validity and reliability was carried out for each dimension since it was the same questions that were repeated for each component of competence, relatedness and autonomy. Each dimension consisted of 25 questions. As a result, the study attempted to yield approximately 125 responses based on the statistical recommendation for testing reliability and validity.

4.7.3 Data collection technique

4.7.3.1 The questionnaire

Developing a questionnaire involves a thorough search of the published literature and the questionnaire items must address research questions and/or hypotheses that are to be tested by the information obtained from the study (Grimmer & Bialocerkowski, 2005; Lietz, 2008). Redundant or irrelevant questions should be avoided (Grimmer & Bialocerkowski, 2005). Items in a questionnaire must reliably address the important concepts of the research questions of the study (Rattray & Jones, 2007).

A questionnaire must meet reliability and validity requirements (Rattray & Jones, 2007). To be valid, a questionnaire must measure what it is meant to measure and a reliable questionnaire must produce consistent results from repeated studies over time (Boynton & Greenhalgh, 2004). Therefore a questionnaire should provide valid and reliable data, which the researcher can use to answer the research question(s) of the study (Grimmer & Bialocerkowski, 2005).

The questionnaire items for this study were derived from the focus areas of the human aspect of information security questionnaire (HAIS-Q) and were then adapted to the self-determination theory. An additional focus area on privacy was included in the questionnaire. The questionnaire was made up of two sections, namely section 1 (biographical information) and section 2, which comprised the information security questions. The questions were organised according to focus areas, and each question was framed from the perspective of each of competence, relatedness and autonomy. This resulted in the 75 questions for the questionnaire.

Google Forms was used to prepare the questionnaire. The development of the questionnaire for this research study included:

- Conducting a literature review and developing the initial questions for the questionnaire,
- Convening an expert panel of reviewers to review the initial questionnaire,
- Pilot testing the revised instrument after including the comments from the expert panel of reviewers,
- Amending the questionnaire by including comments from the pilot test and conducting the final survey,

- Sending the survey sample data file to the statistician for importing into the statistical software (SPSS) to make sure all data values captured in the file were valid, and
- The final instrument was administered.

4.7.3.1.1 Questionnaire design

Below is a discussion of the guidelines used in designing the questionnaire.

Question type

Questionnaire items must be simple, specific and must reflect the aims of the study (Lietz, 2010). Questions must be worded clearly since clarity increases the likelihood of accurate responses (Grimmer & Bialocerkowski, 2005). A questionnaire can be made up of the following: open, closed, single, multiple response questions (Rattray & Jones, 2007). The questionnaire for this study included only closed questions with multiple responses, thus enabling the respondents to choose from a possible number of responses.

Double-barrelled questions

These refer to a single question asking for two different concepts, and this reflects poor question design (Lietz, 2010). Such questions are best handled by splitting them into two questions (Grimmer & Bialocerkowski, 2005). Questions that addressed more than one concept were split into two different questions for each concept or the concept that did not address the objectives of the study was not included in the questionnaire.

Open-ended questions

Open questions do not have response categories for respondents and would elicit a whole range of replies (Grimmer & Bialocerkowski, 2005). The questions allow the respondent to express their views in their own words but are harder to code and analyse (Oates, 2006). These types of questions were not included in the questionnaire.

Closed (multiple-choice) questions

These questions provide response categories where the respondents can select an answer (Oates, 2006). Such questions provide all possible answers and if a question may not apply to some respondents “Not Applicable” is included as one of the answers

(Kothari, 2004). The questionnaire for this study uses the 5-point Likert scale comprising of the following responses: strongly disagree, disagree, neutral, agree and strongly agree.

4.7.3.1.2 Administering the questionnaire

Survey participants were notified by an email invitation which was sent by the Information and Communication (ICT) Department. The reminders were also sent on email.

4.7.3.2 Expert review panel

Expert review is a method for evaluating questionnaires before they can be administered. A panel consisting of experts in the respective research area evaluate the data collection instrument. This expert review panel should result in an improved questionnaire (Oates, 2006; Saunders et al., 2016). The criteria for selecting the expert panel were as follows:

- Experience in information security research,
- At least 3 years' work experience and
- Experience in working in the higher education sector.

A panel of 6 experts reviewed the questionnaire. Four came from the field of psychology and had done research on the human aspects of information security for 11 years. The other reviewers were an Information Technology (IT) security consultant specialising in incident response and a professor in Information Systems (IS) security. The experts were drawn from two countries, that is, 2 from South Africa and 4 from Australia.

Their work experience ranged from 10 to 20 years. In terms of qualifications, 2 panel reviewers have a Master of Psychology degree in Organisational and Human Factors, 1 is currently completing the Master of Psychology degree, the other has a PhD degree in Psychology and the remaining 2 have each a PhD degree in Computer Science. All reviewers possessed experience in research, information security or information security policy compliance as well as designing questionnaires.

The expert panel questionnaire (shown in Appendix C) consisted of section 1 – Expert panel information sheet – which required them to fill the following: experience (in years), highest qualification, current job title and experience working with information security.

The expert panel questionnaire was also accompanied by the participant consent form (Appendix D), a form asking for the participant's permission to participate in the review. Each reviewer had to sign the form to show his or her consent to participate as a panel review expert.

The questionnaire that was sent to the reviewers had a section requiring the reviewers to evaluate whether a question is essential and clear. In summary, the feedback from the members of the expert review panel was as follows:

- Item is essential: All questions were found to be essential by all experts.
- Item is unclear: Table 4-3 shows the questions that were found to be unclear by 5 of the 6 experts and the sixth reviewer indicated that all questions were clear.

Questions that were found to be unclear are shown in Table 4-3. However, no item was removed because it was indicated as unclear. Each of these questions was revised as per the comment raised by the experts to make the question(s) clearer.

Table 4-3: Questions found to be unclear by the panel of experts

Question No.	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5	Expert 6
2	√	√	√	√	√	-
3	-	√	√	√	√	-
4	-	√	√	√	√	-
5	-	√	√	√	√	-
6	-	√	√	√	√	-
8	√	√	√	√	√	-
12	√	-	-	-	-	-
14	-	√	√	√	√	-
16	-	√	√	√	√	-
17	√	√	√	√	√	-
18	-	√	√	√	√	-
32	√	-	-	-	-	-
49	√	√	√	√	√	-
50	-	√	√	√	√	-
51	-	√	√	√	√	-
52	-	√	√	√	√	-
53	√	√	√	√	√	-
54	√	√	√	√	√	-
56	√	-	-	-	-	-
57	-	√	√	√	√	-
58	-	√	√	√	√	-

Question No.	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5	Expert 6
59	√	√	√	√	√	-
60	-	√	√	√	√	-
62	-	√	√	√	√	-
67	-	√	√	√	√	-
68	-	√	√	√	√	-
69	-	√	√	√	√	-
Total	**10**	**24**	**24**	**24**	**24**	**0**

- In the biographical section for gender, the questionnaire included male and female options only. The reviewers suggested that either adding the option for gender neutral or including a 'prefer not to respond' or 'other' option for gender. As a result, the 'prefer not to respond' option was adopted for the questionnaire.
- In the biographical section, the reviewers described the term "length of service" as prone to misinterpretation. They said it was not clear whether it referred to service at a single organisation or the length of service at the latest occupation. Thus, the questionnaire was revised to 'Length of service at current employer'.
- Two questions (i.e. questions 53 & 54) were found to be a double negative and were corrected in the updated questionnaire.
- Some questions were found to use ambiguous words and the reviewers suggested deleting the ambiguous words or to use different words that made the meaning of statements clearer. Changes were, therefore, made to the suggested items (i.e., questions 2,8,12 and 49).
- Suggestions were made about some of the questions addressing two different aspects. Where there was a problem with these becoming double-barrelled, such questions were updated to address only one aspect, which aligned with the objectives of this study. These questions are questions 4, 5 and 64.
- Some questions (i.e., questions 17 & 18) were found to be reverse scored. It was suggested that such items had the potential of confusing the respondents. These items were reworded positively.

4.7.3.3 Pilot testing

Pilot testing is employed to identify potential problems in the research instrument and thus ensure the reliability and validity of the constructs. The pilot testing group is usually a small group selected from the target population (Bhattacherjee, 2012). The pilot testing process helps to determine and improve content validity of the items, question format and scales on the questionnaire (Creswell, 2014). According to Oates (2006), pilot testing seeks to identify the following about the questionnaire:

- Areas where respondents have difficulties in answering the questions.
- Questions that are ambiguous or vague.
- Instructions that are not clear.
- Whether predefined responses cover all possibilities.
- The time it takes to answer the questions.

The pilot test questionnaire is shown in Appendix E. The pilot testing of the questionnaire was conducted among 12 members of staff of an information systems department of the selected university. Each of the staff members received a participant information sheet (Appendix F) and had to sign a consent form (Appendix D). The following criteria were used to select the pilot testing group:

- Information security research experience,
- Higher education experience and
- Availability.

A summary of the feedback received from the questionnaire pilot test is as follows:

- Some questions were not phrased in a way that the participants would interpret correctly and it was recommended that they be specific. For example, where the question referred to the organisation it was recommended that it be changed to the university since the survey was conducted in a university.
- A recommendation was made to add the job level to the biographical section of the questionnaire – which was done.
- Question 12 was found to be negatively phrased; the recommendation was that all questions must be positively phrased.
- The questions were reworded as follows to make the statements clearer:
    - Questions starting with “I am capable” were reworded to “I have the necessary skills”;
    - Questions starting with “I am influenced by my work colleagues”, were reworded to “My colleagues support me”

Once the pilot test was concluded, the questionnaire was revised and updated. The updated questionnaire was then used to collect data from the target population for this study.

4.7.3.4 Administering the questionnaire to the target population

The revised and updated questionnaire was administered as follows:

- An email containing information about this research study and links for completing the questionnaires were drafted and sent to the target sample (Appendix G).
- Since the targeted number of responses was 125, the 263 responses that were received were deemed enough for a meaningful statistical validation of the questionnaire to be conducted. The final questionnaire is shown in Appendix H and the anonymous front page (see Appendix I) was also included as part of the questionnaire.

4.7.4 Data analysis

Quantitative data analysis uses and produces numerical data. Quantitative data can be either categorical or quantifiable (Saunders et al., 2016). The quantitative data analysis, which was carried out using the SPSS software, included the following:

- Validating questionnaire with factor and item analysis,
- Reliability analysis of the questionnaire,
- Calculation of the means for competence, relatedness and autonomy.
- Conducting a correlation analysis,
- Conducting ANOVA tests between the biographical groups for comparative purposes, and
- T-test for gender groups.

4.7.4.1 Descriptive statistics

Descriptive statistics enable the data to be numerically described and to compare variables (Saunders et al., 2016), and this can be done by statistically describing, aggregating, and presenting the associations between constructs (Bhattacherjee, 2012). Frequency distribution is one way of representing data, and it is a complete list of all possible values or scores for a particular variable and the frequency of each value in the data set (Marczyk et al., 2005). Thus, data can be presented as a frequency table and histogram. In this study, descriptive statistics will present a summary of the data.

Descriptive statistics can also be used to describe the relationships between variables: correlation - whether the relationship is positive or negative and whether the relationship is strong or weak (Marczyk et al., 2005; Saunders et al., 2016). This study also seeks to determine if there is a correlation amongst competence, relatedness and autonomy.

4.7.4.2 Inferential statistics

Inferential statistics enable the examination of causal relationships. It also allows for the generalisation of research results, that is, allowing the researcher to make inferences about the population that was sampled (Marczyk et al., 2005). Hypotheses can be tested with inferential statistics as well (Nicholas, 2010). In this study, no generalisations were made about the population since the sample was not selected using a probability sampling method.

4.7.5 Data and design quality

4.7.5.1 Validity

Validity is a determination of whether a research instrument assesses what it was designed to assess and must, therefore, lead to results that are accurate and meaningful (Marczyk et al., 2005).

Content validity is the extent to which the questionnaire items address the objectives of the study (Saunders et al., 2016). The items in the questionnaire, for this study, were supposed to cover the research questions from the perspective of the self-determination theory. Content validity was achieved by having a panel of expert reviewers assess the questionnaire by going through each question and indicating whether it was essential or not and whether it was clear or not.

Face validity is an assessment of a questionnaire to determine whether it logically reflects what it is supposed to assess (Saunders et al., 2016). Face validity was determined through an expert panel of reviewers and a pilot test group who reviewed the questionnaire. The expert panel reviewed the questionnaire items to determine whether they were clear and relevant. The pilot group also completed and reviewed the questionnaire before the final questionnaire was administered. The expert panel and the pilot test provided valuable feedback and this ensured face validity.

Internal validity is the capacity of the research instrument to assess what it is supposed to assess (Kothari, 2004).

External validity, is concerned with the generalisation of the research study results, that is, the application of the results of the study to other environments. This implies that it should be possible to predict results for other similar situations (Bhattacherjee, 2012; Marczyk et al., 2005; Oates, 2006).

Construct validity: It refers to the extent to which a questionnaire measures the constructs it was designed to assess (Creswell & Creswell, 2018). Factor analysis is the procedure that uses statistical analysis to assess the validity of a questionnaire (Creswell, 2014). The result of the analysis assists the researcher to improve the questionnaire for future use and provide statistically valid results. Statistical analysis of the validity of the questionnaire in this study was determined using the exploratory factor analysis (EFA) (Henson & Roberts, 2006). EFA was performed to determine if the individual items load onto the constructs of the questionnaire, that is, items are strongly related to the factors. EFA is also used to determine what the factors are and the number of factors (Child, 2006; Osborne & Costello, 2009).

In this study, the validity of the questionnaire was established by face validity, content validity and by performing exploratory factor analysis. Therefore, the primary use of factor analysis in the development of the questionnaire in this study was done to ensure that the designed questions were related to the constructs or factors that this study intended to assess.

4.7.5.2 Reliability

Reliability refers to the internal consistency of the research instrument such as a questionnaire (Marczyk et al., 2005). Item analysis is performed on the item(s) of a construct to determine the Cronbach alpha coefficient values, which indicate whether the reliability is good, acceptable or unacceptable (Roberts & Priest, 2006).

Cronbach alpha: Creswell (2014) states that reliability checks for the internal consistency of the scales, that is, the correlation of a group of items is conducted using the Cronbach alpha. A reliable Cronbach alpha value confirms that the items that make up a construct measure the same concept in the same way. The criteria for reliability coefficient vary for the different tests or instruments and are considered as follows: greater than 0.8 - good; between 0.6 and 0.8 - acceptable, and less than 0.6 - unacceptable (Roberts & Priest, 2006). However, Nunnally (1978) suggests an acceptable lowest value of the Cronbach alpha coefficient to be 0.7. For this study, the reliability of the questionnaire will be conducted statistically by computing the Cronbach Alpha coefficients.

4.8 Research ethics

During data collection, researchers must respect the rights of the participants and the research sites (Creswell, 2014). In research, ethics refer to the appropriateness of the behaviour of the researcher in relation to the rights of research participants, or those that are affected by the study (Saunders et al., 2016). The researcher will have to uphold the rights of the participants (Oates, 2006), and should not manipulate the research process (Bhattacherjee, 2012). This research study will be guided by the Unisa policy on research ethics (Unisa, 2016). It will also abide by any relevant laws, codes of conduct of professional bodies, institutional guidelines and scientific standards applicable to the specific field of this research study (Unisa, 2016). As such, the following were observed:

4.8.1 Voluntary participation and harmlessness

Participants were made aware that they were voluntarily participating in the survey, and they could at any time pull out of the study without being penalised. Participants were also made aware they were not going to be harmed by participation in the project (Bhattacherjee, 2012; Oates, 2006).

4.8.2 Informed consent

The participants were made aware of the purpose and research objectives of the study, which were in writing. An informed consent letter accompanied the questionnaire for the expert review panel and pilot group, and informed consent was also included as a tick box on the electronic survey questionnaire (Creswell, 2014; Oates, 2006). The informed consent form is included in Appendix D.

4.8.3 Anonymity and confidentiality

The researcher will protect the identity of the study participants including after the study has been completed. Anyone reading the final study report will not be able to link a response to a respondent. No personal identifiable information were collected in the survey and details of study participants will not be included in the final report – they will be kept confidential (Bhattacherjee, 2012; Oates, 2006).

4.8.4 Justice, fairness and objectivity

The selection of participants was considered to be fair and scientific (Unisa, 2016). The study used the convenience sampling method, where the questionnaire invitation was sent to all staff members ensuring that they all had an equal opportunity of participating.

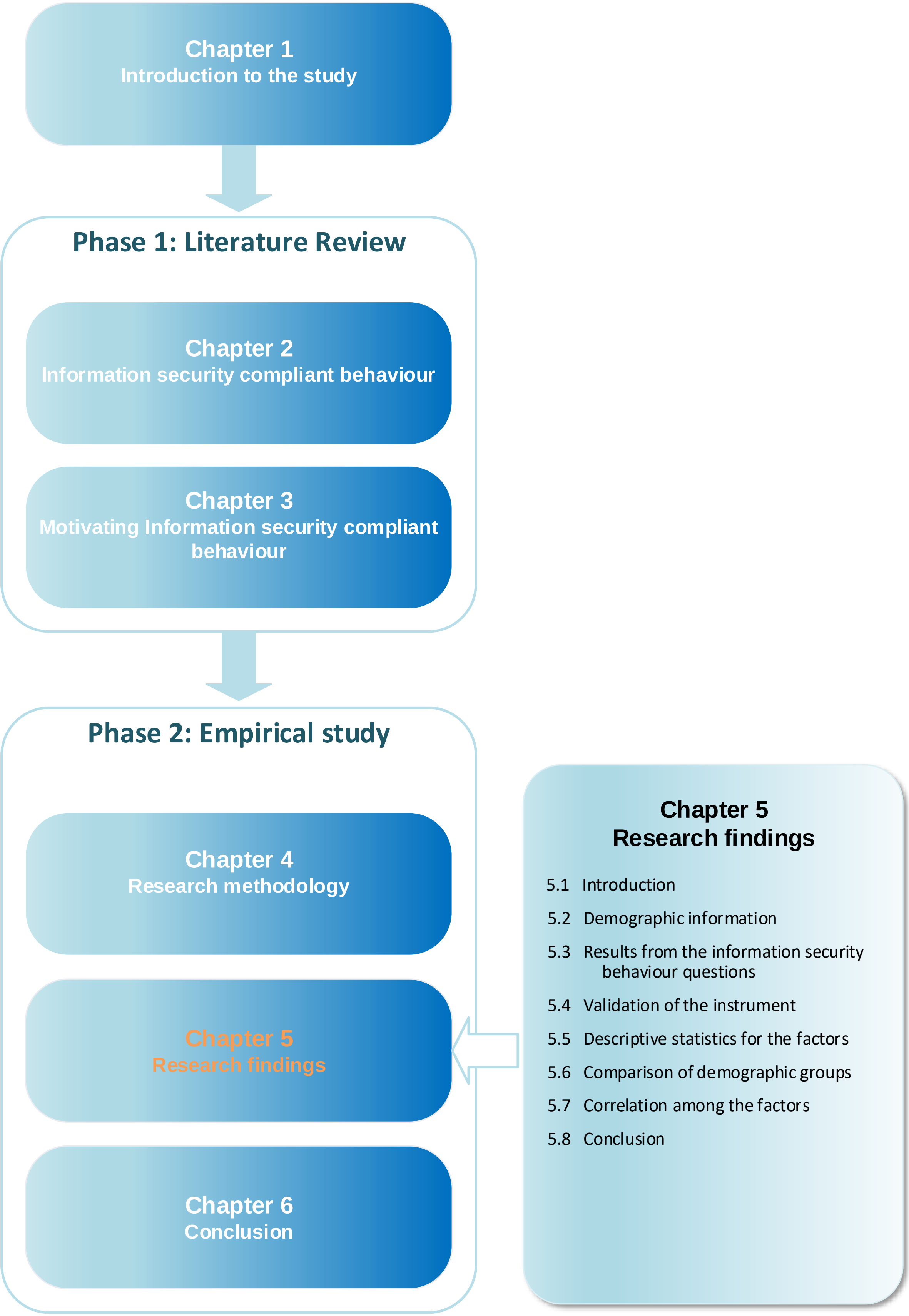
4.8.5 Approval to conduct the study

The academic institution at which the study was conducted gave the approval to conduct the research study. Ethical clearance was also given by the School of Computing (SoC), which falls under the College of Science Engineering and Technology (CSET). Further permission was given by the Research Permission Sub-committee (RPSC) of the Senate Research, Innovation, Postgraduate Degree and Commercialisation Committee (SRIPCC) to conduct the research on the institution's employees. The ethical clearance certificates are included in Appendices A and B.

4.9 Conclusion

The research methodology for this study was presented in this chapter. The research methodology was described using the layers of the research onion, and the chapter explored the stages that apply to this study. The chapter revealed that the study is grounded on a positivist philosophical paradigm and a predominantly inductive approach. For data collection, it employed a mono-method quantitative approach, the survey strategy and a questionnaire. The chapter discussed the development of the questionnaire, the statistical methods used and the ethical issues considered to protect study participants. The next chapter presents the findings and results of the online survey.

CHAPTER 5



Chapter 1
Introduction to the study

Phase 1: Literature Review

Chapter 2
Information security compliant behaviour

Chapter 3
Motivating Information security compliant behaviour

Phase 2: Empirical study

Chapter 4
Research methodology

Chapter 5
Research findings

Chapter 6
Conclusion

Chapter 5
Research findings

5.1 Introduction

5.2 Demographic information

5.3 Results from the information security behaviour questions

5.4 Validation of the instrument

5.5 Descriptive statistics for the factors

5.6 Comparison of demographic groups

5.7 Correlation among the factors

5.8 Conclusion

5 RESEARCH FINDINGS

5.1 Introduction

This study developed a model and questionnaire for information security compliant behaviour in chapter 3, and chapter 4 presented the research methodology that was followed in this study. Chapter 5 will address research question 2 as set out in section 1.4; as well as the empirical study objectives 5, 6, 7 and 8, which are outlined in section 1.5.

The results of the survey that are discussed in this chapter are as follows:

- Demographic information of the survey sample,
- Responses to the information security questions,
- Validation of the research instrument (exploratory factor analysis),
- Reliability analysis of the factors (Cronbach alpha),
- Descriptive statistics per factor,
- ANOVA results,
- T-tests results and
- Pearson correlation results between the factors.

5.2 Demographic information

This section presents the demographical information of the sample. The study involved two hundred and sixty-three (263) employees of a South African university. According to its records, the university had 44.08% and 55.92% employees being male and female, respectively (December 2018). The study was targeted at all employees of the institution, and employees were informed about the survey using email. The first five questions of the questionnaire consisted of biographical questions, that is, gender, age, the highest level of education, length of service at the current employer and job level.

5.2.1 Gender distribution

Figure 5-1 shows a bar graph for the gender information of the survey respondents. Based on the disclosure of the respondents, the sample consisted of 54.8% females, and 44.1% males; 1.1% of the respondents did not disclose their gender. The results show that most participants were female, this could be because the university has more female employees, according to university records.

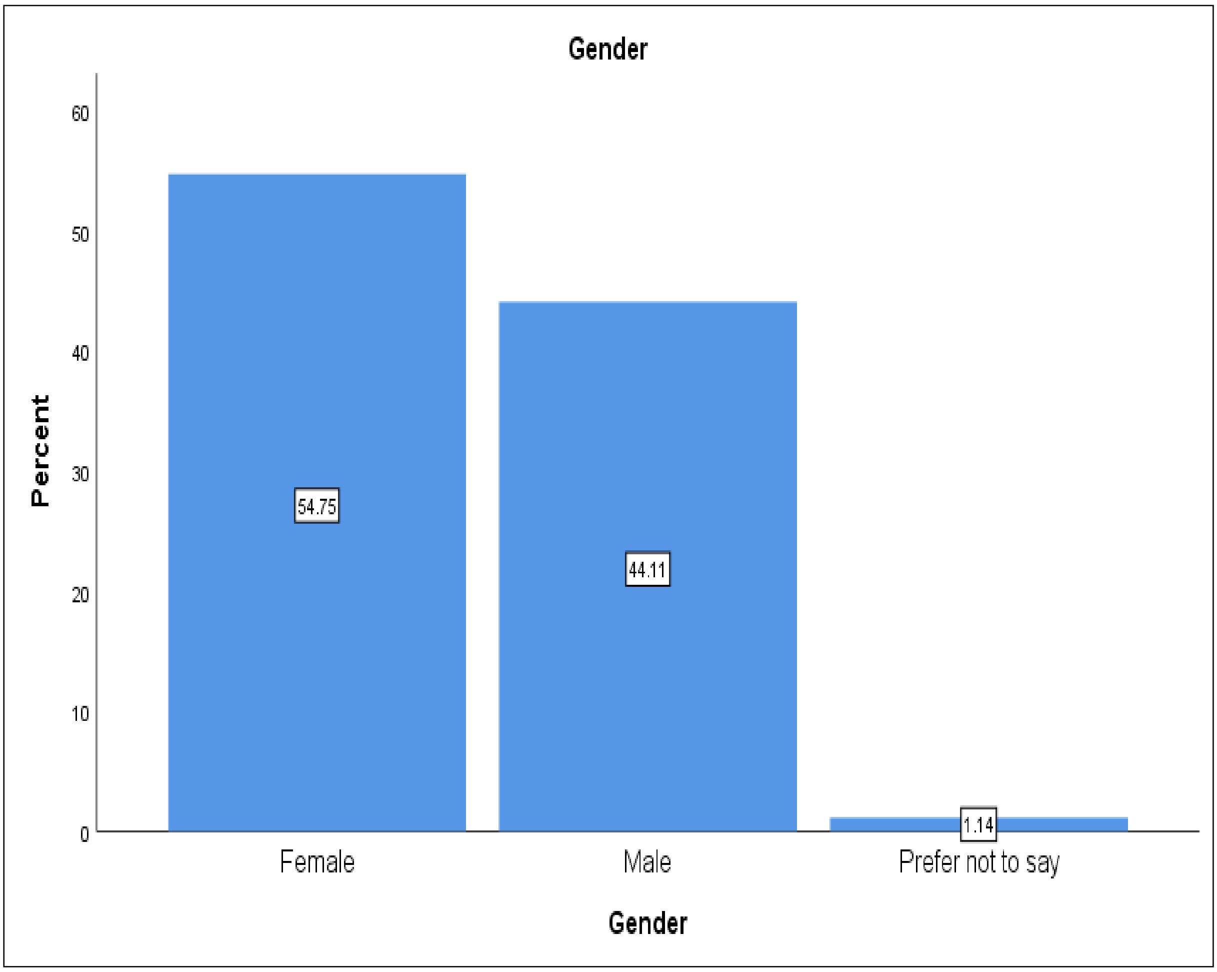


Figure 5-1: Gender information

5.2.2 Age information

The age distribution bar graph depicted in Figure 5-2 shows that respondents born before 1996 make the bulk of the participants (99.24%). However, the biggest group of respondents (38.40%) consists of the 1977 – 1995 age group consists. Respondents born after 1995 consisted of the least number of respondents (0.76%).

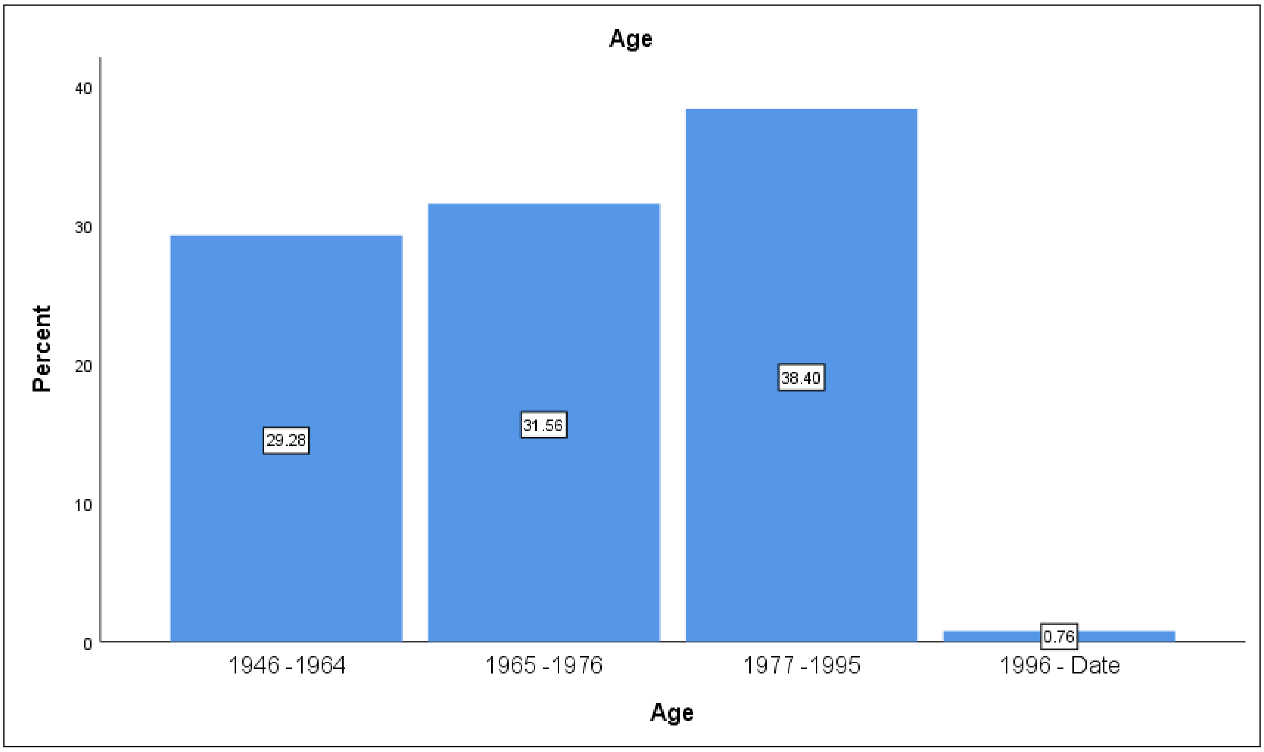


Figure 5-2: Age information of the respondents

5.2.3 Education level information

Figure 5-3, which depicts the categories of qualifications held by the respondent, shows that 69.08% of the respondents have a postgraduate qualification. This is to be expected in an environment such as a university.

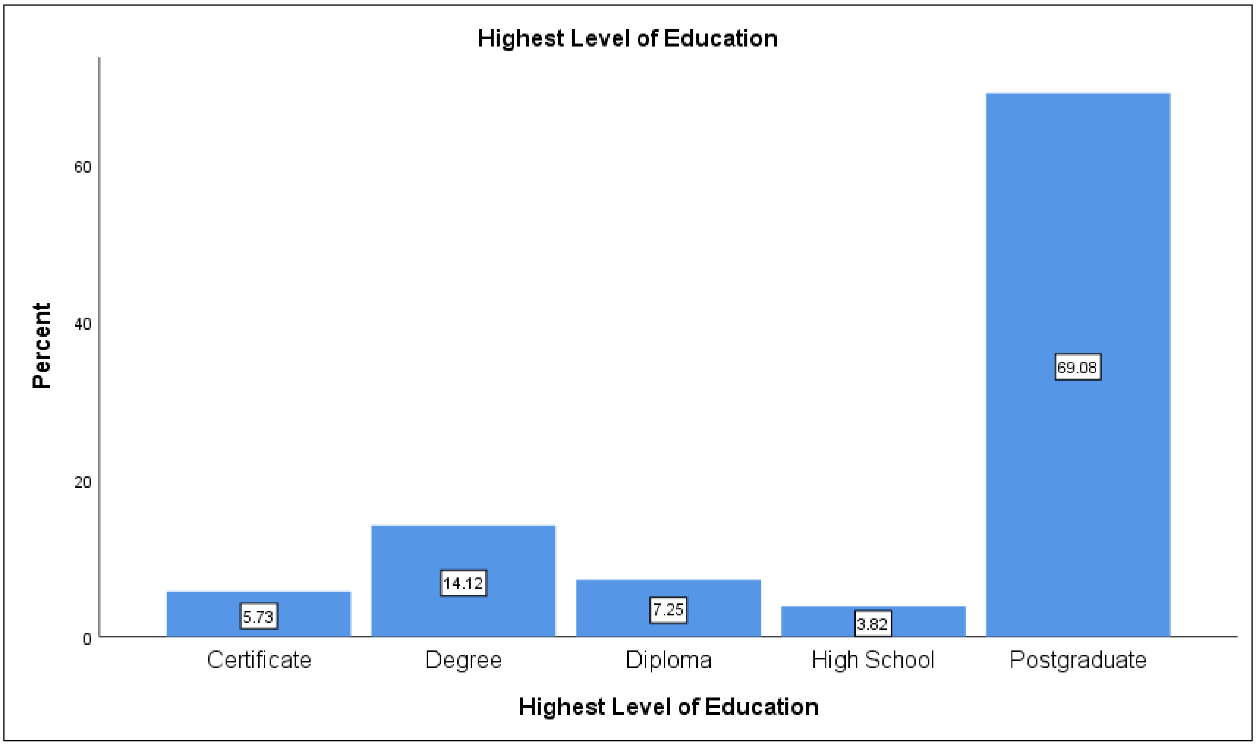


Figure 5-3: Educational qualifications information

5.2.4 Length of service at current employer information

According to Figure 5-4, most of the respondents have been working for 1 to 10 years. The category of workers who had worked for less than a year was the least.

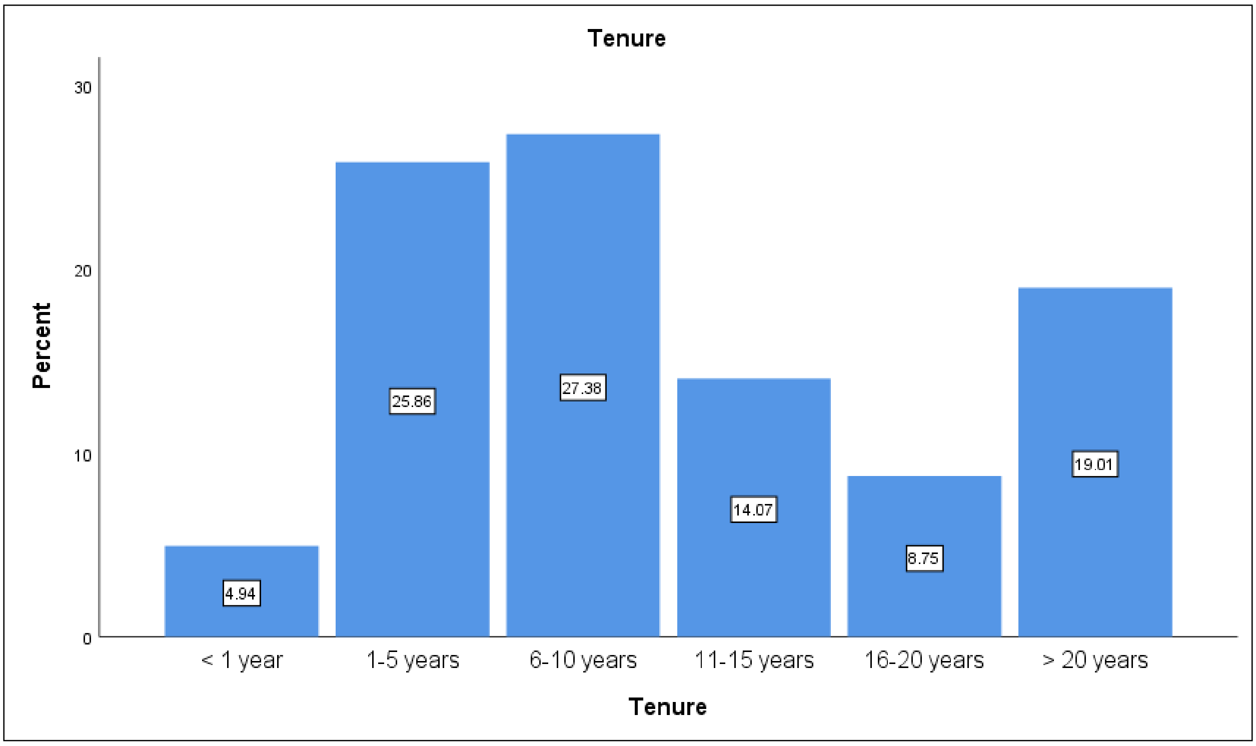


Figure 5-4: Length of service at current employer

5.2.5 Job level information

Figure 5-5 shows a bar graph for the job level for the survey respondents. The graph shows that most of the respondents for the survey were administrative staff, representing 51.53% of the research sample.

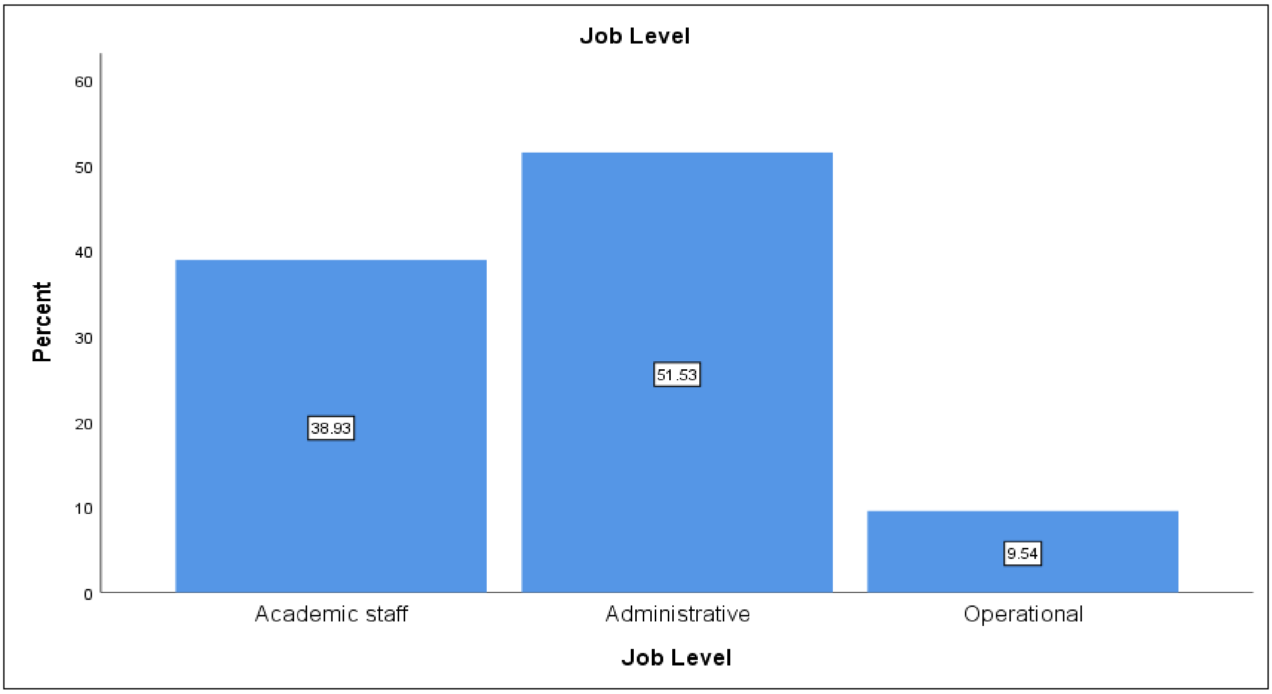


Figure 5-5: Job level information

5.2.6 Summary of the demographical profile sample

The survey sample shows that the majority of respondents were as follows: female respondents (54.75%); older than 25 years (99.24%), with the majority belonging to the 1977 – 1995 age group (38.40%); had worked for more than 1 year (95.06%), with most respondents having worked for the institution for 6 to 10 years (27.38%); administrative staff (51.53%); have at least a high school certificate, with the majority possessing a postgraduate qualification (69.08%).

The next section discusses the results of the responses from the information security behaviour questions.

5.3 Results from the information security behaviour questions

This section presents results of the information security behaviour questions, which were posed in section 2 of the questionnaire. This part of the questionnaire was comprised of

75 questions, which used the Likert scale to measure statements of agreement (strongly disagree, disagree, neutral, agree, strongly agree). The scales were encoded with values which ranged from 1 to 5, with the strongly disagree to have a value of 1 and the strongly agree to have a value of 5. The questions were subdivided into three categories namely, competence, relatedness and autonomy, and with each having 25 questions. The uppermost questions by mean value described in Tables 5-1, 5-2 & 5-3 were selected for discussion because they were the 10 questions with the highest mean values. The lowermost statements by mean value (see Table 5-1, 5-2 & 5-3) were selected because they were the 10 questions with the lowest mean values.

For purposes of interpreting the means, a cut-off mean value of 4.0 was set for the questions (Da Veiga & Martins, 2015). A mean value of 4.0 and above indicates a positive perception, and a mean value that is below 4.0 indicates a neutral or potentially negative perception. All the questions with a mean value that is below 4.0 represent areas for improvement, which can be set as focus areas for which action plans can be identified.

The next three subsections discuss the questions that yielded the highest mean values and those with the lowest mean values, starting with competence, followed by relatedness and lastly, autonomy.

5.3.1 Results of competence questions

Table 5-1 lists the ten uppermost statements and the ten lowermost statements for the competence questions. The uppermost statements had mean values ranging from 4.36 to 4.77, and the lowermost questions ranged from 3.86 to 4.19. Table 5-1 shows that all ten of the uppermost questions had mean values greater than 4.0. This suggests that participants responded positively to these questions and they perceived themselves to be competent in the areas of password security, protecting the privacy of students' information, protecting their mobile devices, securely using social media and handling sensitive information. For the lowermost 10 questions, 5 had mean values greater than 4.0, and the other 5 questions had mean values less than 4.0, thus indicating that these areas require further improvement.

Table 5-1: Uppermost and lowermost competence statements by mean value

Uppermost competence statements	
Statement	**Mean**
C1 I have the necessary skills to use different passwords for social media and work accounts.	4.52
C3 I have the necessary skills to use a combination of letters, numbers, and symbols in work passwords	4.77
C24 I have the necessary skills to adhere to the privacy policy of the university	4.60
C13 I have the necessary skills to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place	4.59
C12 I have the necessary skills to avoid posting sensitive information about work on social media	4.56
C2 I have the necessary skills to never share my work passwords with colleagues	4.55
C25 I have the necessary skills to adhere to the information security policy of the university	4.49
C11 I have the necessary skills to consider the negative consequences before posting anything on social media	4.46
C23 I have the necessary skills to process student information only for the purpose for which it was collected	4.44
C18 I have the necessary skills to identify when it is risky to leave the information on my desk	4.36
Lowermost statements	
Statement	**Mean**
C6 I have the necessary skills to identify when it is risky to open attachments in emails from people I do not know	4.19
C15 I have the necessary skills to shield my computer screen from strangers when working on a sensitive document	4.17
C8 I have the necessary skills to avoid accessing websites that could be dubious (malicious).	4.12
C7 I have the necessary skills to identify when it is risky to download files onto my work computer	4.12
C16 I have the necessary skills to securely dispose of sensitive information	4.04
C21 I have the necessary skills to report any information security incidents if I notice them	3.97
C17 I have the necessary skills to identify when it is risky to insert an external device (e.g. a USB stick or phone) into a computer	3.95
C20 I have the necessary skills to notice poor information security behaviour by colleagues	3.93
C10 I have the necessary skills to review the privacy settings of my social media accounts	3.91
C9 I have the necessary skills to assess the safety of a website before entering information online	3.86

5.3.2 Results of relatedness questions

The uppermost ten statements and the lowermost ten statements are shown in Table 5-2 for the relatedness questions. The uppermost statements had mean values ranging from 3.05 to 3.51 and the lowermost statement ranged from 2.68 to 3.01. Uppermost questions and lowermost questions had mean values below 4.0. This suggests that participants had neutral and potentially negative views towards the relatedness questions, indicating that these areas require further improvement.

Table 5-2: Uppermost and lowermost relatedness statements by mean value

Uppermost relatedness statements	
Statement	**Mean**
R23 My colleagues support me to process student information only for the purpose for which it was collected	3.52
R2 My colleagues support me never to share my work passwords with colleagues	3.51
R24 My colleagues support me to adhere to the privacy policy of the university	3.49
R25 My colleagues support me to adhere to the information security policy of the university	3.46
R22 My colleagues support me to process student information in a lawful manner	3.35
R5 My colleagues support me to avoid clicking on links in emails from people I do not know	3.15
R7 My colleagues support me to identify when it is risky to download files onto my work computer.	3.10
R13 My colleagues support me to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place	3.08
R12 My colleagues support me to avoid posting sensitive information about work on social media	3.06
R19 My colleagues support me to report any suspicious behaviour if I notice it	3.05
Lowermost relatedness statements	
Statement	**Mean**
R18 My colleagues support me to remove information on my desk, which could be risky	3.01
R21 My colleagues support me to report any information security incidents if I notice them	2.98
R9 My colleagues support me to assess the safety of a website before entering information online	2.98
R14 My colleagues support me to avoid sending sensitive work files over a public Wi-Fi network	2.97
R20 My colleagues support me to notice poor information security behaviour by colleagues	2.91
R17 My colleagues support me to identify when it is risky to insert an external device (e.g. a USB stick or phone) into a work computer	2.88
R16 My colleagues support me to securely dispose of sensitive information	2.87
R15 My colleagues support me to shield my computer screen from strangers when working on a sensitive document	2.82
R10 My colleagues support me to review the privacy settings of my social media accounts	2.69
R1 My colleagues support me to use different passwords for social media and work accounts.	2.68

5.3.3 Results of autonomy questions

Table 5-3 presents the ten uppermost statements and the ten lowermost statements for the autonomy questions of the survey. The uppermost statements had mean values ranging from 4.41 to 4.68 and the lowermost statements ranged from 3.91 to 4.27. All the mean values of the uppermost questions are above 4.0, suggesting that respondents perceived these questions positively. These results suggest that the respondents perceived their information security behaviour to be out of their own choice in the areas of password security, protecting the privacy of students' information, protecting their mobile devices, securely using social media, compliance with the ISP and handling of sensitive information. Eight of the lowermost 10 questions had mean values that are greater than 4.0, and 2 questions had mean values that are lower than 4.0. The two questions with a mean value that is less than 4.0 fall in the dimensions of social media use and incident reporting; these are areas which require further improvement.

Table 5-3: Uppermost and lowermost autonomy statements by mean value

Uppermost autonomy statements	
Statement	**Mean**
A3 I choose to use a combination of letters, numbers, and symbols in work passwords	4.68
A12 I choose to avoid posting sensitive information about work on social media	4.67
A24 I choose to adhere to the privacy policy of the university	4.65
A13 I choose to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place	4.61
A25 I choose to adhere to the information security policy of the university	4.60
A2 I choose never to share my work passwords with my colleagues	4.54
A11 I choose to consider the negative consequences before posting anything on social media	4.53
A23 I choose to process student information only for the purpose for which it was collected	4.48
A18 I choose not to leave the information on my desk, which could be risky	4.48
A22 I choose to process student information in a lawful manner	4.41
Lowermost autonomy statements	
Statement	**Mean**
A8 I choose to avoid accessing websites that could be dubious (malicious).	4.27
A17 I choose not to insert external devices (e.g. a USB stick or phone) into a work computer if it could pose a risk	4.21
A16 I choose to securely dispose of sensitive information	4.18
A19 I choose to report any suspicious behaviour	4.18
A4 I choose to click only on links in emails from people I know	4.18
A1 I choose to use different passwords for social media and work accounts	4.17
A9 I choose to assess the safety of a website before entering information online	4.08
A21 I choose to report any information security incidents if I notice them	4.00
A10 I choose to review the privacy settings of my social media accounts	3.91
A20 I choose to notice poor information security behaviour by colleagues	3.73

5.4 Validation of the instrument

This section presents the steps followed in determining the validity and the reliability of the questionnaire. Validity is discussed in section 5.4.1 and reliability is discussed in section 5.4.2

5.4.1 Validity

Determining the validity of the survey questions and the underlying factors of the questionnaire was done using the Exploratory factor analysis (EFA). O'Rourke & Hatcher (2013) suggests that the minimum number of respondents must be five times the number of items in the research instrument for the sample to be statistically viable for use in questionnaire validation. The questionnaire consisted of 75 questions, excluding the biographical questions. The questions where subdivided into three categories of competence, relatedness and autonomy. Each category had 25 questions adapted for the respective categories, and responses were considered for each category. As a result, the required minimum number of responses was 125. The EFA was carried out per category thus new factors were determined for each category. The 263 responses received from the online survey were considered adequate for the statistical validation of the research instrument. A professional statistician facilitated the statistical processing of the collected survey data using SPSS Version 25. The confidentiality agreement with the statistician is shown in Appendix J. A discussion of the EFA results follows.

EFA was employed for the questionnaire validation and to summarise the collected data so that the underlying relationships between the variables could be revealed (Yong & Pearce, 2013). EFA is also used to determine the construct validity of data collection instruments which are self-reporting (Williams, Onsman & Brown, 2010).

The Kaiser-Meyer-Olkin (KMO) and the Bartlett sphericity tests were done to determine if the collected data met the conditions for performing the EFA. The tests were conducted per category, that is, competence, relatedness and autonomy. To produce distinct factors that are reliable, Field (2009) recommends a KMO value that is close to 1. The probability should be less or equal to 0.05 for the Bartlett sphericity test – a result suggesting a high correlation among variables (Williams et al., 2010).

Table 5-4 shows that a KMO value of 0.915 was obtained for the competence questions; this suggests excellent sampling adequacy to proceed with the EFA. The results of the Bartlett sphericity test for the competence questions are also shown in Table 5-4 and is statistically significant (p = 0.000).

Table 5-4: KMO and Bartlett's test for the competence category

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.915
Bartlett's Test of Sphericity	Approx. Chi-Square	3451.121
	df	300
	Sig.	0.000

A KMO value of 0.965 was obtained for the relatedness questions (see Table 5-5), this suggests excellent sampling adequacy to proceed with the EFA. The results of the Bartlett sphericity test for the relatedness questions shows a value that is statistically significant (p = 0.000).

Table 5-5: KMO and Bartlett's test for relatedness category

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.965
Bartlett's Test of Sphericity	Approx. Chi-Square	6125.315
	df	300
	Sig.	0.000

The KMO value of 0.885, which was obtained for the autonomy questions (see Table 5-6), suggests a good sampling adequacy to proceed with the EFA. The results of the Bartlett sphericity test for the autonomy questions indicates statistically significant (p = 0.000) results.

Table 5-6: KMO and Bartlett's test for autonomy category

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.885
Bartlett's Test of Sphericity	Approx. Chi-Square	2719.525
	df	300
	Sig.	0.000

As shown in Tables 5-4, 5-5, and 5-6, results of the KMO and Bartlett's tests for the three categories are adequate to proceed with the exploratory factor analysis.

5.4.1.1 Determining the number of factors

The Eigenvalues, scree plots and cumulative percentages were used to identify the number of underlying factors (Gerber & Hall, 2017). The Eigenvalues and the scree plots were generated for each of the categories of competence, relatedness and autonomy.

The factors were determined as follows:

- Statements must have loading values greater than 0.4,
- The cumulative percentage must be above 60%,
- Eigenvalues must be greater than 1,
- A minimum of 3 statements per factor was required,
- Where the cumulative percentage is less than 60, the combination of statements for a factor that makes theoretical sense were considered and
- Cross-loading items with cross-loading differences less than 0.2 were dropped.

The resulting factors are as follows:

- **Competence:** The solution with 4 factors was chosen and had a cumulative percentage exceeding 60%. However, the factors were reduced to 3 because the last dimension had 1 statement. The third factor initially had 4 statements, which were reduced to 3 after item C25 was removed on the basis that it was cross loading on another factor and the cross-loading difference was less than 0.2. This combination was adopted because it had a higher cumulative percentage and made theoretical sense. Table 5-7 shows the selected competence category factors that had Eigenvalues greater than 1 and cumulative Eigenvalue of 62.38%.

Table 5-7: Eigenvalues for the competence factors

Total Variance Explained						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	11.002	44.010	44.010	11.002	44.010	44.010
2	2.121	8.484	52.494	2.121	8.484	52.494
3	1.294	5.177	57.671	1.294	5.177	57.671
4	1.178	4.710	62.381	1.178	4.710	62.381

- **Relatedness:** The 2-factors combination was adopted for this research study because it had a cumulative percentage that is higher than 60% and made theoretical sense. Table 5-8 shows the selected factors for the relatedness category that had Eigenvalues that exceed 1 and cumulative Eigenvalue of 70.735%.

Table 5-8: Eigenvalues for factors the relatedness factors

Total Variance Explained						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	16.034	64.134	64.134	16.034	64.134	64.134
2	1.650	6.601	70.735	1.650	6.601	70.735

- **Autonomy:** The 6-factors combination was selected on the basis that it had a cumulative percentage of over 60% and it made theoretical sense. Table 5-9 shows the selected factors for the autonomy category that had Eigenvalues that are greater than 1 and a cumulative Eigenvalue of 63.681%.

Table 5-9: Eigenvalues for factors the autonomy factors

Total Variance Explained						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	8.646	34.585	34.585	8.646	34.585	34.585
2	2.101	8.405	42.991	2.101	8.405	42.991
3	1.548	6.192	49.183	1.548	6.192	49.183
4	1.360	5.442	54.625	1.360	5.442	54.625
5	1.182	4.726	59.351	1.182	4.726	59.351
6	1.083	4.330	63.681	1.083	4.330	63.681

Scree plots

The scree plot is a graph showing each factor against its associated Eigenvalues on the y-axis and is used for determining the factors that should be to retained. The factors to be retained are indicated by the data points that are above the turning point at which the graph levels out (Gerber & Hall, 2017; Yong & Pearce, 2013). The scree plots for each of the categories are shown in Figures 5-6 to 5-8.

Figure 5-6 shows scree plot for the competence questions. Four factors were retained for this category.

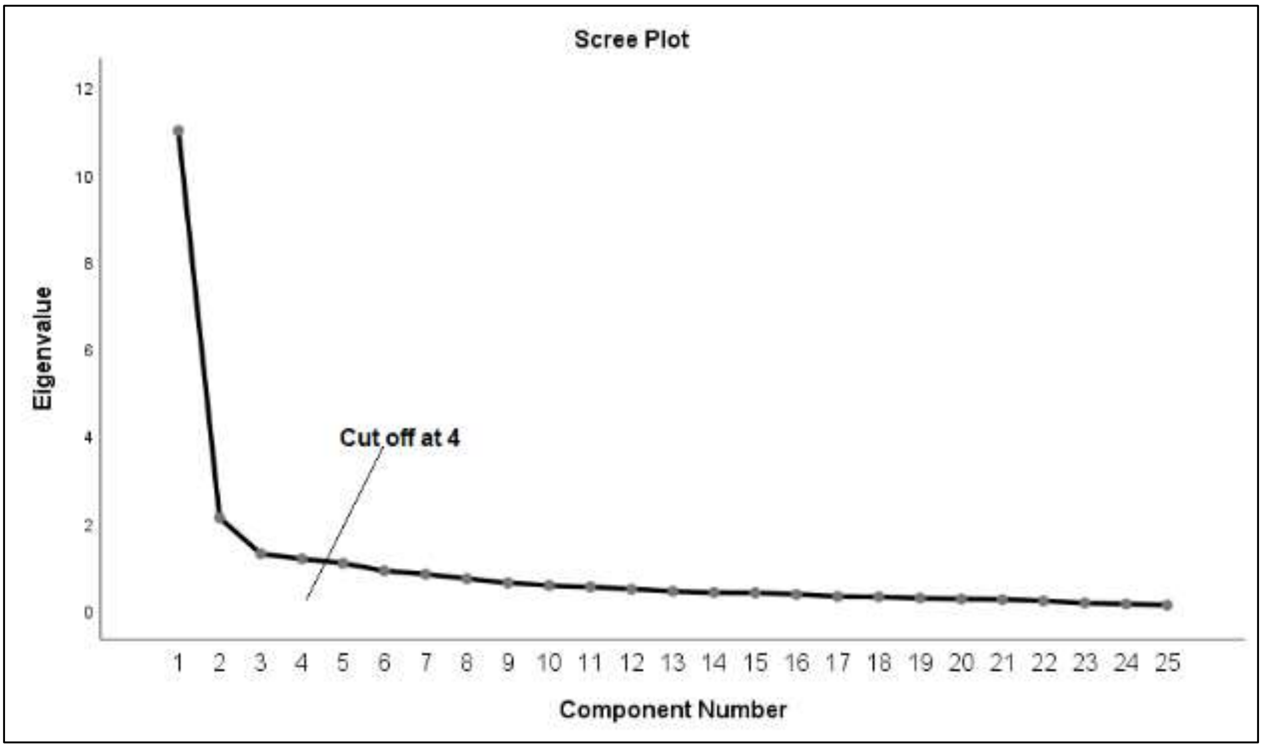


Figure 5-6: Competence Scree plot, compiled from survey data

Figure 5-7 shows the scree plot for the relatedness questions. Two factors were retained for this category.

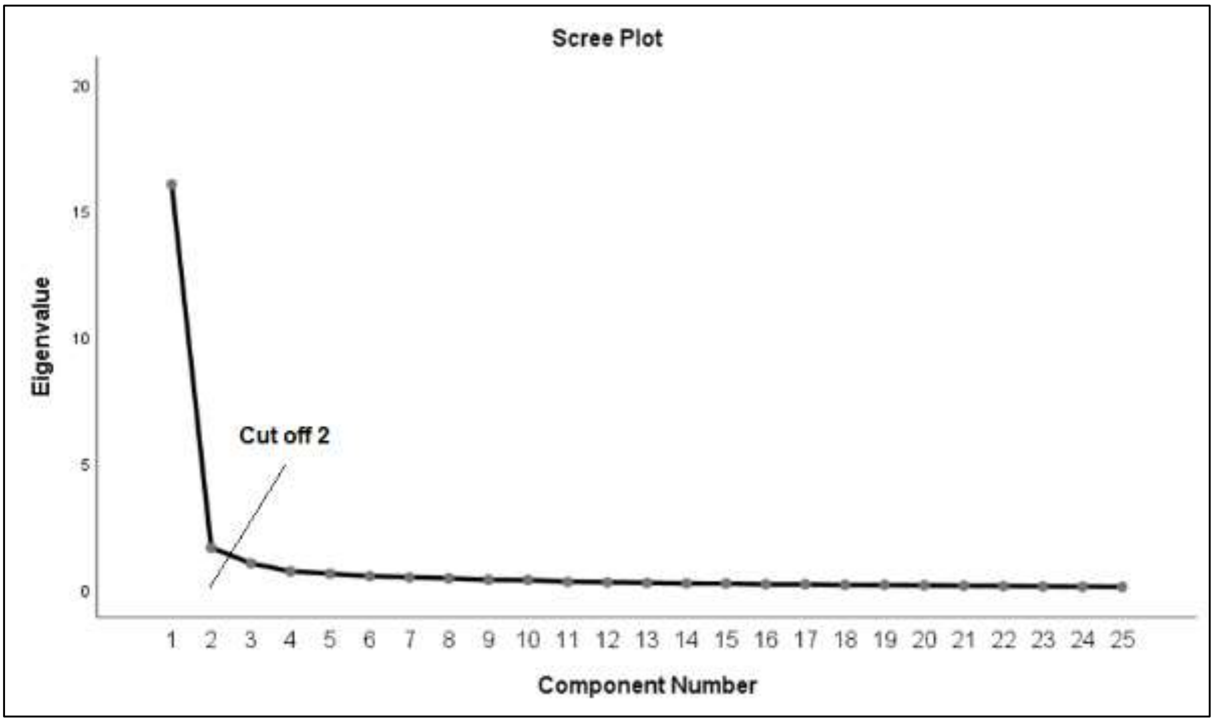


Figure 5-7: Relatedness scree plot, compiled from survey data

Figure 5-8 shows the scree plot for the autonomy questions. Six factors were retained for this category.

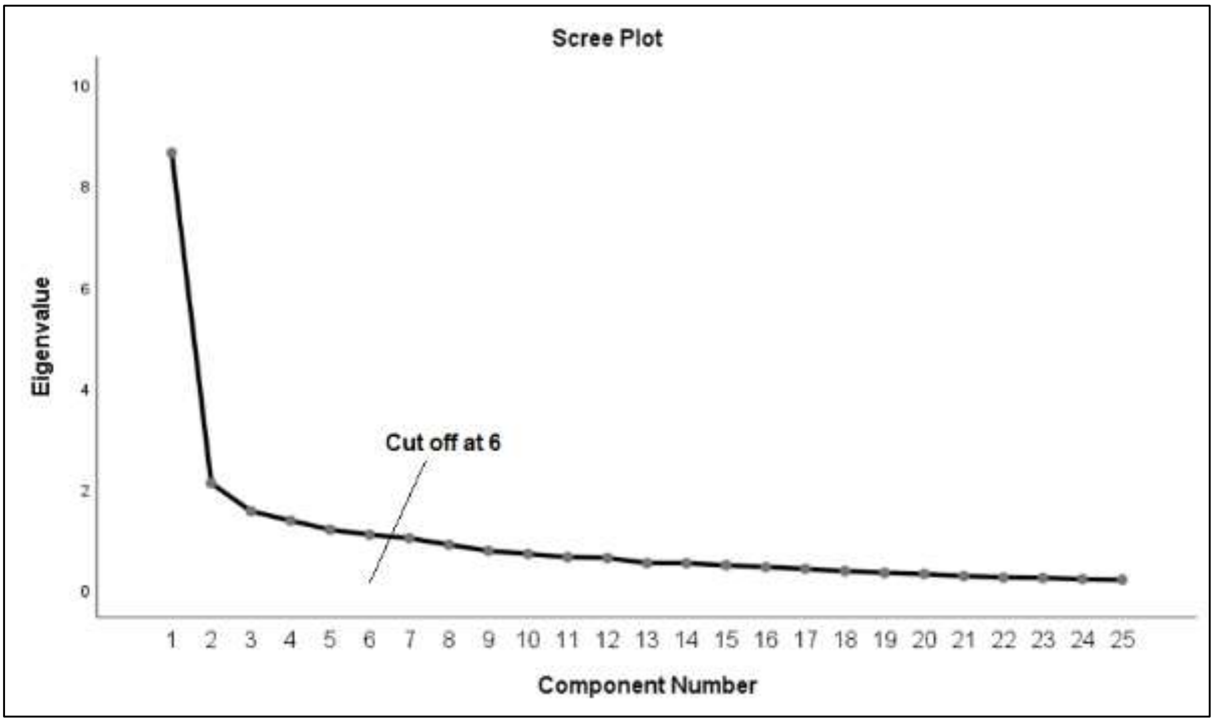


Figure 5-8: Autonomy scree plot, compiled from survey data

Communalities

Items with communalities greater than 0.4 were selected, and those with communalities less than 0.4 were left out. According to Costello & Osborne (2005), items with communalities less than 0.4 may not have an association with other items. The communalities shown in Appendix K indicate that the communalities were greater than 0.4 for the relatedness items, and none of these items was therefore discarded. The communalities for the autonomy category indicate that 5 statements were below 0.4 and these also were left out. The communalities for competence show that only a single statement had communality below 0.4 and was as a result also discarded.

The evidence obtained through the Eigenvalues, the scree plots and the cumulative percentages, shows that the survey data were suitable for the EFA (Costello & Osborne, 2005; Williams et al., 2010; Yong & Pearce, 2013). The principal axis factoring (PAF) extraction method was applied using the Direct Oblimin with Kaiser Normalization rotation method and the rotation converged in 12 iterations. Stevens (2002) recommend retaining items with loading values greater than 0.4, and it is on this basis that the item loading cut off was set at 0.4. The results of the PAF are shown in Tables 5-10 to 5-12.

Table 5-10: Rotated pattern matrix - competence, compiled from survey data

Question	**Factor**			
	1	2	3	4
12	0.757			
21	0.707			
20	0.680			
11	0.673			
16	0.654			
15	0.629			
19	0.582			
1	0.561			
14	0.525			
18	0.494			
10	0.443			
13				
7		-0.862		
6		-0.852		
8		-0.815		
4		-0.685		
9		-0.653		
5		-0.617		
17		-0.498		
2				
23			-0.878	
22			-0.753	
24			-0.595	
25	0.409		-0.440	
3				0.417
Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalization.				

In the final analysis factor 3 item, C25 was removed because it had a cross loading difference less than 0.2. Factor 4 was dropped since it had a single item, C3. Therefore, the final number of competence category factors was reduced to 3.

Table 5-11: Rotated pattern matrix - relatedness statements

Question	Factor	
	1	2
4	0.960	
5	0.930	
8	0.864	
9	0.857	
3	0.850	
6	0.820	
10	0.808	
7	0.775	
13	0.766	
11	0.743	
15	0.723	
16	0.714	
12	0.702	
1	0.688	
14	0.675	
18	0.510	0.412
17	0.480	0.402
2	0.449	
22		0.901
23		0.883
25		0.871
24		0.764
20		0.598
21		0.581
19		0.483
Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalization.		

For relatedness factors, items Q17 and Q18 were discarded because they each had a cross-loading difference that is lower than 0.2.

Table 5-12: Rotated pattern matrix - autonomy statements

Question	Factor					
	1	2	3	4	5	6
9	0.621					
10	0.562					
8	0.429					
17						
1						
5		-0.757				
6		-0.745				
4		-0.663				
7		-0.466				
3						
23			0.916			
22			0.878			
21				-0.921		
19				-0.666		
20				-0.578		
25					0.609	
24					0.525	
18						
2						
13						-0.765
11						-0.620
12						-0.535
15						-0.485
16						-0.432
14						
Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalization.						

For the autonomy category, 6 items (A1, A2, A3, A14, A17and A18) were dropped because they had loading values of less than 0.4.

Based on the rotated pattern matrices presented in Tables 5-10, 5-11 and 5-12, the resultant factors are as follows: 3 factors for competence, 3 factors for relatedness and 6 for autonomy. The factor names are shown in table 5-13.

Table 5-13: Factor names

Category	Factor name	Items
Competence	Employee skills for data safety awareness	11
	Employee skills for email and website safety	7
	Employee skills for privacy awareness	4
Relatedness	Organisational support for employee device and information protection awareness	16
	Organisational support for employee information privacy protection awareness	16
	Organisational support for employee information privacy protection awareness	7
Autonomy	Employee choice on privacy awareness	3
	Employee choice to avoid malicious emails and downloads	4
	Employee choice to keep the privacy of student personal information	2
	Employee choice to report bad security behaviour	3
	Employee choice to adhere to information security and privacy policies	2
	Employee choice to keep devices and information secure	5

The factors *employee choice to keep the privacy of student personal information* and *employee choice to adhere to information security and privacy policies*, which had two statements each, were retained because both factors had very good reliability as shown by the Cronbach alpha coefficient results in Table 5-14.

5.4.2 Reliability – Cronbach alpha

Cronbach Alpha coefficients were calculated for the 11 factors resulting from the EFA. Reliability refers to whether the measuring instrument is dependable or not, and if the measuring instrument produces consistent results in similar environments (Marczyk et al., 2005). According to Gerber & Hall (2017), Cronbach Alpha coefficient can be interpreted as follows: values greater than 0.8 - good; values from 0.6 to 0.8 - acceptable ; and values less than 0.6 - unacceptable for. Table 5-14 shows the results of the Cronbach Alpha for the 11 factors (the detailed statistics are shown in Appendix L). All the Cronbach Alphas are described as being good because they were found to be above 0.7.

Table 5-14: Reliability results for the factors

Category	Factor	Items	No. of items	Items omitted	Cronbach's Alpha	Reliability
Competence	Employee skills for data safety awareness	12, 21, 20, 11, 16, 15, 19, 1, 14, 18, 10	11		0.906	Good
	Employee skills for email and website safety	4, 5, 6, 7, 8, 9, 17	7		0.905	Good
	Employee skills for privacy awareness	22, 23, 24	4		0.799	Good
Relatedness	Organisational support for employee device and information awareness	4, 5, 8, 9, 3, 6, 7, 10, 11, 13, 15, 16, 12, 1, 14, 2	16	2	0.967	Good
	Organisational supporting for employee information privacy protection awareness	22, 23, 24, 25, 20, 21, 19	7		0.945	Good
Autonomy	Employee choice on privacy awareness	8, 9, 10	3		0.775	Acceptable
	Employee choice to avoid malicious emails and downloads	4, 5, 6, 7	4		0.836	Good
	Employee choice to keep the privacy of student personal information	22, 23	2		0.904	Good
	Employee choice to report bad security behaviour	19, 20, 21	3		0.791	Acceptable
	Employee choice to adhere to information security and privacy policies	24, 25	2		0.868	Good
	Employee choice to keep devices and information secure	11, 13, 15, 16, 12	5		0.793	Acceptable
Overall					9.489	Good

The Cronbach Alpha for the 11 factors was found to be between 0.775 and 0.970. The overall Cronbach alpha coefficient for all the factors was 9.489, which indicates good internal consistency.

5.5 Descriptive statistics for the factors

This section discusses the mean values for the factors of per category (i.e., competence, relatedness and autonomy).

5.5.1 Overall mean values for the factors

Figure 5-9 shows that the mean values for the three categories as follows: autonomy (M = 4.32) > competence (M = 4.28) > relatedness (M = 3.08). This suggests that while on the one hand the autonomy questions, which was followed closely by the competence questions, received a more positive perception, relatedness questions on the other hand received neutral or potentially negative perceptions. The mean value of less than 4 for relatedness indicates an area that requires further improvement.

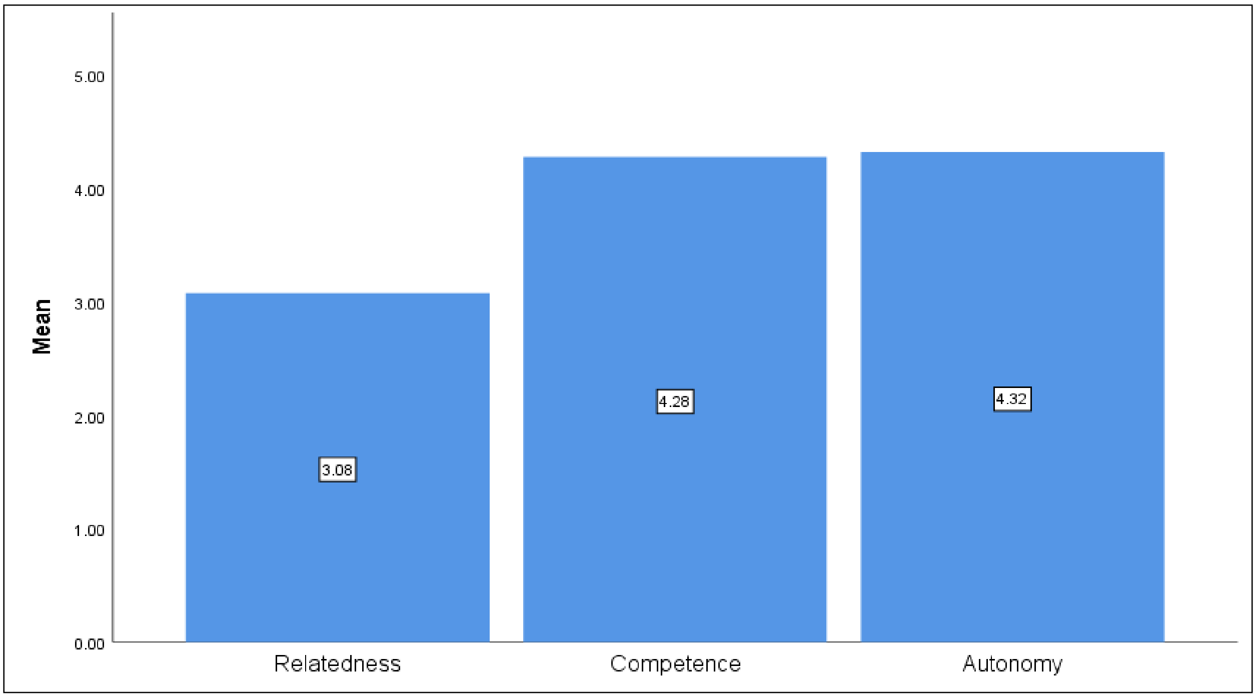


Figure 5-9: Overall group mean values

5.5.2 Competence category factors

Figure 5-10 shows the means for the three factors for the competence category. The highest mean value achieved for the *employee skills for privacy awareness* item (M = 4.41) suggests a positive perception by participants towards this factor. Perceptions of the other two competence factors (i.e., *employee skills for data safety awareness* (M = 4.22) and *employee skills for email and website safety* (M = 4.13)) were less favourable.

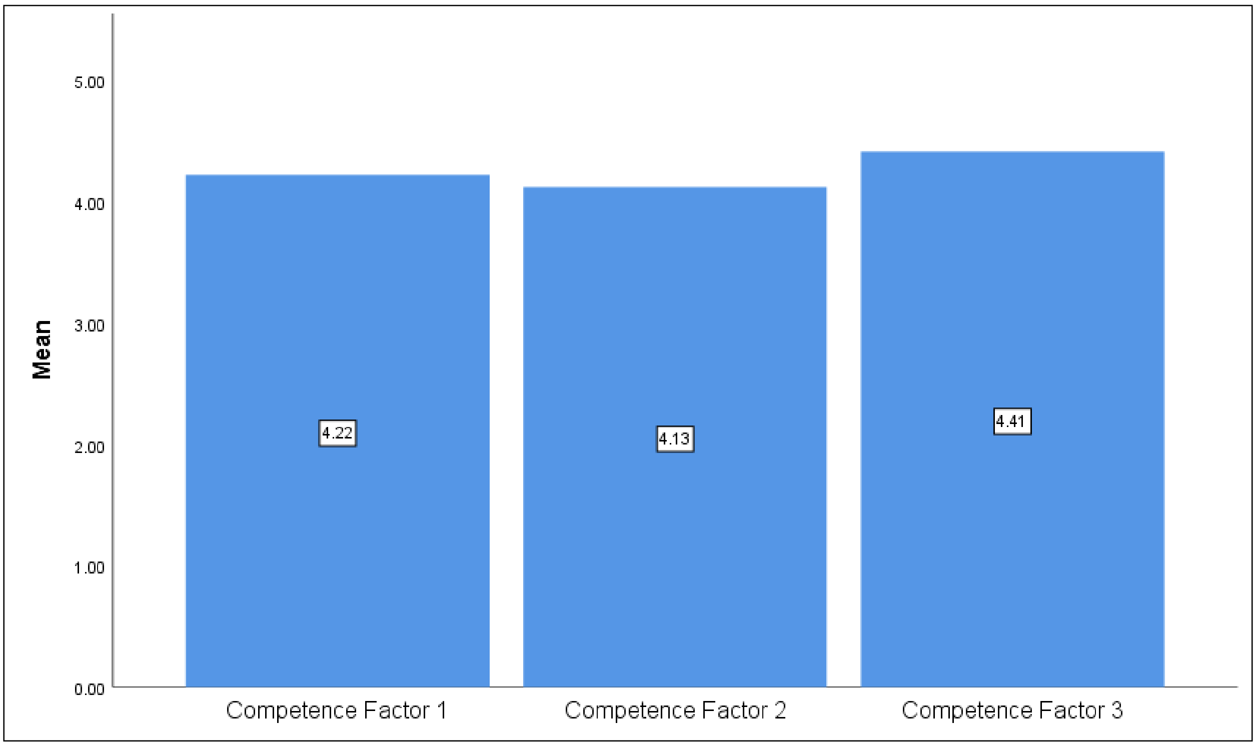


Figure 5-10: Competence category factors means

5.5.3 Relatedness category factors

According to Figure 5-11, a higher mean value (M = 3.25) was obtained for the relatedness category factor *organisational support for employee device and information protection awareness* compared to the factor *organisational support for employee information privacy protection awareness* factor (M = 3.01). The mean values of the two factors suggest that participants have a neutral or potentially negative perception of the relatedness questions. A mean value of less than 4.0 obtained for both factors suggests that both factors require further improvement.

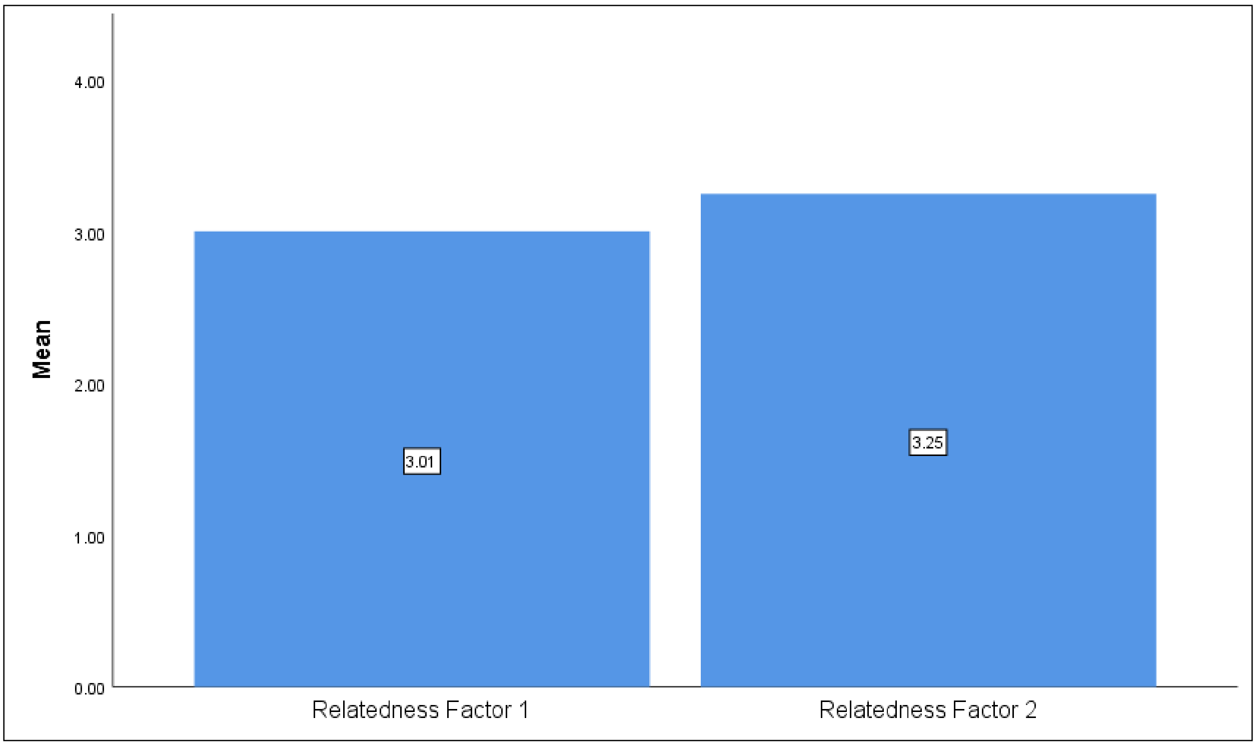


Figure 5-11: Relatedness category factors means

5.5.4 Autonomy category factors

Figure 5-12 shows the means for the six factors for the autonomy category. The order of the mean values for the autonomy factor is as follow (highest to lowest): *employee choice to adhere to information security and privacy policies* (M = 4.62); *employee choice to keep devices and information secure* (M = 4.46); *employee choice to keep the privacy of student personal information* (M = 4.44); *employee choice to avoid malicious emails and downloads* (M = 4.30); *employee choice on privacy awareness* (M = 4.09); and *employee choice to report bad security behaviour* (M=3.96). The values suggest that respondents have a positive opinion of all the autonomy factors.

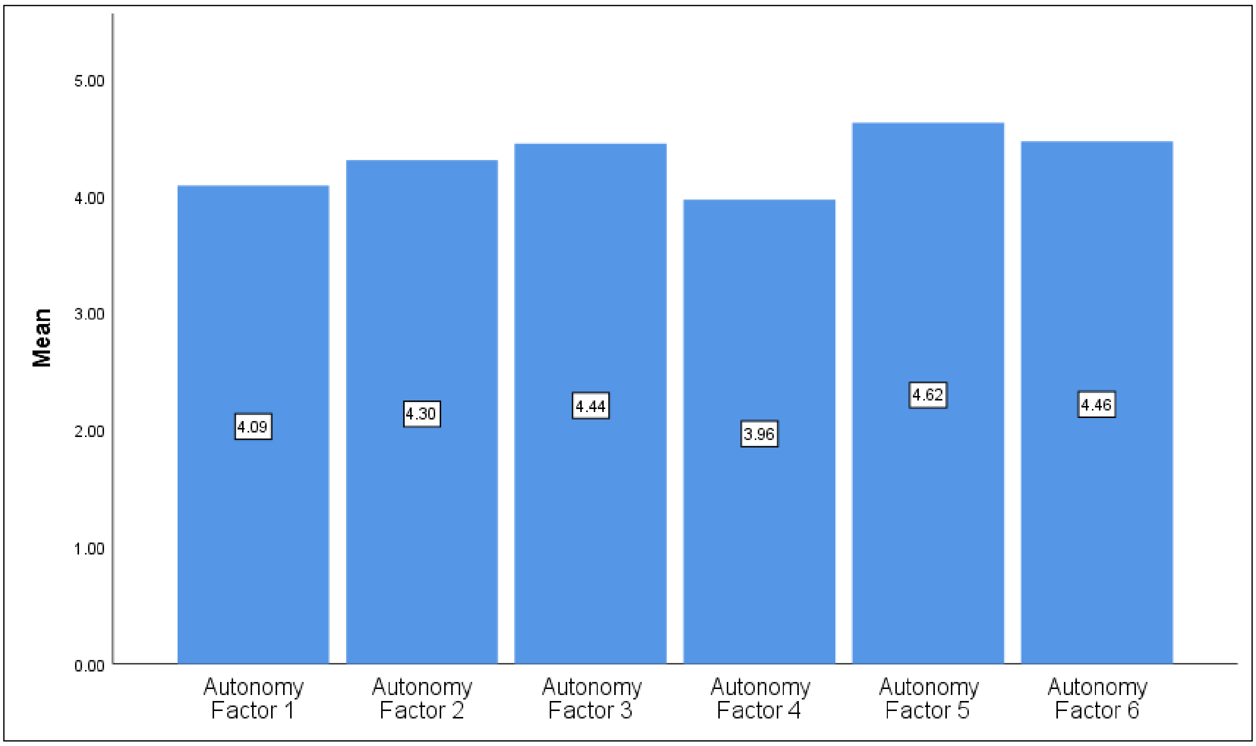


Figure 5-12: Mean values for the autonomy category factors

5.6 Comparison of demographic groups

One-way ANOVA was conducted for each of the factors and the biographical variables to determine whether the mean values differed among the biographical variables groups. Scheffe's method was used for the post hoc test to identify where the significant differences lied among the groups. The information is shown in Appendix M. For the ANOVA and the Scheffe test, the significance level was set at .05. The post-hoc results are presented for the significant ANOVAs only. ANOVA was carried out for each of the following groups: age, tenure, job level and the highest level of education. T-tests were conducted for the gender groups.

5.6.1 Test of normality

A test of normality was carried out before proceeding with ANOVA, t-tests and correlation analysis to assess whether the data had a normal distribution. If the result of the normality test is non-significant (*p* >.05) a normal distribution of the data is assumed. However, if the normality test produces a significant result (*p* <.05), the data does not have a normal distribution (Field, 2009). Table 5-15 presents the Kolmogorov-Smirnov test and the Shapiro-Wilk test results. The results of both tests show that the data deviate from normality. However, "parametric methods examining differences between means, for sample sizes greater than 5, do not require the assumption of normality and will yield nearly correct answers even for manifestly non-normal and asymmetric distributions" (Norman 2010, p4). While the survey data was not normally distributed, the sample size was large (N=263), therefore the study still proceeded with parametric methods, that is, the Pearson, the t-tests and the ANOVAs. The assumption of a normal distribution is, therefore, not necessary for the t-test when the sample is large (Lumley, Diehr, Emerson & Chen, 2002). Blanca, Alarcón, Arnau, Bono & Bendayan, (2017) state that the ANOVA is still robust in situations where the data does not have a normal distribution and the sample is large. Norman (2010) is of the view that parametric tests can still be carried out on small sample data, which has unequal variances or data that does not have a normal distribution.

Table 5-15: Normality test result for the factors

	Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
	Statistic	**df**	**Sig.**	**Statistic**	**df**	**Sig.**
Organisational support for employee device and information protection awareness	0.071	259	0.003	0.954	259	0.000
Organisational support for employee information privacy protection awareness	0.091	259	0.000	0.940	259	0.000
Employee skills for data safety awareness	0.145	259	0.000	0.887	259	0.000
Employee skills for email and website safety	0.158	259	0.000	0.875	259	0.000
Employee skills for privacy awareness	0.223	259	0.000	0.804	259	0.000
Employee choice on privacy awareness	0.155	259	0.000	0.874	259	0.000
Employee choice to avoid malicious emails and downloads	0.215	259	0.000	0.802	259	0.000
Employee choice to keep the privacy of student personal information	0.319	259	0.000	0.691	259	0.000
Employee choice to report bad security behaviour	0.148	259	0.000	0.903	259	0.000

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Employee choice to adhere to information security and privacy policies	0.366	259	0.000	0.669	259	0.000
Employee choice to keep devices and information secure	0.215	259	0.000	0.786	259	0.000
a. Lilliefors Significance Correction						

5.6.2 ANOVA - age groups

Table 5-16 shows the ANOVA results for purposes of undertaking a comparative analysis of the age groups for the eleven factors. The data shows that only 2 factors had significant differences for age groups. The *organisational support for employee information privacy protection awareness* factor shows a significant mean difference between age groups F(2, 259) = 3.369 (p = 0.036) (indicated with "*"). The employee *choice to avoid malicious emails and downloads* factor also shows a significant mean difference between age groups F(2, 259) = 3.672 (p = 0.027) (indicated with a "*"). The remaining 9 factors did not show any significant mean differences. The ANOVA was followed by the post hoc assessments to explore the source of the significant mean difference.

Table 5-16: ANOVA results from Age groups

ANOVA							Descriptive				
		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**	**Age groups**	**N**	**Mean**	**Std. Deviation**	**Std. Error**
Organisational support for employee device and information protection awareness	Between Groups	6.679	2	3.339	2.381	0.095	1946 -1964	77	3.0433	1.20495	0.13732
	Within Groups	363.296	259	1.403			1965 -1976	83	2.7952	1.13025	0.12406
	Total	369.975	261				1977 -date	102	3.1749	1.21133	0.11994
Organisational support for employee information privacy protection awareness	Between Groups	9.898	2	4.949	3.369	**0.036***	1946 -1964	76	3.2437	1.19344	0.13690
	Within Groups	376.040	256	1.469			1965 -1976	82	2.9988	1.28610	0.14203
	Total	385.938	258				1977 -date	101	3.4663	1.16293	0.11572
Employee skills for data safety awareness	Between Groups	2.180	2	1.090	2.011	0.136	1946 -1964	77	4.2270	0.69195	0.07885
	Within Groups	140.937	260	0.542			1965 -1976	83	4.1042	0.78719	0.08641
	Total	143.117	262				1977 -date	103	4.3220	0.72583	0.07152
Employee skills for email and website safety	Between Groups	3.319	2	1.659	2.218	0.111	1946 -1964	77	4.2319	0.69215	0.07888
	Within Groups	193.727	259	0.748			1965 -1976	83	3.9633	0.95990	0.10536
	Total	197.045	261				1977 -date	102	4.1762	0.89973	0.08909
Employee skills for privacy awareness	Between Groups	0.648	2	0.324	0.574	0.564	1946 -1964	77	4.3636	0.79689	0.09081
	Within Groups	146.225	259	0.565			1965 -1976	83	4.3855	0.77823	0.08542
	Total	146.873	261				1977 -date	102	4.4755	0.69153	0.06847
Employee choice on privacy awareness	Between Groups	3.352	2	1.676	2.055	0.130	1946 -1964	77	4.0996	0.80034	0.09121
	Within Groups	211.237	259	0.816			1965 -1976	83	3.9357	0.96196	0.10559
	Total	214.589	261				1977 -date	102	4.2059	0.92638	0.09173
Employee choice to avoid malicious emails and downloads	Between Groups	5.424	2	2.712	3.672	**0.027***	1946 -1964	77	4.5011	0.66523	0.07581
	Within Groups	191.294	259	0.739			1965 -1976	83	4.1335	0.94397	0.10361
	Total	196.718	261				1977 -date	102	4.2892	0.91518	0.09062
Employee choice to keep the privacy of student personal information	Between Groups	0.614	2	0.307	0.418	0.659	1946 -1964	77	4.4091	0.89490	0.10198
	Within Groups	189.331	258	0.734			1965 -1976	82	4.4024	0.95076	0.10499
	Total	189.944	260				1977 -date	102	4.5049	0.73960	0.07323
Employee choice to report bad security behaviour	Between Groups	0.585	2	0.293	0.333	0.717	1946 -1964	77	4.0173	0.80911	0.09221
	Within Groups	227.344	259	0.878			1965 -1976	83	3.8996	1.04989	0.11524
	Total	227.929	261				1977 -date	102	3.9788	0.92920	0.09200

ANOVA							Descriptive				
		Sum of Squares	df	Mean Square	F	Sig.	Age groups	N	Mean	Std. Deviation	Std. Error
Employee choice to adhere to information security and privacy policies	Between Groups	0.062	2	0.031	0.083	0.921	1946 -1964	77	4.6234	0.61855	0.07049
	Within Groups	96.657	259	0.373			1965 -1976	83	4.6446	0.55508	0.06093
	Total	96.719	261				1977 -date	102	4.6078	0.64726	0.06409
Employee choice to keep devices and information secure	Between Groups	0.739	2	0.370	0.798	0.451	1946 -1964	77	4.5221	0.55834	0.06363
	Within Groups	119.953	259	0.463			1965 -1976	83	4.3912	0.80444	0.08830
	Total	120.692	261				1977 -date	102	4.4838	0.65397	0.06475

The post-hoc test results, using the Scheffe procedure, are shown in Table 5-17. The *organisational support for employee information privacy protection awareness* results factor shows that the mean difference is significant between the 1965 – 1976 and 1977 to date age groups. Participants from the 1977 – date age group had significantly higher scores on the *organisational support for employee information privacy protection awareness* items (M=3.47) than participants from the 1965 – 1976 age group (M=2.999). The results suggest that both groups had a potentially neutral and negative perception *of organisational support for employee information privacy protection awareness*.

The *employee choice to avoid malicious emails and downloads factor* had a significant difference between the 1946 – 1964 and 1965 – 1976 age groups. Participants from the 1946 – 1964 age group had significantly higher scores on the *employee choice to avoid malicious emails and downloads* items (M= 4.5) than participants from the 1965 – 1976 age group (M = 4.13). This implies that participants from the 1946 – 1964 age group had a more positive perception of the *employee choice to avoid malicious emails and downloads* questions compared to 1965 – 1976 age group.

Table 5-17: Post hoc analysis - Age group

Multiple Comparisons							
Scheffe							
						95% Confidence Interval	
Dependent Variable			**Mean Difference (I-J)**	**Std. Error**	**Sig.**	**Lower Bound**	**Upper Bound**
Organisational support for employee information privacy protection awareness	1946 - 1964	1965 -1976	0.24490	0.19298	0.448	-0.2302	0.7200
		1977 -date	-0.22256	0.18404	0.482	-0.6757	0.2306
	1965 - 1976	1946 -1964	-0.24490	0.19298	0.448	-0.7200	0.2302
		1977 -date	-.46745*	0.18016	**0.036**	-0.9110	-0.0239
	1977 - date	1946 -1964	0.22256	0.18404	0.482	-0.2306	0.6757
		1965 -1976	.46745*	0.18016	**0.036**	0.0239	0.9110
Employee choice to avoid malicious emails and downloads	1946 - 1964	1965 -1976	.36755*	0.13598	**0.027**	0.0328	0.7023
		1977 -date	0.21187	0.12974	0.265	-0.1076	0.5313
	1965 - 1976	1946 -1964	-.36755*	0.13598	**0.027**	-0.7023	-0.0328
		1977 -date	-0.15568	0.12704	0.473	-0.4685	0.1571
	1977 - date	1946 -1964	-0.21187	0.12974	0.265	-0.5313	0.1076
		1965 -1976	0.15568	0.12704	0.473	-0.1571	0.4685
*. The mean difference is significant at the 0.05 level.							

5.6.3 ANOVA results for the job level

The ANOVA results for comparing the job level groups for the eleven factors are presented in Table 5-18. The data shows that the mean differences are significant (p<0.05) between six factors for the job level groups. The *employee skills for data safety awareness* factor shows a significant mean difference between job level groups F(2, 259) = 4.976 (p = 0.008) (indicated with a "*"). The *employee skills for email and website safety* factor shows a significant mean difference between job level groups F(2, 258) = 10.482 (p = 0.000) (indicated with a "*"). The *employee skills for privacy awareness* factor shows a significant mean difference between job level groups F(2, 258) = 8.653 (p = 0.000) (indicated with "*"). The *employee choice to avoid malicious emails and downloads* factor shows a significant mean difference between job level groups F(2, 258) = 6.458 (p = 0.002) (indicated with a "*"). The *employee choice to keep the privacy of student personal information* factor shows a significant mean difference between job level groups F(2, 257) = 8.251 (p = 0.000) (indicated with a "*"). The *employee choice to keep devices and information secure* factor shows a significant mean difference between job level groups F(2, 258) = 4.256 (p = 0.015) (indicated with a "*"). The remaining five factors do not show any significant differences relating to job level. The ANOVA was followed by post hoc test to explore the source of the significant mean differences. The post hoc test results are shown in Table 5-19.

The *employee skills for data safety awareness* factor results show that the mean difference between job level groups academic staff group and operational staff group is significant. Participants' responses from the academic staff group had a significantly higher mean (M = 4.38) on the *employee skills for data safety awareness* questions than participants' responses from the operational staff group (M = 3.94). This suggests that participants from the academic staff group had a more positive perception towards the *employee skills for data safety awareness* questions.

Employee skills for email and website safety factor indicated that all 3 comparisons had significant differences. The differences between these groups academic staff and administrative staff, the academic staff and operational staff, as well as the administrative staff and operational staff, were all significant. Results show that participants' responses from the academic staff group had significantly higher scores (M = 4.34), followed by participants' responses from the administrative group (M = 4.07), and the operational staff group (M = 3.94) had the lowest scores. The results suggest that the academic staff group had a positive perception towards the *employee skills for email and website safety* questions, followed by the administrative staff group and lastly the operational staff group.

The *employee skills for privacy awareness* factor results show that there are two significant differences between academic and the administrative staff groups as well as the academic and operational staff groups. For the first comparison, results show that mean scores for the participants from the academic staff group were significantly higher (M = 4.68) than the administrative group participants (M = 4.34). For the second comparison, results show that the academic staff group scored significantly higher than the operational staff group (M = 3.98). This implies that the academic staff group had a more positive perception towards the e*mployee skills for privacy awareness* questions, followed by administrative staff and lastly the operational staff.

The results for the *employee choice to avoid malicious emails and downloads* factor show that the mean differences between academic staff group and operational staff group as well as the administrative staff group and operational staff group were significant. For the first comparison, the results show that mean scores for the participants from the academic staff group were significantly higher (M = 4.38) than for participants from the operational staff group (M = 3.72). For the second comparison, results show that administrative staff group scored significantly higher (M = 4.35) compared to the operational staff group. This implies that the academic staff group had a more positive perception towards the *employee choice to avoid malicious emails and downloads* questions, followed by administrative staff group and lastly the operational staff group.

The e*mployee choice to keep the privacy of student personal information* factor, results indicate two statistically significant mean differences between academic staff group and administrative staff group as well as the academic staff group and operational staff group. For the first comparison, results show that mean scores for the participants from the academic staff group were significantly higher (M = 4.67) than for participants from the administrative group (M = 4.36). For the second comparison, results show that the academic staff group had significantly higher scores compared to the operational staff group (M = 3.98). This implies that the academic staff group had a more positive perception towards the *employee chooses to keep the privacy of student personal* *information* questions, followed by administrative staff group and then lastly the operational staff group.

The e*mployee choice to keep devices and information secure* factor results show that there is a significant difference between academic and administrative staff groups. The results show that the mean score for the participants from the academic staff group was significantly higher (M = 4.61) than for the participants from the administrative group (M = 4.39). This implies that the academic staff group had a more positive perception towards the e*mployee choice to keep devices and information secure* questions, than administrative staff group.

Table 5-18: ANOVA results from Job Levels

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**		**Mean**	**Std. Deviation**	**Std. Error**
Organisational support for employee device and information protection awareness	Between Groups	6.548	2	3.274	2.350	0.097	Academic staff	3.1102	1.16574	0.11543
	Within Groups	359.475	258	1.393			Administrative	3.0181	1.17209	0.10125
	Total	366.024	260				Operational	2.5403	1.28300	0.25660
Organisational support for employee information privacy protection awareness	Between Groups	7.224	2	3.612	2.452	0.088	Academic staff	3.3343	1.21546	0.12035
	Within Groups	375.650	255	1.473			Administrative	3.2737	1.19795	0.10467
	Total	382.874	257				Operational	2.7429	1.28902	0.25780
Employee skills for data safety awareness	Between Groups	5.274	2	2.637	4.976	**0.008***	Academic staff	4.3839	0.59559	0.05897
	Within Groups	137.241	259	0.530			Administrative	4.1522	0.79969	0.06883
	Total	142.515	261				Operational	3.9433	0.80930	0.16186
Employee skills for email and website safety	Between Groups	14.751	2	7.375	10.482	**0.000***	Academic staff	4.3429	0.64235	0.06360
	Within Groups	181.526	258	0.704			Administrative	4.0677	0.89920	0.07768
	Total	196.277	260				Operational	3.5095	1.16033	0.23207
Employee skills for privacy awareness	Between Groups	9.210	2	4.605	8.653	**0.000***	Academic staff	4.6078	0.59409	0.05882
	Within Groups	137.318	258	0.532			Administrative	4.3433	0.81027	0.07000
	Total	146.529	260				Operational	3.9800	0.77328	0.15466
Employee choice on privacy awareness	Between Groups	3.998	2	1.999	2.459	0.088	Academic staff	4.2255	0.81402	0.08060
	Within Groups	209.757	258	0.813			Administrative	4.0249	0.97043	0.08383
	Total	213.756	260				Operational	3.8400	0.85592	0.17118
Employee choice to avoid malicious emails and downloads	Between Groups	9.355	2	4.678	6.458	**0.002***	Academic staff	4.3807	0.79599	0.07881
	Within Groups	186.874	258	0.724			Administrative	4.3458	0.81095	0.07006
	Total	196.229	260				Operational	3.7200	1.21475	0.24295
Employee choice to keep the privacy of student personal information	Between Groups	11.442	2	5.721	8.251	**0.000***	Academic staff	4.6667	0.64229	0.06360
	Within Groups	178.192	257	0.693			Administrative	4.3571	0.92231	0.07997
	Total	189.635	259				Operational	3.9800	1.00499	0.20100
Employee choice to report bad	Between Groups	1.253	2	0.626	0.716	0.489	Academic staff	4.0098	0.96410	0.09546

		Sum of Squares	df	Mean Square	F	Sig.		Mean	Std. Deviation	Std. Error
security behaviour	Within Groups	225.601	258	0.874			Administrative	3.9614	0.93768	0.08100
	Total	226.854	260				Operational	3.7600	0.78481	0.15696
Employee choice to adhere to information security and privacy policies	Between Groups	0.554	2	0.277	0.745	0.476	Academic staff	4.6765	0.56572	0.05601
	Within Groups	96.022	258	0.372			Administrative	4.5970	0.63565	0.05491
	Total	96.577	260				Operational	4.5400	0.64420	0.12884
Employee choice to keep devices and information secure	Between Groups	3.845	2	1.923	4.256	**0.015***	Academic staff	4.6095	0.51401	0.05090
	Within Groups	116.560	258	0.452			Administrative	4.3884	0.78541	0.06785
	Total	120.406	260				Operational	4.2720	0.57120	0.11424

Table 5-19: Post hoc analysis: Job level

Multiple Comparisons

Scheffe							
						95% Confidence Interval	
Dependent Variable			**Mean Difference (I-J)**	**Std. Error**	**Sig.**	**Lower Bound**	**Upper Bound**
Employee skills for data safety awareness	Academic staff	Administrative	0.23170	0.09550	0.054	-0.0034	0.4668
		Operational	.44064*	0.16245	0.027	0.0407	0.8406
	Administrative	Academic staff	-0.23170	0.09550	0.054	-0.4668	0.0034
		Operational	0.20894	0.15849	0.421	-0.1813	0.5991
	Operational	Academic staff	-.44064*	0.16245	0.027	-0.8406	-0.0407
		Administrative	-0.20894	0.15849	0.421	-0.5991	0.1813
Employee skills for email and website safety	Academic staff	Administrative	.27521*	0.11022	0.046	0.0038	0.5466
		Operational	.83338*	0.18719	0.000	0.3725	1.2943
	Administrative	Academic staff	-.27521*	0.11022	0.046	-0.5466	-0.0038
		Operational	.55817*	0.18274	0.010	0.1083	1.0081
	Operational	Academic staff	-.83338*	0.18719	0.000	-1.2943	-0.3725
		Administrative	-.55817*	0.18274	0.010	-1.0081	-0.1083
Employee skills for privacy awareness	Academic staff	Administrative	.26456*	0.09586	0.023	0.0285	0.5006
		Operational	.62784*	0.16281	0.001	0.2270	1.0287
	Administrative	Academic staff	-.26456*	0.09586	0.023	-0.5006	-0.0285
		Operational	0.36328	0.15894	0.075	-0.0280	0.7546
	Operational	Academic staff	-.62784*	0.16281	0.001	-1.0287	-0.2270
		Administrative	-0.36328	0.15894	0.075	-0.7546	0.0280
Employee choice to avoid malicious emails and downloads	Academic staff	Administrative	0.03495	0.11183	0.952	-0.2404	0.3103
		Operational	.66072*	0.18993	0.003	0.1931	1.1283
	Administrative	Academic staff	-0.03495	0.11183	0.952	-0.3103	0.2404
		Operational	.62577*	0.18541	0.004	0.1693	1.0823
	Operational	Academic staff	-.66072*	0.18993	0.003	-1.1283	-0.1931
		Administrative	-.62577*	0.18541	0.004	-1.0823	-0.1693
Employee choice to keep the privacy of student personal information	Academic staff	Administrative	.30952*	0.10959	0.020	0.0397	0.5794
		Operational	.68667*	0.18583	0.001	0.2291	1.1442
	Administrative	Academic staff	-.30952*	0.10959	0.020	-0.5794	-0.0397
		Operational	0.37714	0.18151	0.118	-0.0698	0.8240

Multiple Comparisons							
Scheffe							
Dependent Variable			**Mean Difference (I-J)**	**Std. Error**	**Sig.**	**95% Confidence Interval**	
						Lower Bound	**Upper Bound**
	Operational	Academic staff	-.68667*	0.18583	0.001	-1.1442	-0.2291
		Administrative	-0.37714	0.18151	0.118	-0.8240	0.0698
Employee choice to keep devices and information secure	Academic staff	Administrative	.22104*	0.08832	0.045	0.0036	0.4385
		Operational	0.33748	0.15000	0.082	-0.0318	0.7068
	Administrative	Academic staff	-.22104*	0.08832	0.045	-0.4385	-0.0036
		Operational	0.11643	0.14643	0.729	-0.2441	0.4770
	Operational	Academic staff	-0.33748	0.15000	0.082	-0.7068	0.0318
		Administrative	-0.11643	0.14643	0.729	-0.4770	0.2441
*. The mean difference is significant at the 0.05 level.							

5.6.4 ANOVA results for the level of education

Table 5-20, which shows the ANOVA results for the level of education groups, suggests that for the *organisational support for employee device and information protection awareness* factor, there is a significant mean difference between level of education groups F(3, 257) = 3.109 (p = .027) (indicated with an asterisk), and the *organisational support for employee information privacy protection awareness* factor*,* also shows a significant mean difference between level of education groups F(3, 254) = 3.116 (p = .027) (indicated with an asterisk). However, the post-hoc tests show that the two factors do not have a significant difference. The factors show significant differences, but the post hoc test indicate that no significant mean differences exist among the educational levels as shown by the post hoc tests in Table 5-21.

Table 5-20: ANOVA results from Level of education

		Sum of Squares	df	Mean Square	F	Sig.		Mean	Std. Deviation	Std. Error
Organisational support for employee device and information protection awareness	Between Groups	12.818	3	4.273	3.109	**0.027***	High School Certificate	3.3708	1.14026	0.22805
	Within Groups	353.205	257	1.374			Diploma	3.5996	1.12988	0.25921
	Total	366.024	260				Degree	3.0665	1.32320	0.22053
							Postgraduate	2.8846	1.14926	0.08542
Organisational support for employee information privacy protection awareness	Between Groups	13.593	3	4.531	3.116	**0.027***	High School Certificate	3.8457	1.14131	0.22826
	Within Groups	369.281	254	1.454			Diploma	3.6015	1.28358	0.29447
	Total	382.874	257				Degree	3.1389	1.36191	0.22698
							Postgraduate	3.1458	1.17277	0.08790
	Between Groups	0.404	3	0.135	0.244	0.865	High School Certificate	4.1184	0.75515	0.15103

		Sum of Squares	df	Mean Square	F	Sig.		Mean	Std. Deviation	Std. Error
Employee skills for data safety awareness	Within Groups	142.111	258	0.551			Diploma	4.2967	0.81312	0.18654
	Total	142.515	261				Degree	4.2501	0.68874	0.11323
							Postgraduate	4.2234	0.74329	0.05525
Employee skills for email and website safety	Between Groups	4.690	3	1.563	2.097	0.101	High School Certificate	3.8181	1.03526	0.20705
	Within Groups	191.587	257	0.745			Diploma	4.3158	0.81173	0.18622
	Total	196.277	260				Degree	3.9505	1.02002	0.16769
							Postgraduate	4.1787	0.80691	0.06014
Employee skills for privacy awareness	Between Groups	2.834	3	0.945	1.690	0.170	High School Certificate	4.3600	0.76328	0.15266
	Within Groups	143.694	257	0.559			Diploma	4.4737	0.73127	0.16777
	Total	146.529	260				Degree	4.1667	0.84620	0.13911
							Postgraduate	4.4630	0.72585	0.05410
Employee choice on privacy awareness	Between Groups	6.390	3	2.130	2.640	0.050	High School Certificate	3.7467	1.18743	0.23749
	Within Groups	207.365	257	0.807			Diploma	4.4561	0.69576	0.15962
	Total	213.756	260				Degree	4.2342	0.81599	0.13415
							Postgraduate	4.0630	0.88703	0.06612
Employee choice to avoid malicious emails and downloads	Between Groups	2.911	3	0.970	1.290	0.278	High School Certificate	4.0100	0.79543	0.15909
	Within Groups	193.318	257	0.752			Diploma	4.4474	0.70009	0.16061
	Total	196.229	260				Degree	4.2365	0.88378	0.14529
							Postgraduate	4.3370	0.88813	0.06620
Employee choice to keep the privacy of student personal information	Between Groups	3.103	3	1.034	1.420	0.237	High School Certificate	4.3400	0.96523	0.19305
	Within Groups	186.532	256	0.729			Diploma	4.4474	0.91127	0.20906
	Total	189.635	259				Degree	4.2027	0.92391	0.15189
							Postgraduate	4.5056	0.81590	0.06098
Employee choice to report bad security behaviour	Between Groups	2.438	3	0.813	0.931	0.426	High School Certificate	4.1267	0.90175	0.18035
	Within Groups	224.416	257	0.873			Diploma	4.1754	0.72323	0.16592
	Total	226.854	260				Degree	4.0360	0.94210	0.15488
							Postgraduate	3.9000	0.95582	0.07124
Employee choice to adhere to information security and privacy policies	Between Groups	0.211	3	0.070	0.188	0.905	High School Certificate	4.6400	0.53072	0.10614
	Within Groups	96.365	257	0.375			Diploma	4.5526	0.66447	0.15244
	Total	96.577	260				Degree	4.6757	0.57995	0.09534
							Postgraduate	4.6167	0.62334	0.04646
Employee choice to keep devices and information secure	Between Groups	2.484	3	0.828	1.805	0.147	High School Certificate	4.2320	0.79515	0.15903
	Within Groups	117.922	257	0.459			Diploma	4.6211	0.47560	0.10911
	Total	120.406	260				Degree	4.5959	0.49894	0.08203
							Postgraduate	4.4520	0.70795	0.05277

Table 5-21: Post-hoc analysis: Level of education

Multiple Comparisons							
Scheffe							
Dependent Variable			**Mean Difference (I-J)**	**Std. Error**	**Sig.**	**95% Confidence Interval**	
						Lower Bound	**Upper Bound**
Organisational support for employee device and information protection awareness	High School Certificate	Diploma	-0.22878	0.35680	0.938	-1.2329	0.7753
		Degree	0.30429	0.30520	0.803	-0.5546	1.1632
		Postgraduate	0.48618	0.25013	0.289	-0.2177	1.1901
	Diploma	High School Certificate	0.22878	0.35680	0.938	-0.7753	1.2329
		Degree	0.53306	0.33243	0.464	-0.4024	1.4686
		Postgraduate	0.71495	0.28271	0.097	-0.0806	1.5105
	Degree	High School Certificate	-0.30429	0.30520	0.803	-1.1632	0.5546
		Diploma	-0.53306	0.33243	0.464	-1.4686	0.4024
		Postgraduate	0.18189	0.21394	0.868	-0.4202	0.7839
	Postgraduate	High School Certificate	-0.48618	0.25013	0.289	-1.1901	0.2177
		Diploma	-0.71495	0.28271	0.097	-1.5105	0.0806
		Degree	-0.18189	0.21394	0.868	-0.7839	0.4202
Organisational support for employee information privacy protection awareness	High School Certificate	Diploma	0.24421	0.36698	0.931	-0.7886	1.2770
		Degree	0.70683	0.31391	0.170	-0.1766	1.5903
		Postgraduate	0.69991	0.25753	0.063	-0.0249	1.4247
	Diploma	High School Certificate	-0.24421	0.36698	0.931	-1.2770	0.7886
		Degree	0.46261	0.34191	0.609	-0.4996	1.4249
		Postgraduate	0.45570	0.29101	0.485	-0.3633	1.2747
	Degree	High School Certificate	-0.70683	0.31391	0.170	-1.5903	0.1766
		Diploma	-0.46261	0.34191	0.609	-1.4249	0.4996
		Postgraduate	-0.00691	0.22035	1.000	-0.6270	0.6132
	Postgraduate	High School Certificate	-0.69991	0.25753	0.063	-1.4247	0.0249
		Diploma	-0.45570	0.29101	0.485	-1.2747	0.3633
		Degree	0.00691	0.22035	1.000	-0.6132	0.6270

5.6.5 Independent samples test between gender groups

T-test results are shown in Table 5-22 for the gender groups (also shown in Appendix N with the group statistics). A t-test (independent samples) was done to determine if the differences between mean scores of the two groups (male and females) were significant. The t-test results are discussed below.

The female group (N=144) was associated with the *organisational support for employee device and information protection awareness* mean (M = 3.09, SD = 1.23) and the male group (N=115) was associated with *organisational support for employee device and information protection awareness* mean (M = 2.91, SD = 1.14). A t-test was performed to test whether the female and male groups were associated with the statistically significant different mean. The homogeneity of variances assumption was verified with the Levene's test F(257) = .835, p=.362. The independent t-test result for the *organisational support for employee device and information protection awareness* shows a difference that is not statistically significant t(257) =1.182, p=.238.

The female group (N=142) was associated with the *organisational support for employee information privacy protection awareness* mean (M = 3.27, SD = 1.26) and the male group (N=114) was associated with the *organisational support for employee information privacy protection awareness* mean (M= 3.24, SD=1.19). A t-test was performed to test if the female and male groups were associated with the statistically significant different mean. The homogeneity of variances assumption was verified with the Levene's test F(254) = .576, p=.449. The independent t-test result for *the organisational support for employee information privacy protection awareness* factor shows that there was no statistically significant difference t(254) =.181, p=.857.

The female group (N=144) was associated with the *employee skills for data safety awareness* mean (M = 4.23, SD = .73) and the male group (N=116) was associated with the *employee skills for data safety awareness* mean (M= 4.23, SD=.76). A t-test was performed to test if the female and male groups were associated with the statistically significant mean difference. The homogeneity of variances assumption was tested with the Levene's test F(258) = .599, p=.440. The independent t-test result for the *employee skills for data safety awareness* shows that there was no statistically significant mean difference t(258) =.095, p=.925.

The female group (N=143) was associated with the *employee skills for email and website safety* mean (M = 4.16, SD = .81) and the male group (N=116) was associated with the *employee skills for email and website safety* mean (M= 4.10, SD=.97). A t-test was performed to test if the female and male groups were associated with the statistically significant mean difference. The homogeneity of variances assumption was tested using the Levene's test F(257) = 1.981, p=.160. The independent t-test result for the *employee skills for email and website safety* shows that there was no statistically significant difference t(257) =.055, p=.583.

The female group (N=143) was associated with the *employee skills for privacy awareness safety* mean (M = 4.16, SD = .81) and the male group (N=116) was associated with the *employee skills for privacy awareness* mean (M= 4.10, SD=.97). A t-test was performed to test whether the female and male groups were associated with the statistically significant different mean. The homogeneity of variances assumption was tested with the Levene's test F(257) = 1.981, p=.160. The independent t-test result for the *employee skills for privacy awareness* shows that there was no statistically significant difference t(257) =.055, p=.583.

The female group (N=143) was associated with the *employee choice on privacy awareness safety* mean (M = 4.17, SD = .87) and the male group (N=116) was associated with the *employee choice on privacy awareness* mean (M= 3.9971, SD=.94). A t-test was performed to test whether the female and male groups were associated with the statistically significant different mean. The homogeneity of variances assumption was tested using the Levene's test F(257) = .507, p=.477. The independent t-test result for the *employee choice on privacy awareness* shows that there was no statistically significant difference t(257) = 1.531, p=.127.

The female group (N=143) was associated with the *employee choice to avoid malicious emails and downloads safety* mean (M = 4.40, SD = .77) and the male group (N=116) was associated with the *employee choice to avoid malicious emails and downloads* mean (M= 4.19, SD=.96). A t-test was performed to test whether the female and male groups were associated with the statistically significant different mean. The homogeneity of variances assumption was tested using Levene's test F(218) = 6.99, p=.009. The independent t-test result for the *employee choice to avoid malicious emails and downloads* shows that there was no statistically significant difference t(218) = 1.965, p =.051.

The female group (N =142) was associated with the *employee choice to keep the privacy of student personal information* mean (M = 4.43, SD = .92) and the male group (N =116) was associated with the *employee choice to keep the privacy of student personal information* mean (M = 4.66, SD =.78). A t-test was performed to test whether the female and male groups were associated with the statistically significant mean difference. The homogeneity of variances assumption was tested using Levene's test F(258) = 1.826, p

=.178. The independent t-test result for the *employee choice to keep the privacy of student personal information* shows that there was no statistically significant difference t(258) = -367, p =.714.

The female group (N=143) was associated with the *employee choice to report bad security behaviour* mean (M = 3.98, SD = .98) and the male group (N=116) was associated with the *employee choice to report bad security behaviour* mean (M= 3.96, SD=.88). A t-test was performed to test whether the female and male groups were associated with the statistically significant different mean. The homogeneity of variances assumption of was tested using Levene's test F(257) = 3.034, p =.083. The independent t-test result for the *employee choice to report bad security behaviour* shows that there was no statistically significant difference t(257) = -0.218, p =.827.

The female group (N=143) was associated with the *employee choice to adhere to information security and privacy policies* mean (M = 4.64, SD = .63) and the male group (N=116) was associated with the *employee choice to adhere to information security and privacy policies* mean (M = 4.62, SD =.58). A t-test was performed to test whether the female and male groups were associated with the statistically significant different mean. The homogeneity of variances assumption was tested using Levene's test F(257) = 0.023, p=.879. The independent t-test result for the *employee choice to adhere to information security and privacy policies* shows that there was no statistically significant difference t(257) = .206, p=.837.

The female group (N=143) was associated with employee's *choice to keep devices and information secure* mean (M = 4.49, SD = .63) and the male group (N=116) was associated with the *employee choice to keep devices and information secure* mean (M= 4.44, SD=.73). A t-test was performed to determine if the female and male groups were associated with the statistically significant different mean. The homogeneity of variances assumption was tested using Levene's test F(257) = 1.077, p =.300. The independent t-test result for the *employee choice to keep devices and information secure* shows that there was no statistically significant difference t(257) = .685, p=.494.

Thus, the study found that the mean differences for the gender groups for all the factors were not statistically significant.

Table 5-22: Independent samples tests

.Independent sample test							Group statistics				
		Levene's Test for Equality of Variances		t-test for Equality of Means							
		F	Sig.	t	Df	Sig. (2-tailed)	Gender	N	Mean	Std. Deviation	Std. Error Mean
Organisational support for employee device and information protection awareness	Equal variances assumed	0.835	0.362	1.182	257	**0.238**	Female	144	3.0897	1.23406	0.10284
	Equal variances not assumed			1.192	251.365	0.234	Male	115	2.9131	1.14318	0.10660
Organisational support for employee information privacy protection awareness	Equal variances assumed	0.576	0.449	0.181	254	**0.857**	Female	142	3.2651	1.26179	0.10589
	Equal variances not assumed			0.182	247.252	0.856	Male	114	3.2371	1.19330	0.11176
Employee skills for data safety awareness	Equal variances assumed	0.599	0.440	0.095	258	**0.925**	Female	144	4.2347	0.72848	0.06071
	Equal variances not assumed			0.094	242.222	0.925	Male	116	4.2260	0.75677	0.07026
Employee skills for email and website safety	Equal variances assumed	1.981	0.160	0.550	257	**0.583**	Female	143	4.1555	0.80970	0.06771
	Equal variances not assumed			0.541	228.708	0.589	Male	116	4.0959	0.93619	0.08692
Employee skills for privacy awareness	Equal variances assumed	1.065	0.303	-0.196	257	**0.845**	Female	143	4.4068	0.81280	0.06797
	Equal variances not assumed			-0.200	256.798	0.842	Male	116	4.4253	0.67757	0.06291
Employee choice on privacy awareness	Equal variances assumed	0.507	0.477	1.531	257	**0.127**	Female	143	4.1702	0.87467	0.07314
	Equal variances not assumed			1.519	238.104	0.130	Male	116	3.9971	0.94024	0.08730
Employee choice to avoid malicious emails and downloads	Equal variances assumed	6.991	0.009	2.011	257	**0.045**	Female	143	4.4027	0.77020	0.06441
	Equal variances not assumed			1.965	217.696	**0.051**	Male	116	4.1861	0.96380	0.08949
Employee choice to keep the privacy of student personal information	Equal variances assumed	1.826	0.178	-0.367	256	**0.714**	Female	142	4.4261	0.92243	0.07741
	Equal variances not assumed			-0.373	255.756	0.709	Male	116	4.4655	0.77663	0.07211
Employee choice to report bad security behaviour	Equal variances assumed	3.034	0.083	0.218	257	**0.827**	Female	143	3.9825	0.98098	0.08203
	Equal variances not assumed			0.221	254.127	0.825	Male	116	3.9569	0.88414	0.08209
Employee choice to adhere to information security and privacy policies	Equal variances assumed	0.023	0.879	0.206	257	**0.837**	Female	143	4.6364	0.62850	0.05256
	Equal variances not assumed			0.208	252.618	0.835	Male	116	4.6207	0.58093	0.05394
Employee choice to keep devices and information secure	Equal variances assumed	1.077	0.300	0.685	257	0.494	Female	143	4.4942	0.63956	0.05348
	Equal variances not assumed			0.676	230.178	0.500	Male	116	4.4358	0.73143	0.06791

5.7 Correlation among the factors

Pearson correlations were computed among the 11 factors, and these are shown in Table 5-23. The correlation analyses were done to assess the strength and direction of the relationships amongst the factors. The results suggest that there were more statistically significant correlations greater or equal to (r= 0.184, n=263, p < .05) and two-tailed. However, the following correlations were not statistically significant:

- *Organisational support for employee device and information protection awareness* with *employee skills for privacy awareness* (r = .117, n =263, p = .06);
- *Organisational support for employee device and information protection awareness* with *employee choice to report bad security behaviour* (r= .059, n=263, p = .344);
- *Organisational support for employee device and information protection awareness* with *employee choice to adhere to information security and privacy policies* (r = .068, n=263, p = .273);
- *Organisational support for employee device and information protection awareness* with *employee choice to keep devices and information secure* (r = .106, n=263, p = .096); and
- *Organisational support for employee information privacy protection awareness* with *employee choice to keep devices and information secure* (r = .103, n=263, p = .099).

The effect sizes when using Pearson's correlation coefficient were also considered; these effect sizes are used to measure the practical significance of a correlation. The suggested effect sizes are as follows (Field 2009, p57):
r = .10 - small effect: one variable explains 1% of the variance in the other variable;
r= .30 - medium effect: one variable explains 9% of the variance in the other variable; and
r = .50 - large effect: one variable explains 25% of the variance in the other variable.

The following sub-sections discuss the Pearson correlation for the statistically significant results. The focus will be on the correlation among the different factors and the effect sizes.

Table 5-23: Correlation of the factors

		Relatedness Factor 1	Relatedness Factor 2	Competence Factor 1	Competence Factor 2	Competence Factor 3	Autonomy Factor 1	Autonomy Factor 2	Autonomy Factor 3	Autonomy Factor 4	Autonomy Factor 5	Autonomy Factor 6
Relatedness Factor 1	Pearson Correlation	1	.827**	.224**	.229**	0.117	.230**	.184**	0.059	.222**	0.068	0.103
	Sig. (2-tailed)		0.000	0.000	0.000	0.060	0.000	0.003	0.344	0.000	0.273	0.096
Relatedness Factor 2	Pearson Correlation	.827**	1	.246**	.209**	.309**	.180**	.134*	.258**	.307**	.172**	0.103
	Sig. (2-tailed)	0.000		0.000	0.001	0.000	0.004	0.031	0.000	0.000	0.006	0.099
Competence Factor 1	Pearson Correlation	.224**	.246**	1	.703**	.609**	.719**	.490**	.450**	.657**	.585**	.826**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Competence Factor 2	Pearson Correlation	.229**	.209**	.703**	1	.459**	.708**	.743**	.317**	.441**	.371**	.583**
	Sig. (2-tailed)	0.000	0.001	0.000		0.000	0.000	0.000	0.000	0.000	0.000	0.000
Competence Factor 3	Pearson Correlation	0.117	.309**	.609**	.459**	1	.328**	.287**	.832**	.409**	.706**	.467**
	Sig. (2-tailed)	0.060	0.000	0.000	0.000		0.000	0.000	0.000	0.000	0.000	0.000
Autonomy Factor 1	Pearson Correlation	.230**	.180**	.719**	.708**	.328**	1	.566**	.265**	.515**	.336**	.619**
	Sig. (2-tailed)	0.000	0.004	0.000	0.000	0.000		0.000	0.000	0.000	0.000	0.000
Autonomy Factor 2	Pearson Correlation	.184**	.134*	.490**	.743**	.287**	.566**	1	.193**	.404**	.246**	.466**
	Sig. (2-tailed)	0.003	0.031	0.000	0.000	0.000	0.000		0.002	0.000	0.000	0.000
Autonomy Factor 3	Pearson Correlation	0.059	.258**	.450**	.317**	.832**	.265**	.193**	1	.309**	.480**	.330**
	Sig. (2-tailed)	0.344	0.000	0.000	0.000	0.000	0.000	0.002		0.000	0.000	0.000
Autonomy Factor 4	Pearson Correlation	.222**	.307**	.657**	.441**	.409**	.515**	.404**	.309**	1	.488**	.489**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000		0.000	0.000
Autonomy Factor 5	Pearson Correlation	0.068	.172**	.585**	.371**	.706**	.336**	.246**	.480**	.488**	1	.513**
	Sig. (2-tailed)	0.273	0.006	0.000	0.000	0.000	0.000	0.000	0.000	0.000		0.000
Autonomy Factor6	Pearson Correlation	0.103	0.103	.826**	.583**	.467**	.619**	.466**	.330**	.489**	.513**	1
	Sig. (2-tailed)	0.096	0.099	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	
**. Correlation is significant at the 0.01 level (2-tailed).												
*. Correlation is significant at the 0.05 level (2-tailed).												

5.7.1 Correlation between competence factors and autonomy factors

This section presents correlations amongst the factors in the competence category and the factors in the autonomy category.

- Employee skills for data safety awareness with employee choice on privacy awareness, (r = .719, n =263, p = .000, large effect size),
- Employee skills for data safety awareness with employee choice to avoid malicious emails and downloads (r = .490, n =263, p = .000, medium effect size),
- Employee skills for data safety awareness with employee choice to keep the privacy of student personal information (r = .450, n =263, p = .000, medium effect size),
- Employee skills for data safety awareness with employee choice to report bad security behaviour (r = .657, n =263, p = .000, large effect size),
- Employee skills for data safety awareness with employee choice to adhere to information security and privacy policies (r = .585, n =263, p = .000, large effect size),
- Employee skills for data safety awareness with employee choice to keep devices and information secure (r = .826, n =263, p = .000, large effect),
- Employee skills for email and website safety with employee choice on privacy awareness (r = .708, n =263, p = .000, large effect size),
- Employee skills for email and website safety with employee choice to avoid malicious emails and downloads (r = .743, n =263, p = .000, large effect size), and this shows,
- Employee skills for email and website safety with employee choice to keep the privacy of student personal information (r = .317, n =263, p = .000, medium effect size),
- Employee skills for email and website safety with employee choice to report bad security behaviour (r = .441, n =263, p = .000, medium effect size),
- Employee skills for email and website safety with employee choice to adhere to information security and privacy policies (r = .371, n =263, p = .000, medium effect size),
- Employee skills for email and website safety with employee choice to keep devices and information secure (r = .583, n =263, p = .000, large effect size),
- Employee skills for privacy awareness with employee choice on privacy awareness (r = .328, n =263, p = .000, medium effect size),

- Employee skills for privacy awareness with employee choice to avoid malicious emails and downloads (r = .287, n =263, p = .000, small effect size),
- Employee skills for privacy awareness with employee choice to keep the privacy of student personal information (r = .832, n =263, p = .000, large effect size),
- Employee skills for privacy awareness with employee choice to report bad security behaviour (r = .409, n =263, p = .000, medium effect size),
- Employee skills for privacy awareness with employee choice to adhere to information security and privacy policies (r = .706, n =263, p = .000, large effect size) and
- Employee skills for privacy awareness with employee choice to keep devices and information secure (r = .460, n =263, p = .000, medium effect size).

The results suggest a statistically significant positive relationship among competence and autonomy factors. This could suggest that respondents who achieved high scores in competence questions also achieved high scores in autonomy questions. Thus, the relationship between autonomy and competence factors is a statistically significant.

5.7.2 Correlation between competence factors and relatedness factors

This section presents correlation amongst the competence factors in category and relatedness the factors.

- Employee skills for data safety awareness with organisational support for employee device and information awareness (r = .224, n =263, p = .000, small effect size),
- Employee skills for data safety awareness with organisational support for employee information privacy protection awareness, (r = .246, n =263, p = .000, small effect size),
- Employee skills for data safety awareness with organisational support for employee device and information awareness, (r = .229, n =263, p = .000, small effect size),
- Employee skills for data safety awareness with organisational support for employee information privacy protection awareness, (r = .460, n =263, p = .000, medium effect size) and
- Employee skills for privacy awareness with organisational support for employee information privacy protection awareness, (r = .309, n =263, p = .000, medium effect size).

The relationship among competence and relatedness factors indicates that some factors had a statistically significant positive relationship and some did not have a statistically significant relationship. This suggests a partial positive statistically significant relationship between competence and relatedness.

5.7.3 Correlation between relatedness factors and autonomy factors

This section presents the correlations among the factors in the competence and autonomy categories.

- Organisational support for employee device and information awareness with employee choice in privacy awareness (r = .230, n =263, p = .000, small effect size),
- Organisational support for employee device and information awareness with Employee choice to avoid malicious emails and downloads (r = .184, n =263, p = .003, small effect size),
- Organisational support for employee device and information awareness with Employee choice to report bad security behaviour (r = .222, n =263, p = .000, small effect size),
- Organisational support for employee information privacy protection awareness with employee choice in privacy awareness (r = .180, n =263, p = .004, small effect size),
- Organisational support for employee information privacy protection awareness with Employee choice to avoid malicious emails and downloads (r = .134, n =263, p = .031, small effect),
- Organisational support for employee information privacy protection awareness with employee choice to keep the privacy of student personal information (r = .258, n =263, p = .000, small effect size),
- Organisational support for employee information privacy protection awareness with employee choice to report bad security behaviour (r = .307, n =263, p = .000, medium effect size) and
- Organisational support for employee information privacy protection awareness with employee choice to adhere to information security and privacy policies (r = .172, n =263, p = .006, small effect size).

The relationship between autonomy and relatedness factors also indicates that some factors had a statistically positive relationship and some did not have a statistically significant relationship. This suggests a partial positive statistically significant relationship between autonomy and relatedness.

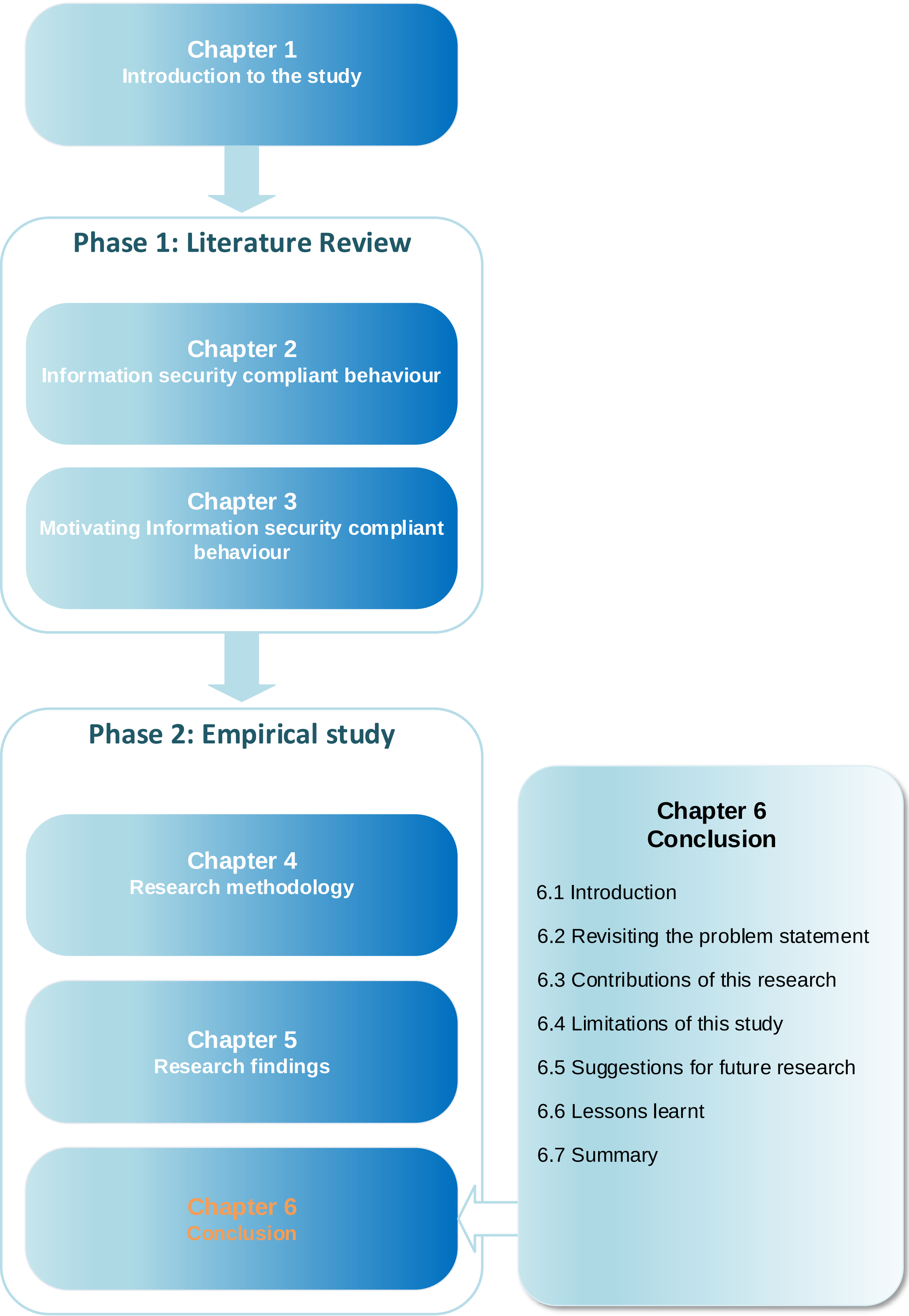
5.8 Conclusion

This study set out to develop a questionnaire for collecting data at an institution of higher learning. This was guided by the research questions and objectives as set out in Chapter 1. This chapter presented the following results, which emanated from the empirical study:

- The demographic distribution of the sample that was illustrated using graphs.
- Summary of the survey responses. This was conducted by analysing the statements with the highest and lowest mean values for each category, mean values for the factors of each category and mean values of the overall categories.
- Validation of the instrument using EFA, which produced 11 factors that were also found to possess good internal consistency using the Cronbach Alpha.
- Conducted the ANOVA on the biological variables, namely age, level of education, length of service and job level at the current employer.
- T-tests that were carried out on the gender groups.
- Pearson correlation that was conducted on the 11 factors to determine the existence of a relationship among the factors.

The results suggest that respondents were more positive regarding competence and autonomy questions with respect to information security behaviour than they were about the relatedness questions. The next chapter wraps up the dissertation by presenting the conclusion and recommendations about the findings of this study.

CHAPTER 6



Chapter 1
Introduction to the study

Phase 1: Literature Review

Chapter 2
Information security compliant behaviour

Chapter 3
Motivating Information security compliant behaviour

Phase 2: Empirical study

Chapter 4
Research methodology

Chapter 5
Research findings

Chapter 6
Conclusion

Chapter 6
Conclusion

6.1 Introduction

6.2 Revisiting the problem statement

6.3 Contributions of this research

6.4 Limitations of this study

6.5 Suggestions for future research

6.6 Lessons learnt

6.7 Summary

6 CONCLUSION, LIMITATIONS AND RECOMMENDATIONS

6.1 Introduction

This quantitative research study set out to evaluate information security behaviour among employees. The theoretical reasoning was derived from the self-determination theory (SDT). This study involved the development of a conceptual model the ISCBM^{SDT} and the development and validation of the ISCBM^{SDT} questionnaire. Data was collected was from a South African university using this questionnaire.

The chapter discusses how the research questions and the research objectives were addressed. This is followed by an evaluation of the contributions of this study. The chapter concludes by discussing the limitations of the current research study and provides suggestions for future research.

6.2 Revisiting the problem statement

The main aim of this study was to assess information security compliant behaviour by developing a validated information security compliance behaviour model based on the self-determination theory (ISCBM^{SDT}) questionnaire, from the perspective of competence, relatedness and autonomy.

This aim was addressed by answering the following research questions.

6.2.1 Research questions

To answer the research questions, each research question was associated with one or more research objectives. To this end, each research question is discussed with the research objective(s) it is associated with.

Research Question 1: What would a model and assessment instrument for information security compliant behaviour comprise of?

Chapter 3 addressed this research question by reviewing the current body of knowledge and before proposing an information security compliant behaviour conceptual model that is based on the self-determination theory (ISCBM^{SDT}). Chapter 2 discussed information security compliant behaviour to provide a context for the current study. To answer

Research Question 1, ISCB was defined and intrinsic factors used in other studies to assess information security behaviour were identified. A scoping review was conducted and the SDT was identified as the theory upon which this study is based. A conceptual model comprising variables from the SDT was thereafter developed. A discussion of the research objectives associated with the Research Question 1 and how the research question was addressed follows below.

Research Objective 1: To investigate what factors influence information security compliant behaviour of employees.

For a full description of the model for information security compliant behaviour, a literature review was carried out and a list of factors that provide an understanding of information security compliant behaviour was identified in Chapter 3. The following intrinsic motivation factors were identified: perceived effectiveness; legitimacy and perceived value congruency; and perceived fairness. Herath & Rao (2009) found that perceived effectiveness promotes ISP compliance positively. Son (2011) found that perceived legitimacy and perceived value congruence also motivates compliance with ISPs. Bulgurcu et al. (2011) state that the perception that the ISP is fair could intrinsically motivate employees to adhere to the ISPs. These studies by Son (2011), Herath & Rao (2009) and Bulgurcu et al. (2011) suggest that intrinsic factors are important in relation to ISP compliance intentions of employees. This study also discussed factors from the SDT perspective, the need for competence, relatedness and autonomy. When these needs are fulfilled, the employee is intrinsically motivated (Ryan & Deci, 2000).

In addition to discussing the factors, it was determined from the reviewed literature that intrinsic factors play an important role in influencing ISP compliance.

Research Objective 2: To explore the existing research with a view to establish theories that have been used for studying information security behaviour.

In Chapter 3, a summary of current research was conducted through a scoping review. The was done to establish the existence of the research gap and as well as summarise theories that have been studied in previous information security research. The review revealed that the following theories were used more than once in the studies considered: TPB, SDT, PMT, GDT, SBT, and SCT. The TPB was the most investigated of the theories. Other studies have found TPB, GDT and PMT to be the most investigated theories

(Angraini et al., 2019; Lebek et al., 2014). The scoping review also revealed that few studies were based on intrinsic factors, for example Alzahrani et al. (2018) and Rhee et al. (2009). Some researchers have investigated both intrinsic and extrinsic factors (e.g., Herath & Rao, 2009; Son, 2011, Padayachee, 2012). The majority of the studies were inclined towards the extrinsic factors (e.g. Abraham, 2011; Hu et al., 2012; Humaidi & Balakrishnan, 2015; Bulgurcu et al., 2011). The review suggests that the intrinsic motivational factors have not received much attention; this view is also supported by researchers such as Son (2011) and Padayachee (2012). This research was, therefore, based on the SDT; this is because in other studies the SDT has been used in conjunction with other theories and was not tested empirically without integrating it with other theories. Therefore, this study was solely based on the SDT and it was not combined with other theories or constructs from other theories.

Research Objective 3: To provide a working definition of information security compliant behaviour.

Information security compliant behaviour was defined in Chapter 2. The chapter discussed behaviour by considering the definition of other fields outside of information security. Such an approach was useful in providing a different perspective for defining the term behaviour. The definitions from other fields were applied information security to define a general concept of information security behaviour. The concept was then integrated with other definitions of information security behaviour and information security compliance to formulate a definition of information security compliant behaviour for this study. Chapter 2 concluded by defining information security compliant behaviour and this definition provides the context for this study. It was defined as follows: Actions users perform to safeguard information and technology resources of their organisation from malicious others to maintain the confidentiality, availability, integrity and privacy of data/information. These actions could be reactions to attacks on the data/information and information systems resources, for example, restoring a database after a system crash. The actions could also be learned procedures performed regularly to protect data/information and information systems resources, for example, taking a backup of their data or changing a password.

Research objective 4: To develop an information security compliant behaviour conceptual model that is based on the SDT.

Chapter 3 presented the information security compliant behaviour conceptual model derived from the SDT (ISCBM^{SDT}). The conceptual model is comprised of three factors, namely competence, relatedness and autonomy derived from the SDT. The SDT states that the fulfilment of these three basic psychological needs enhances intrinsic motivation. The model also includes the security aspects that the employee must comply with. These aspects are derived from industry standards and best practices such as NIST. HAIS-Q focus areas were used for the security aspects of the model and were also mapped to the best practices. The final conceptual model comprises the three concepts from the SDT and the security aspects. The conceptual model shows that the employee will be intrinsically motivated to carry out these security aspects when the three variables of the SDT are fulfilled. The model is the basis upon which the questionnaire was developed.

Research objective 5: To develop an information security compliant behaviour questionnaire that is based on the conceptual model, to assess information security compliant behaviour from a competence, relatedness and autonomy perspective.

A questionnaire was designed based on the ISCBM^{SDT}. The questionnaire combines the ISCBM^{SDT} and HAIS-Q focus areas to ensure content validity. The privacy focus area was added to the questionnaire since privacy is an important aspect when processing, storing and disseminating student information in an institution of higher learning. The HAIS-Q focus areas were mapped to each of the concepts from SDT to devise unique questions for each of the concepts. The HAIS-Q focus areas represent the security aspects discussed under the model. Each focus area from HAIS-Q was framed from the perspective of each of the SDT components of competence, relatedness and autonomy, thus resulting in three unique questions being formulated for each focus area.

To further address the content validity of the questionnaire, a panel of experts reviewed it and a pilot test was carried out. The resulting questionnaire, after considering the suggestions from the expert review and pilot study, was used in the online survey for the study. Also, the questionnaire was statistically validated using the exploratory factor analysis.

Research objective 6: To conduct a survey in an organisation with a to obtain data to statistically validate the questionnaire

The survey administration was discussed in Chapter 4. Research ethical clearance to carry out the survey was given by the relevant university committees. The questionnaire was administered over the internet using Google Forms, and invitations were sent by the ICT department of the university to participants via an email. The email had information on the background of the research study and the link to the online questionnaire. Participants were required to read and understand the information sheet and the consent form. Participants would complete the online questionnaire upon consenting to take part in the research study. From the online survey, two hundred and sixty-three responses were collected and this data was used to validate the questionnaire and to perform statistical analyses such as ANOVA, t-test and Pearson correlation analysis.

Research objective 7: To determine the validity and reliability of the questionnaire

Chapter 5 discussed the statistical analysis that was done to determine the questionnaire validity and reliability. The EFA was conducted separately for each category of the SDT since the questionnaire was categorised into competence, relatedness and autonomy statements. The results yielded a total of 11 factors for all the categories, and these were divided as follows: 3 factors for competence, 2 factors for relatedness and 6 factors for autonomy. The Cronbach Alpha was computed for the 11 factors and all were above 0.7 signifying that the questionnaire statements had high internal consistency. Results of the validity and reliability analysis indicate a questionnaire that possesses good internal consistency.

Research Question 2: What significant relationship exists amongst competence, relatedness and autonomy?

Research objective 8: To determine if there is a significant relationship amongst competence, relatedness and autonomy.

As demonstrated in chapter 5, results of the Pearson correlation show a positive correlation among autonomy and competence factors, and a partial correlation among relatedness and other factors. Such results suggest a direct relationship between competence and autonomy as far as information security behaviour is concerned. This could be interpreted that the respondents who have positive competence perceptions could also have positive autonomy perceptions. Similar results have been reported. For example, Wall et al. (2013) have reported that perceptions of self-determination (autonomy) foster perception of self-efficacy (competence). Kranz and Haeussinger (2014) found that the effect of internal perceived locus of control (a form of autonomous motivation) on self-efficacy (competence) is positive. This could also mean that people with positive autonomy perceptions are likely to feel confident about their competence as well. Autonomy refers to the perception of being the initiator of one's behaviour and goals (Ryan & Deci 2000). Competence is the desire to feel capable, gain mastery of tasks and learn new skills (Ryan & Deci 2000). The need for relatedness is the desire to interact and experience attachment with others (Ryan & Deci 2000). In this study, perceptions of competence were related positively to perceptions of autonomy. Employers should foster the belief that employees are capable of carrying out information security tasks, assisting with the acquisition of relevant skills and problem solving. This could also foster a sense of controller over their work and thus encourage self-initiation. In terms of relatedness, the employee must be made to understand the value of their work and how it relates to their co-workers. The employer should show interest and support toward the employee.

6.3 Contributions of this research

A review was conducted on the various theories used in the study of behavioural information security studies. The summary of these studies helps the reader to identify the theories that were frequently used during the period under consideration. It also highlighted the fact that intrinsic motivation factors were not given as much attention as the extrinsic factors in the behavioural information security studies. The review of the theories also showed that the SDT had been not given much attention in the behavioural information security studies. Therefore, a need exists for further research to be conducted on intrinsic factors.

The study developed an ISCBM^{SDT}, a model that is based on the constructs of the SDT and information security focus areas (security aspects), which were mapped to the HAIS-Q focus areas. The conceptual model is based on intrinsic motivational factors and also shows the significance of intrinsic motivation in information security behaviour. The model also formed a basis upon which a valid instrument was designed to assess information security behaviour.

This study developed a questionnaire, specifically the ISCBM^{SDT} questionnaire, for assessing information security behaviour. The questionnaire was based on the SDT and the HAIS-Q and could contribute to the evaluation and understanding of the information security behaviour of employees. This questionnaire can be administered by university personnel to identify areas needing further development in terms of employee information security behaviour. The questionnaire can also be administered before carrying out information security awareness training and thereafter, to assess whether the training was effective. Therefore, results of the assessment using this questionnaire can be used as part of corrective actions or measures for achieving the desired information security behaviour among employees.

This research, through the ISCBM^{SDT}, helps to understand the role intrinsic motivation in studying information security behaviour. The research shows that, by creating a positive perception of competence, relatedness and autonomy, the information security behaviour of employees could be improved in the organisation. Therefore, this study suggests that management should develop the competence of employees in terms of information security requirements that they must implement and conform with.

Results emanating from the online survey for the information security behaviour questions show that respondents had a more positive perception towards competence and autonomy than they were about relatedness. This was also confirmed by the overall results of the mean values reported for each of the categories, which show that the mean scores for autonomy were the highest (M = 4.32), followed by competence (M = 4.28) and relatedness (M = 3.08). These mean values suggest that competence, autonomy and relatedness affect employees' information security behaviour. The results of the overall means reported for each of the categories indicate that autonomy questions received a more positive perception, and this was closely followed by the competence and relatedness questions. These results suggest that autonomy and competence could have significant impact in fostering information security behaviour whereas the role of relatedness was less pronounced.

6.4 Limitations of this study

The study has limitations that affect the generalisability of the results of this study and should therefore be considered when the results are interpreted.

- The study employed the quantitative research method whereby the information was gathered through a questionnaire. For an in-depth understanding of information security behaviour, a qualitative approach should also be employed for the collection of data through interviews.

- The convenience sampling method which was employed in this study poses some limitations to the conclusions drawn from this study.
- The survey was conducted in a specific South African organisation of higher learning and results emanating from this study cannot be generalised to other academic institutions and/or organisations in other sectors.
- The study followed the cross-sectional design. This design can limit the generalisability of the findings in the following ways: user perceptions concerning information security may change over time and the cross-sectional method does not produce causal relationships.
- All the necessary due diligence should be exercised when interpreting survey responses in this study since the use of a self-reporting measurement instrument can result in participants responding in ways that please the researcher.

6.5 Suggestions for future research

This quantitative study has generated questions for future research, which are outside the scope of this study.

- Results from this research could be extended by a further qualitative examination of the concepts of this study.
- Random sampling could be adopted for future research to enable generalisability of the results.
- The results could be expanded by carrying out the study in an organisation that is in the non-educational sector.
- Future research could carry out further assessments in the same organisation in which this survey was conducted. A comparison with the results of the initial survey could help understand or determine whether information security behaviour is improving following the implementation of the recommendations from the first assessment.
- Future work could extend this study to other organisations in the country to obtain data from other organisations and get an understanding of the information security behaviour of employees in other organisations.

6.6 Lessons learnt

From this study, it is apparent that most of the respondents are confident about their skills (competence) and independence (autonomy) in their work. However, the same cannot be said about relatedness. This suggests that the university will need to encourage employees to appreciate the relationship between their work and that of their colleagues. To this end, employees should display an awareness of the benefits that accrue from collaborations.

Another important lesson is that the result of the current study would more appropriately reflect the university in which it was carried out. The study would have produced results that are reflective of the university environment in South Africa had it been done in more universities.

The results of the survey also show that the respondents had low confidence in their social media privacy settings. This is true from competence, relatedness and autonomy perspectives. The university could set up awareness training to educate its employee about the importance of securing and continuously reviewing their privacy settings. Potential interventions could include training employees on how to locate the privacy settings on major social media platforms and changing them from the default setting to more secure privacy settings.

The results of this survey also show that respondents were not confident about their skills to assess the safety of a website. Similarly, the university could also provide training to employees to equip them with skills on how to determine if a website requesting information is safe and if it sends the information in encrypted form.

Respondents were also not confident about their decisions to notice poor decision information security behaviour by their work colleagues. Employees could be made aware that they have to be alert to bad information behaviour by colleagues in the workplace.

The issues raised in this section will require the university to set up awareness training programs, which will address the employees’ shortcomings in these areas. In particular, the university will need to pay special attention to relatedness issues since the employees were not confident about issues relating to relatedness. The university should thus encourage collaboration among employees.

6.7 Summary

In this study, an assessment of information security compliant behaviour was carried out at a South African institution of higher learning. The SDT was used as the theoretical lens for the study and a conceptual model was developed. The results suggest that competence and autonomy are more important than relatedness for motivating information security behaviour among employees. The findings of this study have, therefore, underscored the significance of the SDT, especially competence and autonomy in the assessment of information security compliant behaviour.

7 REFERENCES

Abraham, S. (2011). Information security behavior: Factors and research directions. *Proceedings of the Seventeenth Americas Conference on Information Systems (AMCIS 2011)*, 1–13. Detroit, Michigan: AIS Electronic Library.

Agyekum Addae, J., Simpson, G., & Oppong Appiagyei Ampong, G. (2019). Factors Influencing Information Security Policy Compliance Behavior. *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, 43–47. https://doi.org/10.1109/ICSIoT47925.2019.00015

Ahmad, Z., Norhashim, M., Song, O. T., & Hui, L. T. (2016). A typology of employees' information security behaviour. *Proceedings of the 4th International Conference on Information and Communication Technology (ICoICT)*.

Alaskar, M., Vodanovich, S., & Shen, K. N. (2015). Evolvement of information security research on employees' behavior: A systematic review and future direction. In T. X. Bui & R. H. Sprague (Eds.), *Proceedings of the 48th Hawaii International Conference on System Sciences* (pp. 4241–4250). Kauai, Hawaii, USA: IEEE.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture : A behaviour compliance conceptual framework. In C. Boyd & W. Susilo (Eds.), *Proceedings of the 8th Australasian Information Security Conference (AISC 2010). Conferences in Research and Practice in Information Technology (CRPIT)* (pp. 47–55). Brisbane, Australia: Australian Computer Society.

Alohali, M., Clarke, N., Furnell, S., & Albakri, S. (2017). Information security behavior: Recognizing the influencers. *Proceedings of the Computing Conference*, 844–853. Hilton Kensington, London, UK: IEEE.

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: a higher education case study. *Information and Computer Security*, *26*(1), 91–108. https://doi.org/10.1108/ICS-09-2016-0073

Alzahrani, A., Johnson, C., & Altamimi, S. (2018). Information security policy compliance : Investigating the role of intrinsic motivation towards policy compliance in the organisation. In S. Li (Ed.), *Proceedings of the 2018 4th International Conference on Information Management (ICIM)* (pp. 125–132). Oxford, United Kingdom: IEEE.

Angraini, Alias, R. A., & Okfalisa. (2019). Information Security Policy Compliance : Systematic Literature Review Review. *The Fifth Information Systems International Conference 2019 Information. Procedia Computer Science*, *161*, 1216–1224.

Surabaya. Indonesia: Elsevier B.V.

Arksey, H., & O’Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology: Theory & Practice*, *8*(1), 19-32.

Aurigemma, S., & Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security*, *25*(4), 421–436. https://doi.org/10.1108/ICS-11-2016-0089

Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with information security policies. *Proceedings of the 45th Hawaii International Conference on System Sciences*, 3248–3257. Grand Wailea, Maui, Hawaii, USA: IEEE.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, Vol. 84, pp. 191–215.

Bandura, A. (1994). Self-efficacy. In V. S. Ramachaudran (Ed.), *Encyclopedia of human behavior* (Vol. 4, pp. 71–81). https://doi.org/10.1002/9780470479216.corpsy0836

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. https://doi.org/10.1016/j.cose.2017.04.009

Baum, W. M. (2013). What Counts as Behavior? The Molar Multiscale View. *The Behavior Analyst*, *2*(36), 283–293.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003

Bergner, R. M. (2011). New Ideas in Psychology What is behavior? And so what? *New Ideas in Psychology*, *29*, 147–155. https://doi.org/10.1016/j.newideapsych.2010.08.001

Bhaharin, S. H., Sulaiman, R., Mokhtar, U. A., & Yusof, M. M. (2019). Issues and Trends in Information Security Policy Compliance. *Proceeding of the 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*. Johor Bahru, Malaysia: IEEE.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices* (2nd ed.). Tampa, Florida, USA: Textbooks Collection.

Blanca, M. J., Alarcón, R., Arnau, J., Bono, R., & Bendayan, R. (2017). Non-normal data: Is ANOVA still a valid option? *Psicothema*, *29*(4), 552–557.

https://doi.org/10.7334/psicothema2016.383

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees' security behaviors. *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, 103–122. Ottawa, Canada: USENIX Association.

Boynton, P. M., & Greenhalgh, T. (2004). Selecting, designing, and developing your questionnaire. *British Medical Journal*, *328*, 1312–1315. https://doi.org/10.1136/bmj.328.7451.1312

Broeck, A. Van den, Vansteenkiste, M., & Witte, H. De. (2008). Self-determination theory: A theoretical and empirical overview in occupational health psychology. In J. Houdmont (Ed.), *Occupational health psychology: European perspectives on research, education, and practice. Pt. 3* (pp. 63–88). Nottingham, United Kingdom: Nottingham University Press.

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

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2011). Information Security Policy Compliance : The Role of Fairness , Commitment , and Cost Beliefs. *Proceedings of the Mediterranean Conference on Information Systems (MCIS 2011)*. Limassol, Cyprus: AIS Electronic Library.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. *Computers & Security*, *98*, 102020. https://doi.org/https://doi.org/10.1016/j.cose.2020.102020

Calic, D., Pattinson, M., Parsons, K., Butavicius, M., & McCormac, A. (2016). Naïve and accidental behaviours that compromise information security : What the experts think. In N. Clarke & S. Furnell (Eds.), *Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)* (pp. 12–21). Frankfurt, Germany: Plymouth University.

Cao, L. (2014). Behavior informatics: A new perspective. *IEEE Intelligent Systems*, *29*(4), 62–80. https://doi.org/10.1109/MIS.2014.60

Carden, L., & Wood, W. (2018). Habit formation and change. *Current Opinion in Behavioral Sciences*, *20*, 117–122. https://doi.org/10.1016/j.cobeha.2017.12.009

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 and Security*, *39*, 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Child, D. (2006). *The Essentials of Factor Analysis* (3rd ed.). New York: Continuum.

Conner, M., & Norman, P. (2017). Health behaviour: Current issues and challenges. *Psychology & Health*, *32*(8), 895–906. https://doi.org/10.1080/08870446.2017.1336240

Connolly, L., Lang, M., Gathegi, J., & Tygar, J. D. (2016). The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study. In N. Clarke & S. Furnell (Eds.), *Proceedings of the Tenth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2016)* (pp. 33–44). Frankfurt, Germany: Plymouth University.

Correia, A., Gonçalves, A., & Teodoro, M. F. (2017). A model-driven approach to information security compliance. *Proceedings of the AIP Conference*, 1–5. Bydgoszcz, Poland: American Institute of Physics.

Costello, A. B., & Osborne, J. W. (2005). Best Practices in Exploratory Factor Analysis : Four Recommendations for Getting the Most From Your Analysis. *Practical Assessment, Research, and Evaluation*, *10*(7), 1–9.

Cram, W. A., Proudfoot, J. G., & D’Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Creswell, J. W. (2012). *Educational Research - Planning, Conducting and Evaluating Quantitative and Qualitative Research* (4th ed.). Boston, USA: Pearson Education Inc.

Creswell, J. W. (2014). *Research Design - Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2018). *Reasearch design : qualitative, quantitative, and mixed methods approaches* (5th ed.). Los Angeles, USA: SAGE.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Curry, M., Marshall, B., Crossler, R. E., & Correia, J. (2018). InfoSec Process Action Model (IPAM): Systematically addressing individual security behavior. *The Database for Advances in Information Systems*, *49*, 49–66.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139–151.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162–176. https://doi.org/10.1016/j.cose.2014.12.006

Davis, R., Campbell, R., Hildon, Z., Hobbs, L., & Michie, S. (2015). Theories of behaviour and behaviour change across the social and behavioural sciences: a scoping review. *Health Psychology Review*, *9*(3), 323–344. https://doi.org/10.1080/17437199.2014.941722

Deci, E. L., Olafsen, A. H., & Ryan, R. M. (2017). Self-determination theory in work organizations: The state of a science. *The Annual Review of Organizational Psychology and Organizational Behavior*, *4*, 19–43. https://doi.org/10.1146/annurev-orgpsych

Deci, E. L., & Ryan, M. R. (2015). Self-Determination Theory. *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, *21*, 486–491. https://doi.org/10.1016/B978-0-08-097086-8.26036-4

Dennedy, M. F., Fox, J., & Finneran, T. R. (2014). Data and Privacy Governance Concepts. In *The Privacy Engineer's Manifesto* (pp. 51–72). https://doi.org/10.1007/978-1-4302-6356-2_3

Doherty, N. F., & Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology and People*, *31*(2). https://doi.org/10.1108/ITP-08-2016-0194

Faizi, S. M., & Rahman, S. S. M. (2020). Effect of Fear on Behavioral Intention to Comply. *Proceedings of Tthe 4th International Conference on Information System and Data Mining*, 65–70. Hawaii, USA: Association for Computing Machinery.

Field, A. (2009). *Discovering statistics using SPSS* (3rd ed.). London: Sage.

Flores, W. R., & Ekstedt, M. (2012). A Model for Investigating Organizational Impact on Information Security Behavior. *Workshop on Information Security and Privacy*, 12–15. AIS Electronic Library.

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

Gagne, M., & Deci, E. L. (2005). Self-determination theory and work motivation. *Journal of Organizational Behavior*, *26*, 331–362.

Gardner, B. (2015). A review and analysis of the use of 'habit' in understanding, predicting and influencing health-related behaviour. *Health Psychology Review*, *9*(3), 277–295.

https://doi.org/10.1080/17437199.2013.876238

Gerber, H., & Hall, N. (2017). *Quantitative research design. In data acquisition - 1 day*. Pretoria: HR Statistics.

Gozli, D. G. (2017). Behaviour versus performance : The veiled commitment of experimental psychology. *Theory & Psychology*, 1–18. https://doi.org/10.1177/0959354317728130

Grimmer, K., & Bialocerkowski, A. (2005). Surveys. *Australian Journal of Physiotherapy*, *51*(3), 185–187. https://doi.org/10.1016/S0004-9514(05)70026-X

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal*, 1–23. https://doi.org/10.1111/isj.12202

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*(1), 242–251. https://doi.org/10.1016/j.cose.2012.10.003

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

Han, J., Jung, Y., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract : Examining a bilateral perspective. *Computers & Security*, *66*, 52–65. https://doi.org/10.1016/j.cose.2016.12.016

Hayenga, A. O., & Corpus, J. H. (2010). Profiles of intrinsic and extrinsic motivations: A person-centered approach to motivation and achievement in middle school. *Motivation and Emotion*, *34*(4), 371–383.

Henson, R. ., & Roberts, J. . (2006). Use of exploratory factor analysis in published research: Common errors and some comment on improved practise. *Educational and Psychological Measurement*, *66*(3), 393–416.

Herath, T., & Rao, H. R. (2009a). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hina, S., & Dominic, P. D. D. (2018). Information security policies ' compliance : a perspective for higher education institutions. *Journal of Computer Information*

Systems, 1–11. https://doi.org/10.1080/08874417.2018.1432996

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies : The Critical Role of Top Management and Organizational Culture. *Decision Sciences Journal*, *43*(4), 615–660.

Huang, H.-W., Parolia, N., & Cheng, K.-T. (2016). Willingness and ability to perform information security compliance behavior: Psychological ownership and self-efficacy perspective. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2016)*. Chiayi City, Taiwan: AIS Electronic Library.

Humaidi, N., & Balakrishnan, V. (2015). The Moderating Effect of Working Experience on Health Information System Security Policies. *Malaysian Journal of Computer Science*, *28*(2), 70–92.

Humaidi, N., & Balakrishnan, V. (2017). Indirect Effect of Management Support on Users' Compliance Behaviour Towards Information Security Policies. *Health Information Management Journal*, *47*(1), 17–27. https://doi.org/10.1177/1833358317700255

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282–293. https://doi.org/10.1016/j.chb.2017.12.022

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security Awareness : The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems*, *4417*. https://doi.org/10.1080/08874417.2019.1650676

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. (2013). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, *51*, 69–79.

Ifinedo, P. (2018). Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions. *Information Resources Management Journal*, *31*(1), 53–82. https://doi.org/10.4018/IRMJ.2018010103

ISO/IEC 27001. (2005). Information technology – Security techniques – Information security management systems – Requirements. *International Organization for Standardization*.

Jonker, J., & Pennink, B. (2010). *The Essence of Research Methodology: A Consice Guide for Master and PhD Students in Management Science* (1st ed.). Berlin Heidelberg, German: Springer-Verlag.

K, O. K., Heather, C., & Danielle, L. (2010). Scoping studies: advancing the methodology. *Implementation Science*, *5*(1), 69. https://doi.org/10.1186/1748-5908-5-69

Kadir, M. R. A., Norman, S. N. S., Rahman, S. A., & Ahmad, A. R. (2016). Information Security Policies Compliance among Employees in Cybersecurity Malaysia. In K. S. Soliman (Ed.), *Proceedings of the 28th International Business Information Management Association Conference* (pp. 2419–2430). Seville, Spain: International Business Information Management Association.

Karyda, M. (2017). Fostering information security culture in organizations : A research agenda. *Proceedings of the 11th Mediterranean Conference on Information Systems (MCIS 2017)*, 1–10. Genoa, Italy: AIS Electronic Library.

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with brazilian users. *Journal of Information Systems and Technology Management*, *13*(3), 479–496. https://doi.org/10.4301/S1807-17752016000300007

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non- compliance : Devising a Value-Based Compliance analysis method. *Journal of Strategic Information Systems*, *26*(1), 39–57. https://doi.org/10.1016/j.jsis.2016.08.005

Kothari, C. (2004). *Research methodology: methods and techniques* (2nd ed.). New Delhi: New Age International.

Kranz, J. J., & Haeussinger, F. J. (2014). Why deterrence is not enough : The role of endogenous motivations on employees ' information security behavior. In M. D. Myers & D. W. Straub (Eds.), *Proceedings of the International Conference on Information Systems - Building a Better World through Information Systems, (CIS) 2014* (pp. 1–14). Auckland, New Zealand: Association for Information Systems.

Krauss, S. E., & Putra, U. (2005). Research Paradigms and Meaning Making : A Primer. *The Qualitative Report*, *10*, 758–770. https://doi.org/10.1176/appi.ajp.162.10.1985

Kuppusamy, P., Narayana, G., & Maarop, N. (2020). Systematic Literature Review of Information Security Compliance Behaviour Theories. *Journal of Physics: Conference Series*, *1551*(1). https://doi.org/10.1088/1742-6596/1551/1/012005

Kwasnicka, D., Dombrowski, S. U., White, M., & Sniehotta, F. (2016). Theoretical explanations for maintenance of behaviour change: a systematic review of behaviour theories. *Health Psychology Review*, *10*(3), 277–296.

https://doi.org/10.1080/17437199.2016.1151372

Lazzeri, F. (2014). On defining behavior: Some notes. *Behavior and Philosophy*, *42*, 65–82. https://doi.org/0.1016/j.anbehav.2009.03.018

Lebek, B., Jörg, U., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior : a theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, S., Park, N. E., & Suk, J. (2019). The effects of consumers ' information security behavior and information privacy concerns on usage of IoT technology. *Proceedings of the XX International Conference on Human Computer Interaction*, 1–2. Donostia, Gipuzkoa, Spain: ACM.

Leedy, P. D., & Ormrod, J. E. (2015). *Practial Research Planning and Design* (11th ed.). Pearson Education Limited.

Legault, L. (2017). Self determination theory. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of personality and individual differences* (pp. 1–9). https://doi.org/10.1007/978-3-319-28099-8

Levitis, D. A., Lidicker, W. Z., & Freund, G. (2009). Behavioural biologists do not agree on what constitutes behaviour. *Animal Behaviour*, *78*(1), 103–110. https://doi.org/10.1016/j.anbehav.2009.03.018

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

Li, Y., Stafford, T., Fuller, B., & Ellis, S. (2017). Beyond Compliance: Empowering Employees' Extra-Role Security Behaviors in Dynamic Environments. *Proceedings of Twenty-Third Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation*, 1–5. Boston, USA: Association for Information Systems.

Lietz, P. (2008). *Questionnaire design in attitude and opinion research: Current state of an art*. 23. https://doi.org/ISSN 1866-0290

Lietz, P. (2010). Research into questionnaire design. *International Journal of Market Research*, *52*(2), 249–272. https://doi.org/10.2501/S147078530920120X

Lumley, T., Diehr, P., Emerson, S., & Chen, L. (2002). The Importance Of The Normality Assumption In Large Public Health Data Sets. *Annual Review of Public Health*, *23*, 151–169. https://doi.org/10.1146/annurev.publheath.23.100901.140546

Mani, D., Mubarak, S., Heravi, A., & Choo, K.K. R. (2015). Employees' intended information security behaviour in real estate organisations: A Protection Motivation perspective. *Proceedings of the 21st Americas Conference on Information Systems*

(AMCIS 2015), 1–11. Fajardo, Puerto Rico: Association for Information Systems.

Marczyk, G., Fertinger, D., & De Matteo, D. (2005). *Essentials of research design and methodology*. Hoboken, New Jersey, USA: John Wiley & Sons.

Matsumoto, D. (Ed.). (2012). *The Cambridge Dictionary of Psychology*. Cambridge, New York: Cambridge University Press.

Mayer, P., Kunz, A., & Volkamer, M. (2017). Reliable behavioural factors in the information security context. *Proceedings of the 12th International Conference on Availability, Reliability and Security - (ARES '17)*, 1–10. Reggio Calabria, Italy: ACM.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Academia and Clinic Annals of Internal Medicine Preferred Reporting Items for Systematic Reviews and Meta-Analyses : *Annals of Internal Medicine*, *151*(4), 264–269.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model Of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

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*, 126–139. https://doi.org/10.1057/ejis.2009.10

Nasir, A., Rashid, M., & Hamid, A. (2017). Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture : A Conceptual Framework. *Proceedings of the 2017 International Conference on Information System and Data Mining*, 56–60. Charleston, SC, USA: Association for Computing Machinery.

Nicholas, W. (2010). *Research Methods: The Basics*. London: Routledge Taylor & Francis Group.

Niemimaa, M., Laaksonen, A. E., & Harnesk, D. (2013). Interpreting Information Security Policy Outcomes: A Frames of Reference Perspective. In R. H. J. Sprague (Ed.), *Proceedings of the 46th Hawaii International Conference on System Sciences* (pp. 4541–4550). Wailea, Maui, HI USA: IEEE.

NIST. (2011). Managing Information Security Risk. In *Nist Special Publication*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

NIST. (2017). Security and privacy controls for federal information systems and organizations: National Institute of Standards and Technology. In *Draft NIST Special Publication 800-53 Revision 5*. Gaithersburg, MD, USA.

Norman, G. (2010). Likert scales , levels of measurement and the "" laws "" of statistics.

Advances in Health Science Education, *15*, 625–632.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

O’Rourke, N., & Hatcher, L. (2013). *A step-by-step approach to using SAS for factor analysis and structural equation*. Cary, NC: SAS Institute.

Oates, B. J. (2006). *Researching information systems and computing*. London: Sage.

Ofori, K. S., Anyigba, H., Ampong, G. O. A., Omoregie, O. K., Nyamadi, M., & Fianu, E. (2020). Factors Influencing Information Security Policy Compliance Behavior. In W. Yaokumah, M. Rajarajan, J. Abdulai, I. Wiafe, & F. A. Katsriku (Eds.), *Modern Theories and Practices for Cyber Ethics and Security Compliance* (pp. 152–171). https://doi.org/10.4018/978-1-7998-3149-5.ch010

Osborne, J. W., & Costello, A. B. (2009). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Pan-Pacific Management Review*, *12*(2), 131–146.

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

Padayachee, K. (2012). Taxonomy of Compliant Information Security Behavior. *Computers and Security*, *31*(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004

Pahnila, S., Karjalainen, M., & Mikko, S. (2013). Information security behavior: Towards multi-stage models. In J.-N. Lee, J.Y. Mao, & J. Y. L. Thong (Eds.), *Proceedings of the Pacific Asia Conference on Information Systems 2013 (PACIS 2013)*. Jeju Island, Korea: AIS Electronic Library.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which Factors Explain Employees’ Adherence to Information Security Policies? An Empirical Study. *Pacific Asia Conference on Information Systems, PACIS 2007*. Auckland, New Zealand: AIS Electronic Library.

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 and Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

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

Pattinson, M., Butavicius, M., Parsons, K., Mccormac, A., & Jerram, C. (2015). Examining attitudes toward information security behaviour using mixed methods. In N. L. C. Steven Furnell (Ed.), *Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)* (pp. 57–70). University of Plymouth.

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Boston, MA, USA: Prentice Hall.

Pfleeger, L. S., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489–510. https://doi.org/10.1515/jhsem-2014-0035

Ponemon Institute. (2020). *2020 Cost of Insider Threats Global Report*. Retrieved from https://www.observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R., & Lowry, P. B. (2013). Insiders' Protection of Organizational Information Assets: Development of a Systematics-based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Quarterly*, *37*(4), 1189–1210.

PriceWaterhouseCoopers. (2018). The Global State of Information Security Survey 2018: PwC. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

PRISMA. (2015). PRISMA Statement. Retrieved from http://www.prisma-statement.org/Extensions/

Rattray, J., & Jones, M. C. (2007). Essential elements of questionnaire design and development. *Journal of Clinical Nursing*, *16*(2), 234–243. https://doi.org/10.1111/j.1365-2702.2006.01573.x

Reeve, J. (2006). *What Teachers Say and Do to Support Students ' Autonomy During a Learning Activity*. *98*(1), 209–218. https://doi.org/10.1037/0022-0663.98.1.209

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in Information Security: Its Influence on end Users' information security Practice Behavior. *Computers and Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Roberts, P., & Priest, H. (2006). Reliability and validity in research. *Nursing Standard*, *20*(44), 41–45.

Ryan, M. R., & Deci, L. E. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, *55*(1), 68–78.

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

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). Essex: Pearson Education Limited.

Schein, E. (1971). The Individual, the Organization, and the Career - A Conceptual Scheme. *Journal of Applied Behavioural Science*, *7*(4), 401–426.

Security Centre for Internet. (2017). The CIS Critical Security Controls for Effective Cyber Defense - version 7. Retrieved April 17, 2019, from The CIS Critical Security Controls for Effective Cyber Defense - version 7 website: https://www.cisecurity.org/controls/

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Signh, Y. K. (2006). *Fundamental of Research Mthodology and Statistics*. New Delhi: New Age International limited.

Sikolia, D., & Biros, D. (2016). Motivating Employees to Comply with Information Security Policies Security Policies. *Proceedings of the Eleventh Midwest Association for Information Systems Conference*, 1–7. Milwaukee, Wisconsin, USA: AIS Electronic Library.

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

Siponen, M., Pahnila, S., & Adam Mahmood, M. (2010). Compliance with Information Security Policies: An Empirical Investigation. *IEEE Computer Society*, *43*(2), 64–71.

Siponen, M., & Puhakainen, P. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778.

Snyman, D., & Kruger, H. A. (2020a). External Contextual Factors in Information Security Behaviour. *Proceedings of the The 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*. Valleta, Malta: SCITEPRESS Digital Library.

Snyman, D., & Kruger, H. A. (2020b). A management decision support system for evaluating information security behaviour. In H. Venter, M. Loock, M. Coetzee, M. Eloff, & J. Eloff (Eds.), *Proceedings of the 18th International Conference on Information Security, ISSA 2019*. Johannesburg, South Africa: Springer.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management and Computer Security*, *22*(1), 42–75. https://doi.org/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*, 1–10. https://doi.org/10.1080/08874417.2017.1368421

Son, J. Y. (2011). Out of fear or desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies. *Information and Management*, *48*(7), 296–302. https://doi.org/10.1016/j.im.2011.07.002

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stage, H., & Fedotov, S. (2018). Anomalous cumulative inertia in human behaviour. *ArXiv:1806.00613 [Physics.Soc-Ph]*. Retrieved from http://arxiv.org/abs/1806.00613

Stevens, J. P. (2002). *Applied multivariate statistics for the social sciences* (4th ed.). Hillsdale: NJ: Erlbaum.

Swartz, P., Da Veiga, A., & Martins, N. (2019). A conceptual privacy governance framework. *Proceeding of the 2019 Conference on Information Communications Technology and Society (ICTAS)*, 1–6. Durban, South Africa: IEEE.

Tileubayeva, M. S., Massalimova, A. R., Kaufman, J. C., & Fernandez, M. V. C. (2017). The problems of thinking about mind , body and experience. *Psychology and Sociology Series*, *1*(60), 111–117.

Torres, C. I., & Crossler, R. E. (2019). Rhetorical Appeals and Legitimacy Perceptions: How To Induce Information Security Policy Compliance. *Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy*, 1–10. Munich, German: AIS E-Library.

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

UNISA. (2016). *Policy on research ethics*. Pretoria, South Africa.

Vallerand, R. J. (2012). From motivation to passion: In search of the motivational processes involved in a meaningful life. *Canadian Psychology/Psychologie Canadienne*, *53*(1), 42–52. https://doi.org/10.1037/a0026377

Vance, A., & Siponen, M. (2010). Neutralizaiton: New Insights into the Problem of Employee Information Systems Security. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/Article

Wahyuni, D. (2012). The Research Design Maze : Understanding Paradigms , Cases , Methods and Methodologies. *Journal of Applied Management Accounting Research*, *10*, 69–80. https://doi.org/10.2139/ssrn.2103082

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy. *Journal of Information Privacy & Security*, *9*(4), 52–79.

Wang, Q. (2015). Intrinsic Motivation: A Cultural Perspective. *International Encyclopedia of the Social & Behavioral Sciences*, *12*, 696–701. https://doi.org/10.1016/B978-0-08-097086-8.92142-1

Williams, B., Onsman, A., & Brown, T. (2010). Exploratory factor analysis: A five-step guide for novices. *Journal of Emergency Primary Health Care*, *8*(3), 1–13.

Willison, R., & Merrill, W. (2013). Beyond Deterrence: An Expanded view of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20.

Woo, C., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education , training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*(2018), 107–118. https://doi.org/10.1016/j.dss.2018.02.009

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*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Yazdanmehr, A., & Wang, J. (2015). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*. https://doi.org/10.1016/j.dss.2016.09.009

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36–46. https://doi.org/10.1016/j.dss.2016.09.009

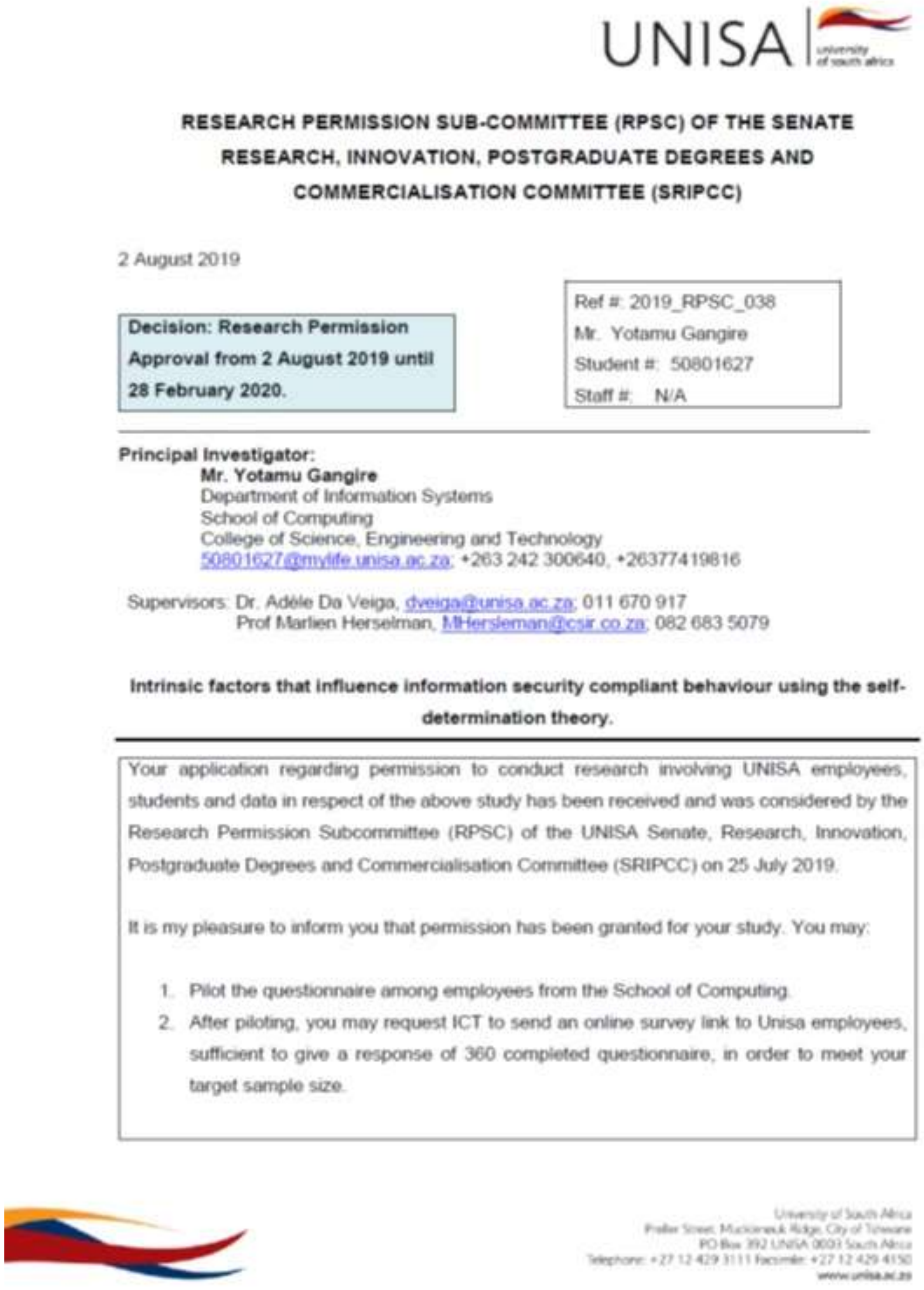
Yong, A. G., & Pearce, S. (2013). A beginner ' s guide to factor analysis : Focusing on exploratory factor analysis. *Tutorials in Quantitative Methods for Psychology*, *9*(2), 79–94.

Zohar, D., Huang, Y., Lee, J., & Robertson, M. M. (2015). Testing extrinsic and intrinsic motivation as explanatory variables for the safety climate–safety performance relationship among long-haul truck drivers. *Transportation Research Part F: Traffic*

Psychology and Behaviour, *30*, 84–96. https://doi.org/10.1016/j.trf.2015.01.014

APPENDICES

Appendix A: Research permission



RESEARCH PERMISSION SUB-COMMITTEE (RPSC) OF THE SENATE RESEARCH, INNOVATION, POSTGRADUATE DEGREES AND COMMERCIALISATION COMMITTEE (SRIPCC)

2 August 2019

Decision: Research Permission Approval from 2 August 2019 until 28 February 2020.

Ref #: 2019_RPSC_038
Mr. Yotamu Gangire
Student #: 50801627
Staff #: N/A

Principal Investigator:
Mr. Yotamu Gangire
Department of Information Systems
School of Computing
College of Science, Engineering and Technology
50801627@mylife.unisa.ac.za; +263 242 300640, +26377419816

Supervisors: Dr. Adèle Da Veiga, dveiga@unisa.ac.za; 011 670 917
Prof Marlien Herselman, MHersleman@csir.co.za; 082 683 5079

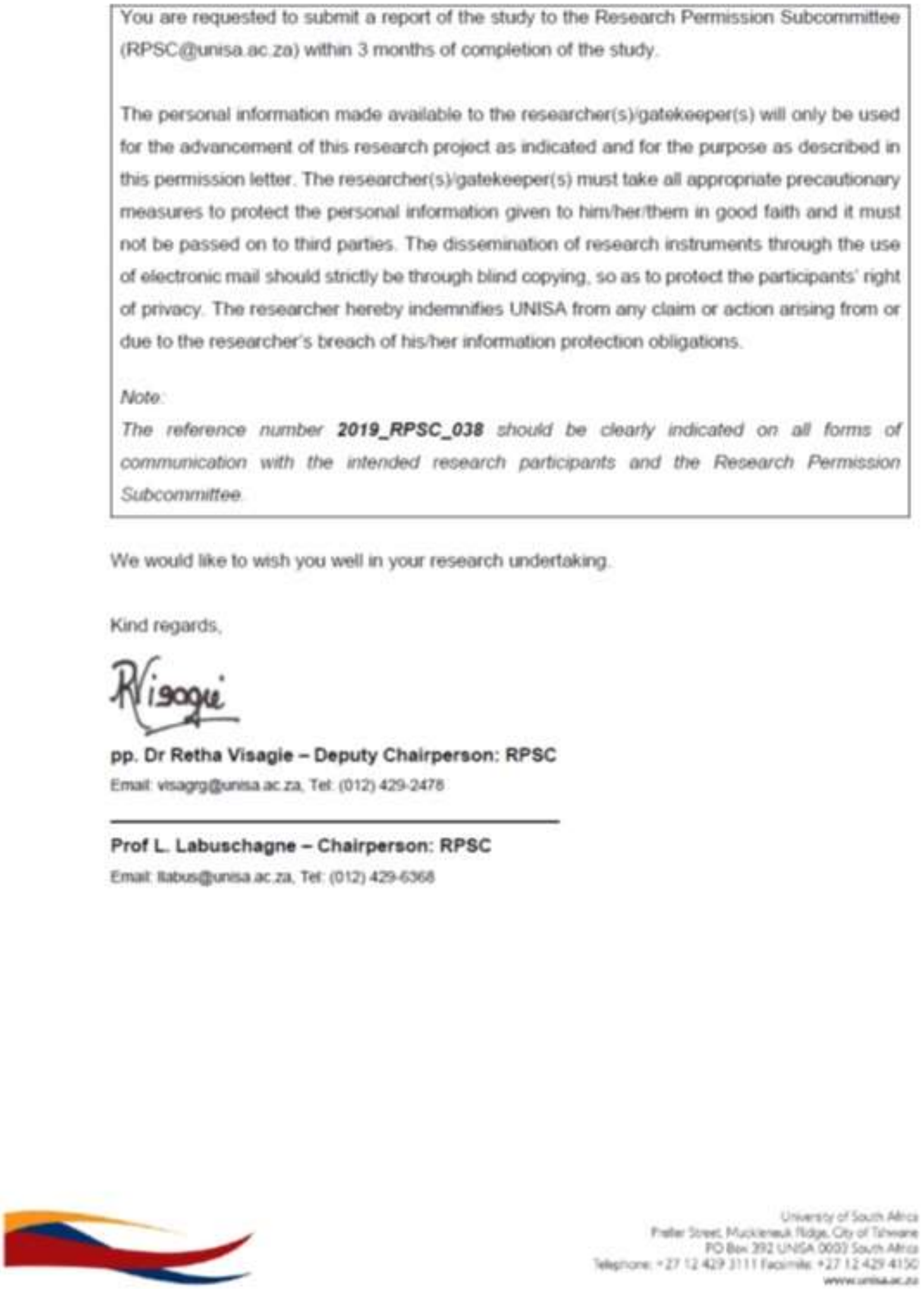
Intrinsic factors that influence information security compliant behaviour using the self-determination theory.

Your application regarding permission to conduct research involving UNISA employees, students and data in respect of the above study has been received and was considered by the Research Permission Subcommittee (RPSC) of the UNISA Senate, Research, Innovation, Postgraduate Degrees and Commercialisation Committee (SRIPCC) on 25 July 2019.

It is my pleasure to inform you that permission has been granted for your study. You may:

1. Pilot the questionnaire among employees from the School of Computing.
2. After piloting, you may request ICT to send an online survey link to Unisa employees, sufficient to give a response of 360 completed questionnaire, in order to meet your target sample size.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za



You are requested to submit a report of the study to the Research Permission Subcommittee (RPSC@unisa.ac.za) within 3 months of completion of the study.

The personal information made available to the researcher(s)/gatekeeper(s) will only be used for the advancement of this research project as indicated and for the purpose as described in this permission letter. The researcher(s)/gatekeeper(s) must take all appropriate precautionary measures to protect the personal information given to him/her/them in good faith and it must not be passed on to third parties. The dissemination of research instruments through the use of electronic mail should strictly be through blind copying, so as to protect the participants' right of privacy. The researcher hereby indemnifies UNISA from any claim or action arising from or due to the researcher's breach of his/her information protection obligations.

Note:

The reference number ***2019_RPSC_038*** *should be clearly indicated on all forms of communication with the intended research participants and the Research Permission Subcommittee.*

We would like to wish you well in your research undertaking.

Kind regards,

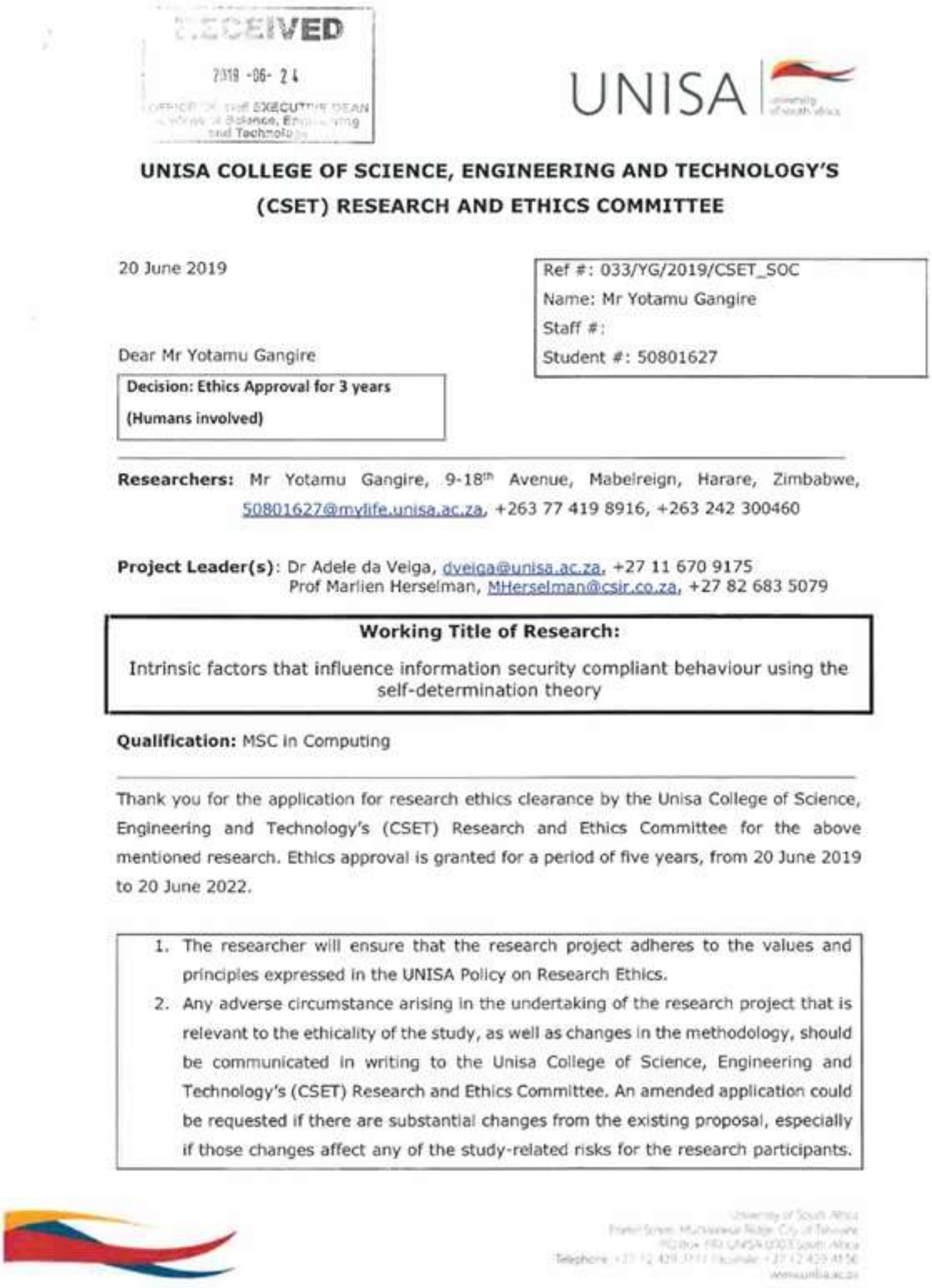
pp. Dr Retha Visagie – Deputy Chairperson: RPSC

Email: visagrg@unisa.ac.za, Tel: (012) 429-2478

Prof L. Labuschagne – Chairperson: RPSC

Email: llabus@unisa.ac.za, Tel: (012) 429-6368

Appendix B: Ethical clearance



UNISA university of south africa

UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) RESEARCH AND ETHICS COMMITTEE

20 June 2019

Ref #: 033/YG/2019/CSET_SOC
Name: Mr Yotamu Gangire
Staff #:
Student #: 50801627

Dear Mr Yotamu Gangire

Decision: Ethics Approval for 3 years
(Humans involved)

Researchers: Mr Yotamu Gangire, 9-18th Avenue, Mabelreign, Harare, Zimbabwe, 50801627@mylife.unisa.ac.za, +263 77 419 8916, +263 242 300460

Project Leader(s): Dr Adele da Veiga, dveiga@unisa.ac.za, +27 11 670 9175
Prof Marlien Herselman, MHerselman@csir.co.za, +27 82 683 5079

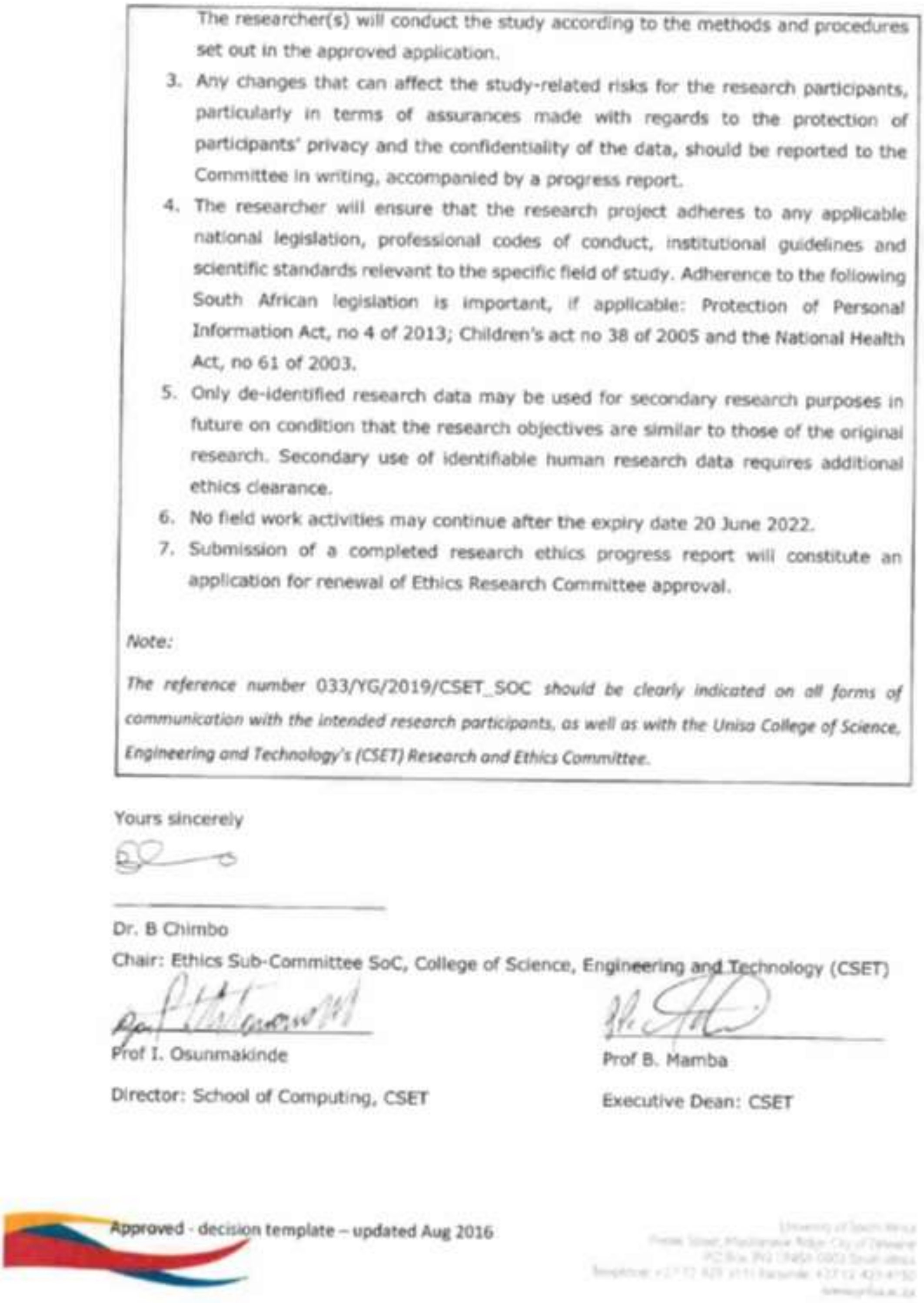
Working Title of Research:

Intrinsic factors that influence information security compliant behaviour using the self-determination theory

Qualification: MSC in Computing

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee for the above mentioned research. Ethics approval is granted for a period of five years, from 20 June 2019 to 20 June 2022.

1. The researcher will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee. An amended application could be requested if there are substantial changes from the existing proposal, especially if those changes affect any of the study-related risks for the research participants.



The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.

3. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
4. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
5. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
6. No field work activities may continue after the expiry date 20 June 2022.
7. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number 033/YG/2019/CSET_SOC *should be clearly indicated on all forms of communication with the intended research participants, as well as with the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee.*

Yours sincerely

Dr. B Chimbo

Chair: Ethics Sub-Committee SoC, College of Science, Engineering and Technology (CSET)

Prof I. Osunmakinde

Director: School of Computing, CSET

Prof B. Mamba

Executive Dean: CSET

Appendix C: Expert panel questionnaire

Please make sure that you have read the participant information sheet and signed the consent form prior to completing the questionnaire.

Information and definition section
It is fully acknowledged that you receive many requests to participate in surveys as a professional in your field. Therefore, your participation in this very important survey is sincerely appreciated.
The questionnaires consist of two sections, namely section one where information about the expert panel is requested and section two with the competence, relatedness and autonomy questions. We require the expert panel to indicate for each question whether they believe the item is essential to include or not and whether it is clear or not.
Below some definitions.
Definition 1: Competence **-** Seek to control the outcome and experience mastery. Gain mastery of tasks, learn new skills

Definition 2: Relatedness - Is the universal want to interact, be connected to, and experience caring for others, belonging and attachment to other people

Definition 3: Autonomy - Is the universal urge to be causal agents of one's own life and act in harmony with one's integrated self. Feel in control of behaviour and goals.
The questionnaire comprises of 73 components from three dimensions as follows:
A - 21- Competence
B - 21 - Relatedness
C - 21 - Autonomy

On the next page please find the questionnaire. Completion is expected to take no more than 20 minutes.

Section 1: Expert panel information

We require some background information about the experts involved in reviewing the questionnaire and would appreciate if you can please complete the questions below.

i. What is your field of expertise (e.g. IT technician, legal, academic, privacy consultant)?
____

ii. What is your current job title?
____

iii. What experience do you have in information security research?
____

iv. How many years’ experience do you have in information security research?
____

v. What experience do you have in research methods?

____

vi. How many years’ experience do you have in services/work relating to research methods?
____

vii. What is your highest qualification?
____

The survey is conducted to determine the perceptions of employees (competence, relatedness and autonomy) for information security aspects.

Instructions
Please provide your review responses, starting on the next page.
Section 2: A comment box is provided in section 2 for general comments about the biographical section which the expert panel would like the researchers to consider or amend in order to improve the questionnaire.
Section 3: Section 3 comprises of competence statements. Indicate with a tick (✔) as to whether you believe the statement is essential to include or not and whether it is clear or not.
Section 4: Section 3 comprises of relatedness statements. Indicate with a tick (✔) as to whether you believe the statement is essential to include or not and whether it is clear or not.
Section 5 Section 3 comprises of autonomy statements. Indicate with a tick (✔) as to whether you believe the statement is essential to include or not and whether it is clear or not.

A comment box is provided at the end of each of sections 3, 4 & 5 for general comments about the statements which the expert panel would like the researchers to consider or amend in order to improve the questionnaire.

Section 2: Biographical information (to the employee – check for relevancy)

We require some background information and would appreciate if you can please complete the questions below.
Instructions
Please provide one response to each item in the questionnaire.
Indicate with a tick (✔) for your selection

Section 2: Biographical Information							
1	Gender	Male			Female		
2	Age	18 – 25	26 – 35	36 – 45	46 - 55	Above 55	
3	Highest Level of Education	High School	Certificate	Diploma	Degree	Postgraduate	
4	Length of service	Less than 1	1 - 5	6 - 10	11 - 15	16 - 20	20 and above

Expert panel feedback for biographical section:

Section 3 Competence questions

Section 3: Perceived Competence							Expert panel select answer here			
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
5	I am capable of using different passwords for social media and work accounts.									
6	I feel able to meet the challenge of never sharing my work passwords with colleagues.									
7	I am confident in my ability to mix letters number and symbols in work passwords.									
7	I am confident in my ability to only click on links in emails from people I know.									
8	I am confident in my ability to avoid clicking on links in emails from people I do not know.									
10	I am confident in my ability to avoid opening attachments in emails from people I do not know.									
11	I am able to identify when it is risky to download files onto my computer if they help with my job									
12	I am confident in my ability to avoid accessing dubious websites.									
13	I am confident of my ability to assess the safety of a website before entering information online.									
14	I am confident in my ability to review the privacy settings of my social media accounts.									
15	I am capable of considering the negative consequences before posting anything on social media.									
16	I am confident in my ability to avoid posting risk information about work on social media.									
17	I feel confident in my ability to keep my laptop with me all the time when working in a public place.									
18	I am confident of how not to send sensitive work files over a public Wi-Fi network.									
19	I am capable of shielding, from strangers, my computer screen when working on a sensitive document.									
20	I am confident in my ability to dispose of sensitive printout by shredding or destroying them									

21	I am confident in my ability to avoid inserting a USB stick I found in a public place into work.									
22	I am confident in my ability to remove printouts with sensitive information on my desk when leaving									
23	I am confident in my ability to report any suspicious behaviour if I noticed it.									
24	I am confident about my abilities to notice poor security behaviour by colleagues.									
25	I am confident in my ability to report any security incidents if noticed it.									

Section 4: Perceived Relatedness							Expert panel select answer here			
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
26	I am influenced by my work colleagues to use different passwords for social media and work accounts because I get along with them.									
27	I am influenced by my work colleagues to never sharing my work passwords with colleagues.									
28	I am encouraged by work colleagues to use a mixture of letters number and symbols in work passwords.									
29	I am influenced by work colleagues to only click on links in emails from people I know.									
30	I am influenced by work colleagues to avoid clicking on links in emails from people I do not know.									
31	I am influenced by work colleagues to avoid opening attachments in emails from people I do not know.									
32	I am influenced by work colleagues to understand that it can be risky to download files on a work computer.									
33	I am influenced by work colleagues to avoid accessing dubious websites.									
34	I am influenced by my work colleagues to assess the safety of a website before entering information online.									
35	I am influenced by my work colleagues to review the privacy settings of my social media accounts.									
36	I am influenced by my work colleagues to consider the negative consequences before posting anything on social media.									

37	I am influenced by my work colleagues to avoid posting risk information about work on social media.									
38	I am influenced by my work colleagues to keep my laptop with me all the time when working in a public place.									
39	I am influenced by my work colleagues to avoid sending sensitive work files over a public Wi-Fi network.									
40	I am influenced by my work colleagues to shield my computer screen from strangers when working on a sensitive document.									
41	I am influenced by my work colleagues to dispose of sensitive printout by shredding or destroying them									
42	I am influenced by my work colleagues to avoid inserting a USB stick I found in a public place into work computer.									
43	I am influenced by my work colleagues to remove printouts with sensitive information on my desk when leaving									
44	I am influenced by my work colleagues to report any suspicious behaviour if noticed it.									
45	I am influenced by my work colleagues to notice poor security behaviour by colleagues.									
46	I am influenced by my work colleagues to report any security incidents if noticed it.									

Section 4: Perceived Autonomy							Expert panel select answer here			
		Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**Not essential**	**Essential**	**Item is clear**	**Item is unclear**
47	I choose to use different passwords for social media and work accounts because the actions are congruent with who I am.									
48	I never share my work passwords with my colleagues because I have to follow instructions									
49	I choose to mix letters number and symbols in work passwords.									
50	I choose to only click on links in email from people I know.									
51	I do not feel pressured to avoid clicking on links in emails from people I do not know.									
52	I do not feel pressured to avoid opening attachments in emails from people I do not know.									
53	I choose not to download risky files onto my computer.									
54	I freely avoid accessing dubious websites.									
55	It is my choice to assess the safety of a website before entering information.									
56	I choose to review the privacy settings of my social media accounts.									
57	I consider the negative consequences before posting anything on social media because it is congruent with who I am									
58	It is my choice to avoid posting risky information about work on social media.									
59	I choose to keep my laptop with me all the time when working in a public place.									
60	It is my choice to send sensitive work files using a public Wi-Fi network.									
61	I choose to shield, from strangers, my computer screen when working on a sensitive document.									
62	I choose to dispose of sensitive printout by shredding or destroying them.									

63	I choose not to insert a USB stick I found in a public place into a work computer.									
64	I choose not to leave printouts with sensitive information on my desk overnight.									
65	I choose to report any suspicious behaviour if noticed it.									
66	I choose to notice poor security behaviour by colleagues.									
67	I choose to report any security incidents if noticed it.									

Expert panel feedback for questionnaire statements (e.g. aspects to revise, add, amend,

Thank you for completing the questionnaire

Appendix D: Informed Consent form

CONSENT TO PARTICIPATE IN THIS STUDY

EXPERT PANEL

I, __________________ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the processing of my feedback for the review of the questionnaire as part of the expert panel.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname……………………………………………. (please print)
Participant Signature……………………………………………..Date…………………

Researcher's Name & Surname: **Yotamu Gangire**

Researcher's signature………… ………………………Date**: 07 June 2019**

CONSENT TO PARTICIPATE IN THIS STUDY

PILOT GROUP

I, __________________ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the processing of my answers in completing the questionnaire for the pilot group.

I have received a signed copy of the informed consent agreement.

Participant Name& Surname…………………………………………… (please print)
Participant Signature……………………………………………..Date…………………

Researcher's Name & Surname: **Yotamu Gangire**

Researcher's signature………… ……………………Date: **07 June 2019**

Appendix E: Pilot group questionnaire

Please make sure that you have read the participant information sheet and signed the consent form prior to completing the questionnaire.

Information and definition section
It is fully acknowledged that you might have received many requests to participate in surveys as a university student in your field. Therefore, your participation in this very important survey is sincerely appreciated. The questionnaire consists of two sections, namely section one where biographical information is requested and section 2 - 5 with perceptions of employees (competence, relatedness and autonomy) for information security aspects questions.

Below some definitions.
Definition 1: Competence - Seek to control the outcome and experience mastery. Gain mastery of tasks, learn new skills

Definition 2: Relatedness - Is the universal want to interact, be connected to, and experience caring for others, belonging and attachment to other people

Definition 3: Autonomy - Is the universal urge to be causal agents of one's own life and act in harmony with one's integrated self. Feel in control of behaviour and goals.

On the next page please find the questionnaire. Completion is expected to take no more than 20 minutes.

Section 1: Biographical information

We require some background information and would appreciate if you can please complete the questions below.

Instructions
Please provide one response to each item in the questionnaire.
Indicate with a tick (✔) for your selection

Section 1: Biographical Information							
1	Gender	Male			Female		
2	Age	18 – 25	26 – 35	36 – 45	46 - 55	Above 55	
3	Highest Level of Education	High School	Certificate	Diploma	Degree	Postgraduate	
4	Length of service	Less than 1	1 - 5	6 - 10	11 - 15	16 - 20	20 and above

Section 2: Perceived Competence

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
5	I am capable of using different passwords for social media and work accounts.					
6	I feel able to meet the challenge of never sharing my work passwords with colleagues.					
7	I am confident in my ability to mix letters number and symbols in work passwords.					
7	I am confident in my ability to only click on links in emails from people I know.					
8	I am confident in my ability to avoid clicking on links in emails from people I do not know.					
10	I am confident in my ability to avoid opening attachments in emails from people I do not know.					
11	I am able to identify when it is risky to download files onto my computer if they help with my job					
12	I am confident in my ability to avoid accessing dubious websites.					
13	I am confident of my ability to assess the safety of a website before entering information online.					
14	I am confident in my ability to review the privacy settings of my social media accounts.					
15	I am capable of considering the negative consequences before posting anything on social media.					
16	I am confident in my ability to avoid posting risk information about work on social media.					
17	I feel confident in my ability to keep my laptop with me all the time when working in a public place.					
18	I am confident of how not to send sensitive work files over a public Wi-Fi network.					
19	I am capable of shielding, from strangers, my computer screen when working on a sensitive document.					
20	I am confident in my ability to dispose of sensitive printout by shredding or destroying them					
21	I am confident in my ability to avoid inserting a USB stick I found in a public place into work.					
22	I am confident in my ability to remove printouts with sensitive information on my desk when leaving					
23	I am confident in my ability to report any suspicious behaviour if I noticed it.					
24	I am confident about my abilities to notice poor security behaviour by colleagues.					
25	I am confident in my ability to report any security incidents if noticed it.					

Section 3: Perceived Relatedness

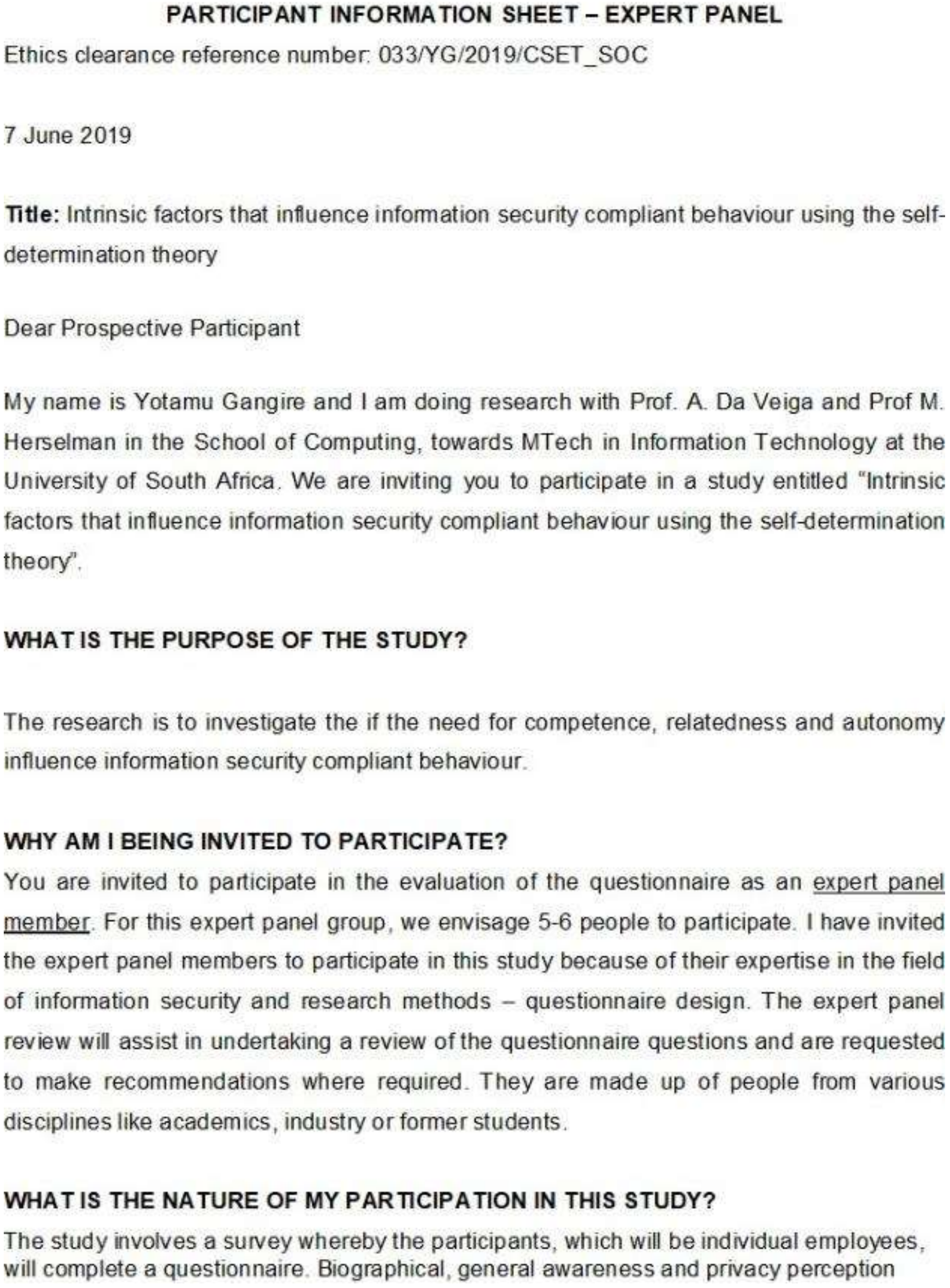
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
26	I am influenced by my work colleagues to use different passwords for social media and work accounts because I get along with them.					
27	I am influenced by my work colleagues to never sharing my work passwords with colleagues.					
28	I am encouraged by work colleagues to use a mixture of letters number and symbols in work passwords.					
29	I am influenced by work colleagues to only click on links in emails from people I know.					
30	I am influenced by work colleagues to avoid clicking on links in emails from people I do not know.					
31	I am influenced by work colleagues to avoid opening attachments in emails from people I do not know.					
32	I am influenced by work colleagues to understand that it can be risky to download files on work computer.					
33	I am influenced by work colleagues to avoid accessing dubious websites.					
34	I am influenced by my work colleagues to assess the safety of a website before entering information online.					
35	I am influenced by my work colleagues to review the privacy settings of my social media accounts.					
36	I am influenced by my work colleagues to consider the negative consequences before posting anything on social media.					
37	I am influenced by my work colleagues to avoid posting risk information about work on social media.					
38	I am influenced by my work colleagues to keep my laptop with me all the time when working in a public place.					
39	I am influenced by my work colleagues to avoid sending sensitive work files over a public Wi-Fi network.					
40	I am influenced by my work colleagues to shield my computer screen from strangers when working on a sensitive document.					
41	I am influenced by my work colleagues to dispose of sensitive printout by shredding or destroying them					
42	I am influenced by my work colleagues to avoid inserting a USB stick I found in a public place into a work computer.					
43	I am influenced by my work colleagues to remove printouts with sensitive information on my desk when leaving					
44	I am influenced by my work colleagues to report any suspicious behaviour if noticed it.					
45	I am influenced by my work colleagues to notice poor security behaviour by colleagues.					
46	I am influenced by my work colleagues to report any security incidents if noticed it.					

Section 4: Perceived Autonomy

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
47	I choose to use different passwords for social media and work accounts because the actions are congruent with who I am.					
48	I never share my work passwords with my colleagues because I have to follow instructions					
49	I choose to mix letters number and symbols in work passwords.					
50	I choose to only click on links in email from people I know.					
51	I do not feel pressured to avoid clicking on links in emails from people I do not know.					
52	I do not feel pressured to avoid opening attachments in emails from people I do not know.					
53	I choose not to download risky files onto my computer.					
54	I freely avoid accessing dubious websites.					
55	It is my choice to assess the safety of a website before entering information.					
56	I choose to review the privacy settings of my social media accounts.					
57	I consider the negative consequences before posting anything on social media because it is congruent with who I am					
58	It is my choice to avoid posting risky information about work on social media.					
59	I choose to keep my laptop with me all the time when working in a public place.					
60	It is my choice to send sensitive work files using a public Wi-Fi network.					
61	I choose to shield, from strangers, my computer screen when working on a sensitive document.					
62	I choose to dispose of sensitive printout by shredding or destroying them.					
63	I choose not to insert a USB stick I found in a public place into work computer.					
64	I choose not to leave printouts with sensitive information on my desk overnight.					
65	I choose to report any suspicious behaviour if noticed it.					
66	I choose to notice poor security behaviour by colleagues.					
67	I choose to report any security incidents if noticed it.					

Thank you for completing the survey!

Appendix F: Participant information sheet



PARTICIPANT INFORMATION SHEET – EXPERT PANEL

Ethics clearance reference number: 033/YG/2019/CSET_SOC

7 June 2019

Title: Intrinsic factors that influence information security compliant behaviour using the self-determination theory

Dear Prospective Participant

My name is Yotamu Gangire and I am doing research with Prof. A. Da Veiga and Prof M. Herselman in the School of Computing, towards MTech in Information Technology at the University of South Africa. We are inviting you to participate in a study entitled "Intrinsic factors that influence information security compliant behaviour using the self-determination theory".

WHAT IS THE PURPOSE OF THE STUDY?

The research is to investigate the if the need for competence, relatedness and autonomy influence information security compliant behaviour.

WHY AM I BEING INVITED TO PARTICIPATE?

You are invited to participate in the evaluation of the questionnaire as an expert panel member. For this expert panel group, we envisage 5-6 people to participate. I have invited the expert panel members to participate in this study because of their expertise in the field of information security and research methods – questionnaire design. The expert panel review will assist in undertaking a review of the questionnaire questions and are requested to make recommendations where required. They are made up of people from various disciplines like academics, industry or former students.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves a survey whereby the participants, which will be individual employees, will complete a questionnaire. Biographical, general awareness and privacy perception type of questions are included in the questionnaire. The expert panel is invited to review the questionnaire questions prior to the phase whereby the pilot group survey and the final survey are sent out to students.

The expected review time for the expert panel is 1-2 weeks. During this time the expert panel will be given an opportunity to review the questionnaire and to give input.

Participation to review the questionnaire questions will not take up any more than 20 minutes of the expert panel member's time.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. The survey will use a pseudonym for the expert panel members in order to protect their confidentiality and to preserve their privacy.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the privacy of student personal information in the participating university from a research perspective. It is anticipated that the information we gain from this survey will help us to develop a comprehensive Information Security Compliant Behaviour Model based on the Self-determination theory questionnaire.

ARE THEIR ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

We do not foresee that you will experience any negative consequences by completing the survey. The survey is anonymous no personal identifiable information will be collected.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

A pseudonym will be recorded and used for the expert panel members. Your feedback will be given a pseudonym and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings. No individual participants will be identifiable in any publications.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

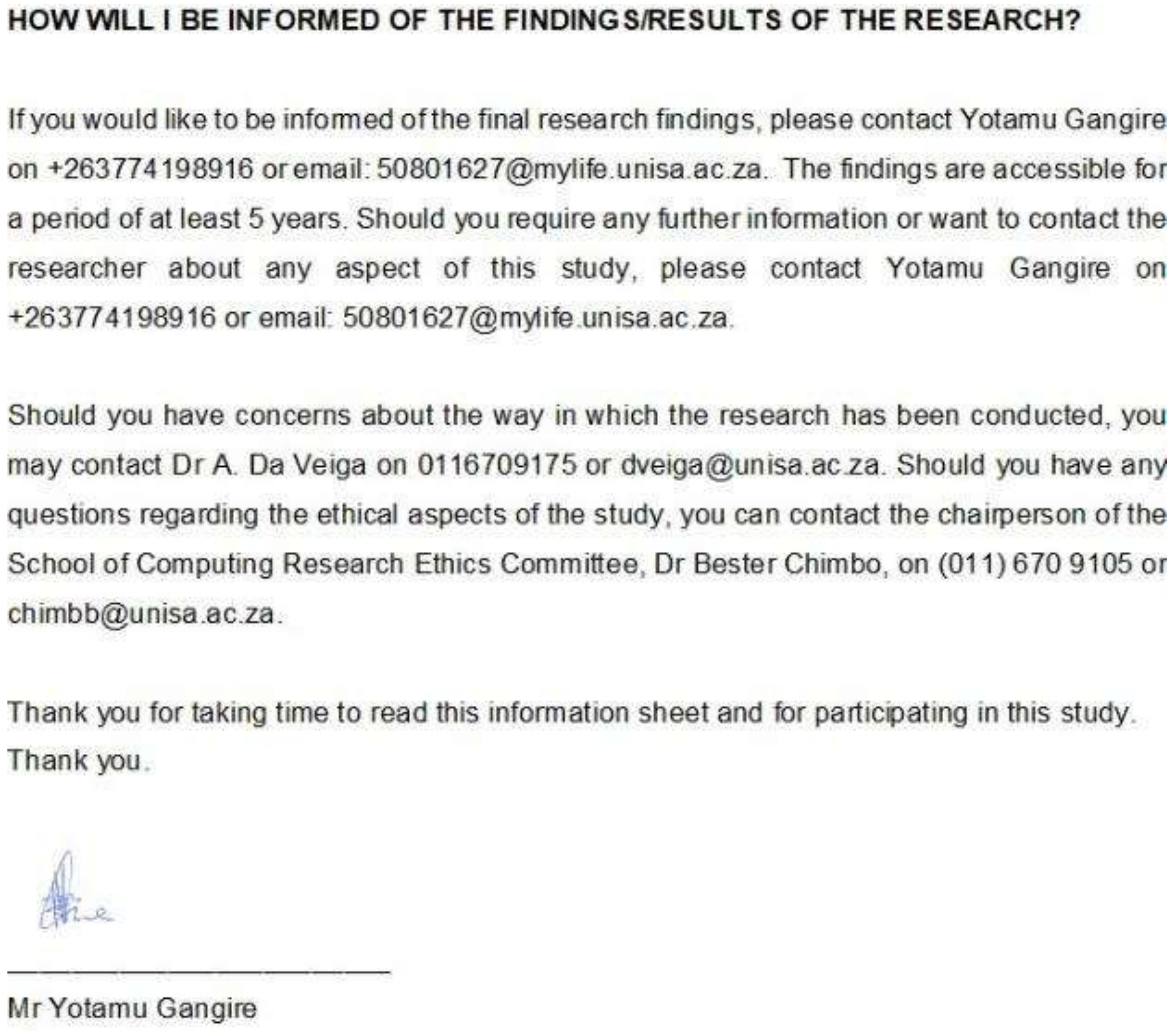
Hard copies of your answers will be stored by the researcher for a minimum period of five years in a locked cupboard/filing cabinet at the student's premises and/or Unisa for future research or academic purposes; electronic information will be stored on a password protected computer. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Hard copies will be shredded and data will be permanently deleted from the survey application database files and hard drive of the computer through the use of a relevant software application once the purpose has been achieved.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the protection of student personal information in Zimbabwean universities from a research perspective. You will not be reimbursed or receive any incentives for your participation in the survey.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the School of Computing, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.



HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

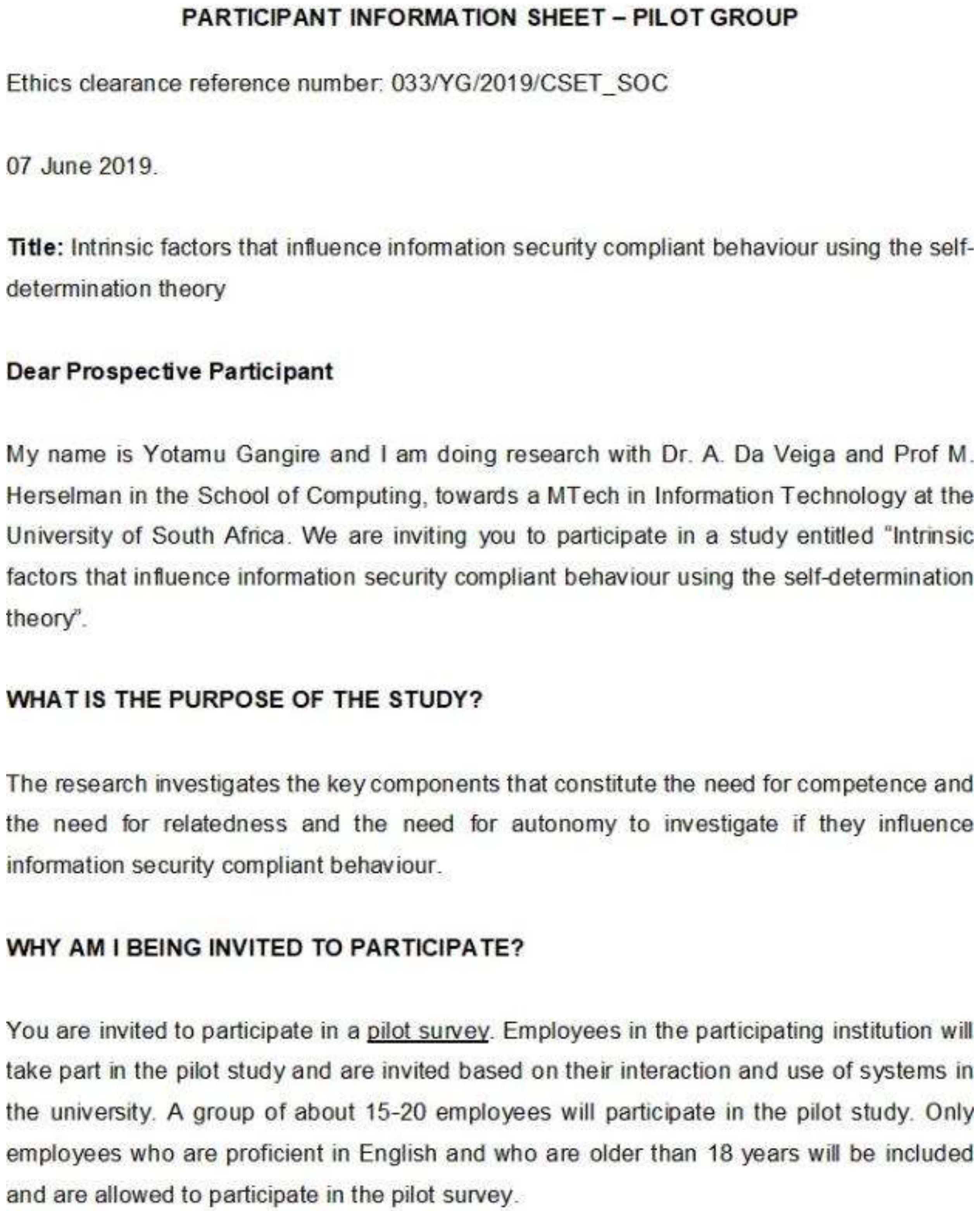
If you would like to be informed of the final research findings, please contact Yotamu Gangire on +263774198916 or email: 50801627@mylife.unisa.ac.za. The findings are accessible for a period of at least 5 years. Should you require any further information or want to contact the researcher about any aspect of this study, please contact Yotamu Gangire on +263774198916 or email: 50801627@mylife.unisa.ac.za.

Should you have concerns about the way in which the research has been conducted, you may contact Dr A. Da Veiga on 0116709175 or dveiga@unisa.ac.za. Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the School of Computing Research Ethics Committee, Dr Bester Chimbo, on (011) 670 9105 or chimbb@unisa.ac.za.

Thank you for taking time to read this information sheet and for participating in this study. Thank you.

____

Mr Yotamu Gangire



PARTICIPANT INFORMATION SHEET – PILOT GROUP

Ethics clearance reference number: 033/YG/2019/CSET_SOC

07 June 2019.

Title: Intrinsic factors that influence information security compliant behaviour using the self-determination theory

Dear Prospective Participant

My name is Yotamu Gangire and I am doing research with Dr. A. Da Veiga and Prof M. Herselman in the School of Computing, towards a MTech in Information Technology at the University of South Africa. We are inviting you to participate in a study entitled "Intrinsic factors that influence information security compliant behaviour using the self-determination theory".

WHAT IS THE PURPOSE OF THE STUDY?

The research investigates the key components that constitute the need for competence and the need for relatedness and the need for autonomy to investigate if they influence information security compliant behaviour.

WHY AM I BEING INVITED TO PARTICIPATE?

You are invited to participate in a pilot survey. Employees in the participating institution will take part in the pilot study and are invited based on their interaction and use of systems in the university. A group of about 15-20 employees will participate in the pilot study. Only employees who are proficient in English and who are older than 18 years will be included and are allowed to participate in the pilot survey.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves a survey whereby the participant must complete a questionnaire. Biographical, general awareness and privacy perception type of questions are included in the questionnaire. No personal identifiable information of the pilot group will be collected.

A facilitated session will be scheduled for students to anonymously complete a hard copy of the questionnaire. Participation in this survey will not take up more than 20 minutes of the pilot group participant's time.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the information security behaviour of employees participating university from a research perspective. It is anticipated that the information we gain from this survey will help us to develop the Information Security Compliant Behaviour Model based on the Self-determination theory questionnaire. The proposed framework & diagnostic instrument will assist to refine and improve the Information Security Compliant Behaviour Model based on the Self-determination theory questionnaire.

ARE THEIR ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

We do not foresee that you will experience any negative consequences by completing the survey. The survey is anonymous no personal identifiable information will be collected.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

Your name will not be recorded anywhere and no one will be able to connect you to the answers /input you give. Your answers/input will be given a code number and your completed questionnaire will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings.

By completing this survey, the anonymous information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings. Articles of the study may be submitted for publication, but individual participants will not be identifiable.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a minimum period of five years in a locked cupboard/filing cabinet at the student's premises and/or Unisa for future research or academic purposes; electronic information will be stored on a password protected computer. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Hard copies will be shredded and data will be permanently deleted from the survey application database files and hard drive of the computer through the use of a relevant software application once the purpose has been achieved.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the information security behaviour in South African universities from a research perspective. You will not be reimbursed or receive any incentives for your participation in the survey.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the School of Computing, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings, please contact Yotamu Gangire on +263774198916 or email: 50801627@mylife.unisa.ac.za. The findings are accessible for a period of at least 5 years. Should you require any further information or want to contact the researcher about any aspect of this study, please contact Yotamu Gangire on +263774198916 or email: 50801627@mylife.unisa.ac.za.

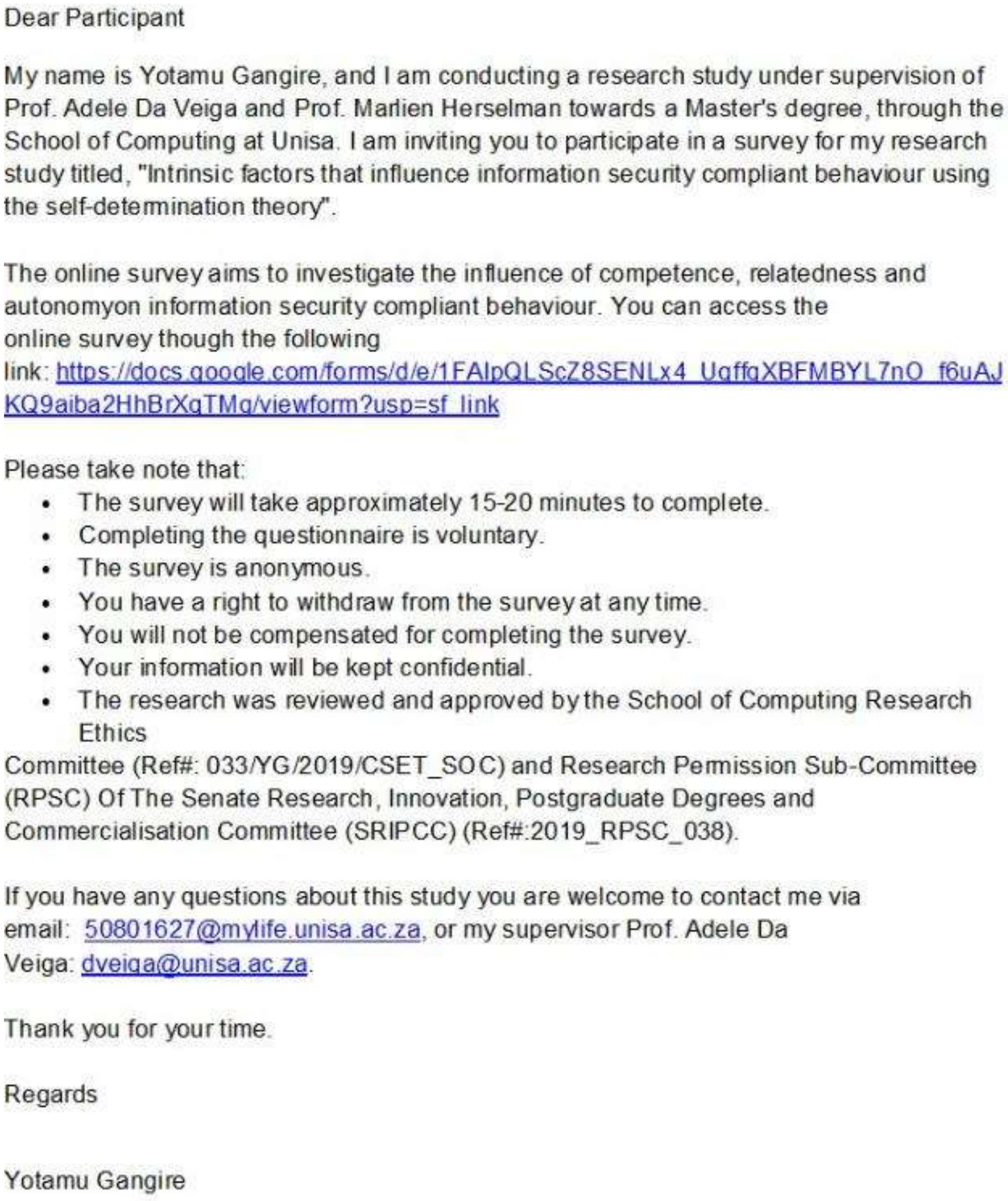
Should you have concerns about the way in which the research has been conducted, you may contact Dr A. Da Veiga on (011) 670-9175 or dveiga@unisa.ac.za. Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the School of Computing Research Ethics Committee, Dr Bester Chimbo, on (011) 670- 9105 or chimbb@unisa.ac.za.

Thank you for taking time to read this information sheet and for participating in this study.

Thank you.

____

Appendix G: Email invitation



Dear Participant

My name is Yotamu Gangire, and I am conducting a research study under supervision of Prof. Adele Da Veiga and Prof. Marlien Herselman towards a Master's degree, through the School of Computing at Unisa. I am inviting you to participate in a survey for my research study titled, "Intrinsic factors that influence information security compliant behaviour using the self-determination theory".

The online survey aims to investigate the influence of competence, relatedness and autonomyon information security compliant behaviour. You can access the online survey though the following link: https://docs.google.com/forms/d/e/1FAIpQLScZ8SENLx4_UgffgXBFMBYL7nO_f6uAJKQ9aiba2HhBrXgTMg/viewform?usp=sf_link

Please take note that:

- The survey will take approximately 15-20 minutes to complete.
- Completing the questionnaire is voluntary.
- The survey is anonymous.
- You have a right to withdraw from the survey at any time.
- You will not be compensated for completing the survey.
- Your information will be kept confidential.
- The research was reviewed and approved by the School of Computing Research Ethics

Committee (Ref#: 033/YG/2019/CSET_SOC) and Research Permission Sub-Committee (RPSC) Of The Senate Research, Innovation, Postgraduate Degrees and Commercialisation Committee (SRIPCC) (Ref#:2019_RPSC_038).

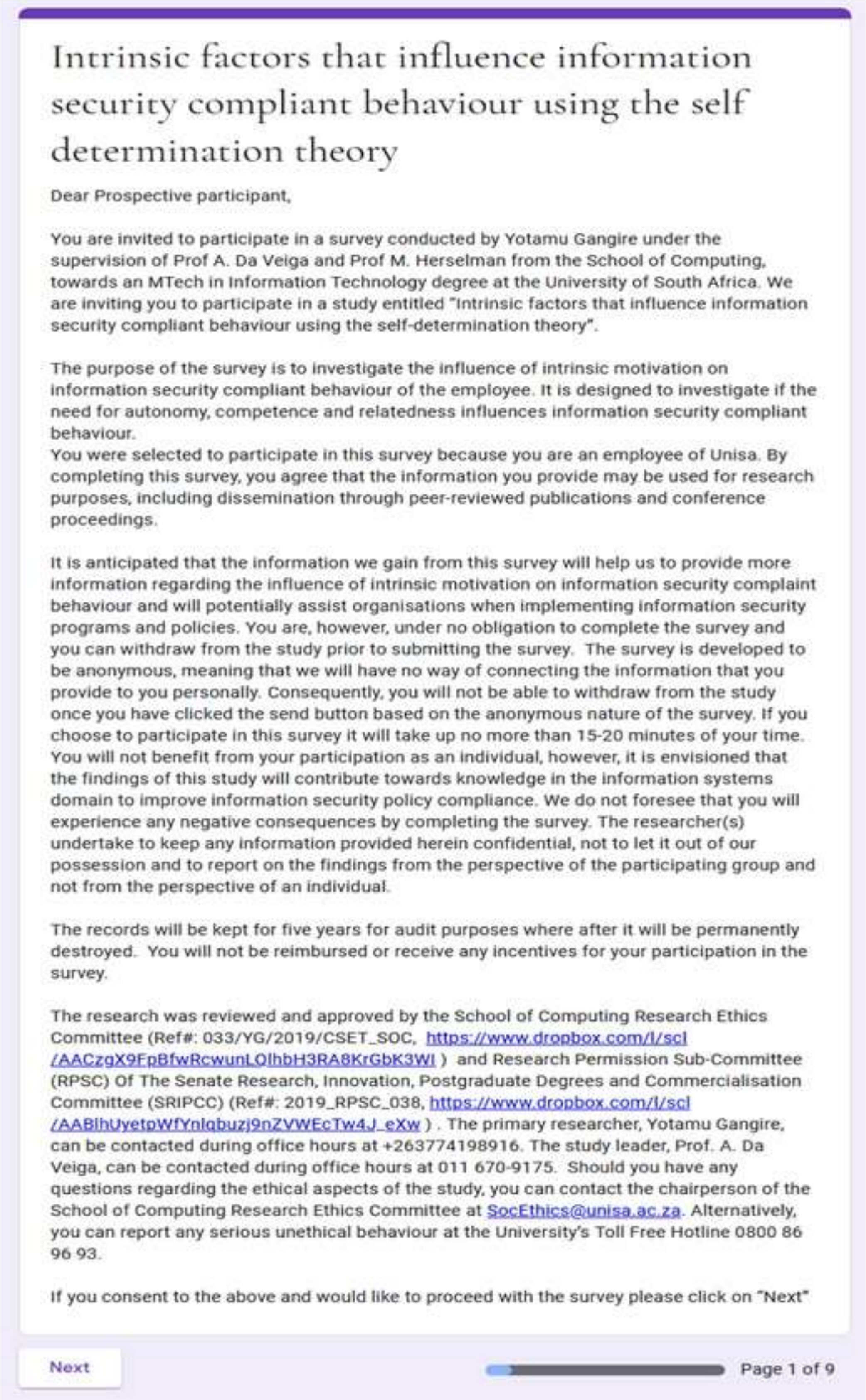
If you have any questions about this study you are welcome to contact me via email: 50801627@mylife.unisa.ac.za, or my supervisor Prof. Adele Da Veiga: dveiga@unisa.ac.za.

Thank you for your time.

Regards

Yotamu Gangire

Appendix H: Final questionnaire



Intrinsic factors that influence information security compliant behaviour using the self determination theory

Dear Prospective participant,

You are invited to participate in a survey conducted by Yotamu Gangire under the supervision of Prof A. Da Veiga and Prof M. Herselman from the School of Computing, towards an MTech in Information Technology degree at the University of South Africa. We are inviting you to participate in a study entitled "Intrinsic factors that influence information security compliant behaviour using the self-determination theory".

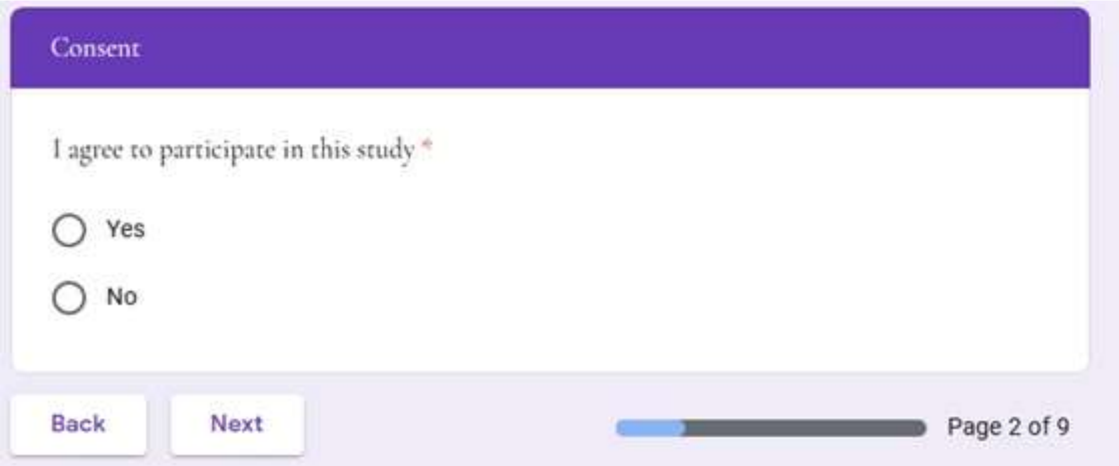
The purpose of the survey is to investigate the influence of intrinsic motivation on information security compliant behaviour of the employee. It is designed to investigate if the need for autonomy, competence and relatedness influences information security compliant behaviour.
You were selected to participate in this survey because you are an employee of Unisa. By completing this survey, you agree that the information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the information we gain from this survey will help us to provide more information regarding the influence of intrinsic motivation on information security complaint behaviour and will potentially assist organisations when implementing information security programs and policies. You are, however, under no obligation to complete the survey and you can withdraw from the study prior to submitting the survey. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the send button based on the anonymous nature of the survey. If you choose to participate in this survey it will take up no more than 15-20 minutes of your time. You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will contribute towards knowledge in the information systems domain to improve information security policy compliance. We do not foresee that you will experience any negative consequences by completing the survey. The researcher(s) undertake to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

The records will be kept for five years for audit purposes where after it will be permanently destroyed. You will not be reimbursed or receive any incentives for your participation in the survey.

The research was reviewed and approved by the School of Computing Research Ethics Committee (Ref#: 033/YG/2019/CSET_SOC, https://www.dropbox.com/l/scl/AACzgX9FpBfwRcwunLQlhbH3RA8KrGbK3WI) and Research Permission Sub-Committee (RPSC) Of The Senate Research, Innovation, Postgraduate Degrees and Commercialisation Committee (SRIPCC) (Ref#: 2019_RPSC_038, https://www.dropbox.com/l/scl/AABlhUyetpWfYnlqbuzj9nZVWEcTw4J_eXw) . The primary researcher, Yotamu Gangire, can be contacted during office hours at +263774198916. The study leader, Prof. A. Da Veiga, can be contacted during office hours at 011 670-9175. Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the School of Computing Research Ethics Committee at SocEthics@unisa.ac.za. Alternatively, you can report any serious unethical behaviour at the University's Toll Free Hotline 0800 86 96 93.

If you consent to the above and would like to proceed with the survey please click on "Next"

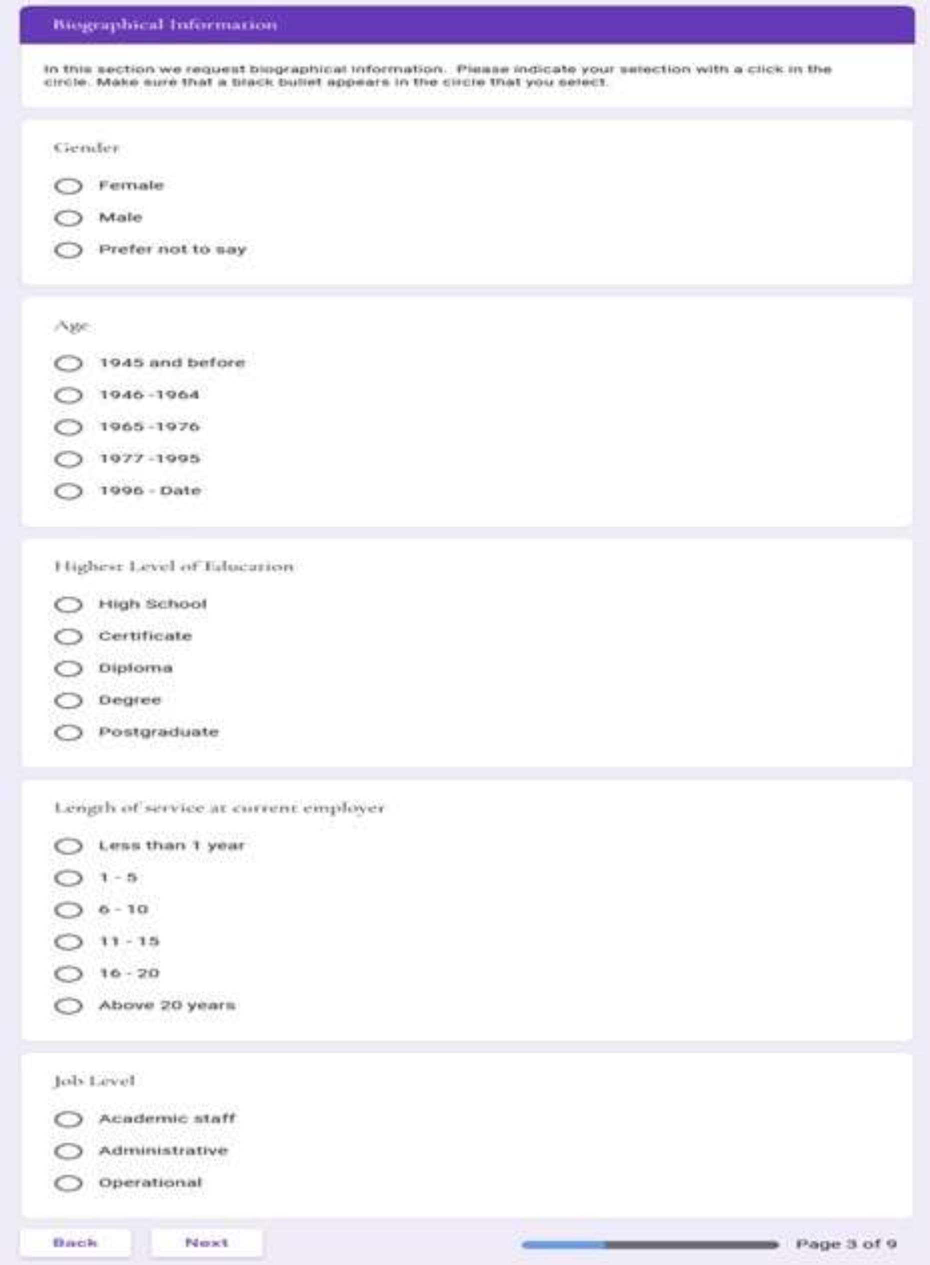


Consent

I agree to participate in this study *

○ Yes

○ No



Biographical Information

In this section we request biographical information. Please indicate your selection with a click in the circle. Make sure that a black bullet appears in the circle that you select.

Gender

○ Female

○ Male

○ Prefer not to say

Age

○ 1945 and before

○ 1946 -1964

○ 1965 -1976

○ 1977 -1995

○ 1996 - Date

Highest Level of Education

○ High School

○ Certificate

○ Diploma

○ Degree

○ Postgraduate

Length of service at current employer

○ Less than 1 year

○ 1 - 5

○ 6 - 10

○ 11 - 15

○ 16 - 20

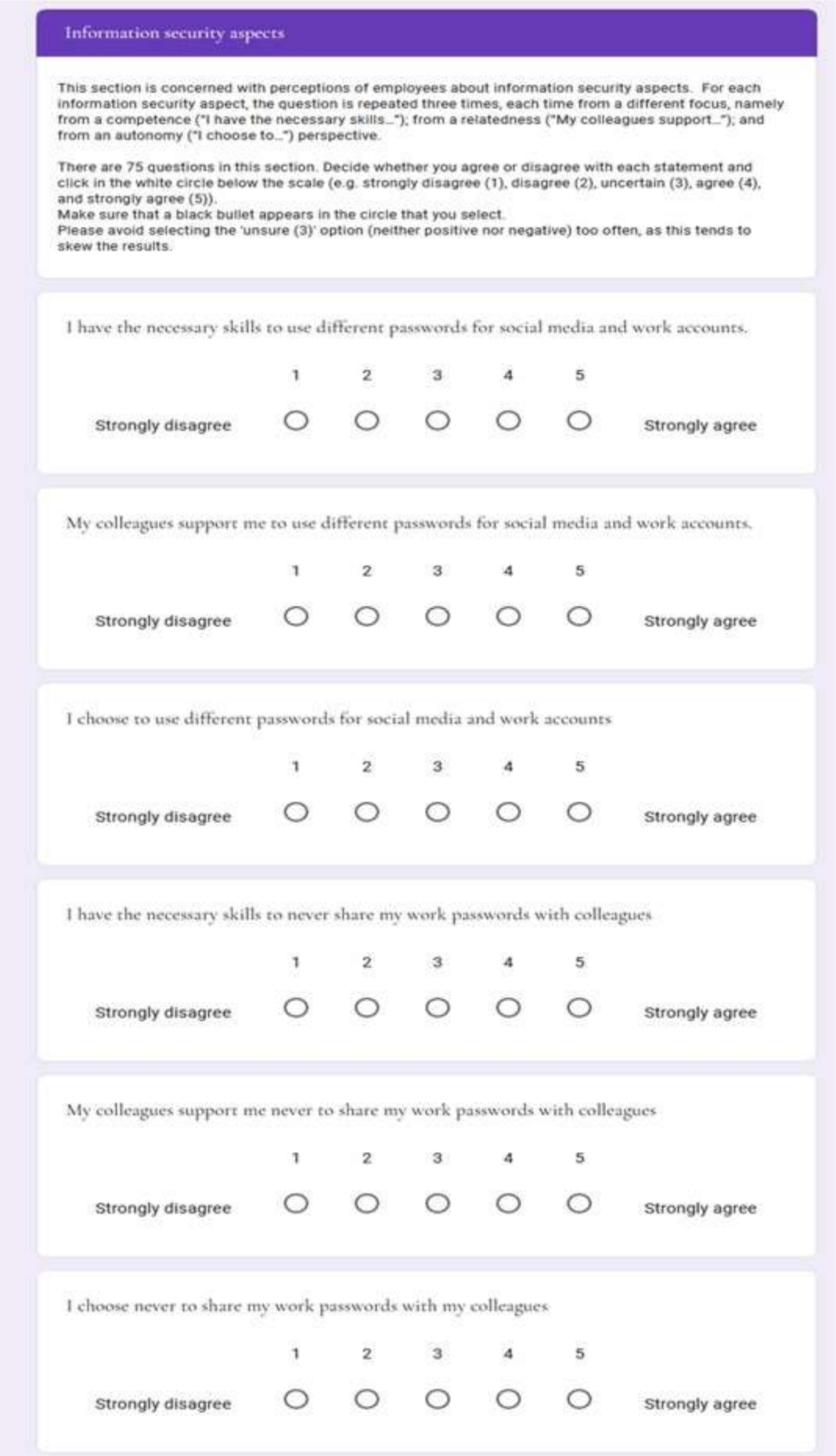
○ Above 20 years

Job Level

○ Academic staff

○ Administrative

○ Operational



Information security aspects

This section is concerned with perceptions of employees about information security aspects. For each information security aspect, the question is repeated three times, each time from a different focus, namely from a competence ("I have the necessary skills..."); from a relatedness ("My colleagues support..."); and from an autonomy ("I choose to...") perspective.

There are 75 questions in this section. Decide whether you agree or disagree with each statement and click in the white circle below the scale (e.g. strongly disagree (1), disagree (2), uncertain (3), agree (4), and strongly agree (5)).
Make sure that a black bullet appears in the circle that you select.
Please avoid selecting the 'unsure (3)' option (neither positive nor negative) too often, as this tends to skew the results.

I have the necessary skills to use different passwords for social media and work accounts.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to use different passwords for social media and work accounts.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to use different passwords for social media and work accounts

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to never share my work passwords with colleagues

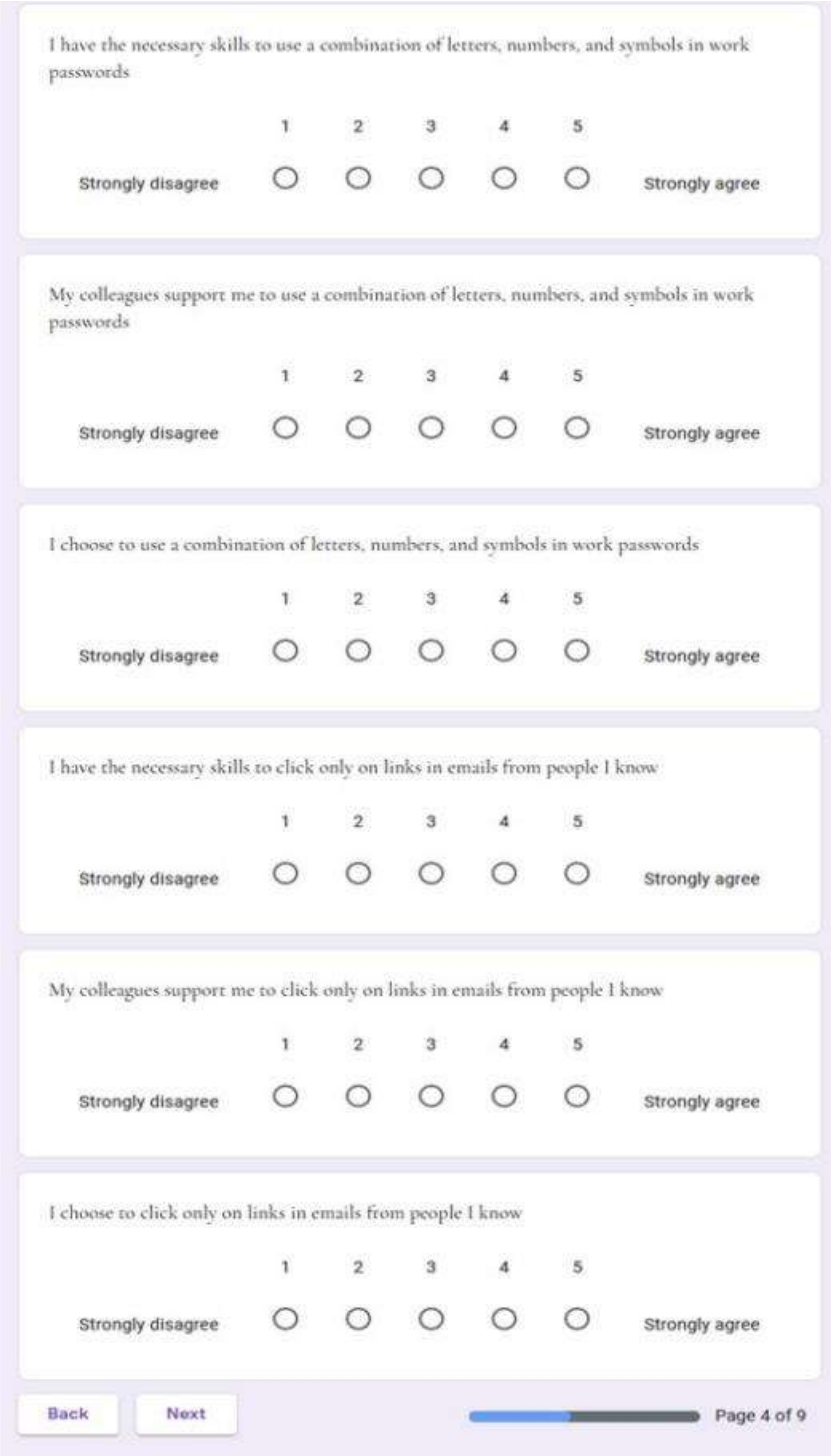
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me never to share my work passwords with colleagues

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose never to share my work passwords with my colleagues

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



I have the necessary skills to use a combination of letters, numbers, and symbols in work passwords

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to use a combination of letters, numbers, and symbols in work passwords

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to use a combination of letters, numbers, and symbols in work passwords

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to click only on links in emails from people I know

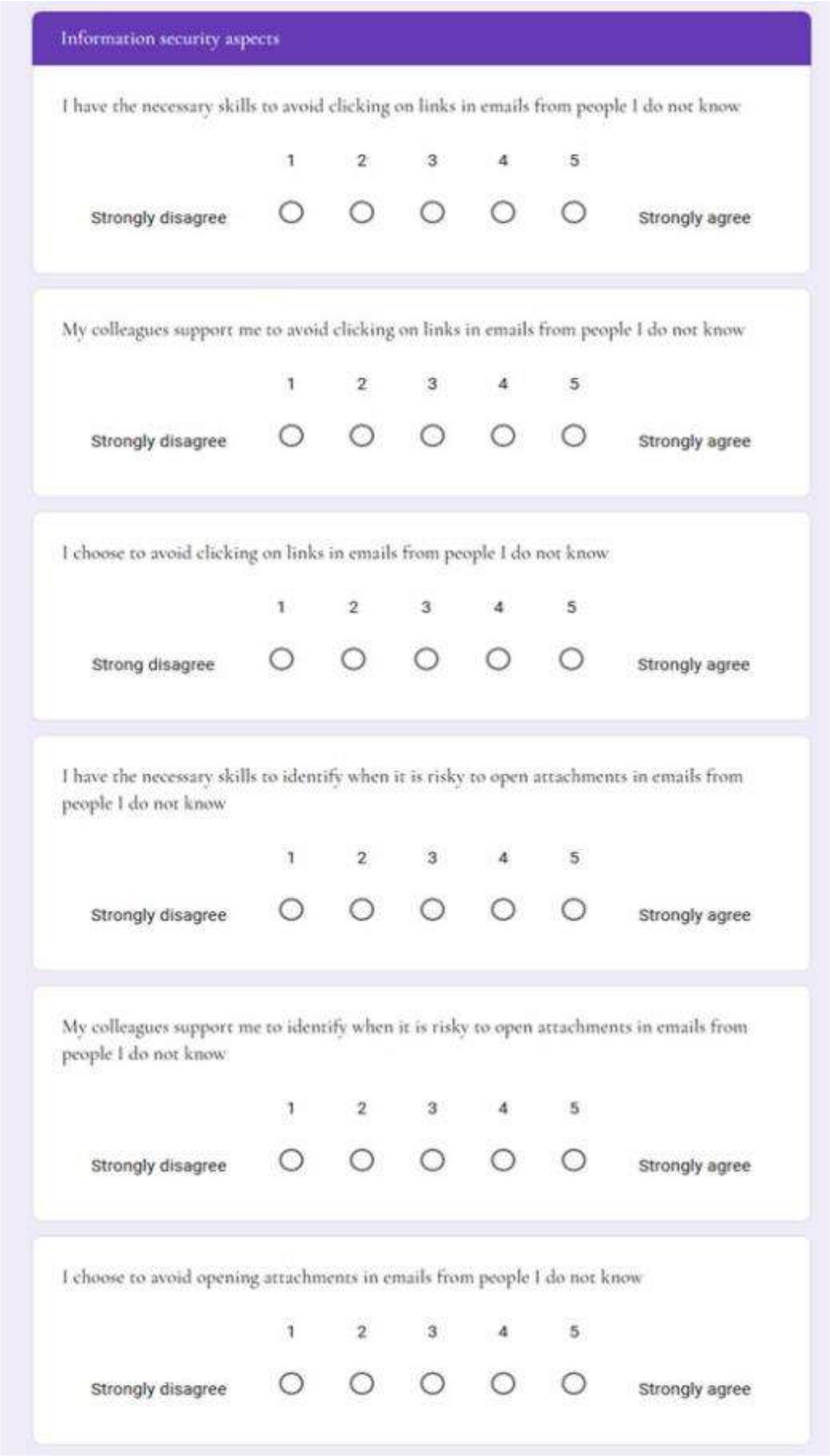
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to click only on links in emails from people I know

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to click only on links in emails from people I know

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



Information security aspects

I have the necessary skills to avoid clicking on links in emails from people I do not know

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to avoid clicking on links in emails from people I do not know

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to avoid clicking on links in emails from people I do not know

	1	2	3	4	5	
Strong disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to identify when it is risky to open attachments in emails from people I do not know

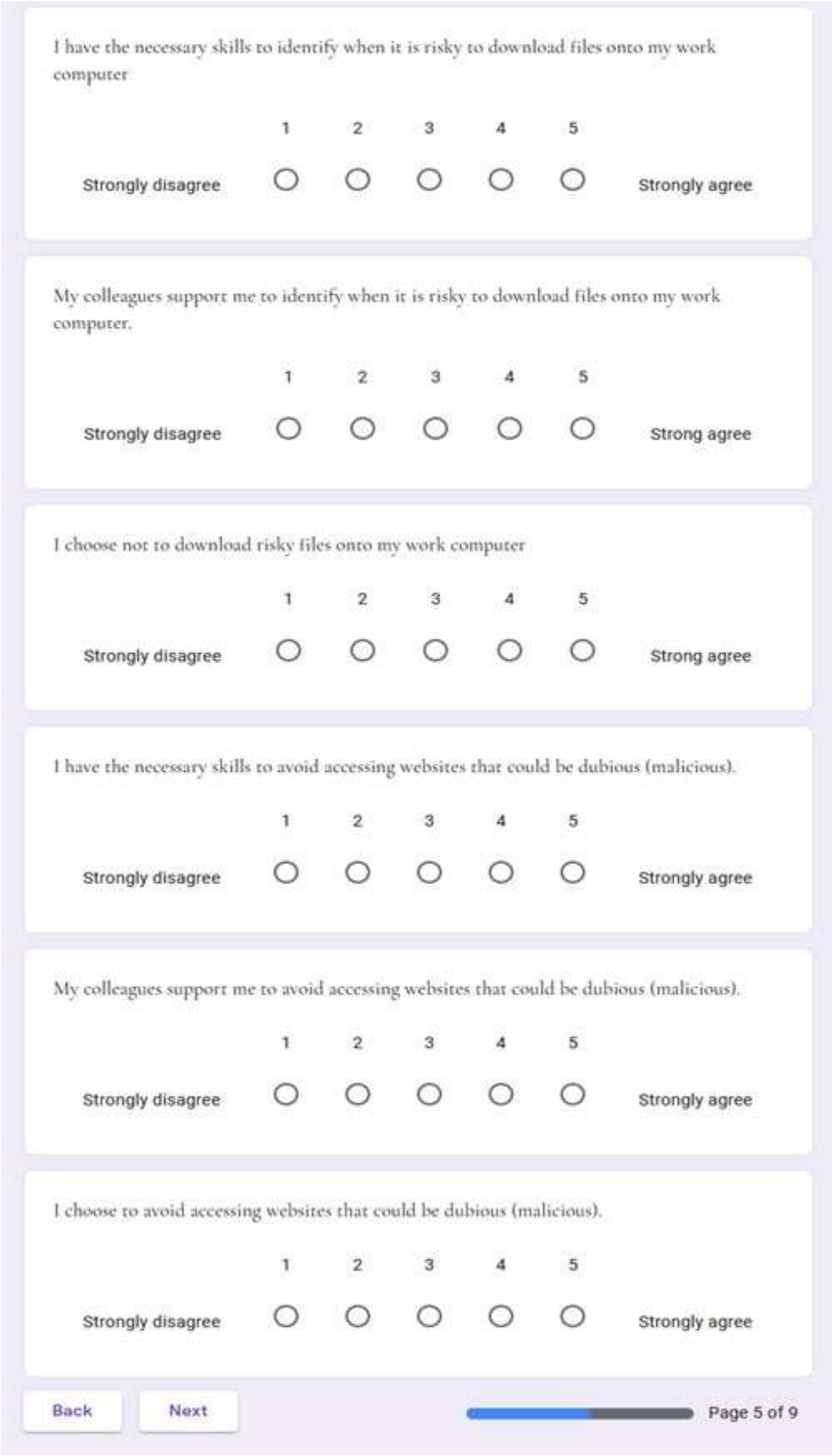
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to identify when it is risky to open attachments in emails from people I do not know

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to avoid opening attachments in emails from people I do not know

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



I have the necessary skills to identify when it is risky to download files onto my work computer

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to identify when it is risky to download files onto my work computer.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strong agree

I choose not to download risky files onto my work computer

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strong agree

I have the necessary skills to avoid accessing websites that could be dubious (malicious).

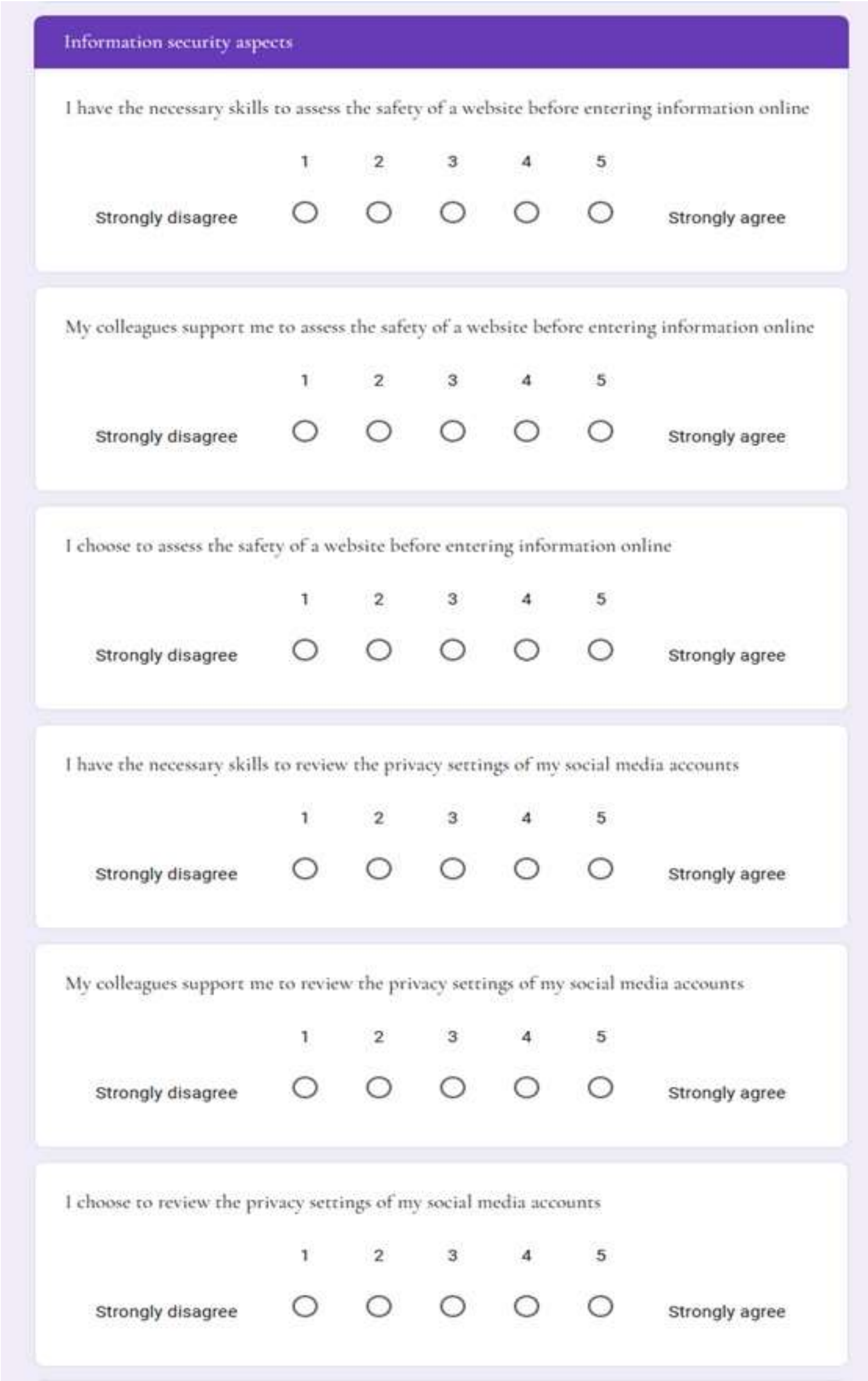
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to avoid accessing websites that could be dubious (malicious).

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to avoid accessing websites that could be dubious (malicious).

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



Information security aspects

I have the necessary skills to assess the safety of a website before entering information online

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to assess the safety of a website before entering information online

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to assess the safety of a website before entering information online

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to review the privacy settings of my social media accounts

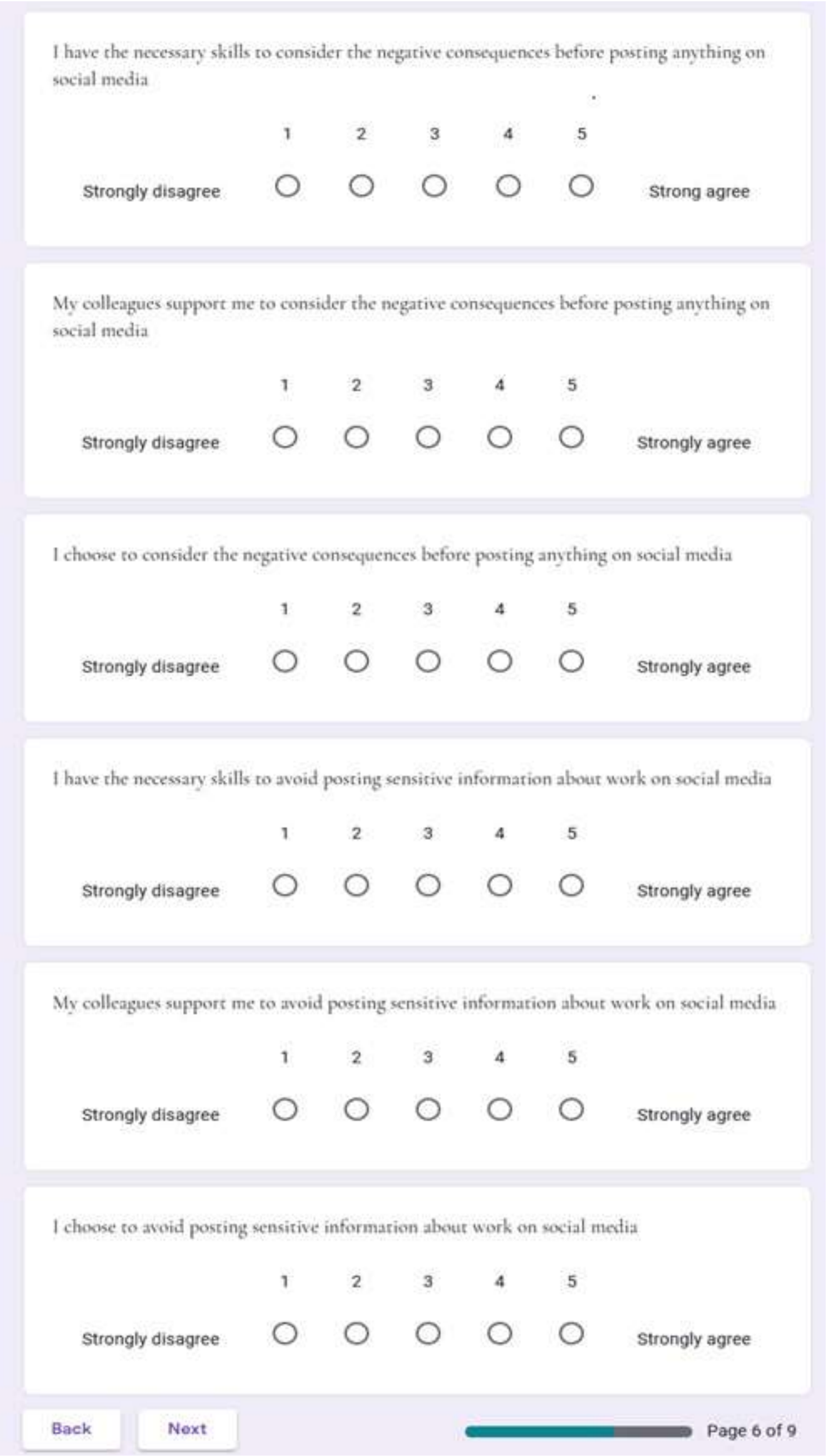
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to review the privacy settings of my social media accounts

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to review the privacy settings of my social media accounts

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



I have the necessary skills to consider the negative consequences before posting anything on social media

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strong agree

My colleagues support me to consider the negative consequences before posting anything on social media

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to consider the negative consequences before posting anything on social media

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to avoid posting sensitive information about work on social media

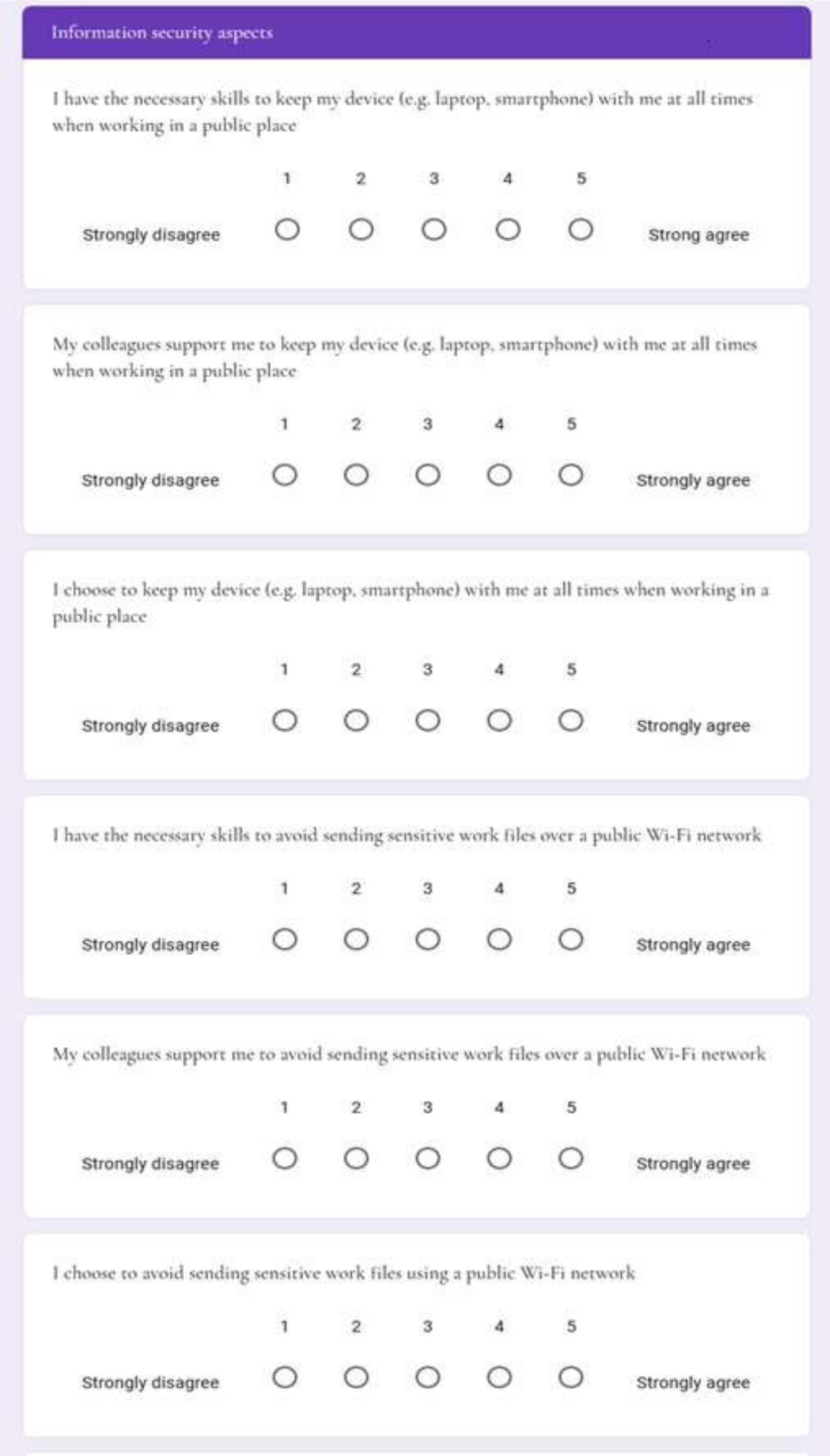
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to avoid posting sensitive information about work on social media

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to avoid posting sensitive information about work on social media

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



Information security aspects

I have the necessary skills to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strong agree

My colleagues support me to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to avoid sending sensitive work files over a public Wi-Fi network

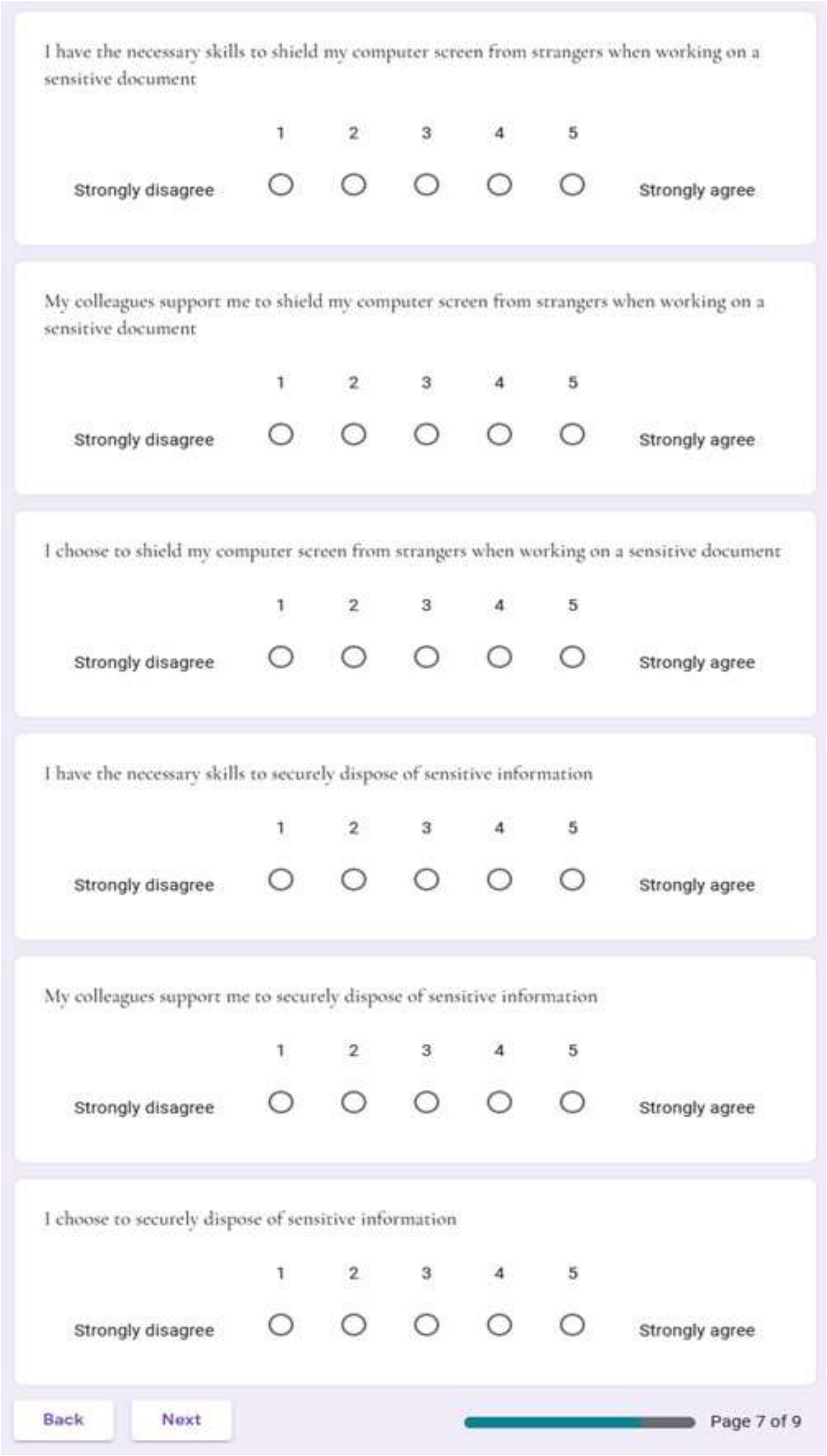
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to avoid sending sensitive work files over a public Wi-Fi network

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to avoid sending sensitive work files using a public Wi-Fi network

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



I have the necessary skills to shield my computer screen from strangers when working on a sensitive document

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to shield my computer screen from strangers when working on a sensitive document

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to shield my computer screen from strangers when working on a sensitive document

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to securely dispose of sensitive information

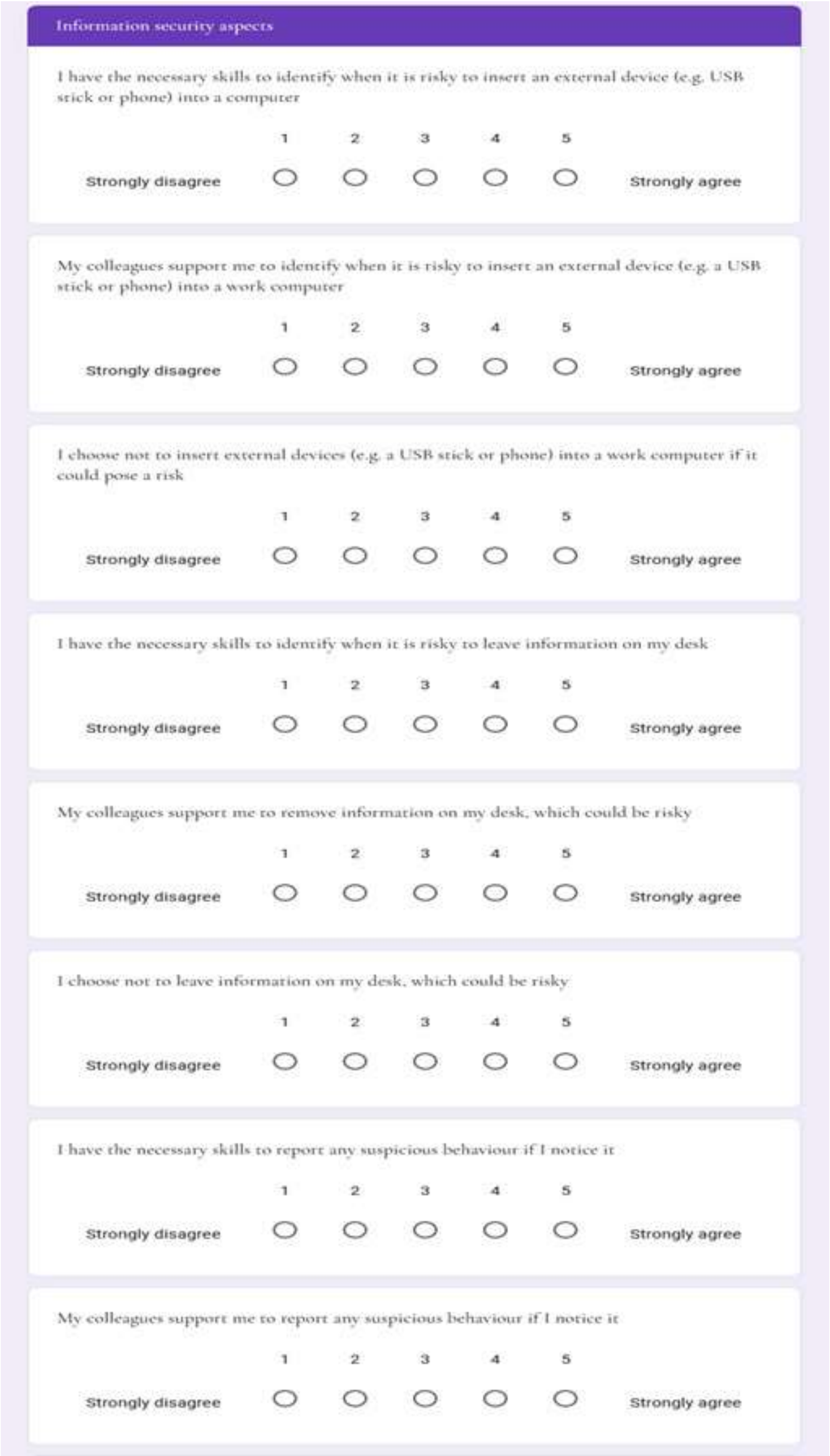
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to securely dispose of sensitive information

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to securely dispose of sensitive information

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



Information security aspects

I have the necessary skills to identify when it is risky to insert an external device (e.g. USB stick or phone) into a computer

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to identify when it is risky to insert an external device (e.g. a USB stick or phone) into a work computer

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose not to insert external devices (e.g. a USB stick or phone) into a work computer if it could pose a risk

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to identify when it is risky to leave information on my desk

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to remove information on my desk, which could be risky

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose not to leave information on my desk, which could be risky

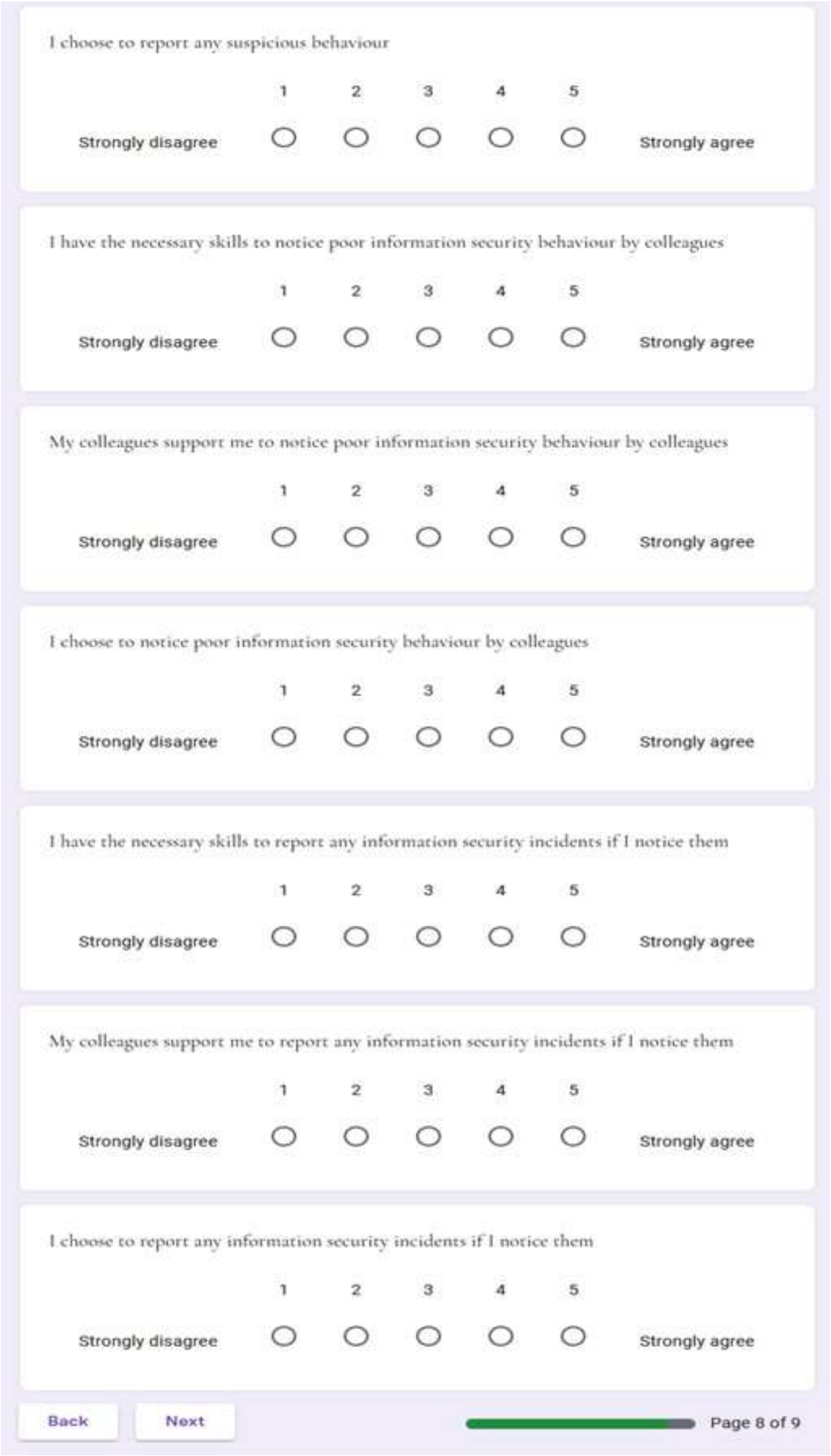
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to report any suspicious behaviour if I notice it

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to report any suspicious behaviour if I notice it

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



I choose to report any suspicious behaviour

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to notice poor information security behaviour by colleagues

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to notice poor information security behaviour by colleagues

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to notice poor information security behaviour by colleagues

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to report any information security incidents if I notice them

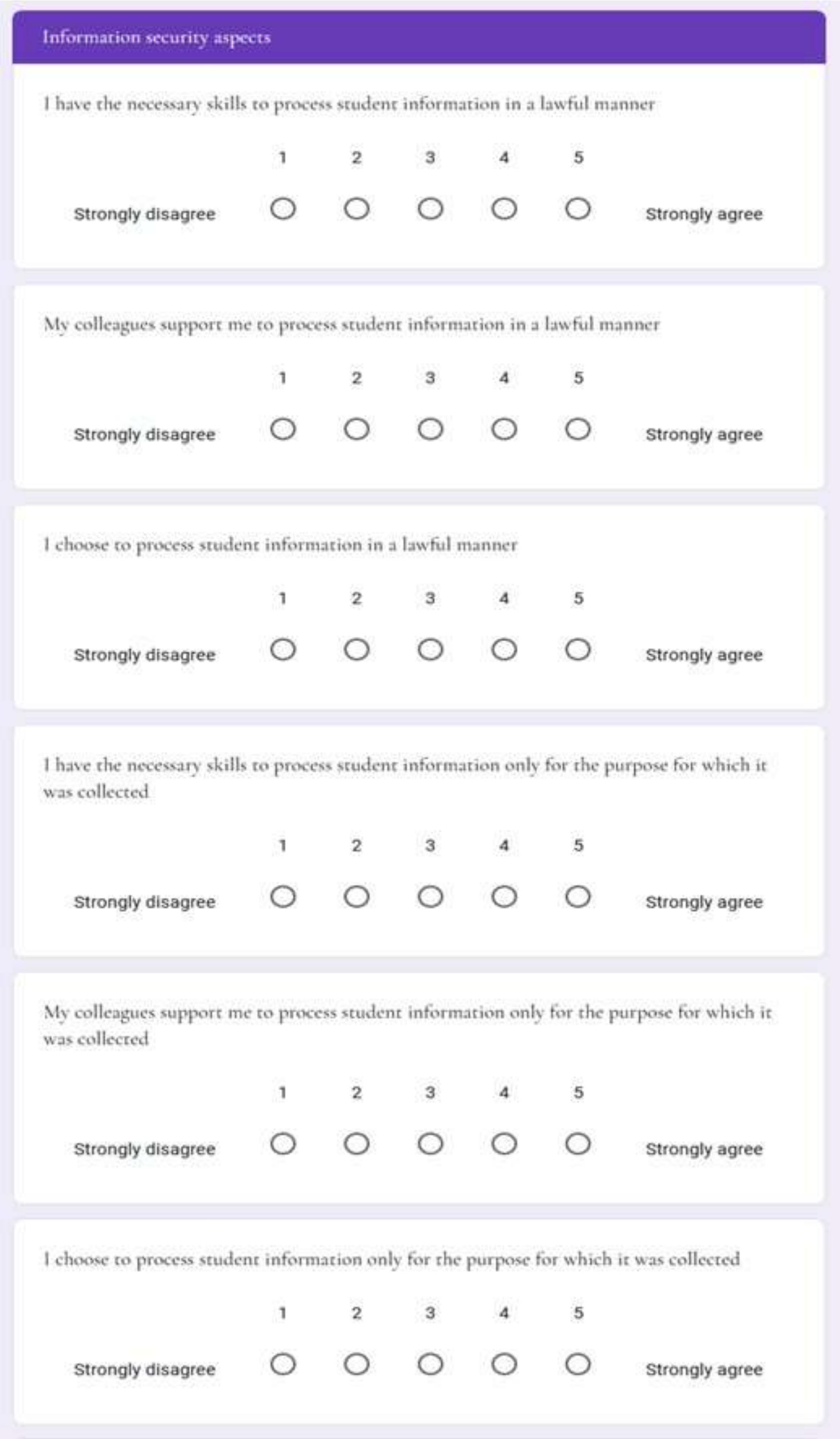
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to report any information security incidents if I notice them

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to report any information security incidents if I notice them

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



Information security aspects

I have the necessary skills to process student information in a lawful manner

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to process student information in a lawful manner

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to process student information in a lawful manner

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to process student information only for the purpose for which it was collected

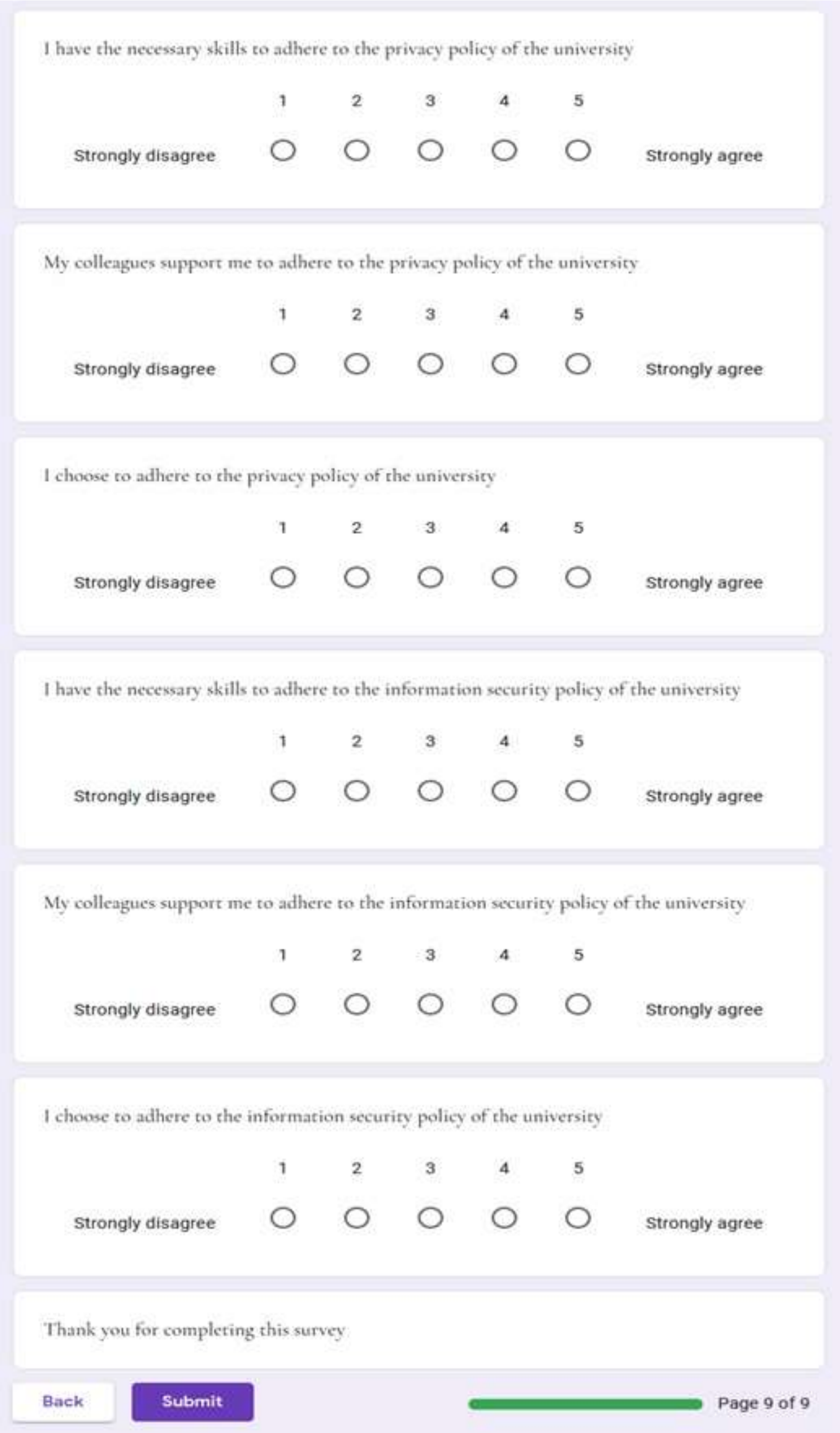
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to process student information only for the purpose for which it was collected

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to process student information only for the purpose for which it was collected

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree



I have the necessary skills to adhere to the privacy policy of the university

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to adhere to the privacy policy of the university

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to adhere to the privacy policy of the university

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I have the necessary skills to adhere to the information security policy of the university

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

My colleagues support me to adhere to the information security policy of the university

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I choose to adhere to the information security policy of the university

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

Thank you for completing this survey

Intrinsic factors that influence information security compliant behaviour using the self determination theory

Thank you for participating in this survey.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Appendix I: Anonymous front page

Ethical clearance #: 033/YG/2019/CSET_SOC

Research permission #: 2019_RPSC_038

COVER LETTER TO AN ONLINE ANONOMOUS WEB-BASED SURVEY

Information Security Compliant Behaviour Questionnaire

Dear Prospective participant,

You are invited to participate in a survey conducted by Yotamu Gangire under the supervision of Prof A. Da Veiga and Prof M. Herselman from the School of Computing, towards an MTech in Information Technology degree at the University of South Africa. We are inviting you to participate in a study entitled "Intrinsic factors that influence information security compliant behaviour using the self-determination theory".

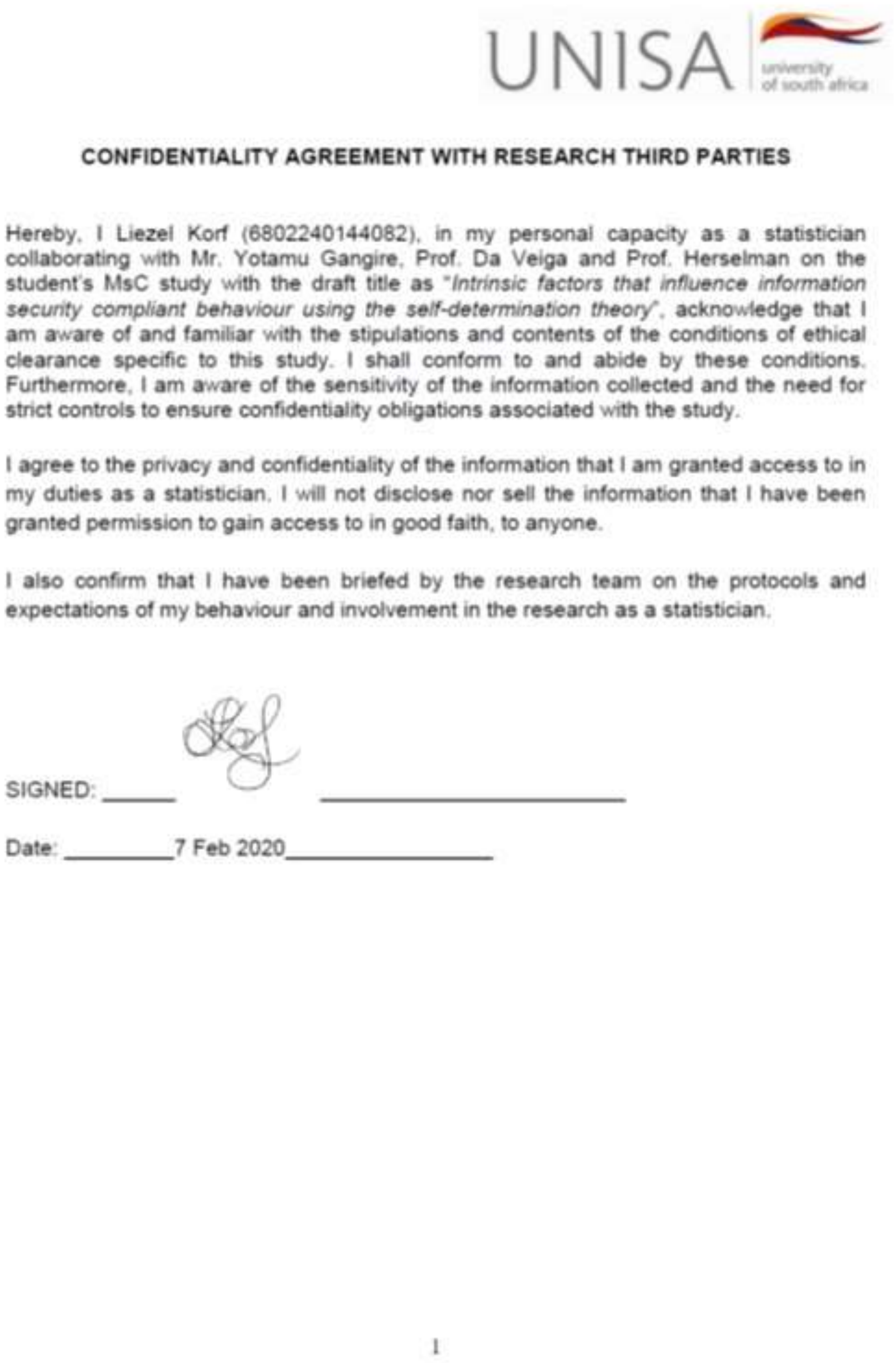
The purpose of the survey is to investigate the influence of intrinsic motivation on information security compliant behaviour of the employee. It is designed to investigate if the need for competence, relatedness and autonomy influences information security compliant behaviour. You were selected to participate in this survey because you are an employee of Unisa. By completing this survey, you agree that the information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the information we gain from this survey will help us to provide more information regarding the influence of intrinsic motivation on information security complaint behaviour and will potentially assist organisations when implementing information security programs and policies. You are, however, under no obligation to complete the survey and you can withdraw from the study prior to submitting the survey. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the send button based on the anonymous nature of the survey. If you choose to participate in this survey it will take up no more than 15-20 minutes of your time. You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will contribute towards knowledge in the information systems domain to improve information security policy compliance. We do not foresee that you will experience any negative consequences by completing the survey. The researcher(s) undertake to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

The records will be kept for five years for audit purposes where after it will be permanently destroyed. You will not be reimbursed or receive any incentives for your participation in the survey.

The research was reviewed and approved by the School of Computing Research Ethics Committee (Ref#: 033/YG/2019/CSET_SOC, https://www.dropbox.com/l/scl/AACzgX9FpBfwRcwunLQlhbH3RA8KrGbK3WI) and Research Permission Sub-Committee (RPSC) Of The Senate Research, Innovation, Postgraduate Degrees and Commercialisation Committee (SRIPCC) (Ref#: 2019_RPSC_038, https://www.dropbox.com/l/scl/AABlhUyetpWfYnlqbuzj9nZVWEcTw4J_eXw) . The primary researcher, Yotamu Gangire, can be contacted during office hours at +263774198916. The study leader, Prof. A. Da Veiga, can be contacted during office hours at 011 670-9175. Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the School of Computing Research Ethics Committee at SocEthics@unisa.ac.za. Alternatively, you can report any serious unethical behaviour at the University's Toll Free Hotline 0800 86 96 93.

Appendix J: Confidentiality agreement with statistician



UNISA university of south africa

CONFIDENTIALITY AGREEMENT WITH RESEARCH THIRD PARTIES

Hereby, I Liezel Korf (6802240144082), in my personal capacity as a statistician collaborating with Mr. Yotamu Gangire, Prof. Da Veiga and Prof. Herselman on the student's MsC study with the draft title as "*Intrinsic factors that influence information security compliant behaviour using the self-determination theory*", acknowledge that I am aware of and familiar with the stipulations and contents of the conditions of ethical clearance specific to this study. I shall conform to and abide by these conditions. Furthermore, I am aware of the sensitivity of the information collected and the need for strict controls to ensure confidentiality obligations associated with the study.

I agree to the privacy and confidentiality of the information that I am granted access to in my duties as a statistician. I will not disclose nor sell the information that I have been granted permission to gain access to in good faith, to anyone.

I also confirm that I have been briefed by the research team on the protocols and expectations of my behaviour and involvement in the research as a statistician.

SIGNED: ______ ________________________

Date: _________7 Feb 2020________________

Appendix K: Communalities

Communalities – Autonomy

	Initial	Extraction
A2 I choose never to share my work passwords with my colleagues	0.262	0.165
A7 I choose not to download risky files onto my work computer	0.579	0.623
A17 I choose not to insert external devices (e.g. a USB stick or phone) into a work computer if it could pose a risk	0.489	0.467
A18 I choose not to leave information on my desk, which could be risky	0.437	0.430
A25 I choose to adhere to the information security policy of the university	0.646	0.674
A24 I choose to adhere to the privacy policy of the university	0.596	0.566
A9 I choose to assess the safety of a website before entering information online	0.610	0.641
A8 I choose to avoid accessing websites that could be dubious (malicious).	0.591	0.595
A5 I choose to avoid clicking on links in emails from people I do not know	0.641	0.702
A6 I choose to avoid opening attachments in emails from people I do not know	0.606	0.651
A12 I choose to avoid posting sensitive information about work on social media	0.394	0.376
A14 I choose to avoid sending sensitive work files using a public Wi-Fi network	0.484	0.470
A4 I choose to click only on links in emails from people I know	0.524	0.507
A11 I choose to consider the negative consequences before posting anything on social media	0.470	0.525
A13 I choose to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place	0.536	0.633
A20 I choose to notice poor information security behaviour by colleagues	0.375	0.388
A22 I choose to process student information in a lawful manner	0.646	0.750
A23 I choose to process student information only for the purpose for which it was collected	0.656	0.818
A21 I choose to report any information security incidents if I notice them	0.585	0.786
A19 I choose to report any suspicious behaviour	0.552	0.571
A10 I choose to review the privacy settings of my social media accounts	0.467	0.445
A16 I choose to securely dispose of sensitive information	0.591	0.562
A15 I choose to shield my computer screen from strangers when working on a sensitive document	0.589	0.620
A3 I choose to use a combination of letters, numbers, and symbols in work passwords	0.315	0.191
A1 I choose to use different passwords for social media and work accounts	0.261	0.199

Extraction Method: Principal Axis Factoring.

Communalities - Competence

	Initial	Extraction
C25 I have the necessary skills to adhere to the information security policy of the university	0.692	0.573
C24 I have the necessary skills to adhere to the privacy policy of the university	0.724	0.604
C9 I have the necessary skills to assess the safety of a website before entering information online	0.692	0.661
C8 I have the necessary skills to avoid accessing websites that could be dubious (malicious).	0.682	0.678
C5 I have the necessary skills to avoid clicking on links in emails from people I do not know	0.605	0.602
C12 I have the necessary skills to avoid posting sensitive information about work on social media	0.585	0.536
C14 I have the necessary skills to avoid sending sensitive work files over a public Wi-Fi network	0.619	0.571
C4 I have the necessary skills to click only on links in emails from people I know	0.561	0.571
C11 I have the necessary skills to consider the negative consequences before posting anything on social media	0.603	0.458
C7 I have the necessary skills to identify when it is risky to download files onto my work computer	0.763	0.756
C17 I have the necessary skills to identify when it is risky to insert an external device (e.g. USB stick or phone) into a computer	0.599	0.571
C18 I have the necessary skills to identify when it is risky to leave information on my desk	0.599	0.556
C6 I have the necessary skills to identify when it is risky to open attachments in emails from people I do not know	0.787	0.785
C13 I have the necessary skills to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place	0.425	0.327
C2 I have the necessary skills to never share my work passwords with colleagues	0.379	0.218
C20 I have the necessary skills to notice poor information security behaviour by colleagues	0.547	0.532
C22 I have the necessary skills to process student information in a lawful manner	0.659	0.602
C23 I have the necessary skills to process student information only for the purpose for which it was collected	0.704	0.721
C21 I have the necessary skills to report any information security incidents if I notice them	0.562	0.535
C19 I have the necessary skills to report any suspicious behaviour if I notice it	0.605	0.543
C10 I have the necessary skills to review the privacy settings of my social media accounts	0.531	0.442
C16 I have the necessary skills to securely dispose of sensitive information	0.631	0.547
C15 I have the necessary skills to shield my computer screen from strangers when working on a sensitive document	0.678	0.552
C3 I have the necessary skills to use a combination of letters, numbers, and symbols in work passwords	0.454	0.447
C1 I have the necessary skills to use different passwords for social media and work accounts.	0.511	0.482
Extraction Method: Principal Axis Factoring.		

Communalities - Relatedness

	Initial	Extraction
R2 My colleagues support me never to share my work passwords with colleagues	0.424	0.281
R3 My colleagues support me to use a combination of letters, numbers, and symbols in work passwords	0.682	0.598
R1 My colleagues support me to use different passwords for social media and work accounts.	0.569	0.462
R25 My colleagues support me to adhere to the information security policy of the university	0.819	0.803
R24 My colleagues support me to adhere to the privacy policy of the university	0.809	0.745
R9 My colleagues support me to assess the safety of a website before entering information online	0.771	0.728
R8 My colleagues support me to avoid accessing websites that could be dubious (malicious).	0.762	0.716
R5 My colleagues support me to avoid clicking on links in emails from people I do not know	0.818	0.729
R12 My colleagues support me to avoid posting sensitive information about work on social media	0.789	0.709
R14 My colleagues support me to avoid sending sensitive work files over a public Wi-Fi network	0.776	0.733
R4 My colleagues support me to click only on links in emails from people I know	0.772	0.703
R11 My colleagues support me to consider the negative consequences before posting anything on social media	0.770	0.677
R7 My colleagues support me to identify when it is risky to download files onto my work computer.	0.798	0.730
R17 My colleagues support me to identify when it is risky to insert an external device (e.g. a USB stick or phone) into a work computer	0.728	0.671
R6 My colleagues support me to identify when it is risky to open attachments in emails from people I do not know	0.770	0.696
R13 My colleagues support me to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place	0.787	0.743
R20 My colleagues support me to notice poor information security behaviour by colleagues	0.748	0.690
R22 My colleagues support me to process student information in a lawful manner	0.797	0.755
R23 My colleagues support me to process student information only for the purpose for which it was collected	0.786	0.707
R18 My colleagues support me to remove information on my desk, which could be risky	0.809	0.734
R21 My colleagues support me to report any information security incidents if I notice them	0.763	0.714
R19 My colleagues support me to report any suspicious behaviour if I notice it	0.724	0.666
R10 My colleagues support me to review the privacy settings of my social media accounts	0.708	0.637
R16 My colleagues support me to securely dispose of sensitive information	0.766	0.704
R15 My colleagues support me to shield my computer screen from strangers when working on a sensitive document	0.813	0.766
Extraction Method: Principal Axis Factoring.		

Appendix L: Reliability statistics

Relatedness F1 (Organisational support for employee device and information protection awareness)

Case processing summary

		N	%
Cases	Valid	238	90.5
	Excluded[a]	25	9.5
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.967	0.967	16

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.648	0.360	0.833	0.474	2.316	0.011	16

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
R4 My colleagues support me to click only on links in emails from people I know	44.64	310.534	0.819	0.763	0.964
R5 My colleagues support me to avoid clicking on links in emails from people I do not know	44.55	310.273	0.835	0.805	0.964
R8 My colleagues support me to avoid accessing websites that could be dubious (malicious).	44.66	311.839	0.831	0.756	0.964
R9 My colleagues support me to assess the safety of a website before entering information online	44.74	313.381	0.829	0.753	0.964
R3 My colleagues support me to use a combination of letters, numbers, and symbols in work passwords	44.70	311.155	0.770	0.666	0.965
R6 My colleagues support me to identify when it is risky to open attachments in emails from people I do not know	44.67	312.618	0.818	0.747	0.964
R7 My colleagues support me to identify when it is risky to download files onto my work computer.	44.61	311.868	0.834	0.778	0.964
R10 My colleagues support me to review the privacy settings of my social media accounts	44.98	315.257	0.779	0.693	0.965
R11 My colleagues support me to consider the negative consequences before posting anything on social media	44.68	312.632	0.808	0.759	0.964
R13 My colleagues support me to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place	44.62	308.970	0.845	0.778	0.964

R15 My colleagues support me to shield my computer screen from strangers when working on a sensitive document	44.88	309.978	0.846	0.787	0.964
R16 My colleagues support me to securely dispose of sensitive information	44.84	311.662	0.814	0.744	0.964
R12 My colleagues support me to avoid posting sensitive information about work on social media	44.63	310.109	0.821	0.778	0.964
R1 My colleagues support me to use different passwords for social media and work accounts.	45.04	318.779	0.670	0.549	0.967
R14 My colleagues support me to avoid sending sensitive work files over a public Wi-Fi network	44.72	311.292	0.823	0.744	0.964
R2 My colleagues support me never to share my work passwords with colleagues	44.18	325.547	0.513	0.336	0.969

Relatedness F2 (Organisational supporting for employee information privacy protection awareness)

Case processing summary

		N	%
Cases	Valid	247	93.9
	Excluded[a]	16	6.1
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.945	0.945	7

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.710	0.591	0.860	0.269	1.455	0.005	7

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
R22 My colleagues support me to process student information in a lawful manner	19.35	53.481	0.826	0.759	0.935
R23 My colleagues support me to process student information only for the purpose for which it was collected	19.18	54.426	0.798	0.748	0.938
R24 My colleagues support me to adhere to the privacy policy of the university	19.20	53.723	0.855	0.785	0.933
R25 My colleagues support me to adhere to the information security policy of the university	19.23	53.373	0.871	0.800	0.931
R20 My colleagues support me to notice poor information security behaviour by colleagues	19.81	54.382	0.798	0.720	0.938
R21 My colleagues support me to report any information security incidents if I notice them	19.75	54.715	0.795	0.705	0.938
R19 My colleagues support me to report any suspicious behaviour if I notice it	19.65	54.749	0.765	0.618	0.940

Competence F1(Employee skills for data safety awareness)

Case processing summary

		N	%
Cases	Valid	238	90.5
	Excluded[a]	25	9.5
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.906	0.908	11

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.472	0.349	0.734	0.385	2.101	0.007	11

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
C12 I have the necessary skills to avoid posting sensitive information about work on social media	41.87	57.079	0.629	0.495	0.899
C21 I have the necessary skills to report any information security incidents if I notice them	42.47	54.149	0.676	0.555	0.896
C20 I have the necessary skills to notice poor information security behaviour by colleagues	42.54	54.005	0.622	0.501	0.899
C11 I have the necessary skills to consider the negative consequences before posting anything on social media	41.95	56.492	0.613	0.535	0.900
C16 I have the necessary skills to securely dispose of sensitive information	42.41	51.872	0.724	0.618	0.893
C15 I have the necessary skills to shield my computer screen from strangers when working on a sensitive document	42.31	52.755	0.729	0.662	0.893
C19 I have the necessary skills to report any suspicious behaviour if I notice it	42.25	55.419	0.655	0.524	0.897
C1 I have the necessary skills to use different passwords for social media and work accounts.	41.90	58.370	0.584	0.415	0.902
C14 I have the necessary skills to avoid sending sensitive work files over a public Wi-Fi network	42.13	54.229	0.701	0.577	0.895
C18 I have the necessary skills to identify when it is risky to leave information on my desk	42.08	55.221	0.643	0.466	0.898
C10 I have the necessary skills to review the privacy settings of my social media accounts	42.55	54.063	0.597	0.378	0.901

Competence F2 (Employee skills for email and website safety)

Case processing summary

		N	%
Cases	Valid	246	93.5
	Excluded[a]	17	6.5
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.905	0.905	7

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.578	0.418	0.801	0.383	1.915	0.010	7

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
C4 I have the necessary skills to click only on links in emails from people I know	24.62	29.576	0.629	0.473	0.900
C5 I have the necessary skills to avoid clicking on links in emails from people I do not know	24.61	29.356	0.635	0.514	0.900
C6 I have the necessary skills to identify when it is risky to open attachments in emails from people I do not know	24.78	26.978	0.809	0.711	0.881
C7 I have the necessary skills to identify when it is risky to download files onto my work computer	24.85	27.111	0.813	0.714	0.880
C8 I have the necessary skills to avoid accessing websites that could be dubious (malicious).	24.86	28.062	0.752	0.611	0.888
C9 I have the necessary skills to assess the safety of a website before entering information online	25.11	27.883	0.711	0.563	0.892
C17 I have the necessary skills to identify when it is risky to insert an external device (e.g. USB stick or phone) into a computer	25.02	27.583	0.682	0.493	0.896

Competence F3 (Employee skills for privacy awareness)

Case processing summary

		N	%
Cases	Valid	251	95.4
	Excluded[a]	12	4.6
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.824	0.842	4

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.570	0.435	0.738	0.302	1.694	0.017	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
C22 I have the necessary skills to process student information in a lawful manner	13.52	3.651	0.678	0.569	0.788
C23 I have the necessary skills to process student information only for the purpose for which it was collected	13.27	4.328	0.721	0.611	0.744
C24 I have the necessary skills to adhere to the privacy policy of the university	13.13	5.296	0.684	0.626	0.781
C25 I have the necessary skills to adhere to the information security policy of the university	13.23	5.122	0.607	0.573	0.799

Autonomy F1 (Employee choice on privacy awareness)

Case processing summary

		N	%
Cases	Valid	257	97.7
	Excluded[a]	6	2.3
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.775	0.780	3

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.542	0.440	0.659	0.219	1.498	0.010	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
A8 I choose to avoid accessing websites that could be dubious (malicious).	8.00	3.887	0.620	0.446	0.687
A9 I choose to assess the safety of a website before entering information online	8.19	3.645	0.693	0.504	0.607
A10 I choose to review the privacy settings of my social media accounts	8.35	3.659	0.531	0.293	0.795

Autonomy F2 (Employee choice to avoid malicious emails and downloads)

Case Processing Summary

		N	%
Cases	Valid	255	97.0
	Excluded[a]	8	3.0
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.836	0.836	4

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.560	0.391	0.697	0.305	1.780	0.011	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
A4 I choose to click only on links in emails from people I know	13.05	6.753	0.639	0.455	0.808
A5 I choose to avoid clicking on links in emails from people I do not know	12.92	6.493	0.762	0.600	0.747
A6 I choose to avoid opening attachments in emails from people I do not know	12.93	6.956	0.732	0.555	0.763
A7 I choose not to download risky files onto my work computer	12.84	8.198	0.549	0.334	0.839

Autonomy F3 (Employee choice to keep the privacy of student personal information)

Case Processing Summary

		N	%
Cases	Valid	260	98.9
	Excluded[a]	3	1.1
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.904	0.906	2

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.829	0.829	0.829	0.000	1.000	0.000	2

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
A22 I choose to process student information in a lawful manner	4.48	0.729	0.829	0.686	
A23 I choose to process student information only for the purpose for which it was collected	4.41	0.876	0.829	0.686	

Autonomy F4 (Employee choice to report bad security behaviour)

Case Processing Summary

		N	%
Cases	Valid	256	97.3
	Excluded[a]	7	2.7
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.791	0.795	3

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.563	0.454	0.694	0.239	1.526	0.012	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
A19 I choose to report any suspicious behaviour	7.73	3.961	0.650	0.490	0.702
A20 I choose to notice poor information security behaviour by colleagues	8.20	3.833	0.543	0.305	0.818
A21 I choose to report any information security incidents if I notice them	7.93	3.477	0.718	0.546	0.621

Autonomy F5 (Employee choice to adhere to information security and privacy policies)

Case Processing Summary

		N	**%**
Cases	**Valid**	**256**	**97.3**
	Excluded[a]	7	2.7
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.868	0.870	2

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.770	0.770	0.770	0.000	1.000	0.000	2

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
A24 I choose to adhere to the privacy policy of the university	4.60	0.468	0.770	0.593	
A25 I choose to adhere to the information security policy of the university	4.64	0.379	0.770	0.593	

Autonomy F6 (Employee choice to keep devices and information secure)

Case Processing Summary

		N	**%**
Cases	Valid	251	95.4
	Excluded[a]	12	4.6
	Total	263	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.793	0.797	5

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.439	0.340	0.644	0.304	1.894	0.007	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlatio n	Cronbach's Alpha if Item Deleted
A11 I choose to consider the negative consequences before posting anything on social media	17.84	7.703	0.511	0.300	0.773
A13 I choose to keep my device (e.g. laptop, smartphone) with me at all times when working in a public place	17.76	7.781	0.604	0.374	0.749
A15 I choose to shield my computer screen from strangers when working on a sensitive document	18.04	6.502	0.656	0.483	0.725
A16 I choose to securely dispose of sensitive information	18.20	6.390	0.625	0.463	0.739
A12 I choose to avoid posting sensitive information about work on social media	17.69	8.231	0.504	0.268	0.776

Appendix M: One-way ANOVA statistics

One-way ANOVA – Age group

		Sum of Squares	df	Mean Square	F	Sig.
Relatedness Factor 1	Between Groups	6.973	2	3.486	2.496	0.084
	Within Groups	361.722	259	1.397		
	Total	368.694	261			
Relatedness Factor 2	Between Groups	9.898	2	4.949	3.369	0.036
	Within Groups	376.040	256	1.469		
	Total	385.938	258			
Competence Factor 1	Between Groups	2.180	2	1.090	2.011	0.136
	Within Groups	140.937	260	0.542		
	Total	143.117	262			
Competence Factor 2	Between Groups	3.319	2	1.659	2.218	0.111
	Within Groups	193.727	259	0.748		
	Total	197.045	261			
Competence Factor 3	Between Groups	0.416	2	0.208	0.431	0.650
	Within Groups	124.869	259	0.482		
	Total	125.285	261			
Autonomy Factor 1	Between Groups	3.352	2	1.676	2.055	0.130
	Within Groups	211.237	259	0.816		
	Total	214.589	261			
Autonomy Factor 2	Between Groups	5.424	2	2.712	3.672	0.027
	Within Groups	191.294	259	0.739		
	Total	196.718	261			
Autonomy Factor 3	Between Groups	0.614	2	0.307	0.418	0.659
	Within Groups	189.331	258	0.734		
	Total	189.944	260			
Autonomy Factor 4	Between Groups	0.585	2	0.293	0.333	0.717
	Within Groups	227.344	259	0.878		
	Total	227.929	261			
Autonomy Factor 5	Between Groups	0.062	2	0.031	0.083	0.921
	Within Groups	96.657	259	0.373		
	Total	96.719	261			
Autonomy_Factor_6	Between Groups	0.739	2	0.370	0.798	0.451
	Within Groups	119.953	259	0.463		
	Total	120.692	261			

One-way ANOVA – Job level

		Sum of Squares	df	Mean Square	F	Sig.
Relatedness Factor 1	Between Groups	7.068	2	3.534	2.549	0.080
	Within Groups	357.654	258	1.386		
	Total	364.722	260			
Relatedness Factor 2	Between Groups	7.224	2	3.612	2.452	0.088
	Within Groups	375.650	255	1.473		
	Total	382.874	257			
Competence Factor 1	Between Groups	5.274	2	2.637	4.976	0.008
	Within Groups	137.241	259	0.530		
	Total	142.515	261			
Competence Factor 2	Between Groups	14.751	2	7.375	10.482	0.000
	Within Groups	181.526	258	0.704		
	Total	196.277	260			
Competence Factor 3	Between Groups	5.697	2	2.849	6.162	0.002
	Within Groups	119.265	258	0.462		
	Total	124.962	260			
Autonomy Factor 1	Between Groups	3.998	2	1.999	2.459	0.088
	Within Groups	209.757	258	0.813		
	Total	213.756	260			
Autonomy Factor 2	Between Groups	9.355	2	4.678	6.458	0.002
	Within Groups	186.874	258	0.724		
	Total	196.229	260			
Autonomy Factor 3	Between Groups	11.442	2	5.721	8.251	0.000
	Within Groups	178.192	257	0.693		
	Total	189.635	259			
Autonomy Factor 4	Between Groups	1.253	2	0.626	0.716	0.489
	Within Groups	225.601	258	0.874		
	Total	226.854	260			
Autonomy Factor 5	Between Groups	0.554	2	0.277	0.745	0.476
	Within Groups	96.022	258	0.372		
	Total	96.577	260			
Autonomy_Factor_6	Between Groups	3.845	2	1.923	4.256	0.015
	Within Groups	116.560	258	0.452		
	Total	120.406	260			

One-way ANOVA - Tenure

		Sum of Squares	df	Mean Square	F	Sig.
Relatedness Factor 1	Between Groups	3.036	4	0.759	0.532	0.713
	Within Groups	366.940	257	1.428		
	Total	369.975	261			
Relatedness Factor 2	Between Groups	2.612	4	0.653	0.433	0.785
	Within Groups	383.326	254	1.509		
	Total	385.938	258			
Competence Factor 1	Between Groups	3.267	4	0.817	1.507	0.201
	Within Groups	139.850	258	0.542		
	Total	143.117	262			
Competence Factor 2	Between Groups	1.414	4	0.353	0.464	0.762
	Within Groups	195.632	257	0.761		
	Total	197.045	261			
Competence Factor 3	Between Groups	1.681	4	0.420	0.744	0.563
	Within Groups	145.192	257	0.565		
	Total	146.873	261			
Autonomy Factor 1	Between Groups	3.724	4	0.931	1.135	0.341
	Within Groups	210.865	257	0.820		
	Total	214.589	261			
Autonomy Factor 2	Between Groups	1.873	4	0.468	0.618	0.650
	Within Groups	194.844	257	0.758		
	Total	196.718	261			
Autonomy Factor 3	Between Groups	4.422	4	1.105	1.525	0.195
	Within Groups	185.523	256	0.725		
	Total	189.944	260			
Autonomy Factor 4	Between Groups	1.920	4	0.480	0.546	0.702
	Within Groups	226.009	257	0.879		
	Total	227.929	261			
Autonomy Factor 5	Between Groups	1.651	4	0.413	1.116	0.349
	Within Groups	95.067	257	0.370		
	Total	96.719	261			
Autonomy Factor 6	Between Groups	2.030	4	0.508	1.099	0.357
	Within Groups	118.662	257	0.462		
	Total	120.692	261			

One-way ANOVA – Highest Level of Education

		Sum of Squares	Df	Mean Square	F	Sig.
Relatedness Factor 1	Between Groups	12.818	3	4.273	3.109	0.027
	Within Groups	353.205	257	1.374		
	Total	366.024	260			
Relatedness Factor 2	Between Groups	13.593	3	4.531	3.116	0.027
	Within Groups	369.281	254	1.454		
	Total	382.874	257			
Competence Factor 1	Between Groups	0.404	3	0.135	0.244	0.865
	Within Groups	142.111	258	0.551		
	Total	142.515	261			
Competence Factor 2	Between Groups	4.690	3	1.563	2.097	0.101
	Within Groups	191.587	257	0.745		
	Total	196.277	260			
Competence Factor 3	Between Groups	2.834	3	0.945	1.690	0.170
	Within Groups	143.694	257	0.559		
	Total	146.529	260			
Autonomy Factor 1	Between Groups	6.390	3	2.130	2.640	0.050
	Within Groups	207.365	257	0.807		
	Total	213.756	260			
Autonomy Factor 2	Between Groups	2.911	3	0.970	1.290	0.278
	Within Groups	193.318	257	0.752		
	Total	196.229	260			
Autonomy Factor 3	Between Groups	3.103	3	1.034	1.420	0.237
	Within Groups	186.532	256	0.729		
	Total	189.635	259			
Autonomy Factor 4	Between Groups	2.438	3	0.813	0.931	0.426
	Within Groups	224.416	257	0.873		
	Total	226.854	260			
Autonomy Factor 5	Between Groups	0.211	3	0.070	0.188	0.905
	Within Groups	96.365	257	0.375		
	Total	96.577	260			
Autonomy Factor 6	Between Groups	2.484	3	0.828	1.805	0.147
	Within Groups	117.922	257	0.459		
	Total	120.406	260			

Post hoc test - age group

Multiple Comparisons

Scheffe

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Relatedness Factor 1	1946 - 1964	1965 -1976	0.24991	0.18699	0.411	-0.2104	0.7103
		1977 -date	-0.13848	0.17841	0.740	-0.5777	0.3008
	1965 - 1976	1946 -1964	-0.24991	0.18699	0.411	-0.7103	0.2104
		1977 -date	-0.38839	0.17470	0.086	-0.8185	0.0417
	1977 - date	1946 -1964	0.13848	0.17841	0.740	-0.3008	0.5777
		1965 -1976	0.38839	0.17470	0.086	-0.0417	0.8185
Relatedness Factor 2	1946 - 1964	1965 -1976	0.24490	0.19298	0.448	-0.2302	0.7200
		1977 -date	-0.22256	0.18404	0.482	-0.6757	0.2306
	1965 - 1976	1946 -1964	-0.24490	0.19298	0.448	-0.7200	0.2302
		1977 -date	-.46745*	0.18016	0.036	-0.9110	-0.0239
	1977 - date	1946 -1964	0.22256	0.18404	0.482	-0.2306	0.6757
		1965 -1976	.46745*	0.18016	0.036	0.0239	0.9110
Competence Factor 1	1946 - 1964	1965 -1976	0.12274	0.11649	0.575	-0.1641	0.4095
		1977 -date	-0.09502	0.11092	0.693	-0.3681	0.1780
	1965 - 1976	1946 -1964	-0.12274	0.11649	0.575	-0.4095	0.1641
		1977 -date	-0.21776	0.10860	0.136	-0.4851	0.0496
	1977 - date	1946 -1964	0.09502	0.11092	0.693	-0.1780	0.3681
		1965 -1976	0.21776	0.10860	0.136	-0.0496	0.4851
Competence Factor 2	1946 - 1964	1965 -1976	0.26863	0.13684	0.148	-0.0683	0.6055
		1977 -date	0.05567	0.13056	0.913	-0.2658	0.3771
	1965 - 1976	1946 -1964	-0.26863	0.13684	0.148	-0.6055	0.0683
		1977 -date	-0.21296	0.12785	0.252	-0.5277	0.1018
	1977 - date	1946 -1964	-0.05567	0.13056	0.913	-0.3771	0.2658
		1965 -1976	0.21296	0.12785	0.252	-0.1018	0.5277
Competence Factor 3	1946 - 1964	1965 -1976	-0.03131	0.10986	0.960	-0.3018	0.2392
		1977 -date	-0.09403	0.10482	0.669	-0.3521	0.1640
	1965 - 1976	1946 -1964	0.03131	0.10986	0.960	-0.2392	0.3018
		1977 -date	-0.06272	0.10264	0.830	-0.3154	0.1900
	1977 - date	1946 -1964	0.09403	0.10482	0.669	-0.1640	0.3521
		1965 -1976	0.06272	0.10264	0.830	-0.1900	0.3154
Autonomy Factor 1	1946 - 1964	1965 -1976	0.16382	0.14289	0.519	-0.1880	0.5156
		1977 -date	-0.10632	0.13634	0.738	-0.4420	0.2293
	1965 - 1976	1946 -1964	-0.16382	0.14289	0.519	-0.5156	0.1880
		1977 -date	-0.27014	0.13350	0.131	-0.5988	0.0585
	1977 - date	1946 -1964	0.10632	0.13634	0.738	-0.2293	0.4420
		1965 -1976	0.27014	0.13350	0.131	-0.0585	0.5988
Autonomy Factor 2		1965 -1976	.36755*	0.13598	0.027	0.0328	0.7023

	1946 - 1964	1977 -date	0.21187	0.12974	0.265	-0.1076	0.5313
	1965 - 1976	1946 -1964	-.36755*	0.13598	0.027	-0.7023	-0.0328
		1977 -date	-0.15568	0.12704	0.473	-0.4685	0.1571
	1977 - date	1946 -1964	-0.21187	0.12974	0.265	-0.5313	0.1076
		1965 -1976	0.15568	0.12704	0.473	-0.1571	0.4685
Autonomy Factor 3	1946 - 1964	1965 -1976	0.00665	0.13594	0.999	-0.3280	0.3413
		1977 -date	-0.09581	0.12932	0.760	-0.4142	0.2226
	1965 - 1976	1946 -1964	-0.00665	0.13594	0.999	-0.3413	0.3280
		1977 -date	-0.10246	0.12706	0.723	-0.4153	0.2104
	1977 - date	1946 -1964	0.09581	0.12932	0.760	-0.2226	0.4142
		1965 -1976	0.10246	0.12706	0.723	-0.2104	0.4153
Autonomy Factor 4	1946 - 1964	1965 -1976	0.11772	0.14824	0.730	-0.2472	0.4827
		1977 -date	0.03856	0.14144	0.964	-0.3097	0.3868
	1965 - 1976	1946 -1964	-0.11772	0.14824	0.730	-0.4827	0.2472
		1977 -date	-0.07916	0.13850	0.849	-0.4201	0.2618
	1977 - date	1946 -1964	-0.03856	0.14144	0.964	-0.3868	0.3097
		1965 -1976	0.07916	0.13850	0.849	-0.2618	0.4201
Autonomy Factor 5	1946 - 1964	1965 -1976	-0.02120	0.09666	0.976	-0.2592	0.2168
		1977 -date	0.01553	0.09222	0.986	-0.2115	0.2426
	1965 - 1976	1946 -1964	0.02120	0.09666	0.976	-0.2168	0.2592
		1977 -date	0.03674	0.09031	0.921	-0.1856	0.2591
	1977 - date	1946 -1964	-0.01553	0.09222	0.986	-0.2426	0.2115
		1965 -1976	-0.03674	0.09031	0.921	-0.2591	0.1856
Autonomy_Factor_6	1946 - 1964	1965 -1976	0.13091	0.10768	0.479	-0.1342	0.3960
		1977 -date	0.03825	0.10274	0.933	-0.2147	0.2912
	1965 - 1976	1946 -1964	-0.13091	0.10768	0.479	-0.3960	0.1342
		1977 -date	-0.09266	0.10060	0.655	-0.3403	0.1550
	1977 - date	1946 -1964	-0.03825	0.10274	0.933	-0.2912	0.2147
		1965 -1976	0.09266	0.10060	0.655	-0.1550	0.3403

*. The mean difference is significant at the 0.05 level.

Post hoc test – Job level

Multiple Comparisons

Scheffe

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Relatedness Factor 1	Academic staff	Administrative	0.09491	0.15471	0.829	-0.2860	0.4758
		Operational	0.59204	0.26276	0.081	-0.0549	1.2390
	Administrative	Academic staff	-0.09491	0.15471	0.829	-0.4758	0.2860
		Operational	0.49714	0.25651	0.155	-0.1344	1.1287
	Operational	Academic staff	-0.59204	0.26276	0.081	-1.2390	0.0549
		Administrative	-0.49714	0.25651	0.155	-1.1287	0.1344
Relatedness Factor 2	Academic staff	Administrative	0.06055	0.16027	0.931	-0.3341	0.4552
		Operational	0.59141	0.27087	0.094	-0.0755	1.2583
	Administrative	Academic staff	-0.06055	0.16027	0.931	-0.4552	0.3341
		Operational	0.53086	0.26490	0.136	-0.1214	1.1831
	Operational	Academic staff	-0.59141	0.27087	0.094	-1.2583	0.0755
		Administrative	-0.53086	0.26490	0.136	-1.1831	0.1214
Competence Factor 1	Academic staff	Administrative	0.23170	0.09550	0.054	-0.0034	0.4668
		Operational	.44064*	0.16245	0.027	0.0407	0.8406
	Administrative	Academic staff	-0.23170	0.09550	0.054	-0.4668	0.0034
		Operational	0.20894	0.15849	0.421	-0.1813	0.5991
	Operational	Academic staff	-.44064*	0.16245	0.027	-0.8406	-0.0407
		Administrative	-0.20894	0.15849	0.421	-0.5991	0.1813
Competence Factor 2	Academic staff	Administrative	.27521*	0.11022	0.046	0.0038	0.5466
		Operational	.83338*	0.18719	0.000	0.3725	1.2943
	Administrative	Academic staff	-.27521*	0.11022	0.046	-0.5466	-0.0038
		Operational	.55817*	0.18274	0.010	0.1083	1.0081
	Operational	Academic staff	-.83338*	0.18719	0.000	-1.2943	-0.3725
		Administrative	-.55817*	0.18274	0.010	-1.0081	-0.1083
Competence Factor 3	Academic staff	Administrative	0.20460	0.08934	0.075	-0.0154	0.4246
		Operational	.49667*	0.15173	0.005	0.1231	0.8702
	Administrative	Academic staff	-0.20460	0.08934	0.075	-0.4246	0.0154
		Operational	0.29206	0.14812	0.145	-0.0726	0.6567
	Operational	Academic staff	-.49667*	0.15173	0.005	-0.8702	-0.1231
		Administrative	-0.29206	0.14812	0.145	-0.6567	0.0726
Autonomy Factor 1	Academic staff	Administrative	0.20061	0.11848	0.240	-0.0911	0.4923
		Operational	0.38549	0.20122	0.162	-0.1099	0.8809
	Administrative	Academic staff	-0.20061	0.11848	0.240	-0.4923	0.0911
		Operational	0.18488	0.19644	0.643	-0.2988	0.6685
	Operational	Academic staff	-0.38549	0.20122	0.162	-0.8809	0.1099
		Administrative	-0.18488	0.19644	0.643	-0.6685	0.2988
Autonomy Factor 2	Academic staff	Administrative	0.03495	0.11183	0.952	-0.2404	0.3103

		Operational	.66072*	0.18993	0.003	0.1931	1.1283
	Administrative	Academic staff	-0.03495	0.11183	0.952	-0.3103	0.2404
		Operational	.62577*	0.18541	0.004	0.1693	1.0823
	Operational	Academic staff	-.66072*	0.18993	0.003	-1.1283	-0.1931
		Administrative	-.62577*	0.18541	0.004	-1.0823	-0.1693
Autonomy Factor 3	Academic staff	Administrative	.30952*	0.10959	0.020	0.0397	0.5794
		Operational	.68667*	0.18583	0.001	0.2291	1.1442
	Administrative	Academic staff	-.30952*	0.10959	0.020	-0.5794	-0.0397
		Operational	0.37714	0.18151	0.118	-0.0698	0.8240
	Operational	Academic staff	-.68667*	0.18583	0.001	-1.1442	-0.2291
		Administrative	-0.37714	0.18151	0.118	-0.8240	0.0698
Autonomy Factor 4	Academic staff	Administrative	0.04836	0.12288	0.925	-0.2542	0.3509
		Operational	0.24980	0.20869	0.489	-0.2640	0.7636
	Administrative	Academic staff	-0.04836	0.12288	0.925	-0.3509	0.2542
		Operational	0.20144	0.20372	0.614	-0.3001	0.7030
	Operational	Academic staff	-0.24980	0.20869	0.489	-0.7636	0.2640
		Administrative	-0.20144	0.20372	0.614	-0.7030	0.3001
Autonomy Factor 5	Academic staff	Administrative	0.07946	0.08016	0.612	-0.1179	0.2768
		Operational	0.13647	0.13615	0.606	-0.1987	0.4717
	Administrative	Academic staff	-0.07946	0.08016	0.612	-0.2768	0.1179
		Operational	0.05701	0.13291	0.912	-0.2702	0.3842
	Operational	Academic staff	-0.13647	0.13615	0.606	-0.4717	0.1987
		Administrative	-0.05701	0.13291	0.912	-0.3842	0.2702
Autonomy Factor 6	Academic staff	Administrative	.22104*	0.08832	0.045	0.0036	0.4385
		Operational	0.33748	0.15000	0.082	-0.0318	0.7068
	Administrative	Academic staff	-.22104*	0.08832	0.045	-0.4385	-0.0036
		Operational	0.11643	0.14643	0.729	-0.2441	0.4770
	Operational	Academic staff	-0.33748	0.15000	0.082	-0.7068	0.0318
		Administrative	-0.11643	0.14643	0.729	-0.4770	0.2441
*. The mean difference is significant at the 0.05 level.							

Post hoc test – Tenure

Multiple Comparisons

Scheffe

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Relatedness Factor 1	< 5 years	6-10 years	0.13159	0.19426	0.977	-0.4712	0.7343
		11-15 years	0.21742	0.23710	0.933	-0.5182	0.9531
		16-20 years	-0.10966	0.28232	0.997	-0.9856	0.7663
		> 20 years	-0.07249	0.21490	0.998	-0.7393	0.5943
	6-10 years	< 5 years	-0.13159	0.19426	0.977	-0.7343	0.4712
		11-15 years	0.08583	0.24228	0.998	-0.6659	0.8376
		16-20 years	-0.24125	0.28668	0.950	-1.1308	0.6483
		> 20 years	-0.20408	0.22060	0.931	-0.8886	0.4804
	11-15 years	< 5 years	-0.21742	0.23710	0.933	-0.9531	0.5182
		6-10 years	-0.08583	0.24228	0.998	-0.8376	0.6659
		16-20 years	-0.32708	0.31728	0.900	-1.3115	0.6574
		> 20 years	-0.28991	0.25912	0.869	-1.0939	0.5141
	16-20 years	< 5 years	0.10966	0.28232	0.997	-0.7663	0.9856
		6-10 years	0.24125	0.28668	0.950	-0.6483	1.1308
		11-15 years	0.32708	0.31728	0.900	-0.6574	1.3115
		> 20 years	0.03717	0.30105	1.000	-0.8969	0.9713
	> 20 years	< 5 years	0.07249	0.21490	0.998	-0.5943	0.7393
		6-10 years	0.20408	0.22060	0.931	-0.4804	0.8886
		11-15 years	0.28991	0.25912	0.869	-0.5141	1.0939
		16-20 years	-0.03717	0.30105	1.000	-0.9713	0.8969
Relatedness Factor 2	< 5 years	6-10 years	0.20727	0.20125	0.900	-0.4172	0.8318
		11-15 years	0.22101	0.24376	0.935	-0.5354	0.9774
		16-20 years	0.22487	0.29025	0.963	-0.6758	1.1255
		> 20 years	0.04217	0.22233	1.000	-0.6477	0.7321
	6-10 years	< 5 years	-0.20727	0.20125	0.900	-0.8318	0.4172
		11-15 years	0.01374	0.25032	1.000	-0.7630	0.7905
		16-20 years	0.01760	0.29578	1.000	-0.9002	0.9354
		> 20 years	-0.16510	0.22950	0.972	-0.8773	0.5470

	11-15 years	< 5 years	-0.22101	0.24376	0.935	-0.9774	0.5354
		6-10 years	-0.01374	0.25032	1.000	-0.7905	0.7630
		16-20 years	0.00386	0.32620	1.000	-1.0083	1.0161
		> 20 years	-0.17884	0.26756	0.978	-1.0091	0.6514
	16-20 years	< 5 years	-0.22487	0.29025	0.963	-1.1255	0.6758
		6-10 years	-0.01760	0.29578	1.000	-0.9354	0.9002
		11-15 years	-0.00386	0.32620	1.000	-1.0161	1.0083
		> 20 years	-0.18270	0.31051	0.987	-1.1462	0.7808
	> 20 years	< 5 years	-0.04217	0.22233	1.000	-0.7321	0.6477
		6-10 years	0.16510	0.22950	0.972	-0.5470	0.8773
		11-15 years	0.17884	0.26756	0.978	-0.6514	1.0091
		16-20 years	0.18270	0.31051	0.987	-0.7808	1.1462
Competence Factor 1	< 5 years	6-10 years	0.06096	0.11925	0.992	-0.3090	0.4309
		11-15 years	0.33201	0.14609	0.274	-0.1213	0.7853
		16-20 years	-0.04615	0.17395	0.999	-0.5859	0.4936
		> 20 years	0.09295	0.13241	0.974	-0.3179	0.5038
	6-10 years	< 5 years	-0.06096	0.11925	0.992	-0.4309	0.3090
		11-15 years	0.27106	0.14893	0.508	-0.1910	0.7331
		16-20 years	-0.10710	0.17634	0.985	-0.6542	0.4400
		> 20 years	0.03200	0.13553	1.000	-0.3885	0.4525
	11-15 years	< 5 years	-0.33201	0.14609	0.274	-0.7853	0.1213
		6-10 years	-0.27106	0.14893	0.508	-0.7331	0.1910
		16-20 years	-0.37816	0.19549	0.444	-0.9847	0.2284
		> 20 years	-0.23906	0.15966	0.692	-0.7344	0.2563
	16-20 years	< 5 years	0.04615	0.17395	0.999	-0.4936	0.5859
		6-10 years	0.10710	0.17634	0.985	-0.4400	0.6542
		11-15 years	0.37816	0.19549	0.444	-0.2284	0.9847
		> 20 years	0.13910	0.18550	0.967	-0.4364	0.7146
	> 20 years	< 5 years	-0.09295	0.13241	0.974	-0.5038	0.3179
		6-10 years	-0.03200	0.13553	1.000	-0.4525	0.3885
		11-15 years	0.23906	0.15966	0.692	-0.2563	0.7344
		16-20 years	-0.13910	0.18550	0.967	-0.7146	0.4364
Competence Factor 2	< 5 years	6-10 years	0.01293	0.14184	1.000	-0.4272	0.4530

		11-15 years	0.16480	0.17312	0.923	-0.3724	0.7020
		16-20 years	-0.10404	0.20614	0.992	-0.7436	0.5356
		> 20 years	-0.05659	0.15691	0.998	-0.5435	0.4303
	6-10 years	< 5 years	-0.01293	0.14184	1.000	-0.4530	0.4272
		11-15 years	0.15187	0.17690	0.946	-0.3970	0.7008
		16-20 years	-0.11698	0.20933	0.989	-0.7665	0.5325
		> 20 years	-0.06952	0.16108	0.996	-0.5693	0.4303
	11-15 years	< 5 years	-0.16480	0.17312	0.923	-0.7020	0.3724
		6-10 years	-0.15187	0.17690	0.946	-0.7008	0.3970
		16-20 years	-0.26884	0.23167	0.853	-0.9876	0.4500
		> 20 years	-0.22139	0.18920	0.849	-0.8084	0.3657
	16-20 years	< 5 years	0.10404	0.20614	0.992	-0.5356	0.7436
		6-10 years	0.11698	0.20933	0.989	-0.5325	0.7665
		11-15 years	0.26884	0.23167	0.853	-0.4500	0.9876
		> 20 years	0.04745	0.21982	1.000	-0.6346	0.7295
	> 20 years	< 5 years	0.05659	0.15691	0.998	-0.4303	0.5435
		6-10 years	0.06952	0.16108	0.996	-0.4303	0.5693
		11-15 years	0.22139	0.18920	0.849	-0.3657	0.8084
		16-20 years	-0.04745	0.21982	1.000	-0.7295	0.6346
Competence Factor 3	< 5 years	6-10 years	0.00640	0.12220	1.000	-0.3727	0.3855
		11-15 years	0.18291	0.14914	0.826	-0.2798	0.6457
		16-20 years	0.22482	0.17759	0.808	-0.3262	0.7758
		> 20 years	0.05119	0.13518	0.998	-0.3682	0.4706
	6-10 years	< 5 years	-0.00640	0.12220	1.000	-0.3855	0.3727
		11-15 years	0.17650	0.15240	0.854	-0.2964	0.6494
		16-20 years	0.21841	0.18033	0.832	-0.3411	0.7779
		> 20 years	0.04479	0.13877	0.999	-0.3858	0.4753
	11-15 years	< 5 years	-0.18291	0.14914	0.826	-0.6457	0.2798
		6-10 years	-0.17650	0.15240	0.854	-0.6494	0.2964
		16-20 years	0.04191	0.19958	1.000	-0.5773	0.6612
		> 20 years	-0.13171	0.16300	0.957	-0.6375	0.3740
	16-20 years	< 5 years	-0.22482	0.17759	0.808	-0.7758	0.3262
		6-10 years	-0.21841	0.18033	0.832	-0.7779	0.3411

		11-15 years	-0.04191	0.19958	1.000	-0.6612	0.5773
		> 20 years	-0.17362	0.18937	0.933	-0.7612	0.4140
	> 20 years	< 5 years	-0.05119	0.13518	0.998	-0.4706	0.3682
		6-10 years	-0.04479	0.13877	0.999	-0.4753	0.3858
		11-15 years	0.13171	0.16300	0.957	-0.3740	0.6375
		16-20 years	0.17362	0.18937	0.933	-0.4140	0.7612
Autonomy Factor 1	< 5 years	6-10 years	-0.01443	0.14726	1.000	-0.4713	0.4425
		11-15 years	0.33400	0.17974	0.487	-0.2237	0.8917
		16-20 years	-0.05260	0.21402	1.000	-0.7166	0.6114
		> 20 years	0.04247	0.16291	0.999	-0.4630	0.5479
	6-10 years	< 5 years	0.01443	0.14726	1.000	-0.4425	0.4713
		11-15 years	0.34843	0.18366	0.465	-0.2214	0.9183
		16-20 years	-0.03817	0.21732	1.000	-0.7125	0.6361
		> 20 years	0.05690	0.16723	0.998	-0.4620	0.5758
	11-15 years	< 5 years	-0.33400	0.17974	0.487	-0.8917	0.2237
		6-10 years	-0.34843	0.18366	0.465	-0.9183	0.2214
		16-20 years	-0.38660	0.24052	0.630	-1.1329	0.3597
		> 20 years	-0.29153	0.19643	0.699	-0.9010	0.3179
	16-20 years	< 5 years	0.05260	0.21402	1.000	-0.6114	0.7166
		6-10 years	0.03817	0.21732	1.000	-0.6361	0.7125
		11-15 years	0.38660	0.24052	0.630	-0.3597	1.1329
		> 20 years	0.09507	0.22822	0.996	-0.6130	0.8032
	> 20 years	< 5 years	-0.04247	0.16291	0.999	-0.5479	0.4630
		6-10 years	-0.05690	0.16723	0.998	-0.5758	0.4620
		11-15 years	0.29153	0.19643	0.699	-0.3179	0.9010
		16-20 years	-0.09507	0.22822	0.996	-0.8032	0.6130
Autonomy Factor 2	< 5 years	6-10 years	-0.16062	0.14156	0.863	-0.5998	0.2786
		11-15 years	-0.18502	0.17277	0.886	-0.7211	0.3511
		16-20 years	-0.11138	0.20573	0.990	-0.7497	0.5269
		> 20 years	-0.21290	0.15660	0.764	-0.6988	0.2730
	6-10 years	< 5 years	0.16062	0.14156	0.863	-0.2786	0.5998
		11-15 years	-0.02439	0.17655	1.000	-0.5722	0.5234

		16-20 years	0.04924	0.20890	1.000	-0.5989	0.6974
		> 20 years	-0.05228	0.16075	0.999	-0.5511	0.4465
	11-15 years	< 5 years	0.18502	0.17277	0.886	-0.3511	0.7211
		6-10 years	0.02439	0.17655	1.000	-0.5234	0.5722
		16-20 years	0.07364	0.23120	0.999	-0.6437	0.7910
		> 20 years	-0.02788	0.18882	1.000	-0.6137	0.5580
	16-20 years	< 5 years	0.11138	0.20573	0.990	-0.5269	0.7497
		6-10 years	-0.04924	0.20890	1.000	-0.6974	0.5989
		11-15 years	-0.07364	0.23120	0.999	-0.7910	0.6437
		> 20 years	-0.10152	0.21938	0.995	-0.7822	0.5791
	> 20 years	< 5 years	0.21290	0.15660	0.764	-0.2730	0.6988
		6-10 years	0.05228	0.16075	0.999	-0.4465	0.5511
		11-15 years	0.02788	0.18882	1.000	-0.5580	0.6137
		16-20 years	0.10152	0.21938	0.995	-0.5791	0.7822
Autonomy Factor 3	< 5 years	6-10 years	0.00326	0.13892	1.000	-0.4278	0.4343
		11-15 years	0.20037	0.16892	0.843	-0.3238	0.7245
		16-20 years	0.43773	0.20114	0.318	-0.1864	1.0618
		> 20 years	0.06469	0.15310	0.996	-0.4104	0.5397
	6-10 years	< 5 years	-0.00326	0.13892	1.000	-0.4343	0.4278
		11-15 years	0.19710	0.17303	0.861	-0.3398	0.7340
		16-20 years	0.43447	0.20460	0.344	-0.2004	1.0693
		> 20 years	0.06143	0.15763	0.997	-0.4277	0.5505
	11-15 years	< 5 years	-0.20037	0.16892	0.843	-0.7245	0.3238
		6-10 years	-0.19710	0.17303	0.861	-0.7340	0.3398
		16-20 years	0.23737	0.22604	0.894	-0.4640	0.9387
		> 20 years	-0.13568	0.18461	0.969	-0.7085	0.4371
	16-20 years	< 5 years	-0.43773	0.20114	0.318	-1.0618	0.1864
		6-10 years	-0.43447	0.20460	0.344	-1.0693	0.2004
		11-15 years	-0.23737	0.22604	0.894	-0.9387	0.4640
		> 20 years	-0.37304	0.21448	0.555	-1.0385	0.2925
	> 20 years	< 5 years	-0.06469	0.15310	0.996	-0.5397	0.4104
		6-10 years	-0.06143	0.15763	0.997	-0.5505	0.4277
		11-15 years	0.13568	0.18461	0.969	-0.4371	0.7085

		16-20 years	0.37304	0.21448	0.555	-0.2925	1.0385
Autonomy Factor 4	< 5 years	6-10 years	0.14881	0.15246	0.917	-0.3242	0.6218
		11-15 years	0.18891	0.18608	0.905	-0.3884	0.7663
		16-20 years	-0.01673	0.22157	1.000	-0.7042	0.6707
		> 20 years	-0.01992	0.16866	1.000	-0.5432	0.5034
	6-10 years	< 5 years	-0.14881	0.15246	0.917	-0.6218	0.3242
		11-15 years	0.04010	0.19014	1.000	-0.5499	0.6301
		16-20 years	-0.16554	0.22499	0.969	-0.8636	0.5326
		> 20 years	-0.16873	0.17313	0.917	-0.7059	0.3684
	11-15 years	< 5 years	-0.18891	0.18608	0.905	-0.7663	0.3884
		6-10 years	-0.04010	0.19014	1.000	-0.6301	0.5499
		16-20 years	-0.20564	0.24900	0.953	-0.9782	0.5670
		> 20 years	-0.20883	0.20336	0.901	-0.8398	0.4222
	16-20 years	< 5 years	0.01673	0.22157	1.000	-0.6707	0.7042
		6-10 years	0.16554	0.22499	0.969	-0.5326	0.8636
		11-15 years	0.20564	0.24900	0.953	-0.5670	0.9782
		> 20 years	-0.00319	0.23627	1.000	-0.7363	0.7299
	> 20 years	< 5 years	0.01992	0.16866	1.000	-0.5034	0.5432
		6-10 years	0.16873	0.17313	0.917	-0.3684	0.7059
		11-15 years	0.20883	0.20336	0.901	-0.4222	0.8398
		16-20 years	0.00319	0.23627	1.000	-0.7299	0.7363
Autonomy Factor 5	< 5 years	6-10 years	0.00548	0.09888	1.000	-0.3013	0.3123
		11-15 years	0.11111	0.12068	0.932	-0.2633	0.4856
		16-20 years	-0.21498	0.14370	0.692	-0.6608	0.2309
		> 20 years	-0.05889	0.10938	0.990	-0.3983	0.2805
	6-10 years	< 5 years	-0.00548	0.09888	1.000	-0.3123	0.3013
		11-15 years	0.10563	0.12332	0.947	-0.2770	0.4883
		16-20 years	-0.22045	0.14592	0.684	-0.6732	0.2323
		> 20 years	-0.06437	0.11229	0.988	-0.4128	0.2840
	11-15 years	< 5 years	-0.11111	0.12068	0.932	-0.4856	0.2633
		6-10 years	-0.10563	0.12332	0.947	-0.4883	0.2770
		16-20 years	-0.32609	0.16150	0.398	-0.8272	0.1750
		> 20 years	-0.17000	0.13189	0.798	-0.5792	0.2392

	16-20 years	< 5 years	0.21498	0.14370	0.692	-0.2309	0.6608
		6-10 years	0.22045	0.14592	0.684	-0.2323	0.6732
		11-15 years	0.32609	0.16150	0.398	-0.1750	0.8272
		> 20 years	0.15609	0.15324	0.904	-0.3194	0.6315
	> 20 years	< 5 years	0.05889	0.10938	0.990	-0.2805	0.3983
		6-10 years	0.06437	0.11229	0.988	-0.2840	0.4128
		11-15 years	0.17000	0.13189	0.798	-0.2392	0.5792
		16-20 years	-0.15609	0.15324	0.904	-0.6315	0.3194
Autonomy Factor 6	< 5 years	6-10 years	0.07008	0.11047	0.982	-0.2727	0.4128
		11-15 years	0.20831	0.13483	0.665	-0.2100	0.6267
		16-20 years	-0.14477	0.16055	0.936	-0.6429	0.3534
		> 20 years	0.03141	0.12221	0.999	-0.3478	0.4106
	6-10 years	< 5 years	-0.07008	0.11047	0.982	-0.4128	0.2727
		11-15 years	0.13822	0.13778	0.909	-0.2893	0.5657
		16-20 years	-0.21485	0.16303	0.784	-0.7207	0.2910
		> 20 years	-0.03868	0.12545	0.999	-0.4279	0.3506
	11-15 years	< 5 years	-0.20831	0.13483	0.665	-0.6267	0.2100
		6-10 years	-0.13822	0.13778	0.909	-0.5657	0.2893
		16-20 years	-0.35307	0.18043	0.431	-0.9129	0.2067
		> 20 years	-0.17690	0.14735	0.837	-0.6341	0.2803
	16-20 years	< 5 years	0.14477	0.16055	0.936	-0.3534	0.6429
		6-10 years	0.21485	0.16303	0.784	-0.2910	0.7207
		11-15 years	0.35307	0.18043	0.431	-0.2067	0.9129
		> 20 years	0.17617	0.17120	0.900	-0.3550	0.7074
	> 20 years	< 5 years	-0.03141	0.12221	0.999	-0.4106	0.3478
		6-10 years	0.03868	0.12545	0.999	-0.3506	0.4279
		11-15 years	0.17690	0.14735	0.837	-0.2803	0.6341
		16-20 years	-0.17617	0.17120	0.900	-0.7074	0.3550

Post hoc tests – Highest Level of Education

Scheffe							
Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Relatedness Factor 1	High School Certificate	Diploma	-0.22878	0.35680	0.938	-1.2329	0.7753
		Degree	0.30429	0.30520	0.803	-0.5546	1.1632
		Postgraduate	0.48618	0.25013	0.289	-0.2177	1.1901
	Diploma	High School Certificate	0.22878	0.35680	0.938	-0.7753	1.2329
		Degree	0.53306	0.33243	0.464	-0.4024	1.4686
		Postgraduate	0.71495	0.28271	0.097	-0.0806	1.5105
	Degree	High School Certificate	-0.30429	0.30520	0.803	-1.1632	0.5546
		Diploma	-0.53306	0.33243	0.464	-1.4686	0.4024
		Postgraduate	0.18189	0.21394	0.868	-0.4202	0.7839
	Postgraduate	High School Certificate	-0.48618	0.25013	0.289	-1.1901	0.2177
		Diploma	-0.71495	0.28271	0.097	-1.5105	0.0806
		Degree	-0.18189	0.21394	0.868	-0.7839	0.4202
Relatedness Factor 2	High School Certificate	Diploma	0.24421	0.36698	0.931	-0.7886	1.2770
		Degree	0.70683	0.31391	0.170	-0.1766	1.5903
		Postgraduate	0.69991	0.25753	0.063	-0.0249	1.4247
	Diploma	High School Certificate	-0.24421	0.36698	0.931	-1.2770	0.7886
		Degree	0.46261	0.34191	0.609	-0.4996	1.4249
		Postgraduate	0.45570	0.29101	0.485	-0.3633	1.2747
	Degree	High School Certificate	-0.70683	0.31391	0.170	-1.5903	0.1766
		Diploma	-0.46261	0.34191	0.609	-1.4249	0.4996
		Postgraduate	-0.00691	0.22035	1.000	-0.6270	0.6132
	Postgraduate	High School Certificate	-0.69991	0.25753	0.063	-1.4247	0.0249
		Diploma	-0.45570	0.29101	0.485	-1.2747	0.3633
		Degree	0.00691	0.22035	1.000	-0.6132	0.6270
Competence Factor 1	High School Certificate	Diploma	-0.17823	0.22588	0.891	-0.8139	0.4574
		Degree	-0.13170	0.19214	0.925	-0.6724	0.4090
		Postgraduate	-0.10499	0.15835	0.932	-0.5506	0.3406

	Diploma	High School Certificate	0.17823	0.22588	0.891	-0.4574	0.8139
		Degree	0.04653	0.20947	0.997	-0.5429	0.6360
		Postgraduate	0.07324	0.17898	0.983	-0.4304	0.5769
	Degree	High School Certificate	0.13170	0.19214	0.925	-0.4090	0.6724
		Diploma	-0.04653	0.20947	0.997	-0.6360	0.5429
		Postgraduate	0.02671	0.13390	0.998	-0.3501	0.4035
	Postgraduate	High School Certificate	0.10499	0.15835	0.932	-0.3406	0.5506
		Diploma	-0.07324	0.17898	0.983	-0.5769	0.4304
		Degree	-0.02671	0.13390	0.998	-0.4035	0.3501
Competence Factor 2	High School Certificate	Diploma	-0.49769	0.26278	0.312	-1.2372	0.2418
		Degree	-0.13236	0.22353	0.950	-0.7614	0.4967
		Postgraduate	-0.36061	0.18428	0.283	-0.8792	0.1580
	Diploma	High School Certificate	0.49769	0.26278	0.312	-0.2418	1.2372
		Degree	0.36534	0.24369	0.524	-0.3204	1.0511
		Postgraduate	0.13709	0.20827	0.933	-0.4490	0.7232
	Degree	High School Certificate	0.13236	0.22353	0.950	-0.4967	0.7614
		Diploma	-0.36534	0.24369	0.524	-1.0511	0.3204
		Postgraduate	-0.22825	0.15585	0.544	-0.6668	0.2103
	Postgraduate	High School Certificate	0.36061	0.18428	0.283	-0.1580	0.8792
		Diploma	-0.13709	0.20827	0.933	-0.7232	0.4490
		Degree	0.22825	0.15585	0.544	-0.2103	0.6668
Competence Factor 3	High School Certificate	Diploma	-0.11368	0.22758	0.969	-0.7541	0.5267
		Degree	0.19333	0.19359	0.802	-0.3514	0.7381
		Postgraduate	-0.10296	0.15960	0.937	-0.5521	0.3462
	Diploma	High School Certificate	0.11368	0.22758	0.969	-0.5267	0.7541
		Degree	0.30702	0.21104	0.550	-0.2869	0.9009
		Postgraduate	0.01072	0.18037	1.000	-0.4969	0.5183
	Degree	High School Certificate	-0.19333	0.19359	0.802	-0.7381	0.3514
		Diploma	-0.30702	0.21104	0.550	-0.9009	0.2869

		Postgraduate	-0.29630	0.13497	0.188	-0.6761	0.0835
	Postgraduate	High School Certificate	0.10296	0.15960	0.937	-0.3462	0.5521
		Diploma	-0.01072	0.18037	1.000	-0.5183	0.4969
		Degree	0.29630	0.13497	0.188	-0.0835	0.6761
Autonomy Factor 1	High School Certificate	Diploma	-0.70947	0.27339	0.084	-1.4788	0.0599
		Degree	-0.48757	0.23256	0.224	-1.1420	0.1669
		Postgraduate	-0.31630	0.19172	0.438	-0.8558	0.2232
	Diploma	High School Certificate	0.70947	0.27339	0.084	-0.0599	1.4788
		Degree	0.22191	0.25352	0.857	-0.4915	0.9353
		Postgraduate	0.39318	0.21668	0.351	-0.2166	1.0029
	Degree	High School Certificate	0.48757	0.23256	0.224	-0.1669	1.1420
		Diploma	-0.22191	0.25352	0.857	-0.9353	0.4915
		Postgraduate	0.17127	0.16214	0.773	-0.2850	0.6276
	Postgraduate	High School Certificate	0.31630	0.19172	0.438	-0.2232	0.8558
		Diploma	-0.39318	0.21668	0.351	-1.0029	0.2166
		Degree	-0.17127	0.16214	0.773	-0.6276	0.2850
Autonomy Factor 2	High School Certificate	Diploma	-0.43737	0.26397	0.434	-1.1802	0.3055
		Degree	-0.22649	0.22454	0.797	-0.8584	0.4054
		Postgraduate	-0.32704	0.18511	0.375	-0.8480	0.1939
	Diploma	High School Certificate	0.43737	0.26397	0.434	-0.3055	1.1802
		Degree	0.21088	0.24479	0.863	-0.4780	0.8997
		Postgraduate	0.11033	0.20921	0.964	-0.4784	0.6991
	Degree	High School Certificate	0.22649	0.22454	0.797	-0.4054	0.8584
		Diploma	-0.21088	0.24479	0.863	-0.8997	0.4780
		Postgraduate	-0.10055	0.15655	0.938	-0.5411	0.3400
	Postgraduate	High School Certificate	0.32704	0.18511	0.375	-0.1939	0.8480
		Diploma	-0.11033	0.20921	0.964	-0.6991	0.4784
		Degree	0.10055	0.15655	0.938	-0.3400	0.5411
Autonomy Factor 3	High School Certificate	Diploma	-0.10737	0.25980	0.982	-0.8385	0.6237
		Degree	0.13730	0.22099	0.943	-0.4846	0.7592

		Postgraduate	-0.16559	0.18225	0.843	-0.6785	0.3473
	Diploma	High School Certificate	0.10737	0.25980	0.982	-0.6237	0.8385
		Degree	0.24467	0.24092	0.794	-0.4333	0.9227
		Postgraduate	-0.05822	0.20596	0.994	-0.6378	0.5214
	Degree	High School Certificate	-0.13730	0.22099	0.943	-0.7592	0.4846
		Diploma	-0.24467	0.24092	0.794	-0.9227	0.4333
		Postgraduate	-0.30288	0.15415	0.279	-0.7367	0.1309
	Postgraduate	High School Certificate	0.16559	0.18225	0.843	-0.3473	0.6785
		Diploma	0.05822	0.20596	0.994	-0.5214	0.6378
		Degree	0.30288	0.15415	0.279	-0.1309	0.7367
Autonomy Factor 4	High School Certificate	Diploma	-0.04877	0.28441	0.999	-0.8491	0.7516
		Degree	0.09063	0.24193	0.987	-0.5902	0.7714
		Postgraduate	0.22667	0.19945	0.731	-0.3346	0.7879
	Diploma	High School Certificate	0.04877	0.28441	0.999	-0.7516	0.8491
		Degree	0.13940	0.26374	0.964	-0.6028	0.8816
		Postgraduate	0.27544	0.22541	0.684	-0.3589	0.9098
	Degree	High School Certificate	-0.09063	0.24193	0.987	-0.7714	0.5902
		Diploma	-0.13940	0.26374	0.964	-0.8816	0.6028
		Postgraduate	0.13604	0.16868	0.885	-0.3386	0.6107
	Postgraduate	High School Certificate	-0.22667	0.19945	0.731	-0.7879	0.3346
		Diploma	-0.27544	0.22541	0.684	-0.9098	0.3589
		Degree	-0.13604	0.16868	0.885	-0.6107	0.3386
Autonomy Factor 5	High School Certificate	Diploma	0.08737	0.18637	0.974	-0.4371	0.6118
		Degree	-0.03568	0.15853	0.997	-0.4818	0.4105
		Postgraduate	0.02333	0.13070	0.998	-0.3445	0.3911
	Diploma	High School Certificate	-0.08737	0.18637	0.974	-0.6118	0.4371
		Degree	-0.12304	0.17283	0.917	-0.6094	0.3633
		Postgraduate	-0.06404	0.14771	0.979	-0.4797	0.3516
	Degree	High School Certificate	0.03568	0.15853	0.997	-0.4105	0.4818

		Diploma	0.12304	0.17283	0.917	-0.3633	0.6094
		Postgraduate	0.05901	0.11053	0.963	-0.2520	0.3701
	Postgraduate	High School Certificate	-0.02333	0.13070	0.998	-0.3911	0.3445
		Diploma	0.06404	0.14771	0.979	-0.3516	0.4797
		Degree	-0.05901	0.11053	0.963	-0.3701	0.2520
Autonomy Factor 6	High School Certificate	Diploma	-0.38905	0.20616	0.315	-0.9692	0.1911
		Degree	-0.36395	0.17537	0.233	-0.8575	0.1296
		Postgraduate	-0.22004	0.14458	0.511	-0.6269	0.1868
	Diploma	High School Certificate	0.38905	0.20616	0.315	-0.1911	0.9692
		Degree	0.02511	0.19118	0.999	-0.5129	0.5631
		Postgraduate	0.16902	0.16340	0.784	-0.2908	0.6288
	Degree	High School Certificate	0.36395	0.17537	0.233	-0.1296	0.8575
		Diploma	-0.02511	0.19118	0.999	-0.5631	0.5129
		Postgraduate	0.14391	0.12227	0.709	-0.2002	0.4880
	Postgraduate	High School Certificate	0.22004	0.14458	0.511	-0.1868	0.6269
		Diploma	-0.16902	0.16340	0.784	-0.6288	0.2908
		Degree	-0.14391	0.12227	0.709	-0.4880	0.2002

Appendix N: Independent samples test (t-test)

T-tests statistics - Gender groups

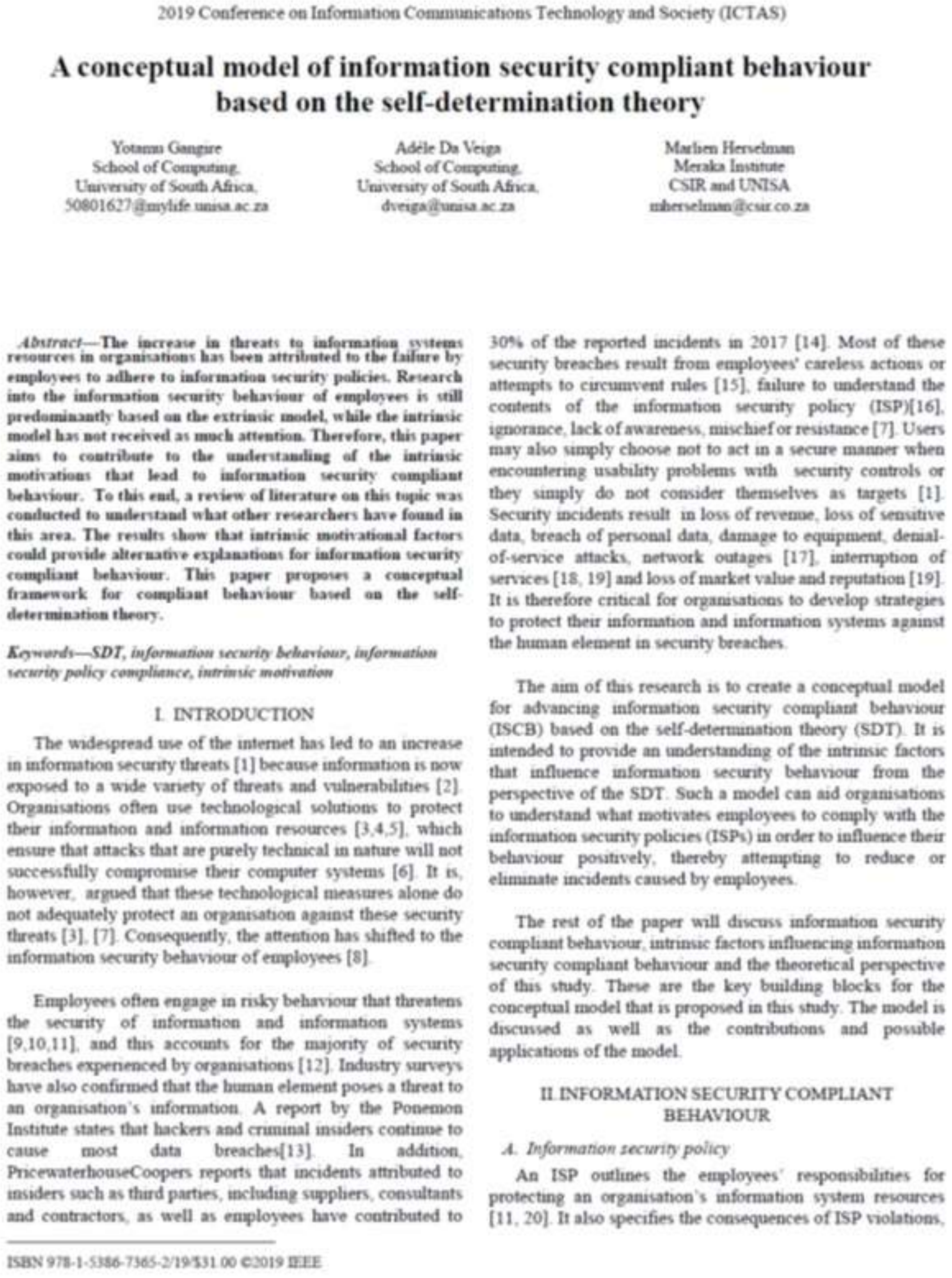
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Relatedness Factor 1	Equal variances assumed	0.835	0.362	1.182	257	0.238	0.17660	0.14940	-0.11760	0.47080
	Equal variances not assumed			1.192	251.365	0.234	0.17660	0.14812	-0.11511	0.46832
Relatedness Factor 2	Equal variances assumed	0.576	0.449	0.181	254	0.857	0.02804	0.15490	-0.27702	0.33310
	Equal variances not assumed			0.182	247.252	0.856	0.02804	0.15396	-0.27520	0.33128
Competence Factor 1	Equal variances assumed	0.599	0.440	0.095	258	0.925	0.00874	0.09248	-0.17336	0.19084
	Equal variances not assumed			0.094	242.222	0.925	0.00874	0.09286	-0.17417	0.19165
Competence Factor 2	Equal variances assumed	1.981	0.160	0.550	257	0.583	0.05966	0.10853	-0.15407	0.27339
	Equal variances not assumed			0.541	228.708	0.589	0.05966	0.11018	-0.15745	0.27676
Competence Factor 3	Equal variances assumed	1.065	0.303	-0.196	257	0.845	-0.01853	0.09438	-0.20438	0.16732
	Equal variances not assumed			-0.200	256.798	0.842	-0.01853	0.09262	-0.20091	0.16386
Autonomy Factor 1	Equal variances assumed	0.507	0.477	1.531	257	0.127	0.17304	0.11303	-0.04955	0.39563
	Equal variances not assumed			1.519	238.104	0.130	0.17304	0.11389	-0.05133	0.39740
Autonomy Factor 2	Equal variances assumed	6.991	0.009	2.011	257	0.045	0.21662	0.10774	0.00445	0.42878
	Equal variances not assumed			1.965	217.696	0.051	0.21662	0.11025	-0.00069	0.43392
Autonomy Factor 3	Equal variances assumed	1.826	0.178	-0.367	256	0.714	-0.03946	0.10763	-0.25141	0.17249
	Equal variances not assumed			-0.373	255.756	0.709	-0.03946	0.10579	-0.24779	0.16887
Autonomy Factor 4	Equal variances assumed	3.034	0.083	0.218	257	0.827	0.02562	0.11732	-0.20541	0.25665
	Equal variances not assumed			0.221	254.127	0.825	0.02562	0.11605	-0.20293	0.25417
Autonomy Factor 5	Equal variances assumed	0.023	0.879	0.206	257	0.837	0.01567	0.07593	-0.13385	0.16520
	Equal variances not assumed			0.208	252.618	0.835	0.01567	0.07531	-0.13264	0.16399
Autonomy Factor 6	Equal variances assumed	1.077	0.300	0.685	257	0.494	0.05840	0.08524	-0.10947	0.22626
	Equal variances not assumed			0.676	230.178	0.500	0.05840	0.08644	-0.11192	0.22872

Group statistics

Gender		N	Mean	Std. Deviation	Std. Error Mean
Relatedness Factor 1	Female	144	3.0897	1.23406	0.10284
	Male	115	2.9131	1.14318	0.10660
Relatedness Factor 2	Female	142	3.2651	1.26179	0.10589
	Male	114	3.2371	1.19330	0.11176
Competence Factor 1	Female	144	4.2347	0.72848	0.06071
	Male	116	4.2260	0.75677	0.07026
Competence Factor 2	Female	143	4.1555	0.80970	0.06771
	Male	116	4.0959	0.93619	0.08692
Competence Factor 3	Female	143	4.4068	0.81280	0.06797
	Male	116	4.4253	0.67757	0.06291
Autonomy Factor 1	Female	143	4.1702	0.87467	0.07314
	Male	116	3.9971	0.94024	0.08730
Autonomy Factor 2	Female	143	4.4027	0.77020	0.06441
	Male	116	4.1861	0.96380	0.08949
Autonomy Factor 3	Female	142	4.4261	0.92243	0.07741
	Male	116	4.4655	0.77663	0.07211
Autonomy Factor 4	Female	143	3.9825	0.98098	0.08203
	Male	116	3.9569	0.88414	0.08209
Autonomy Factor 5	Female	143	4.6364	0.62850	0.05256
	Male	116	4.6207	0.58093	0.05394
Autonomy Factor 6	Female	143	4.4942	0.63956	0.05348
	Male	116	4.4358	0.73143	0.06791

Appendix O: Conference papers published

2019 Conference on Information Communications Technology and Society



2019 Conference on Information Communications Technology and Society (ICTAS)

A conceptual model of information security compliant behaviour based on the self-determination theory

Yotamu Gangire
School of Computing,
University of South Africa,
50801627@mylife.unisa.ac.za

Adéle Da Veiga
School of Computing,
University of South Africa,
dveiga@unisa.ac.za

Marlien Herselman
Meraka Institute
CSIR and UNISA
mherselman@csir.co.za

***Abstract*—The increase in threats to information systems resources in organisations has been attributed to the failure by employees to adhere to information security policies. Research into the information security behaviour of employees is still predominantly based on the extrinsic model, while the intrinsic model has not received as much attention. Therefore, this paper aims to contribute to the understanding of the intrinsic motivations that lead to information security compliant behaviour. To this end, a review of literature on this topic was conducted to understand what other researchers have found in this area. The results show that intrinsic motivational factors could provide alternative explanations for information security compliant behaviour. This paper proposes a conceptual framework for compliant behaviour based on the self-determination theory.**

***Keywords*—SDT, information security behaviour, information security policy compliance, intrinsic motivation**

I. INTRODUCTION

The widespread use of the internet has led to an increase in information security threats [1] because information is now exposed to a wide variety of threats and vulnerabilities [2]. Organisations often use technological solutions to protect their information and information resources [3,4,5], which ensure that attacks that are purely technical in nature will not successfully compromise their computer systems [6]. It is, however, argued that these technological measures alone do not adequately protect an organisation against these security threats [3], [7]. Consequently, the attention has shifted to the information security behaviour of employees [8].

Employees often engage in risky behaviour that threatens the security of information and information systems [9,10,11], and this accounts for the majority of security breaches experienced by organisations [12]. Industry surveys have also confirmed that the human element poses a threat to an organisation's information. A report by the Ponemon Institute states that hackers and criminal insiders continue to cause most data breaches[13]. In addition, PricewaterhouseCoopers reports that incidents attributed to insiders such as third parties, including suppliers, consultants and contractors, as well as employees have contributed to 30% of the reported incidents in 2017 [14]. Most of these security breaches result from employees' careless actions or attempts to circumvent rules [15], failure to understand the contents of the information security policy (ISP)[16], ignorance, lack of awareness, mischief or resistance [7]. Users may also simply choose not to act in a secure manner when encountering usability problems with security controls or they simply do not consider themselves as targets [1]. Security incidents result in loss of revenue, loss of sensitive data, breach of personal data, damage to equipment, denial-of-service attacks, network outages [17], interruption of services [18, 19] and loss of market value and reputation [19]. It is therefore critical for organisations to develop strategies to protect their information and information systems against the human element in security breaches.

The aim of this research is to create a conceptual model for advancing information security compliant behaviour (ISCB) based on the self-determination theory (SDT). It is intended to provide an understanding of the intrinsic factors that influence information security behaviour from the perspective of the SDT. Such a model can aid organisations to understand what motivates employees to comply with the information security policies (ISPs) in order to influence their behaviour positively, thereby attempting to reduce or eliminate incidents caused by employees.

The rest of the paper will discuss information security compliant behaviour, intrinsic factors influencing information security compliant behaviour and the theoretical perspective of this study. These are the key building blocks for the conceptual model that is proposed in this study. The model is discussed as well as the contributions and possible applications of the model.

II. INFORMATION SECURITY COMPLIANT BEHAVIOUR

A. Information security policy

An ISP outlines the employees' responsibilities for protecting an organisation's information system resources [11, 20]. It also specifies the consequences of ISP violations,

ISBN 978-1-5386-7365-2/19/$31.00 ©2019 IEEE

responsibilities for information security and the training that employees should receive [20]. ISPs are implemented to reduce information security risks to organisations [11, 21, 22]. However, employees do not always behave as prescribed by the ISPs [23], due to ignorance [24], complacency, negligence, apathy, mischief, or resistance [11].

B. Compliance

Compliance is referred to as the adherence by employees to the information security policies as they are performing their jobs [4, 8, 25, 26]. Therefore, employees must always consider the effects and consequences of their information security behaviour as they work with the various information systems[7].

For the purposes of this study, information security compliant behaviour refers to actions that employees perform as part of their job, to protect the information and technology resources of their organisation from malicious others in order to maintain the confidentiality, availability, integrity and privacy of data/information.

Compliance with the information security policies is the first step in building the proposed model. Behaviour that conforms to the requirements of the respective information security policies must have some motivating influence. The next section will discuss motivation as it influences ISCB.

III. THE INFLUENCE OF INTRINSIC MOTIVATION ON INFORMATION SECURITY COMPLIANT BEHAVIOUR

Researchers distinguish between intrinsic and extrinsic motivation. Intrinsic motivation refers to behaviour performed for itself [27]; it is performed for the resultant challenge and interest [28]. Extrinsic motivation refers to behaviour performed for a goal such as a reward or avoidance of punishment [29, 30]. Some researchers have used the extrinsic model which is based on deterrence in discouraging employees from misusing information resources in organisations [31]. Although [32] found that the deterrence model is still important, it is not sufficient to motivate employees to comply with the ISPs. The need exists for an approach that will focus on intrinsic motivational factors [8, 33], as few studies have thus far focused on the role of intrinsic motivation [34, 35].

A study by [36] examined the influence of both extrinsic and intrinsic motivational factors on ISP compliance intentions. They reported that perceived effectiveness, and the intrinsic motivational factor, positively influenced information security compliance intentions. On the other hand, extrinsic motivational factors such as severity of penalty, certainty of detection, peer behaviour, and normative beliefs were only partially supported. The findings by [36] suggest that both intrinsic and extrinsic motivators can influence the information systems security behaviour of employees. If employees perceive that their information security behaviour can have a significant effect on the organisation's information security goal, they are more likely to comply with the ISPs [36].

A study by [33] examined the influence of extrinsic motivational factors, namely perceived certainty and severity of sanctions, and intrinsic motivational factors, perceived legitimacy and perceived value congruence of ISP compliance. Perceived legitimacy refers to whether employees view the information security policy as legitimate or not, that is, the extent to which employees view the policy as appropriate, desirable and just [33]. When the significance of the ISPs is properly and successfully communicated, employees will perceive the policies to be legitimate [33,35]. Perceived value congruence refers to employees' assessment of the extent to which they share the same values with the organisation. People will validate and reinforce their beliefs by choosing to interact with others whose beliefs and values align with theirs [33]. The study showed that intrinsic motivational factors significantly influenced information security policy compliance. However, contrary to expectations, the influence of extrinsic factors was not significant.

According to [37] employees will develop intrinsic motivation towards ISP compliance if the ISPs are considered fair. They define ISP fairness as an employee's belief that the requirements of the ISPs are fair. In their study, ISP fairness was examined as a moderator of the perceived organisational cost of non-compliance (CNC) and the perceived organisational cost of compliance (CC), and it was found to influence perceived organisational cost of non-compliance.

In a study that integrated the theory of planned behaviour(TPB) with SDT/organismic integration theory (OIT), [32] found that employees who perceive their behaviour as self-determined and internalise information security policies will comply with these information security policies. In contrast, they found that deterrence mechanisms had no effect on the intention to comply. Internalisation of regulations will likely occur when they align with one's values [8], and when one has the competence to achieve the actions[38]. Therefore, management must prioritise shifting employees' perceived locus of causality from external to internal.

The discussion above suggests that intrinsic motivation is as important as extrinsic motivation (if not more important), and that it could provide additional insights into the study of compliance in information security. The above section has shown what other researchers have found about intrinsic motivation, namely that intrinsic motivation influences information security compliant behaviour. Thus, intrinsic motivation becomes the first building block for the proposed model. The next section will discuss the theory underpinning the proposed model, which is the second building block for the proposed model.

IV. THEORETICAL PERSPECTIVE

There is no consensus among researchers, however, on the best theoretical framework for security policy compliant behaviour [22], as different studies use different theories. A number of theories and models have been used such as the theory of reasoned action (TRA), theory of planned behaviour (TPB), general deterrence theory (GDT), protection motivation theory (PMT), technology acceptance model (TAM), and many more. A literature review by [39] identified the theories frequently studied in information systems security behaviour. They found 54 theories and the following to be the most frequently studied: the protection motivation theory (PMT), theory of planned behaviour (TPB), general deterrence theory (GDT), and technology acceptance model (TAM). In the following section, the researcher will discuss the SDT that was applied in this study. The SDT was chosen because it has not received much attention in information security research [8, 40] and also because it explains individuals' source of intrinsic motivation.

A. The self-determination theory

The self-determination theory states that the fulfilment of the three basic psychological needs of autonomy, competence and relatedness acts as a source of intrinsic motivation [41]–[43]. According to [41], positive competence beliefs, together with a sense of autonomy, tend to enhance intrinsic motivation. Intrinsic motivation is associated with behaviour that is self-determined [43]. The theory also posits that people's relationships and social contexts must support the human needs for autonomy, competence, and relatedness [44]. The environment can support or thwart employees' basic psychological needs for competence, relatedness, and autonomy [45]. The theory has been used before in other information security studies [8], [32], [35], [46].

B. The need for autonomy

Autonomy relates to the inherent desire to act with a sense of choice and volition, with one having the confidence that the behaviour or action is purely self-determined [40, 43]. When the need for autonomy is satisfied, employees will feel more connected to the organisation and feel more effective [45]. Employees who perceive their behaviour to be self-determined are more likely to comply with ISPs[32]. These employees can therefore be trusted to work with minimum supervision, as their behaviour will decrease the costs of security [47].

C. The need for relatedness

Relatedness refers to the desire to feel connected to others as a member of a group [40, 43]. Satisfaction of the need to be connected to others supports people's tendency to internalise the values and regulations of the group[48]. Thus, when work is structured to encourage interdependence among employees, identification with work groups, respect and concern among employees, it influences internalisation and autonomous motivation. [48]. Satisfaction of the need to belong results in attachment to the organisation, which will have a positive influence on employee compliance with ISPs [31], [49].

D. The need for competence

The need for competence relates to people's desire to feel capable and to feel effective in their interactions with the surroundings [40, 43], and it is likened to the self-efficacy concept[50]. Self-efficacy refers to one's belief that one will succeed in carrying out a given task [50]. In the domain of information security, it is the belief that one has the necessary skills required to protect information and information systems from security threats [7], [51]. It implies that employees perceive that they have the ability to adhere to information security policies[7], [49], [52]. Self-efficacy was confirmed to affect employee information security policy compliance intention positively[53]–[55].

V. SECURITY ASPECTS

These aspects refer to the information security compliant behaviours that users are expected to demonstrate in order to protect information and information system resources. Security controls focus on the measures that are required to protect information and the privacy of individuals[56]. They are put in place to prevent, mitigate and detect attacks [57]. *NIST Special Publication* 800-12 R1 defines families of control, where each family has a list of controls that deals with a specific security goal [58]. These security and privacy controls must be effective and adequate to reduce information security risk while complying with security and privacy requirements as required by laws, regulations and policies [56]. Therefore, users must demonstrate certain information security compliant behaviours in order to protect information and information system resources.

The various security controls and procedures that users need to illustrate information security compliant behaviour towards will include for example, selecting strong passwords, avoid using the default security password, avoid sharing passwords with other system users [59]; to back up important data regularly and store the backups in a secure location [49]; and not disclose sensitive information[7].

VI. CONCEPTUAL MODEL

This section introduces the conceptual model which is based on the SDT. The model is predicated on intrinsic motivation, which is aptly explained by the SDT. The theory comprises factors that are presumed to influence information security compliant behaviour, which are perceived competence, perceived autonomy and perceived relatedness, as shown in figure 1.

The conceptual model is based on employees' perception of the three basic needs of the self-determination theory and the security aspects with which the employees are expected to comply, as stipulated in the ISPs. The three basic needs of the SDT result in intrinsic motivation, which is expected to influence a positive attitude towards the information security requirements of ISPs. The next section will discuss the conceptual model.

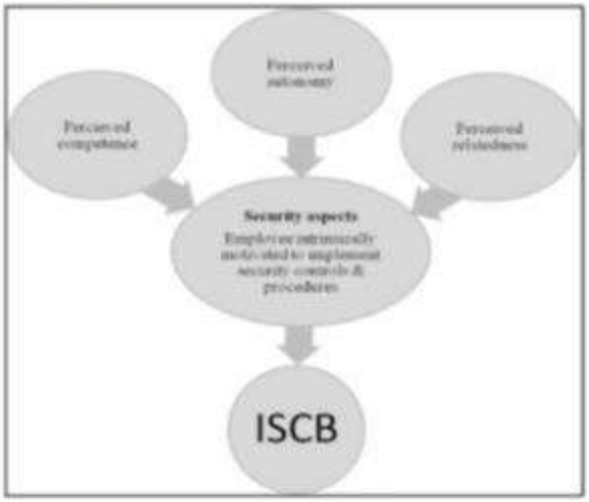


Figure 1: Conceptual model of information security complaint behaviour

A. Perceived competence

The employee has the perception that they are competent to carry out the information security action, that is, they are able to adhere to and implement security controls. The employee will also have the belief that they can learn new ways of carrying out the information security actions.

B. Perceived relatedness

The employee has the perception that they are part of the organisation and that they are valued by the organisation. They are of the belief that they can share information security knowledge and can get help from colleagues and superiors in the workplace.

C. Perceived autonomy

The employee perceives that they are acting out of their own volition when they carry out information security actions.

D. Security aspects

These are the requirements that must be adhered to by employees, as stipulated in the ISPs. For this study, these should be derived from literature and the respective industry standards.

The conceptual framework proposes that the fulfilment of these three will lead to intrinsic motivation and result in the following:

- Increased internalisation of the ISPs.
- Owing to this internalisation, employees will comply because the ISPs are congruent with their internal values.
- Their behaviour therefore becomes self-determined and they comply because they choose to do so.
- They will comply because of the inherent satisfaction and enjoyment resulting from the activity; in other words, they are intrinsically motivated.

VII. RECOMMENDATIONS

This paper presented a conceptual model based on the STD which outlines that intrinsic motivation influences information security compliant behaviour. This paper makes contributions by drawing attention to the factors that motivate an individual's behaviour and applying them to information security. In the workplace, management should put in place ways of shifting employees' motivation from extrinsic motivation to intrinsic motivation (self-determined behaviour). The competence of employees regarding information security can be improved through awareness training. By ensuring that the organisational environment fosters commitment and compliance, management can improve employees' perception of relatedness. The model postulates that compliance should not be a result of external pressure but of individual choice. However, the model is conceptual, and future research will aim to use the model to develop a questionnaire that can be validated statistically to assess the information security compliant behaviour in an organisation. Based on the results gained, recommendations could then be made to organisations to influence information security compliant behaviour positively.

VIII. CONCLUSION

Information security compliant behaviour influences the protection of information resources. This paper has shown from prior research that intrinsic motivation plays an important role in motivating information security compliant behaviour. A conceptual model was presented, which is based on the self-determination theory. This model can be used to study information security compliance in organisations.

ACKNOWLEDGMENT

This work is based on research supported by the Women in Research Grant from Unisa.

IX. REFERENCES

[1] M. Alohali, N. Clarke, S. Furnell, and S. Albakri, "Information security behavior: Recognizing the influencers," in *Proceedings of Computing Conference*, 2017, pp. 844–853.

[2] N. I. Jaafar and A. Ajis, "Organizational Climate and Individual Factors Effects on Information Security Faculty of Business and Accountancy," *Int. J. Bus. Soc. Sci.*, vol. 4, no. 10, pp. 118–131, 2013.

[3] D. Mani, S. Mubarak, A. Heravi, and K.-K. R. Choo, "Employees' intended information security behaviour in real estate organisations: A Protection Motivation perspective," in *Americas Conference on Information Systems, AMCIS 2015*, 2015, pp. 1–11.

[4] L. Connolly, M. Lang, J. Gathegi, and J. D. Tygar, "The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study," in

Proceedings of the Tenth International Symposium on Human Aspects of Information Security and Assurance, 2016, pp. 33–44.

[5] I. Hwang and O. Cha, "Examining technostress creators and role stress as potential threats to employees' information security compliance," *Comput. Human Behav.*, vol. 81, pp. 282–293, 2018.

[6] W. R. Flores and M. Ekstedt, "A Model for Investigating Organizational Impact on Information Security Behavior," in *Workshop on Information Security and Privacy*, 2012, pp. 12–15.

[7] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Comput. Secur.*, vol. 53, pp. 65–78, 2015.

[8] K. Padayachee, "Taxonomy of compliant information security behavior," *Comput. Secur.*, vol. 31, no. 5, pp. 673–680, 2012.

[9] P. Mayer, A. Kunz, and M. Volkamer, "Reliable Behavioural Factors in the Information Security Context," in *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17*, 2017, pp. 1–10.

[10] F. Bélanger, S. Collignon, K. Enget, and E. Negangard, "Determinants of early conformance with information security policies," *Inf. Manag.*, vol. 54, no. 7, pp. 887–901, 2017.

[11] P. Ifinedo, "Roles of Organizational Climate , Social Bonds , and Perceptions of Security Threats on IS Security Policy Compliance Intentions," *Inf. Resour. Manag.*, vol. 31, no. 1, pp. 53–82, 2018.

[12] K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance: a higher education case study," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 91–108, 2018.

[13] Ponemon Institute, "Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview," 2017.

[14] PriceWaterhouseCoopers, "The Global State of Information Security Survey 2018: PwC," 2017.

[15] S. Alfawaz, N. Karen, and K. Mohannak, "Information security culture : A Behaviour Compliance Conceptual Framework," in *Proceedings of the 8th Australasian Information Security Conference*, 2010, vol. 105, pp. 47–55.

[16] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure ! Designing information security awareness programs to overcome users ' non-compliance with information security policies in banks," *Comput. Secur.*, vol. 68, pp. 145–159, 2017.

[17] M. Karyda, "Fostering Information Security Culture In Organizations : A Research Agenda," in *The 11th Mediterranean Conference on Information Systems (MCIS)*, 2017, pp. 1–10.

[18] M. R. A. Kadir, S. N. S. Norman, S. A. Rahman, and A. R. Ahmad, "Information Security Policies Compliance among Employees in Cybersecurity Malaysia," in *Proceedings of the 28th International Business Information Management Association Conference*, 2016, pp. 2419–2430.

[19] A. Correia, A. Gonçalves, and M. F. Teodoro, "A model-driven approach to information security compliance," in *AIP Conference Proceedings*, 2017, pp. 1–5.

[20] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance," *Inf. Manag. Comput. Secur.*, vol. 22, no. 1, pp. 42–75, 2014.

[21] M. Alaskar, S. Vodanovich, and K. N. Shen, "Evolvement of Information Security Research on Employees' Behavior: A Systematic Review and Future Direction," *2015 48th Hawaii Int. Conf. Syst. Sci.*, pp. 4241–4250, 2015.

[22] T. Sommestad, H. Karlzén, and J. Hallberg, "The Theory of Planned Behavior and Information Security Policy Compliance The Theory of Planned Behavior and Information Security Policy Compliance," *J. Comput. Inf. Syst.*, pp. 1–10, 2017.

[23] G. D. Moody, M. Siponen, and S. Pahnila, "Toward a Unified Model Of Information Security Policy Compliance," *MIS Q.*, vol. 42, no. 1, pp. 285–311, 2018.

[24] R. Willison and W. Merrill, "Beyond Deterrence: An Expanded view of Employee Computer Abuse," *MIS Q.*, vol. 37, no. 1, pp. 1–20, 2013.

[25] K. H. Guo, "Security-related behavior in using information systems in the workplace: A review and synthesis," *Comput. Secur.*, vol. 32, no. 1, pp. 242–251, 2013.

[26] Y. Li, T. Stafford, B. Fuller, and S. Ellis, "Beyond Compliance: Empowering Employees' Extra-Role Security Behaviors in Dynamic Environments," in *AMCIS 2017 Proceedings*, 2017, pp. 1–5.

[27] W. T. Wang and Y. P. Hou, "Motivations of employees' knowledge sharing behaviors: A self-determination perspective," *Inf. Organ.*, vol. 25, no. 1, pp. 1–26, 2015.

[28] D. Zohar, Y. Huang, J. Lee, and M. M. Robertson, "Testing extrinsic and intrinsic motivation as explanatory variables for the safety climate–safety performance relationship among long-haul truck drivers," *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 30, pp. 84–96, 2015.

[29] R. J. Vallerand, "From motivation to passion: In search of the motivational processes involved in a meaningful life.," *Can. Psychol. Can.*, vol. 53, no. 1, pp. 42–52, 2012.

[30] Q. Wang, "Intrinsic Motivation: A Cultural Perspective," *Int. Encycl. Soc. Behav. Sci.*, vol. 12, pp. 696–701, 2015.

[31] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," *Comput. Secur.*, vol. 39, no. PART B, pp. 447–459, 2013.

[32] J. J. Kranz and F. J. Haeussinger, "Why Deterrence is not Enough: The Role of Endogenous Motivations

on Employees' Information Security Behavior," in *International Conference on Information Systems*, 2014, pp. 1–14.

[33] J. Y. Son, "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies," *Inf. Manag.*, vol. 48, no. 7, pp. 296–302, 2011.

[34] D. Sikolia and D. Biros, "Motivating Employees to Comply with Information Security Policies Security Policies," in *Proceedings of the Eleventh Midwest Association for Information Systems Conference*, 2016, pp. 1–7.

[35] A. Alzahrani, C. Johnson, and S. Altamimi, "Information Security Policy Compliance : Investigating the role of intrinsic motivation towards policy compliance in the organisation," in *2018 4th International Conference on Information Management (ICIM)*, 2018, pp. 125–132.

[36] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, 2009.

[37] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance : the role of fairness , commitment , and cost beliefs," in *MCIS 2011 Proceedings*, 2011.

[38] R. Ryan and E. Deci, "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions.," *Contemp. Educ. Psychol.*, vol. 25, no. 1, pp. 54–67, 2000.

[39] B. Lebek, U. Jörg, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior : a theory-based literature review," *Manag. Res. Rev.*, vol. 37, no. 12, pp. 1049–1092, 2014.

[40] J. D. Wall, P. Palvia, and P. B. Lowry, "Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy," *J. Inf. Priv. Secur.*, vol. 9, no. 4, pp. 52–79, 2013.

[41] R. Ryan and E. Deci, "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being.," *Am. Psychol.*, vol. 55, no. 1, pp. 68–78, 2000.

[42] A. Van den Broeck, M. Vansteenkiste, and H. De Witte, "Self-determination theory: A theoretical and empirical overview in occupational health psychology," in *Occupational health psychology: European perspectives on research, education, and practice*, 2008, pp. 63–88.

[43] E. L. Deci and R. M. Ryan, "Self-Determination Theory," *Int. Encycl. Soc. Behav. Sci. Second Ed.*, vol. 21, pp. 486–491, 2015.

[44] L. Legault, *Self determination Theory*. 2017.

[45] E. L. Deci, A. H. Olafsen, and R. M. Ryan, "Self-Determination Theory in Work Organizations: The State of a Science," *Annu. Rev. Organ Psychol. Organ. Behav Psychol. Organ. Behav*, vol. 4, pp. 19–43, 2017.

[46] J. D. Wall and P. Palvia, "Control-related motivations and information security policy compliance: The effect of reflective and reactive autonomy," in *Proceedings of the Nineteenth Americas Conference on Information Systems*, 2013, vol. 2, pp. 894–902.

[47] H. C. Pham, D. D. Pham, L. Brennan, and J. Richardson, "Information security and people: A conundrum for compliance," *Australas. J. Inf. Syst.*, vol. 21, pp. 1–16, 2017.

[48] M. Gagne and E. L. Deci, "Self-determination theory and work motivation," *J. Organ. Behav.*, vol. 26, pp. 331–362, 2005.

[49] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012.

[50] A. Bandura, "Self-Efficacy," *Encycl. Hum. Behav.*, vol. 4, no. 1994, pp. 71–81, 1994.

[51] H. S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Comput. Secur.*, vol. 28, no. 8, pp. 816–826, 2009.

[52] S. Pahnila, M. Siponen, and A. Mahmood, "Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study," in *Pacific Asia Conference on Information Systems*, 2007, pp. 438–439.

[53] N. Humaidi and V. Balakrishnan, "The moderating effect of working experience on health information system security policies," *Malaysian J. Comput. Sci.*, vol. 28, no. 2, pp. 70–92, 2015.

[54] H.-W. Huang, N. Parolia, and K.-T. Cheng, "Willingness and Ability To Perform Information Security Compliance Behavior: Psychological Ownership and Self-Efficacy Perspective," in *Pacific Asia Conference on Information Systems*, 2016.

[55] N. Humaidi and V. Balakrishnan, "Indirect effect of management support on users' compliance behaviour towards information security policies," *Heal. Inf. Manag. J.*, vol. 47, no. 1, pp. 17–27, 2017.

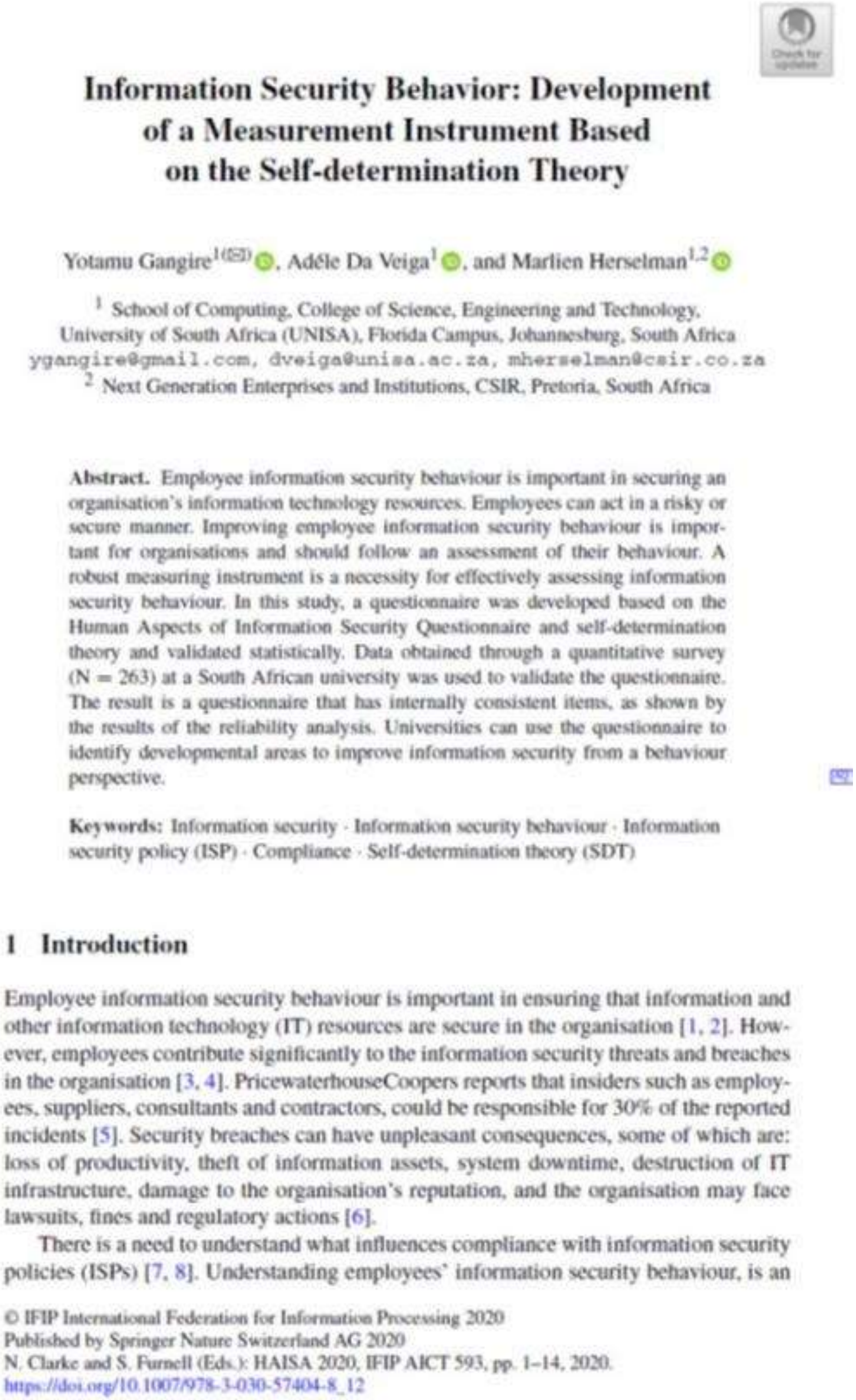
[56] NIST and U.S. Department of Commerce, "Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations," 2013.

[57] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, 4th ed. Prentice Hall, 2010.

[58] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "An introduction to information security," 2017.

[59] J. M. Blythe, L. Coventry, and L. Little, "Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors," in *Eleventh Symposium On Usable Privacy and Security*, 2015, pp. 103–122.

2. IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2020)



Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory

Yotamu Gangire[1](✉), Adéle Da Veiga[1], and Marlien Herselman[1,2]

[1] School of Computing, College of Science, Engineering and Technology,
University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa
ygangire@gmail.com, dveiga@unisa.ac.za, mherselman@csir.co.za
[2] Next Generation Enterprises and Institutions, CSIR, Pretoria, South Africa

Abstract. Employee information security behaviour is important in securing an organisation's information technology resources. Employees can act in a risky or secure manner. Improving employee information security behaviour is important for organisations and should follow an assessment of their behaviour. A robust measuring instrument is a necessity for effectively assessing information security behaviour. In this study, a questionnaire was developed based on the Human Aspects of Information Security Questionnaire and self-determination theory and validated statistically. Data obtained through a quantitative survey (N = 263) at a South African university was used to validate the questionnaire. The result is a questionnaire that has internally consistent items, as shown by the results of the reliability analysis. Universities can use the questionnaire to identify developmental areas to improve information security from a behaviour perspective.

Keywords: Information security · Information security behaviour · Information security policy (ISP) · Compliance · Self-determination theory (SDT)

1 Introduction

Employee information security behaviour is important in ensuring that information and other information technology (IT) resources are secure in the organisation [1, 2]. However, employees contribute significantly to the information security threats and breaches in the organisation [3, 4]. PricewaterhouseCoopers reports that insiders such as employees, suppliers, consultants and contractors, could be responsible for 30% of the reported incidents [5]. Security breaches can have unpleasant consequences, some of which are: loss of productivity, theft of information assets, system downtime, destruction of IT infrastructure, damage to the organisation's reputation, and the organisation may face lawsuits, fines and regulatory actions [6].

There is a need to understand what influences compliance with information security policies (ISPs) [7, 8]. Understanding employees' information security behaviour, is an

Published by Springer Nature Switzerland AG 2020
N. Clarke and S. Furnell (Eds.): HAISA 2020, IFIP AICT 593, pp. 1–14, 2020.
https://doi.org/10.1007/978-3-030-57404-8_12

important step in the assessment and consequently the improvement of information security behaviour [9]. Hence there is a need to assess and evaluate employees' information security awareness [10].

Some studies on employee information security behaviour are based on theories for example, the study by Safa, et al. [1] was based on the protection motivation theory and the theory of planned behaviour (TPB); the study by Ifinedo [11] used the TPB, social bond theory and the social control theory and the study by Kranz and Haeussinger [12] used the TPB and the self-determination theory (SDT). These studies aimed to validate a particular theory, hence they only assessed the variables in the theory under investigation while other variables were not considered. However, employee information security behaviour is influenced by many factors besides variables from theories [13]. This study develops an instrument based on themes from the Human Aspects of Information Security Questionnaire (HAIS-Q) [13] and the information security compliant behaviour model based on the SDT (ISCBM^{SDT}) [14]. This not only contributes to the theory validation of the SDT variables, but combines these with the themes of the HAIS-Q, thereby including more variables in the assessment instrument.

The aim of this study is to develop and validate an information security behaviour questionnaire to assess the influence of perceived competence, perceived relatedness and perceived autonomy on information security behaviour. The study postulates that perceptions of competence, relatedness and autonomy influence efficacy and hence the intention to comply with ISPs. It is therefore, intended that a positive perception of competence, relatedness and autonomy will help mitigate the risk of ISP non-compliance and that developing a questionnaire can aid in measuring and determining this. It is also aimed at outlining the development of this instrument, including the validity and reliability testing of the questionnaire. The instrument could be used to assess employee information security behaviour from the perspective of the SDT. To achieve these aims, a survey was carried out at a South African university using the information security behaviour questionnaire. This paper is structured as follows: Sect. 2 gives an overview of the information security behaviour and Sect. 3 describes the research methodology. The results of the survey and statistical validation of the questionnaire are discussed in Sect. 4. This is followed by the limitations and future directions in Sect. 5 and the conclusion in Sect. 6.

2 Information Security Behaviour

Pattinson et al. [15] refer to information security behaviour as the behaviour performed by computer users, which can be either intentionally risky behaviour or intentionally secure behaviour. According to Guo [16] employee security behaviour can be desirable or undesirable. Desirable behaviour is ISP compliant whereas undesirable behaviour is not. Examples of secure behaviour include taking precautions and reporting security incidents [16]. Employees can also exhibit behaviour aimed at preventing security breaches by taking fewer risks. Other employees engage in inappropriate security behaviour, including using the default security password and relying on the computer to auto-lock when they leave their desk. Employees can also engage in behaviour that aid business continuity and recovery; these employees back up their data and inform colleagues of security issues [17]. It is argued that when employees comply with the ISPs, information security threats are reduced [18].

Alfawaz, Nelson and Mohannak [19] propose security behaviour modes as the knowing-doing mode, knowing-not doing mode, not knowing-doing mode and not knowing-not doing mode. In the not knowing-not doing mode, employees violate information security rules, because they do not know the organisation's information security rules and do not have any security knowledge [19]. In the not knowing-doing mode, employees do not know the information security rules and do not have security knowledge but still exhibit the right security behaviour. These are employees who will ask their co-workers before taking certain actions. In the knowing-not doing mode, employees know the rules and have the necessary security knowledge and skills, but still violate the rules [19]. In the knowing-doing mode, employees know the rules, have the necessary security skills and comply with the rules [19].

Ahmad, Norhashim, Song, & Hui [20] group employees into four types on the basis of whether or not they know the security rules and whether or not they comply with the information security rules. They classify them as discerning, obedient, rebel and oblivious employees. Discerning individuals conform to the information security rules because they have the necessary knowledge; some employees conform to the information security rules not because they have the knowledge but because they follow organisational rules just because they are there; some employees choose not to conform to information security rules despite having the knowledge; and other employees compromise information security because they do not have the security knowledge [20].

Alfawaz et al. [19] and Ahmad et al. [20] propose classification of employees' information security behaviour that also explain why employees fail to comply with organisational ISPs. They postulate that employees fail to comply because they are ignorant of the regulations, they choose not to or they are not competent due to lack of security knowledge. Their classifications suggest that in order for employees to comply with the ISPs, they have to be equipped with the relevant security knowledge and skills. Employees will also have to actively think about the security implications of their actions when they do their work. Therefore, security awareness, knowledge and experience are important [1]. Users must also understand their responsibilities regarding information security because an employee who lacks information security awareness is more vulnerable to information security attacks [21].

2.1 Information Security Compliant Behaviour Model

The Information Security Compliance Behavior Model (ISCBM^{SDT}) is based on the three concepts of the SDT, which are the need for competence, the need for relatedness and the need for autonomy. The three basic psychological needs are regarded as some of the sources contributing to intrinsic motivation [22, 23]. The need for autonomy is the perception that one is acting out of one's own volition and that one's behaviour is self-determined. The need for relatedness refers to the desire be attached to others. Competence is the belief of being capable and effective [22]. The ISCBM^{SDT} postulates that when perceived competence, perceived relatedness and perceived autonomy are fulfilled, the employees will comply with the ISP because it is their choice to do so

[14]. The questionnaire developed for this study is based on the ISCBM^{SDT} and the questionnaire themes/focus areas are discussed next.

2.2 Information Security Behaviour Themes

The focus areas from the HAIS-Q were mapped to the three concepts of the SDT resulting, in each focus area focusing on competence, relatedness and autonomy. The themes are as follows.

Password Management
This involves understanding how to protect information system resources by using strong and secure passwords. This includes regularly changing passwords, choosing strong passwords and not sharing passwords [17, 24, 25].

Email Usage
Employees have to understand safe email use. This includes not downloading unsafe attachments, clicking on links in email from known or unknown senders and opening attachments in emails from unknown senders [1, 15, 17, 21, 24, 26].

Internet Usage
Employees should know how to use the internet safely. This includes downloading files, accessing dubious websites and entering information online [15, 18, 26, 27].

Social Media Usage
Employees should understand safe usage of social media. This includes social media privacy settings, considering the consequences of posting information and acting responsibly regarding posting about work on social media [27].

Mobile Devices Usage
Employees should understand how to secure their mobile devices, which carry work information when working in a public area. This includes physically securing mobile devices, sending sensitive information via public Wi-Fi and guarding against shoulder surfing [27, 28].

Information Handling
Employees have to understand how to handle sensitive information. This includes disposing of sensitive print-outs, inserting removable media in work computers and leaving sensitive material on work areas [17, 27, 29].

Privacy
Employees should understand how to handle personally identifiable information. This includes non-disclosure of sensitive information [1, 17], processing client information in a lawful manner [30], processing client information for the purpose for which it was collected [30, 31], and adhering to the organisation's privacy policy [32]. When employees adhere to the privacy policy they can uphold the privacy of student data they handle. Parsons et al. [33] propose that the link between information security awareness and privacy should be investigated. Table 1 shows an extract of items in the competence, relatedness and autonomy category.

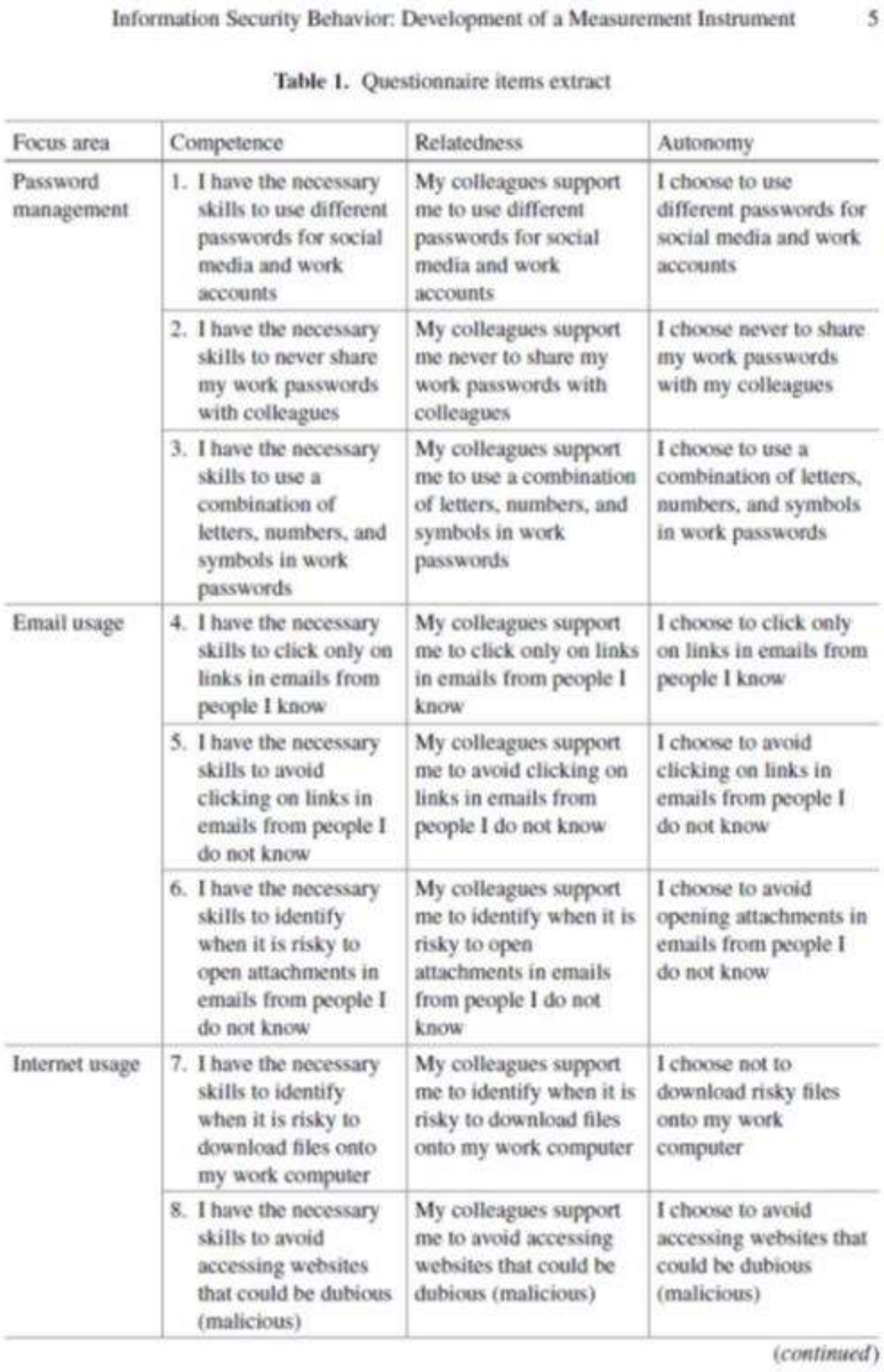


Table 1. Questionnaire items extract

Focus area	Competence	Relatedness	Autonomy
Password management	1. I have the necessary skills to use different passwords for social media and work accounts	My colleagues support me to use different passwords for social media and work accounts	I choose to use different passwords for social media and work accounts
	2. I have the necessary skills to never share my work passwords with colleagues	My colleagues support me never to share my work passwords with colleagues	I choose never to share my work passwords with my colleagues
	3. I have the necessary skills to use a combination of letters, numbers, and symbols in work passwords	My colleagues support me to use a combination of letters, numbers, and symbols in work passwords	I choose to use a combination of letters, numbers, and symbols in work passwords
Email usage	4. I have the necessary skills to click only on links in emails from people I know	My colleagues support me to click only on links in emails from people I know	I choose to click only on links in emails from people I know
	5. I have the necessary skills to avoid clicking on links in emails from people I do not know	My colleagues support me to avoid clicking on links in emails from people I do not know	I choose to avoid clicking on links in emails from people I do not know
	6. I have the necessary skills to identify when it is risky to open attachments in emails from people I do not know	My colleagues support me to identify when it is risky to open attachments in emails from people I do not know	I choose to avoid opening attachments in emails from people I do not know
Internet usage	7. I have the necessary skills to identify when it is risky to download files onto my work computer	My colleagues support me to identify when it is risky to download files onto my work computer	I choose not to download risky files onto my work computer
	8. I have the necessary skills to avoid accessing websites that could be dubious (malicious)	My colleagues support me to avoid accessing websites that could be dubious (malicious)	I choose to avoid accessing websites that could be dubious (malicious)

(continued)

Table 1. *(continued)*

Focus area	Competence	Relatedness	Autonomy
	9. I have the necessary skills to assess the safety of a website before entering information online	My colleagues support me to assess the safety of a website before entering information online	I choose to assess the safety of a website before entering information online

3 Methodology

This study adopted the positivist research paradigm with a quantitative approach. In the positivist research paradigm researchers prefer to work with observable and measurable reality. Positivists use quantitative methods in their research and the research is based on the testing of theories [34, 35]. The survey strategy was chosen and the questionnaire was used for data collection at a university in South Africa. A non-probability purposive sampling method was used. With purposive sampling the researcher deliberately selects the sample for example because they are easy to reach or are available [34]. The selection of the expert panel was done using the purposive sampling method based on the following criteria: they had all done research work in information security and had experience in information security awareness. The pilot sample was selected using convenience sampling in one of the university's departments. The survey participants were selected using purposive sampling. The survey questionnaire was sent electronically to the entire population of administrative and academic staff. Ethical clearance was obtained from the university, adhering to the research ethics policy that focuses on aspects such as anonymity, voluntary participation, confidentiality and consent for participation.

The following statistical tests were performed: ANOVA, t-test and Pearson correlation analysis. ANOVA was carried out to determine if there were significant differences among the demographical groups for age, job level, level of education and length of service groups. The t-test were performed to determine if the mean scores among the gender groups had any significant differences. The correlation analysis was carried out to determine if there was any correlation among the resulting factors from the exploratory factor analysis.

3.1 Questionnaire

A Likert scale (strongly agree, agree, unsure, disagree and strongly disagree) was used to answer the statements. The questionnaire had two sections: Sect. 1 which was for biographical information and Sect. 2 which comprised the information security behaviour questions. The final questionnaire had 75 questions: 25 questions for each of the SDT categories.

3.2 Expert Panel Reviews

A panel of experts in the research area evaluated the questionnaire. This helped to refine and improve the questionnaire [35]. The questionnaire was reviewed by a panel of six experts, four of whom were from the field of psychology (human factors scientists) who had researched the human aspects of cyber security for 11 years and had developed the HAIS-Q. The other two were an academic in information security and an IT security consultant specialising in incident response and awareness. The reviewers had 10 to 20 years of working experience. They pointed out that some of questions were not clear and others addressed two different aspects in one question. The questionnaire was updated and sent for pilot testing.

3.3 Pilot Testing

The pilot test was conducted among 12 staff members in one of the departments in the university. The questionnaire pilot test showed that some questions were not worded clearly and it was recommended that job level be added to the biographical section.

3.4 Main Study

The updated questionnaire was prepared and administered using Google Forms over the internet and participants were notified by an email invitation sent by the ICT department of the university. The email contained information on the research and the links for completing the online questionnaire. The participants were required to read the information sheet and the consent form. If they consented to participate in the study, then they proceeded to complete the online questionnaire

4 Results

Two hundred and sixty-three (263) responses were received from the online survey. The sample consisted of 54.8% females, 44.1% males and 1.1% did not disclose their gender. Those born between 1977 and 1995 were the largest group of respondents (38.40%). The highest number of survey respondents (69.08%) was from the group with postgraduate qualifications. There were more respondents from the groups with higher qualifications (i.e. the higher the qualification the higher the number of respondents). This is consistent with a university environment. Those who had worked for six to ten years were the largest group (27.38%) and most of the respondents were administrative staff (51.53%). The results of the survey are reported next.

A cut-off of 4.0 for the means was set for the information security behaviour questions [36]. A mean score of 4.0 and above indicated a positive perception, while a mean score below 4.0 indicated a neutral or potentially negative perception.

For the competence questions, the top 10 questions all had means above 4.0. This suggests that the respondents had a positive perception of the competence questions. Of the bottom 10 questions, five had means above 4.0 and five had means below 4.0, indicating areas for which further improvement is required.

For the relatedness questions, the mean values for the top statements ranged from 3.05 to 3.51 and the mean values for the bottom statements ranged from 2.68 to 3.01. These mean values for both top questions and bottom questions show that all had means below

4.0. This suggests that the participants had neutral and potentially negative perceptions of the relatedness questions, indicating areas requiring further improvement.

For the autonomy questions, the mean values for the top statements ranged from 4.41 to 4.68 and the mean values for the bottom statements ranged from 3.91 to 4.27. The top questions all had means above 4.0, suggesting that the respondents had a positive perception of the autonomy questions. For the bottom 10 questions, eight questions had means above 4.0 and two had means below 4.0. The two questions with means below 4.0 indicate areas were further improvement is required.

The results of the Pearson correlation showed that the competence and autonomy factors had a statically significant positive correlation ($r >= .287$, $n = 263$, $p < .05$), two tailed. The correlation for the competence and relatedness factors show that some factors had a positive correlation ($r >= .224$, $n = 263$, $p < .05$), two tailed and other factors did not. The correlation results for the autonomy and relatedness factors showed that some factors had a positive correlation ($r >= .134$, $n = 263$, $p < .05$), two tailed and others did not.

The results of the information security behaviour questions suggest that the respondents had a more positive perception of the competence and autonomy questions than of the relatedness questions. The Pearson correlation results show a positive correlation between competence and autonomy, suggesting that the respondents who perceive themselves to be competent also felt confident about their autonomy perception.

4.1 Validation of the Instrument

Factor Analysis

Exploratory factor analysis (EFA) was carried out to determine the underlying relationships between the variables [37], as well as the construct validity of the questionnaire [38]. O'Rourke and Hatcher [39] suggests that to achieve a sample size that is statistically adequate to carry out questionnaire validation, the responses or the collected data must be at least five times the number of questions in the questionnaire. The EFA was done for each category and new factors were determined per category. Since each category had 25 questions, a minimum of 125 responses were required per category. The recommendation of O'Rourke and Hatcher [39] and the received responses were sufficient to carry out the statistical validation of the questionnaire and the data was processed using SPSS Version 25.

Determining the Number of Factors

The Kaiser-Meyer-Olkin (KMO) test and the Bartlett sphericity tests were conducted for each of the three categories competence, relatedness and autonomy. Field [40] recommends a KMO value closer to 1 in order to produce distinct and reliable factors. For the Bartlett sphericity test, the probability should be less or equal to 0.05; this shows highly correlated variables [38]. The KMO for the competence statements was 0.915 and the Bartlett sphericity test result was statistically significant ($p = 0.000$). The KMO for the relatedness statements was 0.965 and the Bartlett sphericity test result was statistically significant ($p = 0.000$). The KMO for the autonomy statements was 0.885 and the Bartlett sphericity result was statistically significant (p = 0.000). As a result, all categories met the criteria for performing the EFA.

The factors were determined using the Eigenvalues, scree plots and cumulative percentages [41]. The item loading cut off was 0.4, as Stevens [42] suggests that item loading values should be greater than 0.4. The cumulative percentage had to be above 60% and the Eigenvalues had to be greater than 1. Competence statements resulted in four factors and these had Eigenvalues greater than 1 and a cumulative Eigenvalue of 62.38%. Relatedness statements resulted in two factors and these had Eigenvalues greater than 1 and a cumulative Eigenvalue of 70.74%. The autonomy statements resulted in six factors and these had Eigenvalues greater than 1 and a cumulative Eigenvalue of 63.68%.

Table 2 shows the resulting factors. For the competence statements, Factor 3 Statement 25 was removed as it had a factor cross-loading with a cross-loading difference of less than 0.2. Factor 4 was dropped as it had only one item, Statement 3 and factors for the competence category were reduced to 3. For the relatedness category, Questions 17 and 18 were dropped as they had cross-loading differences less than 0.2. For the autonomy category Statements 1, 2, 3, 14, 17 and 18 were dropped because they had loadings below 0.4.

Table 2. Resulting factors

Category	Factor	Statements
Competence	Factor 1	1, 10, 11, 12, 14, 15, 16, 18, 19, 20, 21
	Factor 2	4, 5, 6, 7, 8, 9, 17
	Factor 3	22, 23, 24
Relatedness	Factor 1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
	Factor 2	19, 20, 21, 22, 23, 24, 25
Autonomy	Factor 1	8, 9, 10
	Factor 2	4, 5, 6, 7
	Factor 3	22, 23
	Factor 4	19, 20, 21
	Factor 5	24, 25
	Factor 6	11, 12, 13, 15, 16

Naming the Factors

The factors shown in Table 2 were named to reflect the common themes of the statements grouped under that factor.

Competence

Factors in this category reflect the employee's competence/skills to carry out the information security actions. The employees are confident that they can protect the IT resources because they have necessary skills to do so. For the competence statements, Factor 1 (11 items) was named *employee skills for data safety awareness*, Factor 2 (seven items) was named *employee skills for email and website safety and* Factor 3 (four items) was named *employee skills for privacy awareness*.

Relatedness

Factors in this category reflect the employee's need for support from colleagues to carry out information security actions. The employees perceive that they can protect the IT resources if co-workers and superiors support them. For the relatedness statements, Factor 1 (16 items) was labelled *organisational support for employee device and information protection awareness* and Factor 2 (seven items) was named *organisational support for employee information and privacy protection awareness*.

Autonomy

Factors in this category reflect the employees' need to be in control of their information security behaviour. The employees perceive that when they are in control of their information security behaviour they can protect the IT resources of their organisation. For the autonomy statements, Factor 1 (three items) was named *employee choice on privacy awareness*, Factor 2 (four items) was named *employee choice to avoid malicious emails and downloads*, Factor 3 (two items) was named *employee choice to keep privacy of student personal information*, Factor 4 (three items) was named *employee choice to report bad security behaviour*, Factor 5 (two items) was named *employee choice to adhere to information security and privacy policies* and Factor 6 (five items) was named *employee choice to keep devices and information secure*.

Two autonomy factors, *employee choice to keep privacy of student personal information* and *employee choice to adhere to information security and privacy policies*, had two statements each. They were retained because both factors had very good reliability as shown in Table 3.

4.2 Reliability Analysis

The Cronbach alpha coefficient was calculated for each of the 11 factors. Reliability refers to how consistent or dependable the measuring instrument is, and whether under similar conditions the measuring instrument produces consistent results [43]. According to Gerber and Hall [41], the Cronbach alpha coefficient can be interpreted as follows: good for values greater than 0.8, acceptable for values between 0.6 and 0.8, unacceptable for values less than 0.6. Table 3 shows the results of the Cronbach alpha values for the 11 factors. All the Cronbach alpha results were above 0.7, suggesting high reliability.

The final questionnaire had 11 revised dimensions and the individual statements were not changed. The new dimensions were a result of the factor and reliability analysis hence the new questionnaire can be considered to have good internal consistency.

5 Limitations and Future Directions

The following are some of the study's limitations:

The purposive sampling method used in this study, an accepted method of collecting data, may not produce a sample that is representative of the population. Therefore, future

Table 3. Cronbach alpha coefficient results for factors

Category	Factor	No. of items	Cronbach alpha	Comment
Competence	Employee skills for data safety awareness	11	0.906	Good
	Employee skills for email and website safety	7	0.905	Good
	Employee skills for privacy awareness	4	0.799	Good
Relatedness	Organisational support for employee device and information awareness	16	0.967	Good
	Organisational support for employee information and privacy protection awareness	7	0.945	Good
Autonomy	Employee choice on privacy awareness	3	0.775	Acceptable
	Employee choice to avoid malicious emails and downloads	4	0.836	Good
	Employee choice to keep the privacy of student personal information	2	0.904	Good
	Employee choice to report bad security behaviour	3	0.791	Acceptable
	Employee choice to adhere to information security and privacy policies	2	0.868	Good
	Employee choice to keep devices and information secure	5	0.793	Acceptable

research should consider a representative sample of the population and inclusion of more organisations. The survey questionnaire had 75 questions, which may take some time to complete hence some respondents may not complete the survey. Future work will consider reducing the number of questions.

6 Conclusion

The aim of this study was to develop and validate the information security behaviour questionnaire based on the SDT. This questionnaire can be used to investigate how the perception of competence, relatedness and autonomy influence the intention to comply with ISPs. The results of the assessment can be used to design programs to assist employees to comply with ISPs.

The questions were developed by combining the variables from the SDT and the themes from the HAIS-Q as well as privacy to come up with a new questionnaire. Through a quantitative research, data were collected using the survey method. The collected data were used to validate the questionnaire resulting in a revised questionnaire with items with high internal consistency.

Generally, the results suggest that the survey participants were more confident about their competence and autonomy regarding their information security behaviour than they were about the relatedness questions.

The Pearson correlation results indicate a positive correlation between competence and autonomy, with a partial positive correlation between competence and relatedness, as well as a partial positive correlation between relatedness and autonomy. The results suggest, for example, that improving the competence of employees could result in an increased intention to comply with ISPs. In addition, how confident employees are about their information security skills, will influence their perception of autonomy in their information security behaviour. The participants had a neutral ($M = 3.08$) or potentially negative perception of the relatedness questions, suggesting that area requires further development.

The practical implication of this study and this questionnaire is that it can be used by a university to assess individual employees' strengths and weaknesses in terms of their awareness of information security behaviour. The questionnaire could also be administered before and after information security awareness training to assess the effectiveness of the training.

Acknowledgment. This work is based on research supported by the University of South Africa's Women in Research Grant.

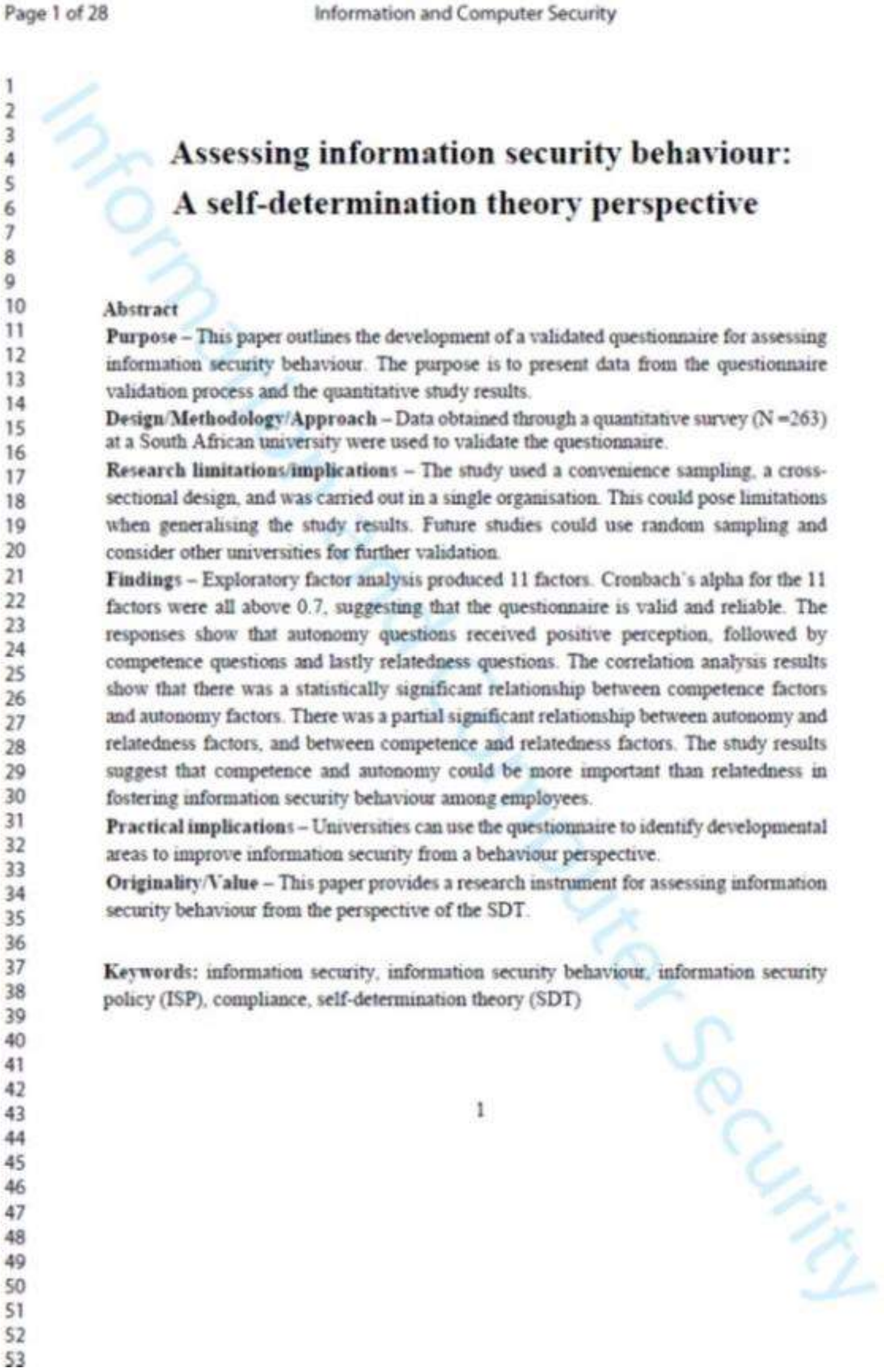
References

1. Safa, N.S., Sookhak, M., Von Solms, R., et al.: Information security conscious care behaviour formation in organizations. Comput. Secur. **53**, 65–78 (2015). https://doi.org/10.1016/j.cose.2015.05.012
2. Humaidi, N., Balakrishnan, V.: Indirect effect of management support on users' compliance behaviour towards information security policies. Heal. Inf. Manag. J. **47**, 17–27 (2017). https://doi.org/10.1177/1833358317700255
3. Pahnila, S., Karjalainen, M., Mikko, S.: Information security behavior : towards multi-stage models. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2013) (2013)
4. Mayer, P., Kunz, A., Volkamer, M.: Reliable behavioural factors in the information security context. In: Proceedings of the 12th International Conference on Availability, Reliability and Security - (ARES 2017), pp. 1–10 (2017)
5. Price Water house Coopers. The Global State of Information Security Survey 2018: PwC (2018). https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html
6. Ponemon Institute: The third annual study on the state of endpoint security risk (2020). https://www.morphisec.com/hubfs/2020StateofEndpointSecurityFinal.pdf

7. Huang, H.W., Parolia, N., Cheng, K.T.: Willingness and ability to perform information security compliance behavior: psychological ownership and self-efficacy perspective. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2016) (2016)
8. Iriqat, Y.M., Ahlan, A.R., Nuha, N.M.A.: Information security policy perceived compliance among staff in palestine universities : an empirical pilot study. In: Proceedings of the Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 580–585. IEEE (2019)
9. Alaskar, M., Vodanovich, S., Shen, K.N.: Evolvement of information security research on employees' behavior: a systematic review and future direction. In: Proceedings of the 48th Hawaii International Conference on System Sciences, pp. 4241–4250. IEEE (2015)
10. Ögütçü, G., Testik, Ö.M., Chouseinoglou, O.: Analysis of personal information security behavior and awareness. Comput. Secur. **56**, 83–93 (2016). https://doi.org/10.1016/j.cose.2015.10.002
11. Ifinedo, P.: Information systems security policy compliance: an empirical study of the effects of socialization, influence, and cognition. Inf. Manag. **51**, 69–79 (2013)
12. Kranz, J.J., Haeussinger, F.J.: Why deterrence is not enough : The role of endogenous motivations on employees' information security behavior. In: Proceedings of the 35th International Conference on Information Systems, pp. 1–14. IEEE (2014)
13. Parsons, K., McCormac, A., Butavicius, M., et al.: Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput. Secur. **42**, 165–176 (2014). https://doi.org/10.1016/j.cose.2013.12.003
14. Gangire, Y., Da Veiga, A., Herselman, M.: A conceptual model of information security compliant behaviour based on the self-determination theory. In: Proceedings of the 2019 Conference on Information Communications Technology and Society, (ICTAS). IEEE (2019)
15. Pattinson, M., Butavicius, M., Parsons, K., et al.: Examining attitudes toward information security behaviour using mixed methods. In: Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA). pp. 57–70 (2015)
16. Guo, K.H.: Security-related behavior in using information systems in the workplace: a review and synthesis. Comput. Secur. **32**, 242–251 (2013). https://doi.org/10.1016/j.cose.2012.10.003
17. Blythe, J.M., Coventry, L., Little, L.: Unpacking security policy compliance : the motivators and barriers of employees' security behaviors. In: Proceedings of the Symposium on Usable Privacy and Security (SOUPS), Ottawa, pp. 103–122 (2015)
18. Klein, R.H., Luciano, E.M.: What influences information security behavior? A study with brazilian users. J. Inf. Syst. Technol. Manag. **13**, 479–496 (2016). https://doi.org/10.4301/S1807-17752016000300007
19. Alfawaz, S., Nelson, K., Mohannak, K.: Information security culture : a behaviour compliance conceptual framework. In: Proceedings of the 8th Australasian Information Security Conference (AISC), pp. 47–55 (2010)
20. Ahmad, Z., Norhashim, M., Song, O.T., Hui, L.T.: A typology of employees' information security behaviour. In: Proceedings of the 4th International Conference on Information and Communication Technology, pp. 3–6 (2016)
21. Alohali, M., Clarke, N., Furnell, S., Albakri, S.: Information security behavior: recognizing the influencers. In: Proceedings of the Computing Conference, pp. 844–853 (2017)
22. Ryan, M.R., Deci, L.E.: Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. Am. Psychol. **55**, 68–78 (2000)
23. Legault, L.: Self determination theory. In: Zeigler-Hill, V., Shackelford, T.K. (eds.) Encyclopedia of Personality and Individual Differences, pp. 1–9. Springer, New York (2017). https://doi.org/10.1007/978-1-4419-1005-9_1620

24. Shropshire, J., Warkentin, M., Sharma, S.: Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Comput. Secur. **49**, 177–191 (2015). https://doi.org/10.1016/j.cose.2015.01.002
25. Calic, D., Pattinson, M., Parsons, K., et al.: Naïve and accidental behaviours that compromise information security : what the experts think. In: Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA), pp. 12–21 (2016)
26. Bélanger, F., Collignon, S., Enget, K., Negangard, E.: Determinants of early conformance with information security policies. Inf. Manag. **54**, 887–901 (2017). https://doi.org/10.1016/j.im.2017.01.003
27. Bauer, S., Bernroider, E.W.N., Chudzikowski, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Comput. Secur. **68**, 145–159 (2017). https://doi.org/10.1016/j.cose.2017.04.009
28. Curry, M., Marshall, B., Crossler, R.E., Correia, J.: InfoSec Process Action Model (IPAM): Systematically addressing individual security behavior. Database Adv. Inf. Syst. **49**, 49–66 (2018). https://doi.org/10.1145/3210530.3210535
29. Aurigemma, S., Mattson, T.: Deterrence and punishment experience impacts on ISP compliance attitudes. Inf. Comput. Secur. **25**, 421–436 (2017). https://doi.org/10.1108/ICS-11-2016-0089
30. Swartz, P., Da Veiga, A., Martins, N.: A conceptual privacy governance framework. In: Proceeding of the 2019 Conference on Information Communications Technology and Society (ICTAS), pp. 1–6 (2019)
31. NIST Security and privacy controls for federal information systems and organizations: National Institute of Standards and Technology (2017)
32. Dennedy, M.F., Fox, J., Finneran, T.R.: Data and privacy governance concepts. The Privacy Engineer's Manifesto, pp. 51–72. Apress, New York (2014)
33. Parsons, K., Calic, D., Pattinson, M., et al.: The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Comput. Secur. **66**, 40–51 (2017). https://doi.org/10.1016/j.cose.2017.01.004
34. Oates, B.J.: Researching Information Systems and Computing. Sage, London (2006)
35. Saunders, M., Lewis, P., Thornhill, A.: Research Methods for Business Students, 7th edn. Pearson Education Limited, Essex (2016)
36. Da Veiga, A., Martins, N.: Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput. Secur. **49**, 162–176 (2015). https://doi.org/10.1016/j.cose.2014.12.006
37. Yong, A.G., Pearce, S.: A beginner' s guide to factor analysis: focusing on exploratory factor analysis. Tutor. Quant. Methods Psychol. **9**, 79–94 (2013)
38. Williams, B., Onsman, A., Brown, T.: Exploratory factor analysis: a five-step guide for novices. J. Emerg. Prim. Heal. Care **8**, 1–13 (2010)
39. O'Rourke, N., Hatcher, L.: A Step-By-Step Approach to Using SAS for Factor Analysis and Structural Equation. SAS Institute, Cary (2013)
40. Field, A.: Discovering Statistics Using SPSS, 3rd edn. Sage, London (2009)
41. Gerber, H., Hall, N.: Quantitative research design. In: Data Acquisition - 1 day. HR Statistics, Pretoria (2017)
42. Stevens, J.P.: Applied Multivariate Statistics for the Social Sciences, 4th edn. Erlbaum, Hillsdale (2002)
43. Marczyk, G., Fertinger, D., DeMatteo, D.: Essentials of Research Design and Methodology. Wiley, Hoboken (2005)

3. Article submitted to the Information and Computer Security Journal



Assessing information security behaviour: A self-determination theory perspective

Abstract

Purpose – This paper outlines the development of a validated questionnaire for assessing information security behaviour. The purpose is to present data from the questionnaire validation process and the quantitative study results.

Design/Methodology/Approach – Data obtained through a quantitative survey (N =263) at a South African university were used to validate the questionnaire.

Research limitations/implications – The study used a convenience sampling, a cross-sectional design, and was carried out in a single organisation. This could pose limitations when generalising the study results. Future studies could use random sampling and consider other universities for further validation.

Findings – Exploratory factor analysis produced 11 factors. Cronbach's alpha for the 11 factors were all above 0.7, suggesting that the questionnaire is valid and reliable. The responses show that autonomy questions received positive perception, followed by competence questions and lastly relatedness questions. The correlation analysis results show that there was a statistically significant relationship between competence factors and autonomy factors. There was a partial significant relationship between autonomy and relatedness factors, and between competence and relatedness factors. The study results suggest that competence and autonomy could be more important than relatedness in fostering information security behaviour among employees.

Practical implications – Universities can use the questionnaire to identify developmental areas to improve information security from a behaviour perspective.

Originality/Value – This paper provides a research instrument for assessing information security behaviour from the perspective of the SDT.

Keywords: information security, information security behaviour, information security policy (ISP), compliance, self-determination theory (SDT)

1. Introduction

Employees are often the source of security incidents in the organisation, thus employees' information security behaviour can contribute to the information security threats and breaches within the organisation (Ofori *et al.*, 2020; Mayer *et al.*, 2017; Pahnila *et al.*, 2013). PricewaterhouseCoopers reports that insiders such as employees, suppliers, consultants and contractors could be responsible for 30% of the reported incidents (PricewaterhouseCoopers, 2018). As a result, employees are still regarded as one of the main sources of security incidents within the organisation (Son, 2011; Herath and Rao, 2009; Hwang *et al.*, 2019).

Security breaches can result in loss of productivity, theft of information assets, system downtime, destruction of information technology (IT) infrastructure and damage to the organisation's reputation; the organisation may face lawsuits, penalties and regulatory action (Ponemon Institute, 2020). Security incidents can also result in the theft of sensitive information (Bhaharin *et al.*, 2019), such as customer and employee records. In some studies, as much as 35% of customer records and 30% of employee records were compromised (PricewaterhouseCoopers, 2018). Therefore, there is a need to understand how to improve employees' information security behaviour from being an information security threat to being information security policy (ISP) compliant (Crossler *et al.*, 2013) so that security incidents resulting from poor information security behaviour can be reduced. There is also a need to assess and evaluate employees' information security awareness (Öütçü *et al.*, 2016) in order to identify areas that need improvement.

Many studies on employee information security behaviour are informed by theories, for example the study by Safa *et al.* (2015) was based on the protection motivation theory and the theory of planned behaviour (TPB); the study by Ifinedo (2013) used the TPB, social bond theory and the social control theory; and the study by Kranz and Haeussinger (2014) used the TPB and the self-determination theory (SDT). Such studies typically validate the theory on which they are based; hence, these studies only assess the variables in the theory under investigation while other variables are not considered. However, employee information security behaviour could be influenced by many factors besides variables from theories (Parsons *et al.*, 2014).

This study developed a questionnaire based on the focus areas of the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons *et al.*, 2014; Parsons *et al.*, 2017) and the information security compliant behaviour model based on the SDT ($ISCBM^{SDT}$) (Gangire *et al.*, 2019). This not only contributes to the theory validation of the SDT variables but also combine these with the focus areas of the HAIS-Q, thereby producing a questionnaire from the perspective of the SDT. The HAIS-Q was selected because it focuses on areas of an ISP that are most prone to non-compliance (*Parsons et al.*, 2014) and because it has been validated on different samples of users (Parsons *et al.*, 2017; Butavicius *et al.*, 2020). The SDT was chosen because the review of the literature showed that it was one of the least used theories in the study of information security behaviour. This is confirmed by Kuppusamy *et al.* (2020) who, in a systematic review, reported that the SDT is one of the less used theories in information security behaviour studies.

2. Aim of the study

The aim of this study was to develop a validated information security compliant behaviour questionnaire based on the SDT (ISCBM^{SDT}) model developed in previous research (Gangire *et al.*, 2019) from the perspective of competence, relatedness and autonomy, as well as to assess information security behaviour (Gangire *et al.*, 2020). The study proposes that the perception of competence, relatedness and autonomy motivates the intention to comply with ISPs which is investigated using correlation analysis. It is therefore intended that a positive perception of competence, relatedness and autonomy will help lower the risk of ISP non-compliance and that developing a questionnaire can aid in assessing and determining this (Gangire *et al.*, 2020). It was also aimed at outlining the development of this questionnaire, including the validity and reliability testing of the questionnaire. The questionnaire could be used to assess employee information security behaviour from the perspective of the SDT. To achieve these aims, a survey was conducted at a South African university using the ISCBM^{SDT} questionnaire and the results of the survey are also presented.

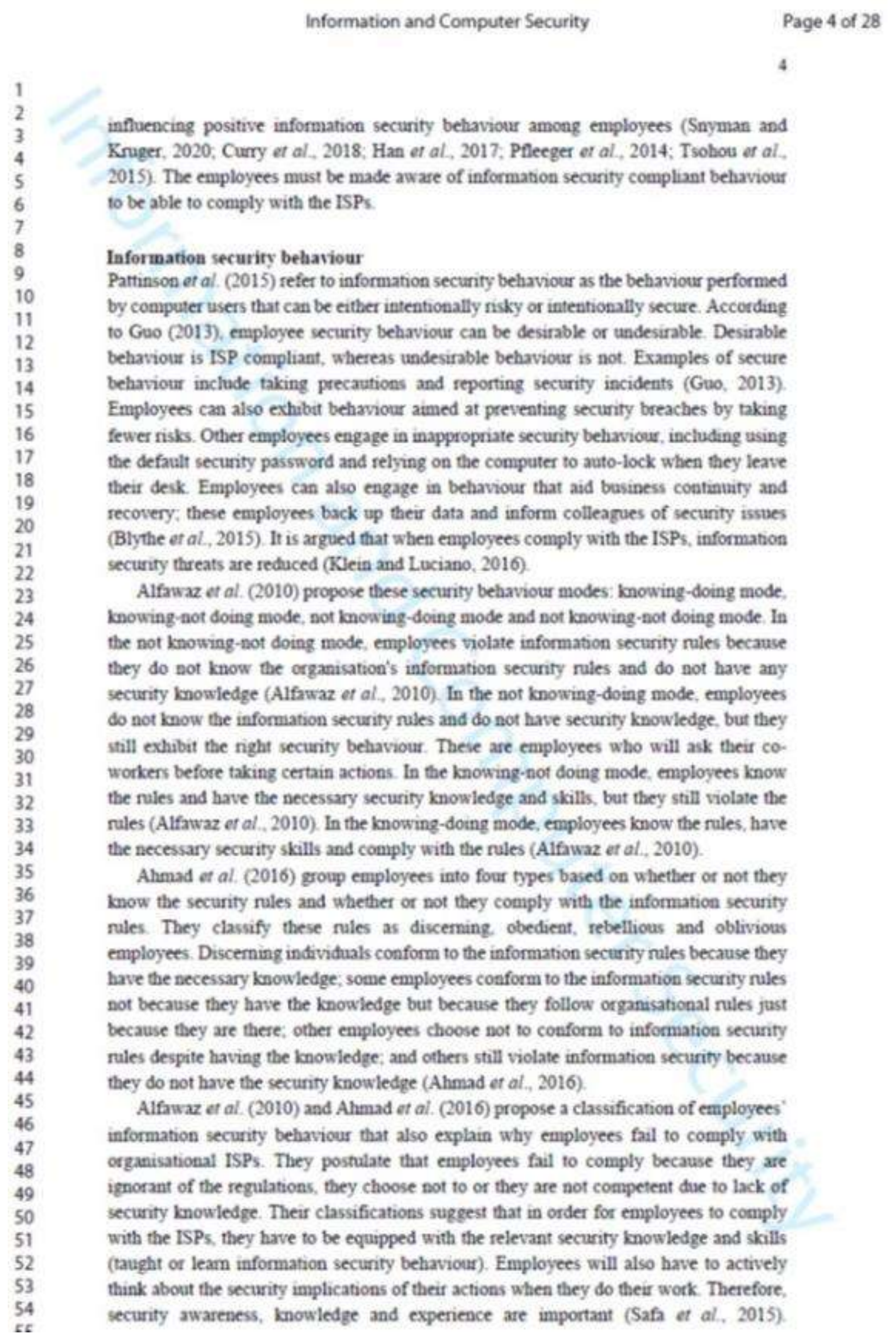
This paper is structured as follows: Section 3 provides a theoretical background to information security behaviour; Section 4 describes the questionnaire; Section 5 discusses the research method, the results of the survey and statistical validation of the questionnaire; Section 6 reports the survey results; Section 7 is the discussion; Section 8 covers the limitations and future research directions; and Section 9 is the conclusion.

3. Theoretical background

Behaviour refers to how organisms act in a given environment (Matsumoto, 2012; Davis *et al.*, 2015; Tileubayeva *et al.*, 2017; Kwasnicka *et al.*, 2016). It is also described as the way in which organisms respond to internal and/or external stimuli (Levitis *et al.*, 2009; Lazzeri, 2014; Davis *et al.*, 2015) and it can be assessed (Tileubayeva *et al.*, 2017; Kwasnicka *et al.*, 2016). Thus, when applied to employees in the workplace, this could suggest that an individual constructs a self-image to deal with their surroundings that enables him or her to fulfil various role expectations in the workplace (Schein, 1971).

Behaviour is influenced by motivational factors such as the joy of carrying out one's actions, results of the actions, and behaviour that aligns with one's beliefs or values (Kwasnicka *et al.*, 2016). Behaviour is re-inforced by repeated performance (Kwasnicka *et al.*, 2016) and repeated learning (Carden and Wood, 2018). An individual learns through socialisation the various norms, values and desirable behaviours through which one fulfils one's expected roles (Schein, 1971). As behaviour becomes habitual, the chances of maintaining it increase (Kwasnicka *et al.*, 2016). The culture in which individuals find themselves and the roles they are expected to fulfil could also determine behaviour (Schein, 1971). The environment and social context can either facilitate or hinder behaviour change. Stable environments make behaviour and habits easier to sustain (Kwasnicka *et al.*, 2016), whereas a change in the environment could disrupt a habit (Carden and Wood, 2018). Extrinsic factors can result in quick changes to behaviour. However, intrinsic factors have a more lasting effect on behaviour than extrinsic motivation (Kwasnicka *et al.*, 2016).

Therefore, behaviour is a result of either external or internal factors, or both and can be learned. People exhibit certain behaviour as they react or adapt to various influences and as they do so, they affect their immediate surroundings. When continuously performed, behaviour becomes habitual (Kwasnicka *et al.*, 2016). In the context of information security, employees can be taught proper information security behaviour. Organisations can use awareness training programmes to teach employees about information security (Bauer *et al.*, 2017). Awareness training programmes are aimed at



influencing positive information security behaviour among employees (Snyman and Kruger, 2020; Curry *et al.*, 2018; Han *et al.*, 2017; Pfleeger *et al.*, 2014; Tsohou *et al.*, 2015). The employees must be made aware of information security compliant behaviour to be able to comply with the ISPs.

Information security behaviour

Pattinson *et al.* (2015) refer to information security behaviour as the behaviour performed by computer users that can be either intentionally risky or intentionally secure. According to Guo (2013), employee security behaviour can be desirable or undesirable. Desirable behaviour is ISP compliant, whereas undesirable behaviour is not. Examples of secure behaviour include taking precautions and reporting security incidents (Guo, 2013). Employees can also exhibit behaviour aimed at preventing security breaches by taking fewer risks. Other employees engage in inappropriate security behaviour, including using the default security password and relying on the computer to auto-lock when they leave their desk. Employees can also engage in behaviour that aid business continuity and recovery; these employees back up their data and inform colleagues of security issues (Blythe *et al.*, 2015). It is argued that when employees comply with the ISPs, information security threats are reduced (Klein and Luciano, 2016).

Alfawaz *et al.* (2010) propose these security behaviour modes: knowing-doing mode, knowing-not doing mode, not knowing-doing mode and not knowing-not doing mode. In the not knowing-not doing mode, employees violate information security rules because they do not know the organisation's information security rules and do not have any security knowledge (Alfawaz *et al.*, 2010). In the not knowing-doing mode, employees do not know the information security rules and do not have security knowledge, but they still exhibit the right security behaviour. These are employees who will ask their co-workers before taking certain actions. In the knowing-not doing mode, employees know the rules and have the necessary security knowledge and skills, but they still violate the rules (Alfawaz *et al.*, 2010). In the knowing-doing mode, employees know the rules, have the necessary security skills and comply with the rules (Alfawaz *et al.*, 2010).

Ahmad *et al.* (2016) group employees into four types based on whether or not they know the security rules and whether or not they comply with the information security rules. They classify these rules as discerning, obedient, rebellious and oblivious employees. Discerning individuals conform to the information security rules because they have the necessary knowledge; some employees conform to the information security rules not because they have the knowledge but because they follow organisational rules just because they are there; other employees choose not to conform to information security rules despite having the knowledge; and others still violate information security because they do not have the security knowledge (Ahmad *et al.*, 2016).

Alfawaz *et al.* (2010) and Ahmad *et al.* (2016) propose a classification of employees' information security behaviour that also explain why employees fail to comply with organisational ISPs. They postulate that employees fail to comply because they are ignorant of the regulations, they choose not to or they are not competent due to lack of security knowledge. Their classifications suggest that in order for employees to comply with the ISPs, they have to be equipped with the relevant security knowledge and skills (taught or learn information security behaviour). Employees will also have to actively think about the security implications of their actions when they do their work. Therefore, security awareness, knowledge and experience are important (Safa *et al.*, 2015).

Employees must also understand their responsibilities regarding information security, because an employee who lacks information security awareness is more vulnerable to information security attacks (Alohali *et al.*, 2017).

Employees are expected to align their actions with the expected behaviours as written in organisational ISPs, because ISP compliance leads to secure behaviour among employees (Sommestad *et al.*, 2014). In the information security literature, compliance is expressed as employees' adherence to the ISPs (Bulgurcu *et al.*, 2010; Padayachee, 2012; Guo, 2013; Connolly *et al.*, 2016). Li *et al.* (2017) define ISP compliance as employee compliance with information security guidelines as they perform their jobs. It is argued that employee compliance with ISPs minimises security incidents (Humaidi and Balakrishnan, 2017; Nasir *et al.*, 2017). Therefore, there is a need to understand what motivates compliance with ISPs (Huang *et al.*, 2016; Curry *et al.*, 2018; Bhaharin *et al.*, 2019), as the human element is also responsible for security breaches (Ofori *et al.*, 2020).

Secure behaviour concerning information security results in the protection of information system resources or the avoidances of security breaches and complies with ISPs (Blythe *et al.*, 2015; Guo, 2013; Safa *et al.*, 2015). The employee takes precautions (Guo, 2013) and always considers the effect of their behaviour (Safa *et al.*, 2015) when using information systems. Secure behaviour also results in business continuity and recovery (Blythe *et al.*, 2015). Secure behaviour is a result of an employee who has a clear intention to comply with the ISP (Guo, 2013; Safa *et al.*, 2015). However, the employee may unintentionally comply with the ISP (Guo, 2013); the employee could comply with the ISP when they are not knowledgeable about information security rules or the existence of the ISP (Alfawaz *et al.*, 2010; Ahmad *et al.*, 2016).

Therefore, human behaviour plays an important role in protecting information and should be directed to prevent information security threats. To behave appropriately, employees must be knowledgeable about the ISPs. Information security compliant behaviour results in:

- the prevention of security breaches;
- business continuity, recovery and availability;
- protection of confidentiality of information (non-disclosure);
- protection of hardware, software, integrity and quality of information; and
- preservation of trust and reputation of both the employee and the organisation.

4. Information Security Compliant Behaviour Questionnaire

The Information Security Compliance Behaviour Model (ISCBM^{SDT}) is based on the three concepts of the SDT, which are the need for competence, the need for relatedness and the need for autonomy. These three basic psychological needs are regarded as some of the sources contributing to intrinsic motivation (Ryan and Deci, 2000; Legault, 2017). The need for autonomy is the perception that one is acting out of one's own volition and that one's behaviour is self-determined. The need for relatedness refers to the desire to be attached to others. Competence is the belief of being capable and effective (Ryan and Deci, 2000). The ISCBM^{SDT} postulates that when perceived competence, perceived relatedness and perceived autonomy are fulfilled, the employees will comply with the ISP because it is their choice to do so (Gangire *et al.*, 2019). To assess information security behaviour, the Information Security Compliant Behaviour Questionnaire (Gangire *et al.*,

2020) that was developed for this study is based on the ISCBM^{SDT} model (Gangire *et al.*, 2019) and the HAIS-Q.

The HAIS-Q was developed to examine the relationships between the user's knowledge of ISP, attitude towards ISP and behaviour when using computers at work (Parsons *et al.,* 2017; Butavicius *et al.,* 2020). The instrument consists of seven information security areas (also referred to as focus areas). These areas are (1) password management, (2) email use, (3) internet use, (4) social media use, (5) mobile devices, (6) information handling and (7) incident reporting. The focus areas are each split into sub-areas, with each sub-area having a separate item for each of knowledge, attitude and behaviour (KAB), resulting in a total of 63 specific statements making up the HAIS-Q. It uses a five-point Likert scale, rated from Strongly Agree to Strongly Disagree, for all the items in the questionnaire. The instrument uses the KAB model, as it is assumed that the improvement in users' knowledge of the ISP and their attitude towards the ISP has a positive impact on their information security behaviour (Parsons *et al.,* 2017).

Questionnaire focus areas

The questionnaire for this study is based on the focus areas of the HAIS-Q (Parsons *et al.,* 2017; Butavicius *et al.,* 2020) and an additional focus area, privacy. The privacy dimension was included since Parsons *et al.* (2017) suggest that there is a need to explore the relationship between information security awareness and privacy. Also, the privacy focus area was included since privacy is an important aspect when processing, storing and disseminating student information in an institution of higher learning. In this study, information privacy refers to how the organisation administers the collection, storage, processing and dissemination of personal information (Kokolakis, 2017). The focus areas have been adapted to the three concepts of the SDT, resulting in each section of the questionnaire focusing on each of competence, relatedness and autonomy. By combining the HAIS-Q and the SDT, this study fills a gap – as suggested by Wall *et al.* (2013) – namely that there could be a need for the development of an instrument to study information security based on the SDT. A discussion of the focus areas of the questionnaire follows.

(1) **Password management:** This involves understanding how to protect information system resources by using strong and secure passwords. This includes regularly changing passwords, choosing strong passwords and not sharing passwords (Shropshire *et al.*, 2015; Calic *et al.*, 2016; Blythe *et al.*, 2015).

(2) **Email usage:** Employees have to understand safe email use. This includes not downloading unsafe attachments, clicking on links in email from known or unknown senders, and opening attachments in emails from unknown senders (Bélanger *et al.*, 2017; Pattinson *et al.*, 2015; Shropshire *et al.*, 2015; Blythe *et al.*, 2015; Safa *et al.*, 2015; Alohali *et al.*, 2017).

(3) **Internet usage:** Employees should know how to use the internet safely. This includes downloading files, accessing dubious websites and entering information online (Bauer *et al.*, 2017; Pattinson *et al.*, 2015; Klein and Luciano, 2016; Bélanger *et al.*, 2017).

(4) **Social media usage:** Employees should understand safe usage of social media. This includes social media privacy settings, considering the consequences of posting information and acting responsibly regarding posting about work on social media (Bauer *et al.*, 2017).

(5) **Mobile devices usage:** Employees should understand how to secure their mobile devices that carry work information when working in a public area. This includes physically securing mobile devices, sending sensitive information via public Wi-Fi and guarding against shoulder surfing (Curry *et al.*, 2018; Bauer *et al.*, 2017).

(6) **Information handling:** Employees have to understand how to handle sensitive information. This includes disposing of sensitive printouts, inserting removable media in work computers and leaving sensitive material on work areas (Aurigemma and Mattson, 2017; Blythe *et al*., 2015; Bauer *et al*., 2017).

(7) **Incident reporting:** This focus area refers to how employees react when security incidents happen in the workplace. This includes reporting suspicious behaviour, reporting all incidents and ignoring poor security behaviour by colleagues (Pattinson *et al*., 2015).

(8) **Privacy:** Employees should understand how to handle personally identifiable information. This includes non-disclosure of sensitive information (Blythe *et al*., 2015; Safa *et al*., 2015), processing client information in a lawful manner (Swartz *et al*., 2019), processing client information for the purpose for which it was collected (NIST, 2017; Swartz *et al*., 2019) and adhering to the organisation's privacy policy (Dennedy *et al*., 2014). When employees adhere to the privacy policy, they can uphold the privacy of student data they handle. Parsons *et al.* (2017) propose that the link between information security awareness and privacy should be investigated.

The list of questions in the competence, relatedness and autonomy category for the focus areas are reported in the appendix.

5. Research method

This study adopted the positivist research paradigm with a quantitative approach. In the positivist research paradigm, researchers prefer to work with observable and measurable reality. Positivists use quantitative methods in their research and the research is based on testing theories (Oates, 2006; Saunders *et al*., 2016). The survey strategy was chosen and the questionnaire was used for data collection at a university in South Africa. A non-probability purposive sampling method was used. With purposive sampling, the researcher deliberately selects the sample, for example based on the accessibility of participants (Oates, 2006). The selection of the expert panel was done using the purposive sampling method based on the following criteria: they had all done research on information security and had experience in information security awareness. The pilot sample was selected using convenience sampling in one of the university's departments. The survey participants were selected using purposive sampling. The survey questionnaire was sent electronically to the entire population of administrative, academic and operational staff. Ethical clearance was obtained from the university, adhering to the research ethics policy that focuses on aspects such as anonymity, voluntary participation, confidentiality and consent for participation.

The following statistical analyses were performed: ANOVA, t-test and Pearson correlation analysis. ANOVA was carried out to determine if there were significant differences among the demographical groups for age, job level, level of education and length of service groups. The t-tests were performed to determine if the mean scores among the gender groups had any significant differences. The correlation analysis was carried out to determine if there was any correlation among the resulting factors from the exploratory factor analysis (EFA).

Questionnaire development

A Likert scale (strongly agree, agree, unsure, disagree and strongly disagree) was used to answer the questions. The questionnaire had two sections: Section 1 was for demographic information and Section 2 comprised the information security behaviour questions. The final questionnaire had 75 questions: 25 questions for each of the SDT categories.

To address face validity, an expert panel and pilot group were convened to review the questionnaire. Face validity is an assessment of a questionnaire to determine whether it logically reflects what it was intended to measure (Saunders *et al.*, 2016). To ensure content validity, the questionnaire was based on the HAIS-Q focus areas and a panel of expert reviewers assessed the questionnaire by going through each question and indicating whether it was essential or not as well as whether it was clear or not. Content validity refers to the extent to which the questionnaire items address the objectives of the study (Saunders *et al.*, 2016).

Expert panel reviews

A panel of experts on the research area evaluated the questionnaire. This helped to refine and improve the questionnaire (Saunders *et al.*, 2016). The questionnaire was reviewed by a panel of six experts, four of whom were from the field of psychology (human factors scientists) who had researched the human aspects of cyber security for 11 years and had developed the HAIS-Q. The other two were an academic in information security and an IT security consultant specialising in incident response and awareness. The reviewers had 10 to 20 years of work experience. They pointed out that some of the questions were not clear and that other questions addressed two different aspects in one question. The unclear questions were re-worded to make them clear and those addressing more than one concept were either split into separate questions or the concept that was irrelevant was dropped.

Pilot testing

The pilot test was conducted among 12 staff members in one of the departments of the university. The questionnaire pilot test showed that some questions were not worded clearly and it was recommended that job levels be added to the biographical section.

Main study

The updated questionnaire was prepared and administered using Google Forms over the internet, and the participants were notified by an email invitation sent by the Information and Communication Technology Department of the university. The email contained information on the research and the links for completing the online questionnaire. The participants were required to read the information sheet and the consent form. If they consented to participate in the study, they proceeded to complete the online questionnaire.

6. Results

Demographics

Two hundred and sixty-three (263) responses were received from the online survey. The sample consisted of 54.8% females and 44.1% males; 1.1% did not disclose their gender. Those born between 1977 and 1995 were the largest group of respondents (38.40%). The highest number of survey respondents (69.08%) was from the group with postgraduate qualifications. There were more respondents from the groups with higher qualifications (i.e. the higher the qualification, the higher the number of respondents). This is consistent with a university environment. Those who had worked for six to 10 years were the largest group (27.38%) and most of the respondents were administrative staff (51.53%). Table 1 shows the demographic data of the respondents.

Table 1: Demographic data of respondents

Demographic Item		Count	Percentage (%)
Gender	Male	116	44.11
	Female	144	54.75
	Prefer not to say	3	1.14
Age	1946–1964	77	29.28
	1965–1976	83	31.56
	1977–1995	101	38.40
	1996–date	2	0.76
Education	High school	10	3.82
	Certificate	15	5.73
	Diploma	19	7.25
	Degree	37	14.12
	Postgraduate	182	69.08
Length of service	Less than 1 year	13	4.94
	1–5 years	68	25.86
	6–10 years	72	27.38
	11–15 years	37	14.07
	16–20 years	23	8.75
	More than 20 years	50	19.00
Job level	Academic	102	38.93
	Administrative	136	51.53
	Operational	25	9.54

Information security behaviour questions scores

This section reports on the results of the information security behaviour questions. A cut-off of 4.0 for the means was set for the information security behaviour questions (Da Veiga and Martins, 2015). A mean score of 4.0 and above indicated a positive perception, while a mean score below 4.0 indicated a neutral or potentially negative perception.

For the competence questions, the top 10 questions all had means above 4.0. This suggests that the respondents had a positive perception of the competence questions. Of the bottom 10 questions, five had means above 4.0 and five had means below 4.0, indicating areas for which further improvement is required.

For the relatedness questions, the mean values for the top statements ranged from 3.05 to 3.51 and the mean values for the bottom statements ranged from 2.68 to 3.01. These mean values for both top questions and bottom questions show that all had means below 4.0. This suggests that the participants had neutral and potentially negative perceptions of the relatedness questions, indicating areas requiring further improvement.

For the autonomy questions, the mean values for the top statements ranged from 4.41 to 4.68 and the mean values for the bottom statements ranged from 3.91 to 4.27. The top questions all had means above 4.0, suggesting that the respondents had a positive perception of the autonomy questions. For the bottom 10 questions, eight questions had means above 4.0 and two had means below 4.0. The two questions with means below 4.0 indicate areas where further improvement is required.

Figure 1 summarises the means of the information security questions per SDT category. It shows that autonomy had the highest scores (M = 4.32), followed by competence (M = 4.28) and lastly relatedness (M = 3.08). This suggests that autonomy questions received a more positive perception, closely followed by competence questions;

relatedness questions received neutral or potentially negative perceptions from the participants.

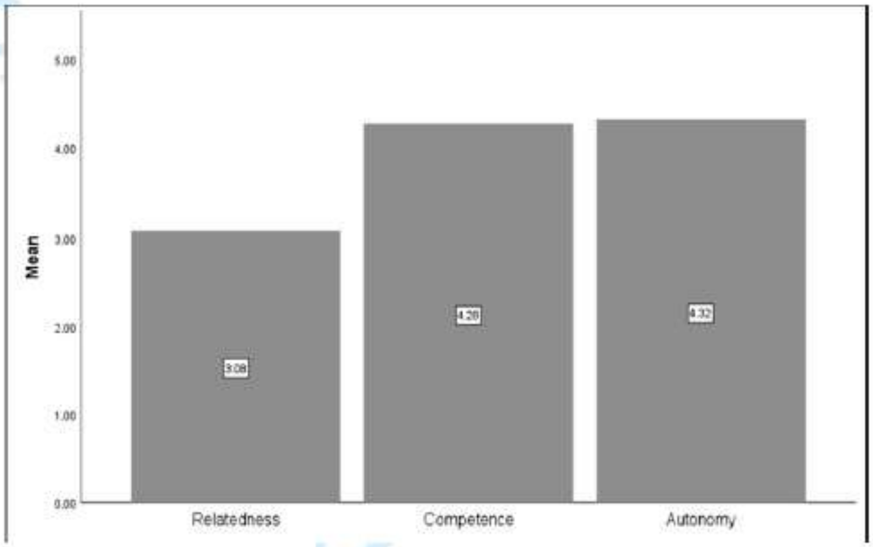


Figure 1: Information security questions means per SDT category

Validation of the instrument

Factor analysis

EFA was carried out to determine the underlying relationships between the variables (Yong and Pearce, 2013) as well as the construct validity of the questionnaire (Williams *et al.*, 2010). O'Rourke and Hatcher (2013) suggest that to achieve a sample size that is statistically adequate to carry out questionnaire validation, the responses or the collected data must be at least five times the number of questions in the questionnaire. EFA was done for each category and the new factors were determined per category. Since each category had 25 questions, a minimum of 125 responses were required per category. As per the recommendation of O'Rourke and Hatcher (2013), the received responses were sufficient to carry out the statistical validation of the questionnaire and the data were processed using SPSS Version 25.

Determining the number of factors

The Kaiser-Meyer-Olkin (KMO) test and the Bartlett sphericity test were conducted for each of the three categories (competence, relatedness and autonomy). Field (2009) recommends a KMO value closer to 1 in order to produce distinct and reliable factors. For the Bartlett sphericity test, the probability should be less or equal to 0.05; this shows highly correlated variables (Williams *et al.*, 2010). The KMO for the competence statements was 0.915 and the Bartlett sphericity test result was statistically significant (p = 0.000). The KMO for the relatedness statements was 0.965 and the Bartlett sphericity test result was statistically significant (p = 0.000). The KMO for the autonomy statements was 0.885 and the Bartlett sphericity result was statistically significant (p = 0.000). As a result, all the categories met the criteria for performing the EFA.

The factors were determined using Eigenvalues, scree plots and cumulative percentages (Gerber and Hall, 2017). The item loading cut off was set at 0.4, as Stevens (2002) suggests that item loading values should be greater than 0.4. The cumulative percentage had to be above 60% and the Eigenvalues had to be greater than 1. Competence statements initially resulted in four factors and these had Eigenvalues greater than 1 and a cumulative Eigenvalue of 62.38%. Relatedness statements resulted in two factors and these had Eigenvalues greater than 1 and a cumulative Eigenvalue of 70.74%. The autonomy statements resulted in six factors and these had Eigenvalues greater than 1 and a cumulative Eigenvalue of 63.68%.

Table 2 shows the resulting factors. For the competence statements, Factor 3 Statement 25 was removed because it had a factor cross-loading with a cross-loading difference of less than 0.2. Factor 4 was dropped, as it had only one item; Statement 3 and factors for the competence category were reduced to 3. For the relatedness category, Questions 17 and 18 were dropped because they had cross-loading differences of less than 0.2. For the autonomy category, Statements 1, 2, 3, 14, 17 and 18 were dropped because they had loadings below 0.4.

Table 2: Resulting factors

Category	Factor	Statements
Competence	Factor 1	1, 10, 11, 12, 14, 15, 16, 18, 19, 20, 21
	Factor 2	4, 5, 6, 7, 8, 9, 17
	Factor 3	22, 23, 24
Relatedness	Factor 1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
	Factor 2	19, 20, 21, 22, 23, 24, 25
Autonomy	Factor 1	8, 9, 10
	Factor 2	4, 5, 6, 7
	Factor 3	22, 23
	Factor 4	19, 20, 21
	Factor 5	24, 25
	Factor 6	11, 12, 13, 15, 16

Naming the factors

The factors shown in Table 2 were named to reflect the common themes of the statements grouped under a given factor.

Competence

Factors in this category reflect the employee's competence/skills to carry out the information security actions. The employees are confident that they can protect the IT resources because they have the necessary skills to do so. For the competence statements, Factor 1 (11 items) was named "employee skills for data safety awareness"; Factor 2 (seven items) was named "employee skills for email and website safety"; and Factor 3 (four items) was named "employee skills for privacy awareness".

Relatedness

Factors in this category reflect the employees' need for support from colleagues to carry out information security actions. The employees perceive that they can protect the IT resources if co-workers and superiors support them. For the relatedness statements, Factor 1 (16 items) was labelled "organisational support for employee device and information protection awareness" and Factor 2 (seven items) was named "organisational support for employee information and privacy protection awareness".

Autonomy

Factors in this category reflect the employees' need to be in control of their information security behaviour. The employees perceive that when they are in control of their information security behaviour, they can protect the IT resources of their organisation. For the autonomy statements, Factor 1 (three items) was named "employee choice on privacy awareness"; Factor 2 (four items) was named "employee choice to avoid malicious emails and downloads"; Factor 3 (two items) was named "employee choice to keep the privacy of student personal information"; Factor 4 (three items) was named "employee choice to report bad security behaviour"; Factor 5 (two items) was named "employee choice to adhere to information security and privacy policies"; and Factor 6 (five items) was named "employee choice to keep devices and information secure".

Two autonomy factors (employee choice to keep privacy of student personal information and employee choice to adhere to information security and privacy policies) had two statements each. They were retained because both factors had very good reliability, as shown in Table 3.

Reliability analysis

The Cronbach alpha coefficient was calculated for each of the 11 factors. Reliability refers to how consistent or dependable the measuring instrument is, and whether under similar conditions the measuring instrument produces consistent results (Marczyk *et al*., 2005). According to Gerber and Hall (2017), the Cronbach alpha coefficient can be interpreted as follows: good for values greater than 0.8, acceptable for values between 0.6 and 0.8, and unacceptable for values less than 0.6. Table 3 shows the results of the Cronbach alpha values for the 11 factors. All the Cronbach alpha results were above 0.7, suggesting high reliability.

Table 3: Cronbach alpha coefficient results for factors

Category	Factor	No. of Items	Cronbach Alpha	Comment
Competence	Employee skills for data safety awareness	11	0.906	Good
	Employee skills for email and website safety	7	0.905	Good
	Employee skills for privacy awareness	4	0.799	Good
Relatedness	Organisational support for employee device and information awareness	16	0.967	Good
	Organisational support for employee information and privacy protection awareness	7	0.945	Good
Autonomy	Employee choice on privacy awareness	3	0.775	Acceptable
	Employee choice to avoid malicious emails and downloads	4	0.836	Good

Category	Factor	No. of Items	Cronbach Alpha	Comment
	Employee choice to keep the privacy of student personal information	2	0.904	Good
	Employee choice to report bad security behaviour	3	0.791	Acceptable
	Employee choice to adhere to information security and privacy policies	2	0.868	Good
	Employee choice to keep devices and information secure	5	0.793	Acceptable

The final questionnaire had 11 revised dimensions and the individual statements were not changed. The new dimensions were the result of the factor and reliability analyses, hence the resulting questionnaire can be considered to have good internal consistency.

Correlation of the factors

The results of the Pearson correlation showed that the competence and autonomy factors had a statically significant positive correlation ($r >= .287$, $n = 263$, $p < .05$), two tailed. The correlation for the competence and relatedness factors showed that some factors had a positive correlation ($r >= .224$, $n = 263$, $p < 0.05$), two tailed, and other factors did not. The correlation results for the autonomy and relatedness factors showed that some factors had a positive correlation ($r >= .134$, $n = 263$, $p < .05$), two tailed, and others did not.

Analysis of variance (ANOVA) results

One-way ANOVA was conducted for each factor and the demographic variables (age, job level, highest level of education and length of service at current employer) to determine whether the means differed among groups. Scheffe's method was used for the post-hoc tests to identify where the significant differences lay among the groups. The post-hoc results are presented for the statistically significant ($p < 0.05$) ANOVAs only.

Age groups

The ANOVAs for the age groups indicated that there was a significant difference ($p < 0.05$) for two factors: the organisational support for employee information privacy protection awareness $F(2, 259) = 3.369$ ($p = 0.036$) and the employee choice to avoid malicious emails and downloads $F(2, 259) = 3.672$ ($p = 0.027$). The post-hoc results indicated that participants from the 1977–date age group had significantly higher scores on the organisational support for employee information privacy protection awareness items ($M = 3.47$) than participants from the 1965–1976 age group ($M = 2.999$). The results suggested that both groups had a potentially neutral and negative perception of organisational support for employee information privacy protection awareness. The post-hoc results also indicated that participants from the 1946–1964 age group had significantly higher scores on the employee choice to avoid malicious emails and downloads items ($M = 4.5$) than participants from the 1965–1976 age group ($M = 4.13$). This suggests that participants from the 1946–1964 age group had a more positive perception of the employee choice to avoid malicious emails and downloads questions compared to the 1965–1976 age group.

Job level

The ANOVA results for job level groups for the 11 factors showed that there were significant differences ($p < 0.05$) between six factors for the job level groups.

The employee skills for data safety awareness factor showed a significant difference between the job level groups F(2, 259) = 4.976 (p = 0.008). The post-hoc results indicated that participants' responses from the academic staff group had significantly higher scores (M = 4.38) on the employee skills for data safety awareness factor questions than participants' responses from the operational staff group (M = 3.94). This suggests that participants from the academic staff group had a more positive perception of the employee skills for data safety awareness questions.

The employee skills for email and website safety factor showed a significant difference between the job level groups F(2, 258) = 10.482 (p = 0.000). The post-hoc results showed that participants' responses from the academic staff group had significantly higher scores (M = 4.34) on the employee skills for email and website safety questions, followed by participants' responses from the administrative group (M = 4.07); the operational staff group (M = 3.94) had the lowest scores. This suggests that the academic staff group had a more positive perception of the employee skills for email and website safety questions, followed by the administrative staff group and lastly the operational staff group.

The employee skills for privacy awareness factor showed a significant difference between the job level groups F(2, 258) = 8.653 (p = 0.000). The post-hoc results showed that participants from the academic staff group had significantly higher scores (M = 4.68) on the employee skills for privacy awareness factor than participants from the administrative group (M = 4.34). Also, the results showed that the academic staff group scored significantly higher than the operational staff group (M = 3.98). This implies that the academic staff group had a more positive perception of the employee skills for privacy awareness questions, followed by the administrative staff and lastly the operational staff.

The employee choice to avoid malicious emails and downloads factor showed a significant difference between the job level groups F(2, 258) = 6.458 (p = 0.002). The post-hoc results showed that participants from the academic staff group had significantly higher scores (M = 4.38) on the employee choice to avoid malicious emails and downloads factor than participants from the operational staff group (M = 3.72). Also, the results showed that the administrative staff group scored significantly higher (M = 4.35) than the operational staff group. This implies that the academic staff group had a more positive perception of the employee choice to avoid malicious emails and downloads questions, followed by the administrative staff group and lastly the operational staff group.

The employee choice to keep the privacy of student personal information factor showed a significant difference between the job level groups F(2, 257) = 8.251 (p = 0.000). The post-hoc results showed that participants from the academic staff group had significantly higher scores (M = 4.67) on the employee choices to keep the privacy of student personal information factor than participants from the administrative group (M = 4.36). Also, the results showed that the academic staff group had significantly higher scores than the operational staff group (M = 3.98). This implies that the academic staff group had a more positive perception of the employee choices to keep the privacy of student personal information questions, followed by the administrative staff group and lastly the operational staff group.

The employee choice to keep devices and information secure factor showed a significant difference between the age groups F(2, 258) = 4.256 (p = 0.015). The post-hoc results showed that participants from the academic staff group had significantly higher scores (M = 4.61) on the employee choice to keep devices and information secure factor than participants from the administrative group (M = 4.39). This implies that the academic staff group had a more positive perception of the employee choice to keep devices and information secure questions than the administrative staff group.

Level of education

The ANOVA results for the level of education groups at the post-hoc tests showed that the two factors did not have a significant difference. On the factor level, there were significant differences; however, the post-hoc test showed that there were no significant differences between any of the educational levels.

Independent samples test (t-test)

The t-test results showed that the mean differences for the gender groups for all the factors were not statistically significant.

7. Discussion

The study was aimed at developing and validating a questionnaire to assess information security behaviour from the perspective of competence, relatedness and autonomy. The questionnaire was designed based on the ISCBM^{SDT} and HAIS-Q focus areas and an additional focus area of privacy. The focus areas of the HAIS-Q were mapped to each of the concepts of the SDT to come up with unique questions for each of the concepts. Each focus area of the HAIS-Q was framed from the perspective of each of the SDT components of competence, relatedness and autonomy, resulting in three unique questions for each focus area. This study contributed towards building upon the HAIS-Q to come up with a questionnaire based on the SDT.

The results of the information security behaviour questions suggest that the respondents had a more positive perception of the competence and autonomy questions than of the relatedness questions. This is confirmed by the overall results of the means per category, which show that autonomy had the highest scores (M = 4.32), followed by competence (M = 4.28) and lastly relatedness (M = 3.08). This suggests that competence, autonomy and relatedness could play an important role in employees' information security behaviour. The results of the overall means per category indicate that autonomy questions received a more positive perception, closely followed by competence questions and relatedness questions. This suggests that autonomy could play an important role in fostering information security behaviour, followed by competence and lastly relatedness. These results could imply that most of the respondents were confident about their skills (competence) and their independence (autonomy) in their work. The study results indicate that this may not be the case with the relatedness aspects. This suggests that the university might need to encourage employees to appreciate how the work of colleagues relates to theirs. Hence, an employee should have awareness of the benefits of collaboration in their work. The university will need to pay special attention to relatedness issues, as the employees were not confident about these. The university should thus encourage collaboration among employees.

The Pearson correlation results show a positive correlation between competence and autonomy, suggesting that the respondents who perceived they were competent also felt confident about their autonomy perception. The Pearson correlation results also indicate a positive correlation between autonomy and competence, whereas there is a partial correlation between relatedness and other factors. This could suggest that as competence increases, autonomy also increases as far as information security behaviour is concerned. The Pearson correlation results suggest that respondents who perceived they were competent could also have felt confident about their autonomy perception. Other studies showed results that align with this result. Wall *et al*. (2013) found in their study that perceptions of self-determination (autonomy) fostered perceptions of self-efficacy (competence). In their study, Kranz and Haeussinger (2014) found that an internally perceived locus of control (a form of autonomous motivation) had a positive effect on self-efficacy (competence). This could also mean that those who have a positive perception of autonomy are likely to feel confident about their competence as well. Autonomy is the desire to be a causal agent of one's behaviour and goals (Ryan and Deci, 2000). Competence is the desire to feel capable, gain mastery of tasks and learn new skills (Ryan and Deci, 2000). The need for relatedness is the desire to interact and experience attachment with others (Ryan and Deci, 2000). In this study, perceptions of competence were related positively to perceptions of autonomy. Employers should foster the belief that employees are capable of carrying out information security tasks, assist with the acquisition of relevant skills and problem solving. This could also foster a sense of control over their work and encourage self-initiation. In terms of relatedness, the employee should be made to understand the value of their work and how it relates to their co-workers. The employer should show interest and support toward the employee.

The ANOVA results show that the age and the job level groups showed significant differences between groups. For the job level, there were significant differences between the 1977–date and 1965–1976 groups. Both groups' mean scores were less than 4.0 for the organisation support for employee information privacy protection awareness factor. This suggests that both groups should be prioritised for privacy training. The job level groups also had significant differences between groups. For all the factors that had significant differences for the job level groups, the operational staff group scored lower than the academic and administrative groups. The scores were less than the cut off of 4.0. The results suggest that the operational staff group should be prioritised for training in the following areas: email usage, website usage, privacy, social media usage and mobile device usage.

The survey results also show that respondents had low confidence about their social media privacy settings. This is true from the competence, relatedness and autonomy perspectives. The university could set up awareness training to educate its employees about the importance of securing their privacy settings and continuously reviewing them. This could include training employees on how to locate the privacy settings on major social media platforms and to change them from the default setting to more secure privacy settings.

8. Limitations of the study and future research directions

The convenience sampling method used in this study (an accepted method of collecting data) may not produce a sample that is representative of the population. Therefore, future research should consider a representative sample of the population and inclusion of more organisations. The survey questionnaire had 75 questions, which may take some time to complete and hence some respondents may not complete the survey. Future work should consider reducing the number of questions.

The study developed a questionnaire and assessed information security behaviour from the competence, relatedness and autonomy perspectives. The study did not determine the influence of competence, relatedness and autonomy on information security compliant behaviour. Future work could consider determining the influence of competence, relatedness and autonomy on positive information security behaviour.

9. Conclusion

The aim of this study was to develop and validate the information security behaviour ISCBM^{SDT} questionnaire based on the SDT. This questionnaire can be used to investigate how the perception of competence, relatedness and autonomy influence the intention to comply with ISPs. The results of the assessment can be used to design programmes to assist employees in complying with ISPs.

The questions were developed by combining the variables from the SDT and the themes from the HAIS-Q as well as privacy to come up with a new questionnaire. Through a quantitative research study, data were collected using the survey method. The collected data were used to validate the questionnaire, resulting in a revised questionnaire with items with high internal consistency.

Generally, the results suggest that the survey participants were more confident about their competence and autonomy regarding their information security behaviour than they were about the relatedness questions. There was also a correlation between the competence factors and the autonomy factors.

The practical implication of this study and this questionnaire is that it can be used by a university to assess individual employees' strengths and weaknesses in terms of their awareness of information security behaviour and to direct training and awareness interventions. The questionnaire could also be administered before and after information security awareness training to assess the effectiveness of the training.

Acknowledgment

This work is based on research supported by the University of South Africa's Women in Research Grant. The University of South Africa's School of Computing in the College of Science, Engineering and Technology also supported this project financially.

References

Ahmad, Z., Norhashim, M., Song, O. T. and Hui, L. T., (2016), "A typology of employees' information security behaviour". 4th International Conference on Information and Communication Technology (ICoICT), New Delhi, India, pp. 3–6.

Alfawaz, S., Karen, N. and Mohannak, K., (2010), "Information security culture: A Behaviour Compliance Conceptual Framework", In Boyd, C. & Susilo, W., (Eds), 8th Australasian Information Security Conference (AISC 2010). Conferences in Research and Practice in Information Technology (CRPIT), Brisbane, Australia, Australian Computer Society, pp. 47–55.

Alohali, M., Clarke, N., Furnell, S. and Albakri, S., (2017), "Information security behavior: Recognizing the influencers", Computing Conference, IEEE, London, UK, pp. 844–853.

Aurigemma, S. and Mattson, T., (2017), "Deterrence and punishment experience impacts on ISP compliance attitudes", Information and Computer Security, Vol. 25 No. 4, pp. 421–436.

Bauer, S., Bernroider, E. W. N. and 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, Vol. 68, pp. 145–159.

Bélanger, F., Collignon, S., Enget, K. and Negangard, E., (2017), "Determinants of early conformance with information security policies", Information & Management, Vol. 54 No. 7, pp. 887–901.

Bhaharin, S. H., Sulaiman, R., Mokhtar, U. A. and Yusof, M. M., (2019), "Issues and trends in information security policy compliance", 6th International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE, Johor Bahru, Malaysia.

Blythe, J. M., Coventry, L. and Little, L., (2015), "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors", Symposium on Usable Privacy and Security (SOUPS), USENIX Association, Ottawa, Canada, pp. 103–122.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I., (2010), "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", MIS Quarterly, Vol. 34 No. 3, pp. 523–548.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M. and Calic, D., (2020), "When believing in technology leads to poor cyber security: Development of a trust in technical controls scale", Computers & Security, Vol. 98.

Calic, D., Pattinson, M., Parsons, K., Butavicius, M. and McCormac, A., (2016), "Naïve and accidental behaviours that compromise information security: What the experts think". In Clarke, N. & Furnell, S., (Eds), 10th International Symposium on Human Aspects of

Information Security & Assurance (HAISA 2016), Plymouth University, Frankfurt, Germany, pp. 12–21.

Carden, L., and Wood, W., (2018), "Habit formation and change", Current Opinion in Behavioral Sciences, Vol. 20, pp. 117–122.

Connolly, L., Lang, M., Gathegi, J. and Tygar, J. D., (2016), "The effect of organisational culture on employee security behaviour: A qualitative study", In Clarke, N. & Furnell, S., (Eds), 10th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2016), Plymouth University, Frankfurt, Germany, pp. 33–44.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. and Baskerville, R., (2013), "Future directions for behavioral information security research", Computers & Security, Vol. 32, pp. 90–101.

Curry, M., Marshall, B., Crossler, R. E. and Correia, J., (2018), "InfoSec Process Action Model (IPAM): Systematically addressing individual security behavior", The Database for Advances in Information Systems, Vol. 49, pp. 49–66.

Da Veiga, A. and Martins, N., (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", Computers & Security, Vol. 49, pp. 162–176.

Davis, R., Campbell, R., Hildon, Z., Hobbs, L., and Michie, S., (2015), "Theories of behaviour and behaviour change across the social and behavioural sciences: a scoping review", Health Psychology Review, Vol. 9 No. 3, pp. 323–344.

Dennedy, M. F., Fox, J. and Finneran, T. R., (2014), Data and privacy governance concepts, The privacy engineer's manifesto, New York, Apress, pp. 51–72.

Field, A., (2009), Discovering statistics using SPSS, 4th ed. London, Sage Publications.

Gangire, Y., Da Veiga, A. and Herselman, M., (2019), "A conceptual model of information security compliant behaviour based on the self-determination theory", Conference on Information Communications Technology and Society (ICTAS 2019), IEEE, Durban, South Africa.

Gangire, Y., Da Veiga, A. and Herselman, M., (2020), "Information security behavior: Development of a measurement instrument based on the self-determination theory", In Clarke, N. & Furnell, S. (Eds), 14th IFIP WG 11.12 International Symposium (HAISA 2020), Springer International Publishing, Mytilene, Lesbos, Greece, pp. 144–157.

Gerber, H. and Hall, N., (2017), Quantitative research design. In Data Acquisition – 1 Day. Pretoria: HR Statistics (Pty) Ltd, pp. 1–64.

Guo, K. H., (2013), "Security-related behavior in using information systems in the workplace: A review and synthesis", Computers & Security, Vol. 32 No. 1, pp. 242–251.

Han, J. Y., Kim, Y. J. and Kim, H., (2017), "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective", Computers & Security, Vol. 66, pp. 52–65.

Herath, T. and Rao, H. R., (2009), "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", Decision Support Systems, Vol. 47 No. 2, pp. 154–165.

Huang, H-W., Parolia, N. and Cheng, K-T., (2016), "Willingness and ability to perform information security compliance behavior: Psychological ownership and self-efficacy perspective", Pacific Asia Conference on Information Systems (PACIS 2016), AIS Electronic Library, Chiayi City, Taiwan.

Humaidi, N. and Balakrishnan, V., (2017), "Indirect effect of management support on users' compliance behaviour towards information security policies", Health Information Management Journal, Vol. 47 No. 1, pp. 17–27.

Hwang, I., Wakefield, R., Kim, S. and Kim, T., (2019), "Security awareness: The first step in information security compliance behavior", Journal of Computer Information Systems, pp. 1–12.

Ifinedo, P., (2013), "Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition", Information & Management, Vol. 51, pp. 69–79.

Klein, R. H. and Luciano, E. M., (2016), "What influences information security behavior? A study with Brazilian users", Journal of Information Systems and Technology Management, Vol. 13 No. 3, pp. 479–496.

Kokolakis, S., (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", Computers & Security, Vol. 64, pp. 122–134.

Kranz, J. J. and Haeussinger, F. J., (2014), "Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior", 35th International Conference on Information Systems, Auckland, New Zealand, pp. 1–14.

Kuppusamy, P., Narayana, G. and Maarop, N., (2020), "Systematic literature review of information security compliance behaviour theories", Journal of Physics: Conference Series, Vol. 1551 No. 1.

Kwasnicka, D., Dombrowski, S. U., White, M. and Sniehotta, F., (2016), "Theoretical explanations for maintenance of behaviour change: A systematic review of behaviour theories", Health Psychology Review, Vol. 10 No. 3, pp. 277–296.

Lazzeri, F., (2014), "On defining behavior: Some notes", Behavior and Philosophy, Vol. 42, pp. 65–82.

Legault, L., (2017), Self-determination theory. In Zeigler-Hill, V. & Shackelford, T. K, (Eds), Encyclopedia of personality and individual differences. Cham, Switzerland, Springer, pp. 1–9.

Levitis, D. A., Lidicker, W. Z., & Freund, G., (2009), "Behavioural biologists do not agree on what constitutes behaviour", Animal Behaviour, Vol. 78 No. 1, pp. 103–110.

Li, Y., Stafford, T., Fuller, B. and Ellis, S., (2017), "Beyond compliance: Empowering employees' extra-role security behaviors in dynamic environments", 23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation, Association for Information Systems, Boston, USA, pp. 1–5.

Marczyk, G., Fertinger, D. and DeMatteo, D., (2005), Essentials of research design and methodology. Habogen, NJ, Wiley & Sons.

Matsumoto, D. (Ed.). (2012). The Cambridge Dictionary of Psychology. Cambridge, New York: Cambridge University Press.

Mayer, P., Kunz, A. and Volkamer, M., (2017), "Reliable behavioural factors in the information security context", 12th International Conference on Availability, Reliability and Security (ARES '17), Reggio Calabria, Italy, pp. 1–10.

Nasir, A., Rashid, M. and Hamid, A., (2017) "Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework", 2017 International Conference on Information System and Data Mining, Association for Computing Machinery, Charleston, USA, pp. 56–60.

NIST, (2017), Security and privacy controls for federal information systems and organizations. Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

Oates, B. J., (2006). Researching information systems and computing. London: Sage Publications.

Ofori, K. S., Anyigba, H., Ampong, G. O. A., Omoregie, O. K., Nyamadi, M. and Fianu, E., (2020), "Factors influencing information security policy compliance behavior". In Yaokumah, W., Rajarajan, M., Abdulai, J., Wiafe, I. & Katsriku, F. A, (Eds), Modern theories and practices for cyber ethics and security compliance. Hershey, PA, IGI Global, pp. 152–171.

O'Rourke, N. and Hatcher, L., (2013), A step-by-step approach to using SAS for factor analysis and structural equation modelling, Cary, NC, SAS Institute.

Öütçü, G., Testik, Ö. M. and Chouseinoglou, O., (2016), "Analysis of personal information security behavior and awareness", Computers & Security, Vol. 56, pp. 83–93.

Padayachee, K., (2012), "Taxonomy of compliant information security behavior", Computers & Security, Vol. 31 No. 5, pp. 673–680.

Pahnila, S., Karjalainen, M. and Mikko, S., (2013), "Information security behavior: Towards multi-stage models". In Lee, J-N., Mao, J-Y. & Thong, J. Y. L., (Eds), Pacific Asia Conference on Information Systems 2013 (PACIS 2013), AIS Electronic Library, Jeju Island, Korea.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T., (2017), "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies", Computers & Security, Vol. 66, pp. 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C., (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", Computers & Security, Vol. 42, pp. 165–176.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. and Jerram, C., (2015), "Examining attitudes toward information security behaviour using mixed methods". In Furnell, S., (Ed.), 9th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2015). Plymouth, University of Plymouth, pp. 57–70.

Pfleeger, L. S., Sasse, M. A. and Furnham, A., (2014), "From weakest link to security hero: Transforming staff security behavior", Journal of Homeland Security and Emergency Management, Vol. 11 No. 4, pp. 489–510.

Ponemon Institute, (2020). The Third Annual Study on the State of Endpoint Security Risk. Available at: https://www.morphisec.com/hubfs/2020 State of Endpoint Security Final.pdf

PricewaterhouseCoopers, (2018). The Global State of Information Security Survey 2018. Available at: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.htm

Ryan, M. R. and Deci, L. E., (2000), "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being", American Psychologist, Vol. 55 No. 1, pp. 68–78.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. and Herawan, T, (2015), "Information security conscious care behaviour formation in organizations", Computers & Security, Vol. 53, pp. 65–78.

Saunders, M., Lewis, P. and Thornhill, A., (2016). Research methods for business students, 7th ed. Essex, Pearson Education.

Schein, E., (1971), "The Individual, the Organization, and the Career - A Conceptual Scheme", Journal of Applied Behavioural Science, Vol. 7 No. 4, pp. 401–426.

Shropshire, J., Merrill, W. and Sharma, S., (2015), "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior", Quaternary Geochronology, Vol. 49, pp. 177–191.

Snyman, D. and Kruger, H. A., (2020), "Information and cyber security", 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), Springer International, Johannesburg, South Africa.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J., (2014), "Variables influencing information security policy compliance: A systematic review of quantitative studies", Information Management and Computer Security, Vol. 22 No. 1, pp. 42–75.

Son, J. Y., (2011), "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies", Information and Management, Vol. 48 No. 7, pp. 296–302.

Stevens, J. P., (2002). Applied multivariate statistics for the social sciences, 4th ed. Hillsdale, Erlbaum.

Swartz, P., Da Veiga, A. and Martins, N., (2019), "A conceptual privacy governance framework", 2019 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, pp. 1–6.

Tileubayeva, M. S., Massalimova, A. R., Kaufman, J. C., and Fernandez, M. V. C., (2017), "The problems of thinking about mind, body and experience", Psychology and Sociology Series, Vol. 1 No. 60, pp. 111–117.

Tsohou, A., Karyda, M. and 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, Vol. 52, pp. 128–141.

Wall, J. D., Palvia, P. and Lowry, P. B., (2013), "Control-related motivations and information security policy compliance: The role of autonomy and efficacy", Journal of Information Privacy & Security, Vol. 9 No. 4, pp. 52–79.

Williams, B., Onsman, A. and Brown, T., (2010), "Exploratory factor analysis: A five-step guide for novices", Journal of Emergency Primary Health Care, Vol. 8 No. 3, pp. 1–13.

Yong, A. G. and Pearce, S., (2013), "A beginner' s guide to factor analysis: Focusing on exploratory factor analysis", Tutorials in Quantitative Methods for Psychology, Vol. 9 No. 2, pp. 79–94.

Appendix

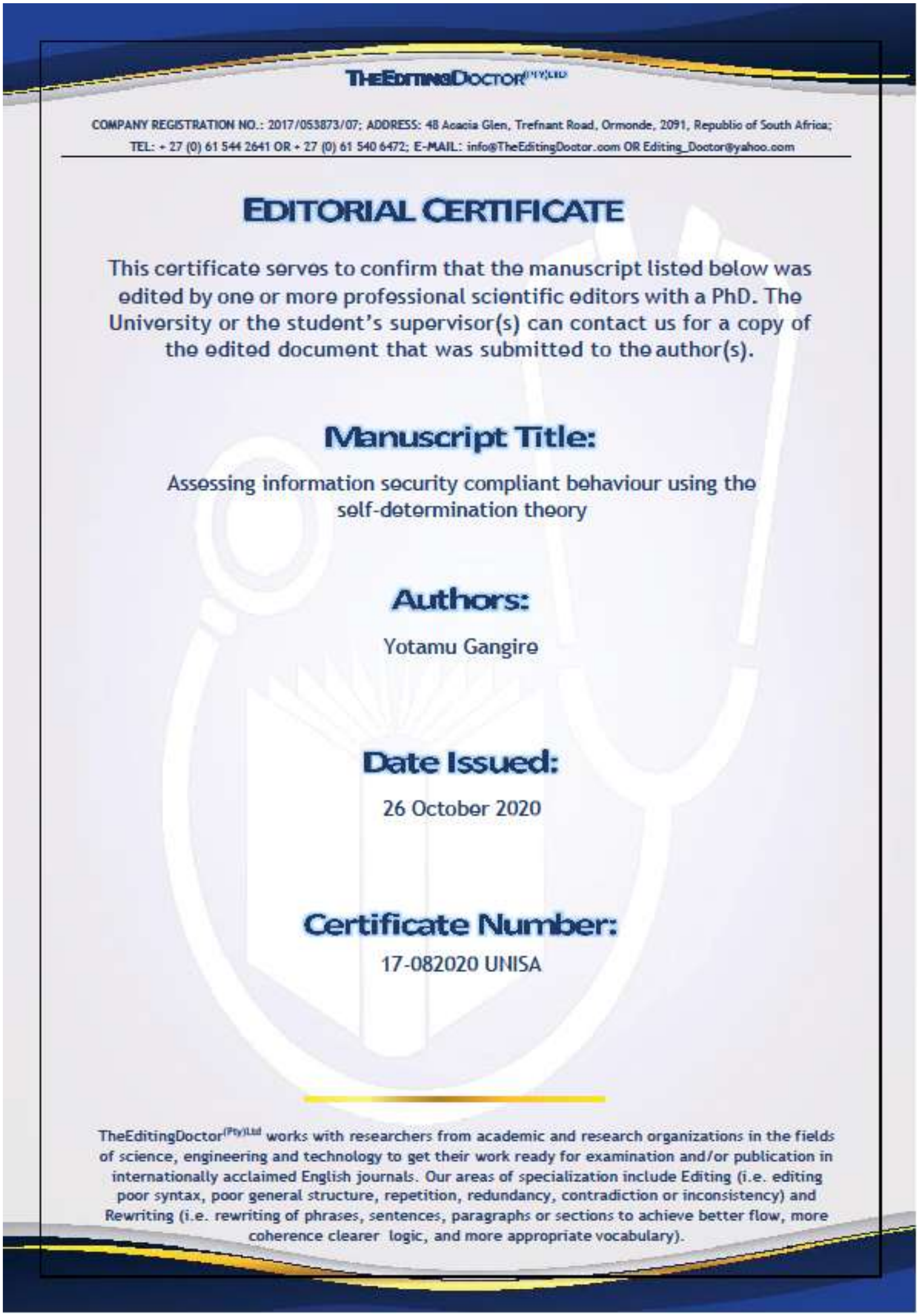
Focus Area	Competence	Relatedness	Autonomy
Password management	1. I have the necessary skills to use different passwords for social media and work accounts.	My colleagues support me to use different passwords for social media and work accounts.	I choose to use different passwords for social media and work accounts.
	2. I have the necessary skills to never share my work passwords with colleagues.	My colleagues support me never to share my work passwords with colleagues.	I choose never to share my work passwords with my colleagues.
	3. I have the necessary skills to use a combination of letters, numbers and symbols in work passwords.	My colleagues support me to use a combination of letters, numbers and symbols in work passwords.	I choose to use a combination of letters, numbers and symbols in work passwords.
Email usage	4. I have the necessary skills to click only on links in emails from people I know.	My colleagues support me to click only on links in emails from people I know.	I choose to click only on links in emails from people I know.
	5. I have the necessary skills to avoid clicking on links in emails from people I do not know.	My colleagues support me to avoid clicking on links in emails from people I do not know.	I choose to avoid clicking on links in emails from people I do not know.
	6. I have the necessary skills to identify when it is risky to open attachments in emails from people I do not know.	My colleagues support me to identify when it is risky to open attachments in emails from people I do not know.	I choose to avoid opening attachments in emails from people I do not know.
Internet usage	7. I have the necessary skills to identify when it is risky to download files onto my work computer.	My colleagues support me to identify when it is risky to download files onto my work computer.	I choose not to download risky files onto my work computer.
	8. I have the necessary skills to avoid accessing websites that could be dubious (malicious).	My colleagues support me to avoid accessing websites that could be dubious (malicious).	I choose to avoid accessing websites that could be dubious (malicious).

Focus Area	Competence	Relatedness	Autonomy
	9. I have the necessary skills to assess the safety of a website before entering information online.	My colleagues support me to assess the safety of a website before entering information online.	I choose to assess the safety of a website before entering information online.
Social media usage	10. I have the necessary skills to review the privacy settings of my social media accounts.	My colleagues support me to review the privacy settings of my social media accounts.	I choose to review the privacy settings of my social media accounts.
	11. I have the necessary skills to consider the negative consequences before posting anything on social media.	My colleagues support me to consider the negative consequences before posting anything on social media.	I choose to consider the negative consequences before posting anything on social media.
	12. I have the necessary skills to avoid posting sensitive information about work on social media.	My colleagues support me to avoid posting sensitive information about work on social media.	I choose to avoid posting sensitive information about work on social media.
Mobile devices usage	13. I have the necessary skills to keep my device (e.g. laptop and smartphone) with me at all times when working in a public place.	My colleagues support me to keep my device (e.g. laptop and smartphone) with me at all times when working in a public place.	I choose to keep my device (e.g. laptop and smartphone) with me at all times when working in a public place.
	14. I have the necessary skills to avoid sending sensitive work files over a public Wi-Fi network.	My colleagues support me to avoid sending sensitive work files over a public Wi-Fi network	I choose to avoid sending sensitive work files over a public Wi-Fi network.
	15. I have the necessary skills to shield my computer screen from strangers when working on a sensitive document.	My colleagues support me to shield my computer screen from strangers when working on a sensitive document.	I choose to shield my computer screen from strangers when working on a sensitive document.
Information	16. I have the necessary skills to securely dispose of sensitive information.	My colleagues support me to securely dispose of	I choose to securely dispose of sensitive information.

Focus Area	Competence	Relatedness	Autonomy
ng		sensitive information.	
	17. I have the necessary skills to identify when it is risky to insert an external device (e.g. USB stick and phone) into a computer.	My colleagues support me to identify when it is risky to insert an external device (e.g. USB stick and phone) into a computer.	I choose to identify when it is risky to insert an external device (e.g. USB stick and phone) into a computer.
	18. I have the necessary skills to identify when it is risky to leave information on my desk.	My colleagues support me to remove information from my desk, which could be risky.	I choose not to leave information on my desk, which could be risky.
Incident reporting	19. I have the necessary skills to report any suspicious behaviour if I notice it.	My colleagues support me to report any suspicious behaviour if I notice it.	I choose to report any suspicious behaviour if I notice it.
	20. I have the necessary skills to notice poor information security behaviour by colleagues.	My colleagues support me to notice poor information security behaviour by colleagues.	I choose to notice poor information security behaviour by colleagues.
	21. I have the necessary skills to report any information security incidents if I notice them.	My colleagues support me to report any information security incidents if I notice them.	I choose to report any information security incidents if I notice them.
Privacy	22. I have the necessary skills to process student information in a lawful manner.	My colleagues support me to process student information in a lawful manner.	I choose to process student information in a lawful manner.
	23. I have the necessary skills to process student information only for the purpose for which it was collected.	My colleagues support me to process student information only for the purpose for which it was collected.	I choose to process student information only for the purpose for which it was collected.
	24. I have the necessary skills to adhere to the privacy policy of the university.	My colleagues support me to adhere to the privacy policy of the university.	I choose to adhere to the privacy policy of the university.

Focus Area	Competence	Relatedness	Autonomy
	25. I have the necessary skills to adhere to the information security policy of the university.	My colleagues support me to adhere to the information security policy of the university.	I choose to adhere to the information security policy of the university.

Appendix P: Editorial Certificate by language practitioner



THEEDITINGDOCTOR(PTY)LTD

COMPANY REGISTRATION NO.: 2017/053873/07; ADDRESS: 48 Acacia Glen, Trefnant Road, Ormonde, 2091, Republic of South Africa;
TEL: + 27 (0) 61 544 2641 OR + 27 (0) 61 540 6472; E-MAIL: info@TheEditingDoctor.com OR Editing_Doctor@yahoo.com

EDITORIAL CERTIFICATE

This certificate serves to confirm that the manuscript listed below was edited by one or more professional scientific editors with a PhD. The University or the student's supervisor(s) can contact us for a copy of the edited document that was submitted to the author(s).

Manuscript Title:

Assessing information security compliant behaviour using the self-determination theory

Authors:

Yotamu Gangire

Date Issued:

26 October 2020

Certificate Number:

17-082020 UNISA

TheEditingDoctor(Pty)Ltd works with researchers from academic and research organizations in the fields of science, engineering and technology to get their work ready for examination and/or publication in internationally acclaimed English journals. Our areas of specialization include Editing (i.e. editing poor syntax, poor general structure, repetition, redundancy, contradiction or inconsistency) and Rewriting (i.e. rewriting of phrases, sentences, paragraphs or sections to achieve better flow, more coherence clearer logic, and more appropriate vocabulary).