Investigating the Relationship between Learning Styles and Delivery Methods in Information Security Awareness Programs

A Dissertation Presented to the

Department of Information Systems

University of Cape Town

By

Blaise Ntwali

NTWBLA001

Supervised by: Dr Jacques Ophoff

February 2020

In partial fulfilment of the requirements for the Master of Commerce in Information Systems

Plagiarism Declaration

COMPULSORY DECLARATION:

1. This dissertation has been submitted to Turnitin and I confirm that my supervisor has seen my report and any concerns revealed by such have been resolved with my supervisor.
2. I certify that I have received Ethics approval from the Commerce Ethics Committee.
3. This work has not been previously submitted in whole, or in part, for the award of any degree in this or any other university. It is my own work. Each significant contribution to, and quotation in, this dissertation from the work, or works of other people has been attributed, and has been cited and referenced.

Student number	NTWBLA001
Student name	Blaise Ntwali
Signature of Student	BN
Date:	10 February 2020

Acknowledgement

Firstly, I would like to thank God for giving me the strength and wisdom to complete this master's dissertation.

I would also like to thank my supervisor, Dr Jacques Ophoff, for being extremely supportive, patient, and guiding me throughout the research processes and providing constructive feedback.

I am also grateful to Capitec Bank for supporting me with a bursary and giving me time to focus on this degree.

Finally, I wish to thank my family (Shadrack, Philomene, Robert, Lambert and Celine) and friends for their support and encouragement throughout my master's research.

Abstract

Information security threats are continually growing as new technologies emerge. Literature confirms that the human factor is an important issue, as cyber threats and exploitation of vulnerabilities continue to proliferate due to human error. There are significant risks associated with this, such as the organisation's reputational damage and associated costs, to name a few. Information Security Awareness (ISA) programs have proven to be one of the best methods to reduce human linked security vulnerabilities and misbehaviour, which also reduces risks. The purpose of this research is twofold. First, it is to identify and explain the value of aligning ISA programs with user-preferred learning styles and delivery methods. Second, to indicate how aligning ISA programs with preferred learning styles and delivery methods influences security posture.

Using the Knowledge, Attitude, and Behaviour (KAB) model as a theoretical lens, the study depicts how information security posture can be improved through the betterment of security knowledge, attitude, and behaviour. Additionally, the aligned learning styles and delivery methods' construct was added to the KAB model to investigate the research questions.

The Human Aspect of Information Systems Questionnaire (HAIS-Q) was used to measure ISA levels of organisational employees in South Africa. The chosen parts of these HAIS-Q focused on password management, email and internet use. The ISA scores are essential for this research as they indicate the current ISA levels. This result can be used to improve information security posture. The Visual, Aural, Read/Write, and Kinaesthetic (VARK) inventory model was used to better understand the provided and preferred learning styles. Additionally, ISA programs focused on text-based, video-based, and game-based delivery methods commonly used and applied in prior academic research.

Using a survey methodology, the study recruited 322 South African organisational employees to complete an online questionnaire. The questionnaire contained a subset of HAIS-Q, the VARK inventory model, delivery methods, and demographic questions.

Bivariate Pearson correlation tests in conjunction with the ISA scores indicated that user-preferred learning styles achieve greater ISA. The results also showed that video-based delivery methods are the most preferred but does not yield the highest ISA scores. The highest ISA scores are achieved from a mixture of delivery methods.

The study proposes user aligned learning styles and preferred delivery methods to positively influence the knowledge, attitude, and behaviour leading to improved cybersecurity resilience. As a result, this leads to self-reported and risk-averse behaviour, as end-users' self-efficacy has improved.

Table of Contents

List of Figures

List of Tables

1. Introduction

Technology is growing faster than ever and emerging at a fast pace, leading to high demand and dependency from various sectors that require it to survive and prosper by solving complex problems (Ven et al., 2017). Although technology creates a competitive advantage through efficiency and other means, it has also opened up a world of information security risks. According to the report by Accenture (The Cost of Cybercrime), the digital landscape continues to change and thrive. Additionally, cyber-attacks are also changing due to the following factors: evolving targets, evolving impact and evolving techniques (Accenture and Ponemon Institute, 2019).

An example of the risks organisations face is the case of City Power, Johannesburg's electricity utility, which was compromised by a ransomware attack that managed to encrypt databases, applications and networks (ITWeb, 2019). Ransomware is a type of malicious software with the intention of restricting access to a computer system or data until a ransom is paid to the threat actor (ITWeb, 2019). It is commonly spread through malicious email attachments and when the user clicks on a malicious link. As a result of this ransomware attack, customers could not purchase electricity and therefore were unable to run daily operations. According to the global cybersecurity company Kaspersky Lab, in the first quarter of 2019, malware attacks increased to 22% compared to the previous year's first quarter (Fin24, 2018). There were 13 842 attempted cyber-attacks per day in South Africa to explain this further, targeting critical infrastructures such as nuclear facilities, electricity and water treatment facilities (Fin24, 2018). The afore-mentioned risks are likely to be a result of poor security awareness or poor security controls. ISA programs are capable of reducing these risks. This enables end-users to understand security risks and how to behave and react in risky situations. Additionally, security control configurations according to best practice is key. According to best practice, security awareness and security control configurations play an important role in securing organisational environments (Scrimgeour & Ophoff, 2019).

Abawajy (2014) study indicated that single or multiple learning styles that match an end user's learning style are more effective. Also, a combination of various awareness delivery methods is preferred by end-users. As a result, matching user learning styles and preferred awareness delivery method yielded a greater ISA (Abawajy, 2014). Therefore, improving ISA knowledge, attitude towards security, and risk-averse behavioural intentions (Abawajy, 2014). Implementing the above-mentioned findings is a problem for organisations as it is costly and time-consuming.

This study focuses on three types of delivery methods, namely text-based, game-based and video-based. Also, the VARK model is employed to examine end-user learning styles. The VARK model focuses on visual, aural, read/write and kinaesthetic learning styles (Malcolm Pattinson, Butavicius, Ciccarello, & Liilie, 2018; Peyman et al., 2014). The VARK model attempts to accommodate these learning styles in ISA programs' delivery. It is believed that end users may have one of the four modalities or multiple modalities making a preference (Malcolm Pattinson et al., 2018). Lastly, the HAIS-Q instrument is used to measure the ISA by focusing on the following focus areas: password management, email use and internet use.

1.1 Background

According to the Global Information Security Survey conducted by EY (2017), it was found that the number of security breaches is increasing despite organizations implementation of information security mitigation techniques. It is said that the primary root cause of security breaches is a result of a lack of awareness of employees (2013 – 53%, 2014 – 57%, 2015 – 44%, 2016 – 55%) (Ernst and Young, 2017). Furthermore, in 2017 and 2018, it is reported that 6.4 billion fake emails were sent worldwide, which resulted in 1.9 billion data breaches that cost approximately 3.62 million dollars (Van Kessel, 2018). Afore-mentioned statistics depict continuous growth in data breaches, an indication that the current efforts to mitigate cyber threats are inefficient.

Researchers have confirmed that the majority of information security risks are due to human error or negligence. Moreover, humans have been identified to be the weakest link in the protection of Confidentiality, Integrity, and Availability (CIA) of information (Metalidou et al., 2014). As a result, this triggers internal or external threats (Stone, 2018). Internal threats are defined as threats from within the organisation, and external threats are threats from outside the organisation. Furthermore, it is emphasised that human error plays a significant role in information security breaches. Therefore end users are identified as the main source of comprise, being the number one target, and should therefore be the core focus in cyber defence by introducing end-user behaviour security controls and awareness (Amankwa, Loock, & Kritzinger, 2016; PWC, 2015; Stone, 2018).

Studies focusing on human factors and associated effects have improved over the years (Haeussinger & Kranz, 2017a; Metalidou et al., 2014; Safa et al., 2016). Previously studies focused on Computer Information Security (CIS) by utilising technological controls to mitigate human negligence towards security (Metalidou et al., 2014). This is problematic because human factors have a significant role in computer security. In an effort to address this problem, this research will address human factors, specifically behavioural intentions. Researchers have stressed that ISA is key to mitigating threats caused by human weakness (Metalidou et al., 2014; Scrimgeour & Ophoff, 2019).

The internet is becoming more dependent on the internet, making it easier for cyber-attacks (de Bruijn & Janssen, 2017). This is because the internet is a highly used medium for communication, entertainment, transportation, collaboration and information sharing, among other activities (Nadeau, 2017; South African Cyber Security Academic Alliance, 2015). Although the internet yields positive opportunities and enables efficiency to organisations and business owners, many internet users are not aware of the dangers and risks. This is why ISA programs are imperative. It helps end-users to understand and be able to identify malicious or dangerous activities on the internet.

South African Cyber Security Academic Alliance (SACSAA) explains that cyber security programs aim to protect internet users' sensitive information by protecting, detecting and responding to cyber threats (South African Cyber Security Academic Alliance, p.8, 2015). This is one of the forms of ISA programs currently being used to mitigate security risks and improve user behavioural intention in South Africa.

In the process of mitigating information security risks, the focus has predominantly been on information security technology tools such as having the right security systems in place and

technical control programs to prevent data breaches, as mentioned in several studies (Chmura, 2017; Gritzalis & Tejay, 2013; Montesdioca & Maçada, 2015). Furthermore, several authors argue that technical controls protection is insufficient to combat against information security threats and the associated risks (Stone, 2018 and McCormac et al., 2017). Technical tools are not scalable enough to protect and prevent risky and naive human actions or negligence (Stone, 2018). To date, there has been little work published on the human aspect of people performing security checks and protecting themselves from various attacks, specifically phishing attacks. Security controls should detect, prevent, and deter malicious activities such as phishing attacks (Alsharnouby, Alaca, & Chiasson, 2015).

Therefore, in the face of modern threats, it is advised that careful attention is directed to human behaviour (Stone, 2018). Awareness and training programs aim to change one's behavioural intentions and better understand information security (Chmura, 2017). When end users perform a control measure or report malicious incidents, it results from effective training and awareness. These actions can aid significantly in thwarting security risks. It is further recommended that technical controls (hardware and software) address human vulnerabilities should work in parallel (Sohrabi, Solms, Furnell, Elizabeth, & Africa, 2016). Managing each component in isolation is unlikely to yield the same result.

To address the issues mentioned above, this research aims to examine security awareness programs in South African organisations. Furthermore, the alignment of ISA programs' delivery methods and learning styles. As a result, this examination outcome should assist in developing strategies to improve information security posture and end-user behavioural intentions. The following section details the research problem statement.

1.2 Problem Statement

It has been found and proven that human error is the leading cause of data CIA violations. As a result, organisations continue to face unexpected costs and reputational damages, among other consequences. To mitigate this by providing an improved information security education, training, and awareness is more effective when aligned with the user's preferred learning styles and delivery methods (Pattinson et al., 2018). Other forms of enhancing ISA are Managerial Information Security Awareness (MISA) (Rotvold, 2008), management support, communication, and commitment (Tu & Yuan, 2014), user participation (Spears & Barki, 2010) and information security policy provision (ISPP) (Alshboul & Steff, 2016).

This leads to the research problem statement below:

ISA programs do not accommodate user-preferred or matching learning styles and delivery methods. As a result, users find it difficult to understand and internalise provided ISA programs. This lack of understanding reduces the confidence to act with a risk-averse approach at a workplace or home (Haeussinger & Kranz, 2017).

Also, it is believed that ISA programs are often too technical. Therefore, only technically inclined individuals can understand it, whereas the less technically inclined struggle to understand and apply provided ISA programs. This does not accommodate a diverse, preferred user learning styles and delivery methods.

Increasing training frequency is time-consuming and costly. Therefore, it is recommended to focus on delivering ISA programs that match end-user learning preferences (Malcolm Pattinson

et al., 2018). Suppose organisations do not consider the alignment of delivery methods and the individual learning styles. In that case, the results may not be effective in improving security knowledge, attitude, behaviour, and thus improving an organisation's security posture.

1.3 Research Questions

This section consists of the research questions and objectives. Research questions and objectives are essential to the research as they serve as a guide to identifying the problems and addressing them through set goals. The research questions and objectives were used to conduct the study, specifically addressing information security education, training, and awareness, to achieve risk-averse behavioural intentions.

The main research question:

What effect does ISA programs' alignment with users' preferred learning styles and delivery methods have on security awareness?

Sub-questions:

- Which properties of preferred learning styles influence information security awareness?
- Which properties of information security delivery methods influence information security awareness?

The purpose of this research is twofold. Firstly, to identify and explain the value of employing aligned learning styles with ISA programs. Secondly, to explore how aligned ISA programs with preferred learning styles and delivery methods influences security posture. The afore-mentioned research purpose aims to improve information security posture through better knowledge, attitude and risk-averse behavioural intention towards security (Parsons et al., 2017; Malcolm Pattinson, Butavicius, Ciccarello, & Liilie, 2018).

1.4 Significance of the research

This study can assist any industry that utilises electronic devices and systems to increase information security and cyber resilience. This can be achieved by providing ISA programs aligned with employees' preferences - delivery methods and learning styles. This alignment should improve information security awareness and security posture (Sohrabi Safa, Von Solms, & Furnell, 2016). As a result, company assets are protected from threats and employees' risk-averse behavioural intentions (Pattinson et al., 2016).

This helps the industry, management and stakeholders by saving time and money, also having a working strategy that can be used whenever security issues arise (Haeussinger & Kranz, 2017). Additionally, a secured organisation attracts more clients, investors, and employees feel safer.

Therefore, management and security practitioners must understand the primary source of information security threats – human error. With a thorough understanding of human error, strategies to combat and educate end-users about information security can be developed and be assigned to the necessary persons.

This study validates previous studies in a new context, South Africa. Previous studies looked at organisational and banking employees in Australia and made similar findings. This study focuses on South African employees from different industries.

Identifying and understanding the properties that influence information security posture is crucial for IT professionals, management and practitioners. This process ensures that effective and efficient programs are achieved and are implemented after that (Haeussinger & Kranz, 2017). Also, the study by (Haeussinger & Kranz, 2017) suggests that identifying and understanding antecedents of employees' ISA are critical to stakeholders who are interested in improving ISA effectiveness, and in the end, lowers threats that affect information security systems (ISS) in the organisation.

This research will assist organisations in designing better ISA programs and delivery methods that match employee learning styles. The findings from this research seek to assist security practitioners and IT management in designing and implementing effective security controls: ISA, policies and frameworks, among others.

The research findings can assist in identifying gaps and where security is most lacking. This information is essential to IT practitioners and management because it allows them to plan more strategically and address the actual problems.

1.5 Chapter Layout

The following chapters of the dissertation are presented in the order below:

Chapter 2 compromises the literature review on information and cybersecurity, information security threats, information security risk controls and improved information security awareness. It also shows the gaps identified in the literature review and the conceptual research model rooted from the knowledge, attitude and behaviour model. The KAB model illustrates the relationship between the constructs and the proposed outcome. This section also outlines the propositions formulated and tested in the study.

Chapter 3 provides details on the research design by discussing the philosophical stances adopted, the research methodology. This compromise of research paradigm for the study, the research purpose, research approach, research strategy, the data collection and analysis method utilised, and the ethics and confidentiality issues considered for this study.

Chapter 4 consists of a presentation of the results and the findings of the data analysis implemented and the discussions based on these findings and the results from the propositions testing.

Chapter 5 consists of the conclusion to the dissertation. The conclusion includes the theoretical and practical implications, recommendations and lastly, suggestions for further research.

2. Literature Review

The literature review sections detail the research model used in the study, ISA delivery methods and learning styles, properties for improving information security awareness and posture. First, the following section explains the difference between cyber security and information security.

2.1 Information and Cyber Security

Information security and cyber security are often used interchangeably with an assumption that they have exactly the same meaning. However, both terms are different and should be used with careful consideration. Information security refers to the preservation of CIA for various forms of information, such as written, printed, digital, transmitted and internet-based (von Solms & von Solms, 2018). Cyber security is understood to be a subset of information security because it focuses on the protection of CIA but more specifically CIA of digital information assets against threats and attacks that use or are connected to the internet (von Solms & von Solms, 2018).

Historically information security is seen to be a technical problem and as a result, technical solutions are sought after to resolve technical problems (von Solms & von Solms, 2018). As technology evolves and new forms of technologies emerge, the solutions that are used to secure the technology and the information they hold have to evolve (Wood, 2004).

2.2 Information Security Threats

Information security threats pose risks which lead to danger. An example: unexploited vulnerability of a system, user action or threat can be a risk and therefore cause danger to an individual or an organisation. Arachchilage and Love (2014) listed the following security threats: viruses, malware, spam, spyware, distributed denial of service (also known as DDoS attacks), social engineering and phishing (Arachchilage & Love, 2014).

Arachchilage and Love (2014) defined viruses as computer programs with the intention to disturb the normal operational behaviour of a computer. Malware is defined as malicious software that is installed in most cases on an end-user machine without the user knowing. Spam is defined as the types of emails which an end-user is not previously associated with, furthermore these emails are unauthorised by the user. All these threats have similar objectives, to cause danger or intrude normal systems' operation.

According to the World Economic Forum (2018), cyber-crime is one of the top three global risks for the year 2018 (Gholami & Hamzehloei, 2013). Furthermore, the Information Systems Audit and Control (ISACA) asserted that cyber-crime and cyber-attacks are going to continue increasing and potentially not slow down as time progresses (Cybersecurity Nexus, 2016). The same report alluded that whilst cybercriminals, threat actors or hackers were the main cause of security incidents, following closely to threat actors were incidents caused by unintentional behaviour by unknowing employees. This is a clear indication that while external threats are of great concern, we also need to focus on insider threats.

The following dangers could be associated with information security threats: economic cost, reputational damage and legal consequences, among others are associated with information security risks. The loss of data's CIA leads to such above-mentioned dangers (Pattinson et al., 2018). In order to manage these dangers or risks, the following section discusses human behaviour oriented risk controls.

2.3 Information Security Risk Controls

This section discusses the security controls and security awareness programs set to mitigate risks.

2.3.1 Information Security Controls

Pattinson et al. (2018) identifies policies, procedures, software and hardware as information security controls. Organisations put in place afore-mentioned controls to prevent, deter, detect and enable the recovery of CIA. When vulnerabilities are identified by set security controls, a highly effective form of remediation is patching.

From an end-user perspective, security controls are set policies, procedures, rules and guidelines. The end-user is advised to adhere to afore-mentioned controls to avoid data breaches and virus outbreaks. However, end-users do not understand set security controls and also do not know how to react in the case of a data breach or virus outbreak. Furthermore, in the study by (Stone, 2018), it was found that trainers do not often understand materials, lack skills to educate and are not able to simplify technical knowledge for end-users to understand.

In order to ensure that end-users understand information security training provided, IT practitioners should ensure that training programs are tailored for specific roles (Stone, 2018). Improved knowledge allows the end-user to understand how and why various security controls are performed. This allows an end-user to understand associated damages and consequences, and to behave accordingly to prevent a data breach or a virus outbreak.

2.3.2 Information Security Awareness (ISA) Programs

ISA programs aim to address and implement information security techniques and training for an organisation. Additionally, it targets a variety of users in an organisation with specific programs relevant to their jobs and in line with their technical expertise. The objective of ISA programs is to ensure that an in-depth knowledge of security is used in design, implementation and operation to protect organisations and systems (Whitman & Mattord, 2014). This is achieved by educating, training and increasing security awareness among computer users emphasising the need to protect system resources.

It has been indicated that ISA programs are the most essential "institutional countermeasures" to reduce human-related security negligence and misbehaviour (D'Arcy, Hovav, & Galletta, 2009; Siponen, Adam Mahmood, & Pahnila, 2014). In an attempt to deliver security programs that match end-users' learning styles and preferred delivery methods, ISA programs are a key consideration. The alignment of ISA programs with user-preferred learning styles and delivery methods is believed to be effective by several researchers. Also, there are organisations that have employed ISA programs and as a result, noticed significant changes in their security posture (Haeussinger & Kranz, 2017).

Haeussinger et al. (2017) asserts that an ISA programs' aim and objective is to increase users' knowledge and awareness of "potential security risks, policies and security responsibilities and by developing the general understanding and skills necessary to perform any required security procedure" (D'Arcy et al., 2009). As a result, this will ultimately increase the level of an organisation's ISS and therefore improve organisational security posture.

Furthermore, it has been found that the most used form of ISA programs are: ISS workshops, seminars, online and computer-based learning tutorials, periodic newsletters, emails, and

presentations cues: posters, flyers and other awareness material (Haeussinger & Kranz, 2017). It is important that the message is carried through various forms of ISA programs in an organisation. Ensuring that the message is clear and consistent, as a result, this will increase users' ISA (Dhillon, Almusharraf, & Samonas, 2015). In addition, there is a wide variety of ISA delivery methods. However, this research will focus on three common ISA delivery methods, which are text-based, video-based and game-based.

2.3.3 Delivery Methods

Improving ISA by utilising a range of information security training and delivery methods is a key success factor given the alignment of training and delivery methods such that it is suitable for an individual or a group of end-users. Therefore, organisations should aim to utilise preferred delivery methods that are aligned to end-users' learning styles as the results and outcomes clearly indicate a significant improvement in security posture. In the study by Abawajy (2014), the three ISA delivery methods were identified to be commonly used. Therefore, it will be fitting for this study to utilise the very same delivery methods, to align it with the afore-mentioned learning styles.

Traditional methods, also known as text-based (1) include both paper and electronic resources: information leaflets, posters, newsletters, and educational presentations, which provide information on password, email, anti-virus protection management, as well as general rules regarding information security in organisations (Abawajy, 2014). However, the issue and concern of this method is the omission of information on the posters. The advantage of a traditional method is cost-effective, the implementation process is not expensive in comparison to the other delivery methods (Abawajy, 2014).

The method of game-based (2) includes games which are aimed at stimulating one's information knowledge through fun and training. This method is highly interactive and has a high impact on users' attitude, however not the best method to provide detailed information regarding information security (Cone, Irvine, Thompson, & Nguyen, 2007). Furthermore, it is believed that because this method is highly interactive, it is more effective than the traditional method. The limitations of this method are costly and lacks interaction between the trainer and students (Chmura, 2017).

The video-based method (3) includes animations and multimedia. This method is deemed to be the most effective in providing information regarding safety (Abawajy, 2014). However, the limitation of this method is the lack of guarantee that the video content will be understood (Chmura, 2017).

The objective is to align user-preferred ISA delivery methods, aiming to improve information security knowledge, and better attitude towards security and risk-averse behavioural intentions. In addition, it is argued that a mixture of delivery methods is better than a single security awareness and training delivery method (Abawajy, 2014). This research will address such discussions and synthesise the arguments around ISA delivery methods.

2.4 Information Security Awareness Programs

The following subsections define ISA, by examining and providing methods of improving ISA. ISA is defined as the extent that a user comprehends safe information security behaviour which is highlighted in the organisation's policy, procedures, rules and guidelines (Parsons et al., 2017). Also defined by Pattinson et al. (2016) as a combination of knowledge of an

organisation's information security policies and procedures, and users' attitude towards having to adhere to them. An organisation's information security policies and procedures generally contain recommendations on how employees are to behave in the organisation's space when dealing with password management, internet security, and incident management and reporting. As a result, these recommendations will provide a guideline when a user has to choose a safe password, deal with a malicious website, and report bad security behaviour of colleagues.

The definition of ISA includes the level of user understanding of information security policies and procedures and the importance and implications of abiding to set policies and procedures. Also, how a user behaves in accordance with the organisation's information security policies and procedures (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

KAB model introduced next is closely aligned with the above-mentioned definition of ISA. The model asserts that an employee's knowledge increases or enhances through ISA programs. As a result, the attitude towards security improves, resulting in improved behavioural intentions (Parsons et al., 2014).

2.4.1 Research Model

This section introduces and explains the research model employed for this study. The KAB model will guide this study.

The KAB model constructs include knowledge, attitude, and behaviour. These constructs will be utilised throughout the study. Furthermore, the constructs are linked to security education, training and awareness. In addition, the KAB model incorporates ISA delivery methods and learning styles as a single construct.

The KAB model has been used in several studies examining the impact of knowledge, attitude, and behaviour. Moreover, it was developed for the following fields: health, criminology and environmental psychology (Kruger & Kearney, 2006), with the aim to better health, criminology, and environmental psychology through improved knowledge, attitude and behaviour.

The KAB model has been used in information security and information security awareness previously by Thomson and Solms in 1988. As time progressed, it was extended by Kruger and Kearney in 2006, but there was some criticism towards the KAB model. These criticisms rooted mostly from the departments such as health and climate change (Baranowski, Cullen, Nicklas, Thompson, & Baranowski, 2003; Kollmuss & Agyeman, 2002). However, recent research has strongly indicated a link between knowledge, attitude and behaviour that supports the KAB model (Parsons et al., 2017; M. Pattinson et al., 2016; M. R. Pattinson, Butavicius, Parsons, McCormac, & Jerram, 2015).

In the study by Parsons et al. (2014), the KAB model indicated the relationship between the knowledge of understanding policy and procedures and the impact this relationship has on the good security posture. An example of this impact is a good defense against cyber-attacks, changed behavioural intentions, risk-averse attitude and self-reported behaviour as a result of improved user efficacy. Previous research has indicated a strong relationship between knowledge, attitude and behaviour (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014), this relationship strongly indicated that "knowledge and attitude have been shown to predict self-reported behaviour" (M. Pattinson et al., 2016). As a result, this will potentially aid

in reducing risk-inclined computer-based behaviour and lead to more secure information security assets (Stanton, Stam, Mastrangelo, & Jolton, 2005; Trček, Trobec, Pavešić, & Tasič, 2007) as users will be risk-averse through changed behaviour.

As a result of improved knowledge of policy and procedures, users' attitude towards information security policy and procedures, and security posture was carefully examined and observed. It was noted that acquired and internalised knowledge and attitude towards policy and procedures lead to self-reported behaviour (Parsons et al., 2014). The afore-mentioned KAB model processes are depicted in Figure 1.

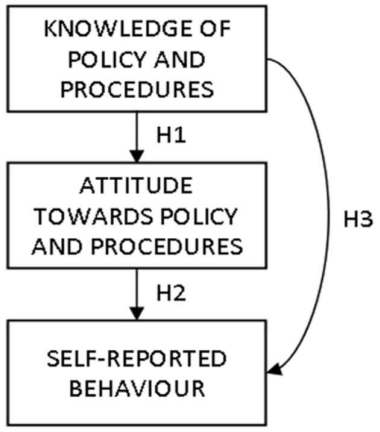

Figure 1. KAB model (Parsons et al., 2014)

Parsons et al. (2014) study indicated that knowledge of policy and procedures had a significant positive impact on attitude towards policy and procedures than self-reported behaviour. This is an indication of increased knowledge and improved behaviour intentions – self-reported behaviour is associated with risk-averse behaviour as a result of self-efficacy (Parsons et al., 2014). The above-mentioned findings indicate that the KAB model is suitable for this study as it has been previously used to investigate and assist in improving user behavioural intentions.

This study employs the KAB model because this model is well aligned with the research aims and objectives. Additionally, it has been previously used within information security research (Malcolm Pattinson et al., 2018).

2.4.2 Learning Styles

In this section, the focus is on user learning styles. The research explains what it is and why learning styles are required for user education, training and awareness. In addition, the study explores different types of learning styles and how they are aligned with the preferred delivery methods.

A learning style is defined as the "characteristic strengths and preferences in the ways they take in and process information" (Felder, p.1, 1996). Chmura (2017) listed the below-learning style types that are part of the VARK model.

- Visual
- Aural
- Read/Write
- Kinaesthetic

Organisations deliver information security training and awareness to users in various forms. Such forms are through videos, interactive modules, tests, infographics, posters, and podcasts among others (Chmura, 2017). It is believed that each of these forms has the potential of conflicting or corresponding with a user's learning preference. It has been found that a student prefers a learning style that is predominant and that overrules other formats. Therefore, these learning styles can assist in ensuring that users receive ISA programs that hopefully match their learning styles.

In addition, research indicates that learning styles can be measured through the use of individual learning preferences (Leite et al, 2010). As a result of different learning preferences for individuals, one can deduce that information security training can be more effective when an individual learning style is consistent with their learning style (Pattinson et al, 2018). In other words, an individual will find learning valuable when he or she is taught in a manner that matches their learning preference (Pattinson et al, 2018).

Pattinson et al. (2018) explore various models and assessment tools which have been created for learning styles. Some of the models and assessment tools are the Index of Learning Styles Questionnaire, the Kolb Learning Styles Inventory, and the VARK Learning Style Inventory. These models and assessment tools have been used in several kinds of research and were found to be useful. However, the VARK Learning Style model has been employed in this study because it has been widely used in research – in comparison to others. In addition, the VARK learning style inventory is said to be brief, freely available, easy to administer and has a clear practical implication (Pattinson et al, 2018). The VARK model is quite simple, therefore easily adapted and scaled to suit and guide set research objectives. This is why this research will utilise the model in the context of user learning styles.

2.4.3 Properties for Improving Information Security Awareness

In order to improve ISA, it should be centered on an organisation's users, including users in the planning and execution processes of ISA. Research findings argue that the frequency of information security training does not directly indicate the level of ISA. On the other hand, researchers claim that a better indication is based on the level on which the training received matches with an individual's learning preferences. This approach has indicated a positive relationship with ISA (Malcolm Pattinson et al., 2018).

It is imperative that users' ISA is identified. Identifying employees' ISA allows information security management to develop more effective ISA programs where ISA is found to be weak or requires some improvements (Pattinson et al. 2016). Identifying and knowing employees' ISA can potentially "reduce the amount of risk-inclined computer-based behaviour and therefore improve the security of the information assets of the organisation" (Stanton et al., 2005; Trček et al., 2007).

The effectiveness of matching learning styles and user-preferred delivery methods are determined by the ISA score, this is calculated using the HAIS-Q (Parsons et al., 2017). It indicates how well (risk-averse) a user behaves whilst using an organisation's digital device (McCormac et al., 2017). This measure can be utilised to measure the level of ISA. Therefore, assist in identifying ISA gaps and address them accordingly.

In addition to the above-mentioned, HAIS-Q is employed in this study to measure and calculate an end user's ISA by focusing on password management, email use, and internet use (Parsons

et al., 2017). HAIS-Q questions pertaining to the aforementioned focus areas are divided into knowledge, attitude and behaviour.

In Figure 2, the KAB model is depicted with an additional construct: learning styles and delivery methods. This construct influences the relationship between knowledge, attitude and behaviour. Research propositions below shows that matching learning styles (visual, aural, read and write, and kinaesthetic) and preferred delivery method (text-based, video-based, and game-based) positively affect security awareness and posture through the betterment of knowledge, attitude and behaviour.

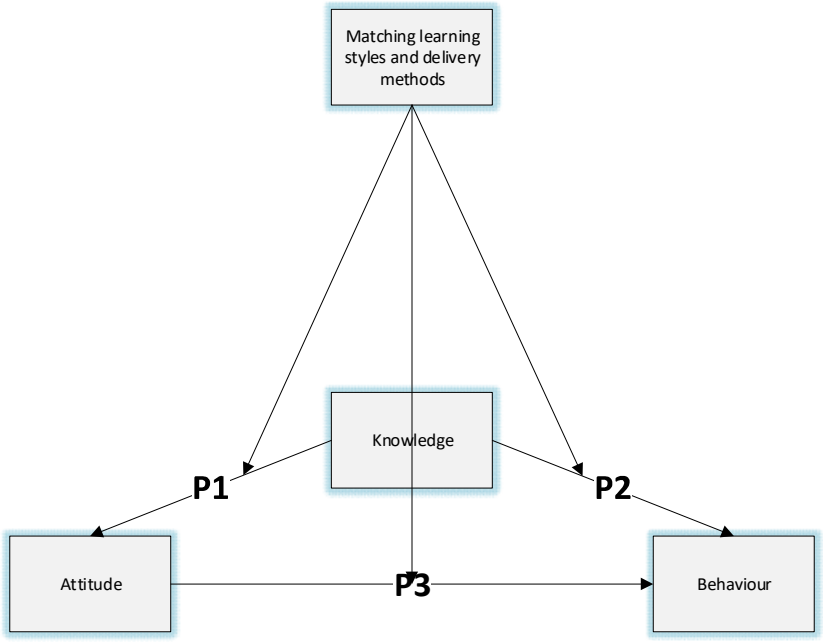

Figure 2. Research KAB model: ISA programs aligned with preferred learning styles and delivery methods

Figure 2, depicts proposed relationships between aligned learning styles and delivery methods and knowledge, attitude and behaviour. Firstly, it proposes that aligning ISA programs with preferred learning styles is associated with better knowledge and attitude towards security. Secondly, it indicates that aligning ISA programs with preferred learning style is associated with better knowledge and risk-averse behaviour towards security. Thirdly, it indicates that aligning ISA programs with preferred learning style is associated with a better attitude and risk-averse behaviour towards security.

It is apparent that ISA and the KAB model are closely associated through knowledge, attitude, and behaviour. Moreover, the scenarios below indicate how the KAB model constructs can be utilised to gain user risk-averse behavioural intentions.

- What an end-user 'knows' about behaving in a safe manner: knowledge
- How an end-user 'feels' about behaving in a safe manner: attitude
- What an end-user actually 'does' when using a digital device: behaviour

The above scenarios is an indication of how well the user behaves when making use of his or her digital device given an improved ISA – improved knowledge. Ultimately, effective ISA

leads to improved individual knowledge, attitude and risk-averse behaviour whilst using the organisation's digital device (Pattinson et al., 2018).

The first research proposition is centered on knowledge. What and how improved knowledge can contribute to attitude towards information security and behavioural intentions.

Knowledge is acquired through information security education, training and awareness. In order for information security knowledge to be exercised, it needs to be accessible, easy to understand, incorporated into organisational roles or departmental focus, and needs to be audited and continuously improved. Most importantly, the delivery and the learning style should match that of a user.

P_1: Aligning ISA programs to match preferred learning styles and delivery methods is associated with a better impact of knowledge on attitude.

P_2: Aligning ISA programs to match preferred learning styles and delivery methods is associated with a better impact of knowledge on end users' behaviour.

P_3: Aligning ISA programs to match preferred learning styles and delivery methods is associated with a better impact of attitude on end users' behaviour.

2.5 Summary

ISA programs are aimed at improving an individual or a group's knowledge, attitude and risk-averse online behaviour. Over time, it has been found that ISA programs are rolled out to be used and exercised from small businesses to larger organisations, however, set objectives are far from being reached as the number of data breaches and threats continue to rise.

In most recent studies, it is said that generic and repetitive ISA programs do not influence improved knowledge and user attitude towards information security. Therefore, it is evident that the knowledge of policy, procedures and security controls are less effective through generic and repetitive programs. The study advocates for non-repetitive ISA programs and further recommends ISA programs which are relevant and suitable for an individual and groups of end-users. Previous research studies indicate that such programs and strategies yield risk-averse behavioural attention. As a result, it positively influences security awareness.

The research employs the KAB model to serve as a guide and a lens throughout the study. The KAB model is aligned to the development of proposed research questions, objectives and propositions.

In addition to the above-mentioned, the study focuses on the properties which are likely to enhance ISA programs. These are matching learning styles and preferred delivery methods. The learning styles focus on visual, aural, read, write and kinaesthetic. These learning styles are adapted from the VARK inventory model that is widely used in previous research. On the other hand, the delivery methods focus on traditional, also known as text-based, video and gamification delivery methods. These are the common delivery methods identified in recent studies (Abawajy, 2014).

3. Research Design

3.1 Introduction

In research, the research design is defined as the overall structure of the research project. Furthermore, the research design focuses on the type of study planned by the researcher and the expected results from the research (Tobi et al., 2017 and PEDIAA, 2017). Whereas, research methodology is defined as the procedures, processes and tools which are used to collect and analyse data. In addition, the research methodology focuses on the type of methods which are suitable to collect and analyse the gathered data (PEDIAA, 2017).

The following sections consist of research purpose, approach, philosophy, method, strategy, timeframe, instrument, sample population, data collection, validity, reliability, and lastly data analysis.

The objective of the research design and methodology was to provide details of how each section was conducted and also to highlight well defined, functional and practical processes (Saunders, Lewis, & Thornhill, 2016). Each section is motivated with reasons for choice, relevance and backed up by literature from previous studies.

3.2 Research Philosophy

In research, it is important to state and clarify philosophical assumptions employed. These assumptions are imperative as they represent implications for the entire research (Holden & Lynch, 2006). Philosophical assumptions consist of the following sections: ontology, epistemology, and methodology.

Ontology answers questions relating to the nature of reality and from this reality, what is observed and unobserved (Saunders et al., 2016). Epistemology is concerned with how reality is observed – given it is observable. In addition, it illustrates the relationship between the viewer and the observed reality (Guba and Lincoln, 1994; Gelo, 2012). Epistemology answers the questions relating to the nature of knowledge – what is the nature of knowledge (Saunders et al., 2016). Lastly, the methodology is concerned with the tools, techniques, and procedures utilised to obtain and analyse gathered data. Furthermore, the researcher attempts to investigate and discover reality through methodology processes (Guba and Lincoln, 1994; Gelo, 2012).

3.2.1 Ontological Stance – Objectivism

There are two types of ontological stances, namely: objectivism and subjectivism (Saunders et al., 2016). The ontological stance employed in this study is objectivism. Objectivism is the reality that exists without interference to human or social actors (Saunders et al., 2009; Hatch, 2012).

Researchers who have employed this ontological stance "objectify phenomena and refer to them as objects" (Lusinga & Kyobe, 2015). With this belief, objects exist without our knowledge. Therefore, the independent technique can be used to measure and confirm – techniques which do not require a researcher's intervention or interaction but rather acted upon independently (Hatch, 2012). Furthermore, it is stated that these observations are "determined and developed by theories, whereby theories are tested against observations of the real world" (Hatch, 2012).

Ontology is concerned with the nature of reality (Wahyuni, 2012). The nature of the reality of which information security knowledge is attained (Wahyuni, 2012). Due to the nature of this study, it is acknowledged that knowledge is available and can be acquired and consumed. Furthermore, it can be attained from a diverse range of people; for the sake of this study – employed South Africans are able to internalise, consume, interact, and make use of the knowledge attained from various ISA programs.

More specifically to this study, the knowledge that is shared among people regarding information security is real, independent and external to the researcher (Wahyuni, 2012). Therefore, the ontological stance for this research is objectivism. The researcher conducted the research objectively; without any shared meaning amongst research participants.

3.2.2 Epistemology Stance – Positivism

There are three types of epistemology that one can employ whilst conducting research. These are interpretive, positivist and critical realist stances (Saunders et al., 2016).

Positivist epistemology assumes that the truth can be discovered through scientific methods (Hatch, 2012). Therefore, since knowledge is of key interest, it is acceptable if it is generated through the process of research hypotheses or propositions with respect to the research theory. The knowledge is further tested in order to accept or reject the findings and data analysis that helps to compare the implication of the research theory to the external reality (Orlikowski & Baroudi, 1991).

Epistemology is concerned with what the acceptable knowledge is in this field of study – information security (Saunders et al., 2016). This research's philosophical stance is of scientific nature as it is preferred to collect the data about the observed reality and search for a causal relationship from the collected data in order to make the generalisation about the target population (Saunders et al., 2016). Furthermore, the employed research theory is approached deductively, makes use of a large sample, uses measurement, is highly structured and employs a quantitative method of analysis (Saunders et al., 2016). As a result, the collected data was analysed using statistical tests, tools to draw inferences and make conclusions. The epistemology stance of this research is therefore positivism.

3.2.3 Methodology - Quantitative

The research method employed is quantitative. It is believed that a quantitative research method is generally associated with a positivism stance as it consists of scientific methods such as highly structured data collection techniques through the use of surveys (Saunders et al., 2016). Such processes aid in uncovering the truth about reality.

The research approach is deductive as the collected data is utilised to test the theory. The key characteristics of quantitative research methodology include examining relationships between variables from the KAB model. These research models' variables are measured numerically and further analysed using a wide range of statistical techniques.

There are controls in place to ensure data is reliable and valid. In addition, it uses probability sampling techniques to ensure there is an unbiased generalisation and lastly, the researcher is independent of the study and does not engage with research participants (Saunders et al., 2016).

3.2.4 Choice of Philosophical Stance Summary

This study adopted the positivist philosophical stance due to the nature of the study. Orlikowski and Baroudi (1991) believe that the nature of this world can be measured and understood objectively. It is understood that the situation explored in this study exists in an objective world view. The researcher's role is to discover the objective of the physical and social reality of information security offered through ISA programs. In order to accomplish this, the researcher created accurate measures that recognised and measured dimensions of interest in information security. Therefore, understanding information security is a matter of modelling and measuring information security through the development of a set of constructs and instruments to capture the essence of information security education, training and awareness.

The researcher is said to play a passive role in the research and does not intervene with the phenomenon itself (Saunders, 2016). By using quantitative methods through administering the online survey, the researcher was able to maintain a passive role in the research of information security education, training and awareness.

3.3 Research Approach

There are two types of research approaches that may be used in research: deductive and inductive.

A deductive research approach involves the development of a proposed theory, where the theory is subjected to testing by making use of the proposed research hypotheses (Saunders et al., 2016). The research theory is developed and tested through the following steps: a theory is developed, hypotheses are formulated, data is collected and analysed (Saunders et al., 2016). Once data has been collected from the questionnaires and analysed, the researcher decided to accept or reject the proposed hypotheses with the help of statistical tests.

In a deductive research approach, there are five stages (Hatch, 2012) as indicated below.

1) Stating the research hypotheses from theory – developing research hypotheses with respect to the theory and relationships among variables.
2) Terms which are measurable to show relationships among variables and can be tested
3) Tested to indicate whether the results:
4) Confirm or show there is a need to modify the proposed theory
5) Based on the findings, the theory may be altered

The above-mentioned stages confirm that the deductive approach is the best suited for this type of study. This is because the five stages can be applied and followed in order to meet the set research objectives. Furthermore, the research approach is aligned with the afore-mentioned stances.

3.4 Research Purpose

There are four research purpose types: explanatory, descriptive, exploratory, and improving (Runeson, 2014). This research purpose is explanatory. Survey research that is explanatory "aims to familiarise with a phenomenon and to test preliminary concepts about it" (Pinsonneault & Kraemer, 1993). In addition, it aims to discover what is happening in the field of interest, seeks to find new insights and assess the phenomena (Saunders & Lewis, 2012). Furthermore, the objective is to study the problem or situation at hand in order to explain the relationships among the variables pertaining to the study.

The current research has an explanatory nature because it seeks to establish causal relationships between variables: knowledge, attitude and behaviour. The relationships among these variables are able to determine, change and improve information security posture. Research with an explanatory purpose consists of questions that start with or contain "why" and "how" as it seeks explanatory answers (Saunders et al., 2016).

The proposed research seeks to improve security awareness and posture, as a result of improved knowledge, attitude and behaviour towards information security risks through the application of user-preferred delivery methods and learning styles. Additionally, the study seeks to better user behaviour intentions, and risk-averse behaviour. This is achievable through user-preferred delivery methods and learning styles (Abawajy, 2014; Malcolm Pattinson et al., 2018).

The approach to theory is deductive and the approach involves the identification of a proposed theory. The theory is subjected to testing using the proposed research hypotheses, research questions and objectives (Saunders et al., 2016).

3.5 Research Strategy

This section explains the strategy adopted in the study. It is said that some research may belong to either the deductive or inductive approach, however, any strategies may be used for any research purpose (Saunders et al., 2016). Some of the research strategies identified in research are: the experiment, survey, case study, action research, design and creation, ethnography, and archival research. It is said that the chosen research strategy is dependent on the research questions and objectives. In addition, " the extent of existing knowledge" and the philosophical assumptions used as a lens for the study (Saunders et al., 2016).

The research strategy adopted for this study is a survey. This is partly because of the adopted philosophical assumptions and adopted research methods. In addition, positivists generally use "large-scale sample surveys" as a fitting research strategy (Mccusker & Gunaydin, 2015). This strategy allows the researcher to gather the respondent's feedback quickly and efficiently.

Using surveys allows the researcher to manipulate the boundaries and research design procedures in order to control data collection and analysis (Orlikowski & Baroudi, 1991). In addition, the survey strategy is affiliated with a deductive approach and is used for explanatory research (Saunders & Lewis, 2012).

The survey was used for data collection. The survey consists of an online questionnaire. The data collection method provides the most accurate and efficient data capturing mechanism for a large sample over a distributed area – reaching people in different locations (Mccusker & Gunaydin, 2015). This research strategy allows the researcher to have the least influence on participants during data collection. The research is conducted objectively, therefore, it is very important that the researcher does not influence collected data and engage with the participants (Saunders et al., 2016).

3.6 Research Timeframe

The research timeframe is cross-sectional. This is because the proposed research on improving information security posture phenomenon was conducted at a point in time (Saunders et al., 2016; Wahyuni, 2012). Data collection was scheduled for mid-2019, after ethics approval.

The cross-sectional timeframe is often employed in a survey method seeking to further describe the research phenomena(Saunders et al., 2016). Furthermore, this research was completed in a

limited time of two years hence why it was suited for a cross-sectional timeframe (Martelli & Greener, 2018).

3.7 Research Instrument

Research instruments are tools (such as an online questionnaire, used to collect data) used by the researcher in order to achieve the research's set objectives. Furthermore, research instruments assist with the collection of data from the participants. This research's main research instrument is a survey in the form of an online questionnaire (Wahyuni, 2012).

The use of the questionnaire is appropriate because research that employs a survey method is said to be either exploratory or explanatory in nature. In this case, it is an explanatory study that assists in examining and clarifying the relationships between research variables, specifically aiming at the cause and effect relationships (Saunders et al., 2016). The questions used in the questionnaire are extracted from the study titled "Matching training to individual learning styles improves information security awareness" (Malcolm Pattinson et al., 2019). These are questions regarding the types of learning styles and the frequency of learning styles. Furthermore, these questions originally referred to training but in this study, it was modified and changed to ISA programs to accommodate education and awareness. The learning styles options are adopted from the VARK inventory model (VARK Learn Limited, 2014). A list of HAIS-Q questions were adapted from HAIS-Q (Parsons et al., 2017). The demographic questions were developed by the researcher, the researcher also ensured they were in line with UCT's questionnaire policy.

The online questionnaire's initial questions aim to create a participant profile, these questions include age category, gender, geolocation, and education level. These questions enriched data analysis, created trends and graphs with respect to a respondent.

The answers to the questions (as per the KAB model constructs) within the questionnaire used a seven-point Likert scale. It is said that rating questions often utilise the Likert-style rating. The rating asked the respondent if he or she agreed disagreed etc., about a statement in the form of a question. The Likert-style rating often uses a four, five, six or seven-point rating scale (Saunders et al., 2016). The seven-point Likert scale categories are indicated below to indicate rating based on the agreement.

1. Strongly agree
2. Agree
3. Somewhat agree
4. Neutral
5. Somewhat disagree
6. Disagree
7. Strongly disagree

As indicated in Figure 3, the type of questionnaire employed for this research is self-completed, web-based, and distributed to respondents via email or social media platforms. Respondents accessed the questionnaire through a hyperlink in a web browser (Saunders et al., 2016). The choice of questions for the questionnaire was influenced by the research questions and objectives (Saunders et al., 2016).

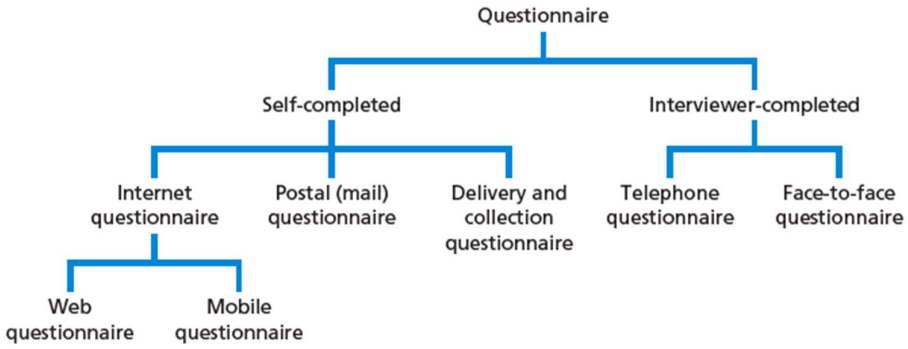

Figure 3. Questionnaire design (Saunders et al., 2016)

There are several online survey platforms, such as Qualtrics, that are widely used in research. Greener & Martelli (2018) mention that online platforms are recommended as they offer a professional feel, automatic response, allowing the researcher to easily design and deploy the survey through email, web, or other compatible online portals. These factors support the use of online questionnaires in this study.

The researcher distributed the questionnaire via email and social media platforms, seeking to reach a large number of participants for feedback by completing the survey. The research participants required access to the internet, a desktop, laptop, or any electronic smart device that is able to receive emails and access social media platforms (LinkedIn, WhatsApp and Facebook).

A pilot test was used to refine the questionnaire and ensured that potential issues were removed at an early stage (Saunders et al., 2016). Furthermore, the pilot test ensured that research participants understood and were able to answer the questionnaire. The pilot test also ensured that the collection and capturing of data did not pose problems. Lastly, the pilot test tested the validity and reliability of the collected data. This process ensured the survey is valid and reliable to draw inferences and make generalisation about south Africa organisational employees (Saunders et al., 2016).

It is imperative that every researcher exercises pilot testing because the process determines whether your questionnaire will succeed or not (Yellow & Bell, 2014). The size of the pilot test and the frequency of the pilot test are dependent on the research questions, objectives, size of the research project, time and money dedicated to the research, and lastly the state of the questionnaire design (Saunders et al., 2016). The pilot test included a small scale – 20 people, this number is sufficient to draw inferences and determine if the questionnaire will succeed.

Yellow and Bell (2014) suggest the below-mentioned questions. These questions are expected to be well answered when developing a questionnaire.

- The time it takes to complete the questionnaire.
- If the questionnaire instructions are clear.
- Identify questions deemed unclear or ambiguous.
- Identify questions that respondents felt anxious about or struggled to answer.
- In respondents' opinions, identify the topics which they opted to exclude details.

- If the questionnaire layout was clear and appealing to respondents.
- Any other suggested comments.

In the delivery and collection of the questionnaire, the researcher employed the following strategies: incentive, length, appearance, delivery, contact, content and communication. These strategies assisted with a high response for the survey and increased the response time (Anseel, Lievens, Schollaert, & Choragwicka, 2010).

Research participants were paid to fill in the survey using the Qualtrics platform. The length of the questions was kept short and straight to the point with sufficient details to understand. The Qualtrics platform allowed the researcher to use bullet points and text-boxes, and provided recommendations to ensure that the survey was captivating and user-friendly. The survey was delivered through multiple platforms to accommodate a diverse range of research participants. Lastly, multiple communications were sent out, to remind research participants, providing additional details and answering ad-hoc queries.

3.8 Sample Population

South Africa faces a high unemployment rate, specifically for the youth. In 2018 (2018 – Q4), unemployment was at 27.1%. In addition to the high unemployment rate, there is a shortage of ICT skills. This is in part due to many schools lacking equipment, resources and teachers trained in Computer Science (Sutherland, 2017). Furthermore, Sutherland (2018) insists that low ICT skills classify South Africans as favourable cyber threat targets because of skill shortage and cyber security education and awareness.

Over the years, ICT university graduates have grown, however it is still low in comparison to other countries (Sutherland, 2017). With this improvement, it is a great opportunity to align ISA programs with ICT skill growth; this will hopefully add to the improvement of information security posture in South Africa. This research will, therefore, focus on currently employed people that are working in South Africa.

Population size is defined as the total number of people which the researcher is attempting to study (SurveyMonkey, 2019). In this case, it is all employees. The sample population, also known as the subset of the population are employees living in South Africa. The suitable sample size for this research is 385 according to the Survey Monkey sample calculator (SurveyMonkey, 2019). The sample size was generated by using the number of employed people in South Africa: 10151000 (Trading Economics, n.d) at 95% sampling confidence interval and with a margin of error equal to 5%. Therefore, the researcher aimed at collecting 385 filled surveys.

The sampling confidence interval is defined as “a percentage that reveals how confident you can be that the population would select an answer within a certain range” (SurveyMonkey, 2019) and the margin of error is defined as “a percentage that tells you how much you can expect your survey results to reflect the views of the overall population (SurveyMonkey, 2019). The smaller the margin of error, the closer you are to having the exact answer at a given confidence level” (SurveyMonkey, 2019). Therefore, it can be stated that the researcher is 95% confident (at 5% margin of error) that the sample of 385 people will accurately represent the population. Therefore, it is sufficient to make a generalisation and draw inferences about the study.

In quantitative research, they are two main types of sampling: probability and non-probability sampling. The difference between the two types of sampling is the use of sample selection called randomisation. According to the Center for Innovation in Research and Training (CIRT), randomisation occurs "when all members of the sampling frame have an equal opportunity of being selected for the study".

Probability sampling makes use of random sampling, whereas non-probability sampling does not use random selection to select participants. Probability sampling consists of random, stratified, systematic, cluster, and multi-stage sampling. Non-probability sampling consists of convenience, purposive, modal instance, expert, proportional and non-proportional quota, diversity, and snowball sampling.

This research employed purposive sampling, whereby certain groups of participants were sought after. In this study, it was employed people on LinkedIn and Facebook that were sought after.

3.9 Data Collection

The Qualtrics survey was distributed to research participants via social media platforms and email. The survey included a cover letter (Appendix C) and a hyperlink to the online questionnaire. The cover letter briefly explained the survey's purpose, objective, the researcher's research background, and re-affirmed that the captured data will be used for research purposes only.

Participants were required to click on the provided hyperlink, the hyperlink redirected respondents to the website hosting the online questionnaire. Once the questionnaire was completed, participants were notified that the survey was completed and that the data had been recorded.

Follow-up communication was sent to remind the sample population target about the survey. This ensured more people completed the survey. A sample questionnaire can be seen in Appendix D.

Below are the high-level processes that the research employed to collect the data successfully.

- The survey was prepared and designed in Qualtrics
- The survey's landing page consisted of a cover letter that highlighted the terms and conditions of the study.
- The survey was emailed and shared across social media platforms (LinkedIn, Facebook, and WhatsApp). Also, follow-up communications were sent to remind and assist potential research participants.
- Respondents were notified that the survey was completed and the results were securely stored into the Qualtrics database.

Research participants were only allowed to complete one questionnaire to ensure there were no duplications. In addition, the feature to force a response to a question before moving to the next page was enabled. This ensured that all the questions were fully answered.

3.10 Data Analysis

In research, it is required that the researcher completes data analysis on the collected data in order to explore, present, describe, and examine relationships and trends in the collected data (Saunders et al., 2016). Data quantification (analysed and interpreted) assists in answering set research questions and objectives.

The collected data assisted in making inferences about information security posture for individuals, groups, and the whole organisation. In addition, data collection assisted in addressing set research questions and objectives, and testing the research propositions. The data collected from the survey was extracted from Qualtrics and imported into Excel for data cleaning, and then imported into Statistica for data analysis. Throughout this process, the researcher ensured the extracted data was correct, error-free, and secure. No data loss or disclosure to the public.

The data cleaning process includes the following lifecycles: screening, diagnosing, and editing (Van Den Broeck, Cunningham, Eeckels, & Herbst, 2005). Afore-mentioned data cleaning lifecycles were used in order to correct, delete or leave unchanged the following data issues: outliers, inconsistencies, strange patterns, errors, and missing data (Van Den Broeck et al., 2005). Excel was used to carry out the data cleaning processes.

Using SPSS, descriptive statistics was extracted using the following measurements: the minimum, maximum, mean, median, mode, lower and upper quartiles, and standard deviation. The aforementioned processes were carried out once the data was cleaned (Saunders et al., 2016). Above-mentioned measures were used to summarise the raw imported data into Statistica. This process assisted with identifying patterns and enabling data visualisation.

The SPSS tool was used to create trending graphs and the charts to visualise data distribution. The researcher examined relationships among variables using the following tests:

- Scatter plot
- Pearson correlation test
- P-value

The research analysis also tested the questionnaire's reliability and validity. Reliability tests ensures that "data collection techniques and analytic procedures" have consistent findings (Saunders et al., 2016)**.** Validity was consistent with the research as it is only associated with positivism and quantitative research (Saunders et al., 2016). A validity test is carried out to measure if the questionnaire is sufficient enough to provide what the researcher intends to measure (Christensen, Johnson, & Turner, n.d.).

In addition, a valid questionnaire ensures accurate data that measures the concepts that the researcher is interested in collecting. On the contrary, reliability ensures the data is collected consistently (Saunders et al., 2016). To explain further in terms of a question and answer example, the question must be understood by the respondent in the way intended by the researcher and the answer given by the respondent must be understood by the researcher in the way intended by the respondent (Foddy & Foddy, 1994). These issues were addressed in the pilot study.

Figure 4 indicates stages needed to occur in order to confirm that the questions are valid and reliable.

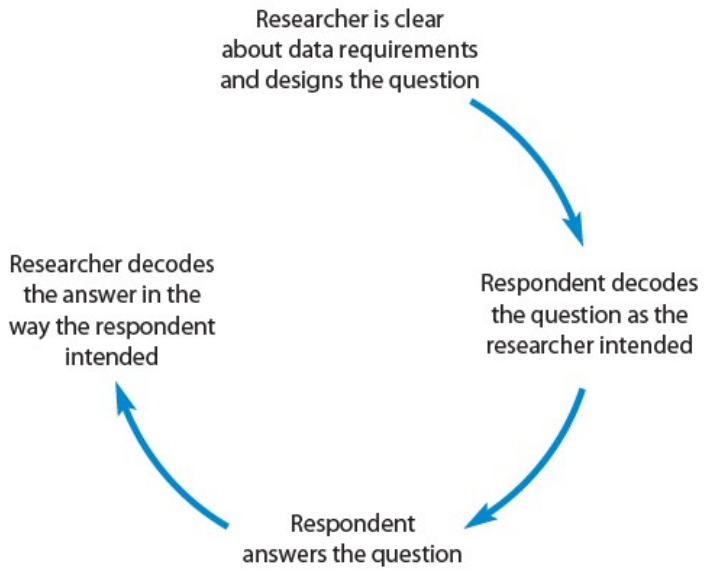

Figure 4. Stages for a valid and reliable question

In research, there are several ways to assess validity: internal validity, content validity, criterion-related validity (also known as predictive validity), construct validity, convergent validity and lastly, discriminant validity. This study used construct validity as the research questionnaire was designed according to the constructs. This assisted with examining "the extent to which a set of questions actually measures the presence of the construct that the researcher intends to measure" (Saunders et al., 2016, pg. 450).

In addition, there are several ways to test for reliability. There are three widely used approaches to assessing reliability. The approaches are: re-test, internal consistency, and alternative form (Berger & Mitchell, 2002). These approaches need to be considered at the questionnaire design stage to ensure that the questionnaire is reliable, therefore ensuring that the research is on the correct path to achieving set objectives. This study used internal consistency that tests for "correlating the responses to questions in the questionnaire with each other". Therefore, this approach measures the respondent's consistency across the subgroup of a question (Saunders et al., 2016). One of the most common measures of internal consistency is Cronbach alpha. Cronbach alpha uses an alpha coefficient value of between 0 and 1. Moreover, the alpha coefficient value of 0.7 or greater indicates that the combined questions are measuring the same thing (Tavakol & Dennick, 2011).

3.11 Ethics and Confidentiality

Research ethics is described as "the standards of the researcher's behaviour in relation to the rights of those who become the subject of a research project, or who are affected by it" (Saunders et al., 2016, p. 726). Furthermore, it is a requirement for any research to highlight ethical considerations that impact the study. For this research, ethical considerations reflected on the researcher's behaviour and actions, research participants and resources used to conduct the study.

Below are common categories of ethical issues, these categories are to be recognised and minimised (Saunders et al., 2016).

Integrity and objectivity of the researcher: This category refers to the researcher's integrity and objectivity of this study. The researcher was required to be open, honest, and promote accuracy in findings. During the course of data collection, analysis, and compiling findings regarding information security posture, the researcher avoided deception, misrepresentation, and poor commitments. Therefore, it is recommended that "where appropriate, any conflict of interest or commercial association should be declared" (Saunders, 2016, pg. 243).

Respect for others: This category alludes to treating research participants, stakeholders, and anyone affected by it with dignity, trust, and respect (Saunders, 2016). If any conflicts arise throughout the research, it is should be resolved in a diplomatic way and reach an amicable agreement that favours both parties.

Avoid of harm: Avoidance of harm towards participants in terms of embarrassment, pain, and discomfort. Revealing research participants sensitive and confidential data can lead to the aforementioned form of harm.

Privacy of those taking part: Voluntary nature of participation and right to withdraw, informed consent of those taking part and ensuring the confidentiality of data, and maintenance of anonymity of those taking part.

In research, privacy is key because violation of privacy can lead to serious consequences. Therefore, it is highly recommended that the information and data gathered in research should be safely stored and secured. As a result, this study ensured data store in password-protected locations and encrypted cloud storage. Furthermore, the researcher highlighted in the survey that answering is voluntarily and withdrawal at any point without any obligation is allowed for respondents. The survey was conducted anonymously, transparent with informed consent, and lastly, research participants were informed that collected data and findings will be used for the research and academic purpose only.

The research ethics form was filled, populated, and signed for approval by the Commerce department's faculty of Ethics and Research Committee. The approval letter served as a verification that the proposed study had undergone ethics examination and no conflicts were identified. The letter granting ethics approval can be found in Appendix B.

- Responsibility in the analysis of data and reporting of findings

In the process of data analysis, if the researcher decides to utilise primary or secondary data. Fabrication, falsification, and manipulation of data were avoided. In addition, research findings were captured and reported in the highest form of accuracy. Furthermore, the sources were clearly acknowledged to prevent plagiarism.

- Compliance in the management of data

The researcher did not collect personal data.Additionally, the researcher adhered to South Africa's regulations and restrictions associated with the gathered data. Such as the Protection of Personal Information Act (POPIA) aimed at protecting personal information (South African Government, 2019).

The researcher adhered to ethics and confidentiality, and avoided potential risks that might affect the research participants and other stakeholders.

3.12 Summary

The research philosophy used an objectivism ontological stance and a positivism epistemology stance. The approach for the research was deductive. As a result, the method used was quantitative.

The research purpose was explanatory, using online surveys as the research seeks to identify causal relationships between the KAB model's constructs. The strategy adopted was the use of a survey, specifically online surveys. Using online surveys was efficient and prevented the researcher from being too involved. As a result, the research did not influence the collected data and the analysis process. This is key as the research aimed to be conducted independently.

The research used a cross-sectional time basis because it was conducted at a point in time. The research instruments can be summarised as the tools used to enable or achieve the research's objectives. Moreover, the research used an online questionnaire as a tool to collect data efficiently.

The research population were determined to be employees and the sample was employees living in South Africa. The sample population utilised purposive sampling as research participants were reached through the use of email and social media platforms. Data collection and analyses used Qualtrics and SPSS software to manage storage, distribution, collection, and completion of the analyses.

4. Data Analysis and Findings

The Qualtrics survey platform was used to distribute the questionnaire and collect the data. Initially, 140 responses were received; the data cleaning process removed 23 incomplete surveys, leaving 117 complete surveys to be used for data analysis. Majority of the responses were collected in the first week. This was achieved through multiple survey distribution channels; WhatsApp, LinkedIn, Facebook, and Twitter. Furthermore, to ensure that the online survey was seen and completed by employed people living in South Africa, participants voluntary shared the survey with colleagues, friends, and family. In addition, the survey was re-shared on Facebook and Twitter to attract more views.

No issues were reported when the survey was distributed, this is a result of a thorough pilot test having been conducted prior to mass distribution. After two weeks, the second round of data collection was performed, using Qualtrics survey panels. These panels assisted with collecting an additional 205 surveys. In the end, 322 fully completed surveys were available for analysis.

4.1 Demographic Analysis

This section details the demographic analysis in accordance with the collected data. The demographic analysis focuses on the following: Gender, Ethnic Groups, Level of Education, Primary Occupation, and Age.

4.1.1 Gender

The respondents' gender distribution is depicted in Table 1 below. The gender categories used for this study were: Male, Female, and Prefer not to Answer. Majority of the respondents were Males at 55%, followed by Females at 45% and 0% preferred not to mention their gender. The gender distribution of males and females are not too far apart, there was a 10% difference.

Table 1. Gender demographics summary

Demography	Category	Frequency	Percentage (%)
Gender	Male	177	55%
	Female	145	45%
	Prefer not to answer	0	0%

4.1.2 Age

The respondents' age groups and distribution are depicted below in Table 2. The age groups were: 18 – 29, 30 – 39, 40 – 49, and 60 and over. Most of the respondents were in the age group of 30 – 39 years at 39%, followed by the age group of 18 – 29 years at 36%, age group of 40 – 49 years at 16%, age group of 50 – 59 years at 7% and lastly, the age group of 60 and over at 2%.

Table 2. Age groups demographic summary

Demography	Category	Frequency	Percentage (%)
Age	18 – 29	117	36%
	30 – 39	125	39%
	40 - 49	52	16%
	50 – 59	21	7%
	60 and over	7	2%

4.1.3 Ethnic Groups

The ethnicity of respondents is depicted in Table 3 below. The categories presented for the ethnic groups were: African, White/Caucasian, Indian, Coloured, and Prefer not to answer. Most of the respondents were Africans at 48%, followed by White/Caucasian at 30%, Coloured at 14%, Indian at 6% and 2% of the respondents preferred not to answer.

Table 3. Ethnic groups' demographic summary

Ethnic group/race	Frequency	Percentage (%)
African	155	48%
White/Caucasian	96	30%
Coloured	45	14%
Indian	19	6%
Prefer not to answer	5	2%
Asian	2	0%

4.1.4 Education

The education levels of the respondents are depicted in Table 4 below. The categories for the level of education were: High School or Lower, Diploma/College Graduate, Bachelor Degree, and Postgraduate and Higher. Most of the respondents had a Diploma or a College Graduate qualification at 29%, followed by both the Bachelor Degree, and Postgraduate and Higher at 27%. Lastly, High School or Lower education level at 17%.

Table 4. Education Demographic Summary

Level of education	Frequency	Percentage (%)
Diploma/College Graduate	94	29%
Bachelor Degree	87	27%
Postgraduate and Higher	87	27%
High school or Lower	54	17%

4.1.5 Primary Occupation

The primary occupation categories are depicted in Table 5 below. Most of the respondents' primary occupation was Computer and Mathematical Occupations at 18%, followed by the Others category at 12%, and followed by Office and Management Occupations at 9%. The category with the least respondents were Building and Grounds Cleaning and Maintenance Occupations, and Community and Social Service Occupations at 0%.

Table 5. Primary Occupation Distribution Summary

Category	Frequency	Percentage (%)
Computer and Mathematical Occupations	58	18%
Other (please specify)	38	12%
Management Occupations	30	9%
Education, Training, and Library Occupations	27	8%
Business and Financial Operations Occupations	26	8%
Office and Administrative Support Occupations	26	8%
Sales and Related Occupations	22	7%
Healthcare Practitioners and Technical Occupations	16	5%
Architecture and Engineering Occupations	10	4%
Installation, Maintenance, and Repair Occupations	9	3%
Production Occupations	9	3%
Life, Physical, and Social Science Occupations	7	2%
Legal Occupations	7	2%
Food Preparation and Serving Related Occupations	6	2%
Transportation and Materials Moving Occupations	6	2%
Healthcare Support Occupations	5	2%
Arts, Design, Entertainment, Sports, and Media Occupations	5	2%
Farming, Fishing, and Forestry Occupations	4	1%
Construction and Extraction Occupations	4	1%
Protective Service Occupations	3	1%
Personal Care and Service Occupations	3	1%
Community and Social Service Occupations	1	0%
Building and Grounds Cleaning and Maintenance Occupations	0	0%

4.2 Reliability and Validity Testing, and Analysis

Reliability testing was performed using the following model constructs: knowledge, attitude, behaviour, and lastly learning style and delivery methods.

As mentioned in the design section, Cronbach's Alpha is used to measure internal consistency for questions listed in the survey. Additionally, an internal consistency measurement is achieved by calculating the Cronbach's value for each construct. As indicated in Table 6, if the Cronbach's Alpha value is greater than 0.7 ($0.8 > \alpha \geq 0.7$, $0.9 > \alpha \geq 0.8$, $\alpha \geq 0.9$) it is regarded as acceptable, good and excellent. This is indicated in Table 6 using the ranges in the internal

consistency column. Internal consistency rated as acceptable, good and excellent shows that there is reliability in the survey and also an indication that "the items within the scale are measuring the same underlying construct" (Cronbach, 1951; Tavakol & Dennick, 2011). Therefore, it is imperative that the survey items show good internal consistency. As a result, the assumptions and claims from the survey items can be regarded reliable and valid.

However, when the Cronbach's Alpha value is under 0.7, the survey is regarded as questionable, poor, and unacceptable. This is indicated in Table 6 as well. It is wise to ensure items do not have a Cronbach's Alpha value below 0.7. with respect to the Cronbach's Alpha range indicated below.

Table 6. Rule of thumb for calculating internal consistency (Gliem & Gliem, 2003)

Cronbach's alpha	Internal consistency
$\alpha \geq 0.9$	Excellent
$0.9 > \alpha \geq 0.8$	Good
$0.8 > \alpha \geq 0.7$	Acceptable
$0.7 > \alpha \geq 0.6$	Questionable
$0.6 > \alpha \geq 0.5$	Poor
$0.5 > \alpha$	Unacceptable

This study used SPSS to analyse the reliability of the items which make up knowledge, attitude, and behaviour constructs. These are the main constructs in this study. The gathered data using HAIS-Q questions in the survey were used to calculate the Cronbach alpha values for knowledge, attitude and behaviour items.

Table 7. Reliability Statistics

Reliability Statistics	
Cronbach's Alpha	N of Items
0.888	27

Tables 7 shows that the items for all three constructs are reliable – greater than alpha value 0.7 (Saunders et al., 2016). With reference to Table 8, this result indicates the state of internal consistency as good. The items that make up the three constructs seem to measure the same values. This result is consistent with previous results using HAIS-Q. Internal consistency was rated good as each of the HAIS-Q 7 focus areas (questions 1- 27) had Cronbach's Alpha ranging between 0.75 and 0.82.

Table 8 shows a detailed table of items with respect to each construct and their respective Cronbach's Alpha values. They are all above 0.7.

Table 8. Reliability analysis for the research constructs

Items ID	Cronbach's Alpha if Item Deleted	
HAIS-Q: Q01	0.879	Knowledge
HAIS-Q: Q02	0.883	
HAIS-Q: Q03	0.89	
HAIS-Q: Q04	0.883	
HAIS-Q: Q05	0.889	
HAIS-Q: Q06	0.882	
HAIS-Q: Q07	0.884	
HAIS-Q: Q08	0.887	
HAIS-Q: Q09	0.883	
HAIS-Q: Q10	0.881	Attitude
HAIS-Q: Q11	0.887	
HAIS-Q: Q12	0.885	
HAIS-Q: Q13	0.883	
HAIS-Q: Q14	0.882	
HAIS-Q: Q15	0.883	
HAIS-Q: Q16	0.885	
HAIS-Q: Q17	0.884	
HAIS-Q: Q18	0.881	
HAIS-Q: Q19	0.886	Behaviour
HAIS-Q: Q20	0.882	
HAIS-Q: Q21	0.886	
HAIS-Q: Q22	0.885	
HAIS-Q: Q23	0.88	
HAIS-Q: Q24	0.884	
HAIS-Q: Q25	0.881	
HAIS-Q: Q26	0.881	
HAIS-Q: Q27	0.885	

To test and confirm validity, factor analysis is used. Factor analysis is defined as a statistical method that can be used to collect validity evidence (Knekta, Runyon, & Eddy, 2019).

Factor analysis in SPSS has the ability to indicate data validity in other words, is there validity in the construct being measured. To achieve this, SPSS uses factor loadings, which represent how much a factor explains a variable. Furthermore, loadings can range from -1 to 1. More specifically, loadings which are close -1 to 1 indicate that the factor strongly affects the variable. Based on the output from SPSS (Figure 5 and Table 10), there are seven factors – as indicated in Scree plot and the component matrix. From the seven factors, strong loadings can be identified. Significant or suitable factor loadings are greater and equal to 0.5 (Williams, Onsman, & Brown, 2010).

The factor loadings, which are equal and greater than 0.5 are highlighted in red. For factor one, the items or HAIS-Q questions 1, 2,4,6,7, and 9 are validity for the construct: knowledge. Construct attitude, items 10, 13,14,15,17, and 18. Lastly, the behaviour construct, items 20, 23, 25, and 26.

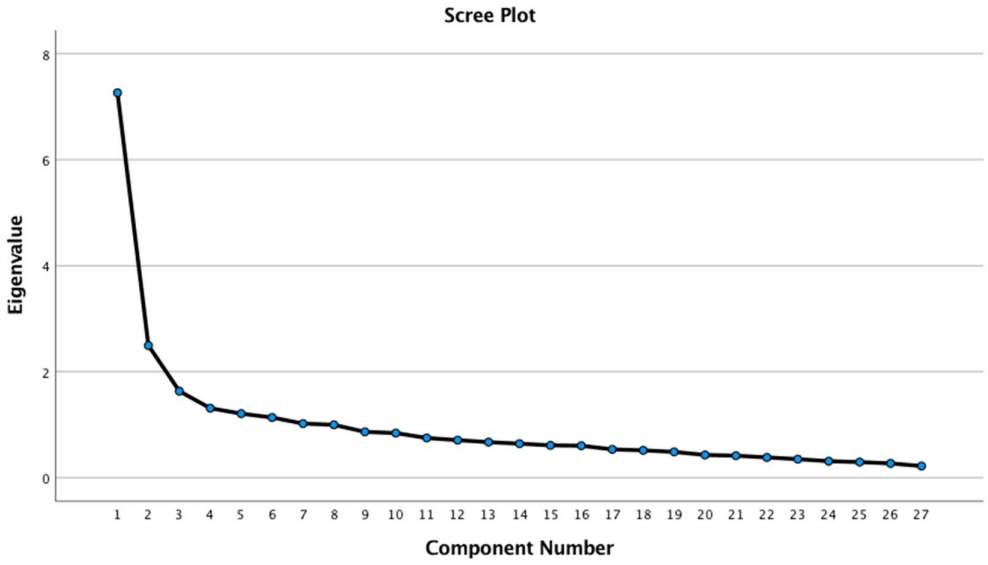

Figure 5. Scree Plot

Table 9 - Component Matrix

	1	2	3	4	5	6	7
Item 1	.693	-.142	-.203	.113	-.234	-.168	.142
Item 2	.561	-.039	-.561	.008	.138	-.201	.063
Item 3	.168	.287	-.255	.496	.201	.447	-.073
Item 4	.538	-.300	.130	.037	.116	-.030	.229
Item 5	.291	.114	.381	.455	.217	-.125	-.061
Item 6	.556	-.224	.048	.264	-.037	-.099	-.126
Item 7	.512	-.504	.072	-.076	.184	.124	.225
Item 8	.337	.173	.212	.471	-.092	-.252	.308
Item 9	.540	-.539	.028	.019	.019	.160	.002
Item 10	.629	.051	-.217	-.064	-.338	-.090	.048
Item 11	.352	.309	-.200	-.280	.540	-.292	-.074
Item 12	.449	.261	-.207	.086	-.068	.493	.037
Item 13	.513	-.284	.079	-.143	.358	.212	.067
Item 14	.649	-.072	-.058	-.168	-.269	.040	-.274
Item 15	.557	.290	.325	-.192	-.139	-.011	-.153
Item 16	.470	.234	.383	-.299	.062	.038	.156
Item 17	.521	.409	.240	-.338	-.139	.124	.276
Item 18	.620	-.245	-.011	-.096	-.146	.293	-.190
Item 19	.399	.419	-.002	-.139	-.012	-.169	.328
Item 20	.597	.070	-.572	-.095	.119	-.210	-.142
Item 21	.429	.448	-.226	.087	.004	.328	.251
Item 22	.451	.168	.161	-.058	.458	.046	-.181
Item 23	.677	-.015	.057	-.026	-.259	-.098	-.331
Item 24	.480	.331	.286	.126	.096	-.048	-.423
Item 25	.608	-.447	.232	-.011	.047	.041	.054
Item 26	.590	-.265	.015	.259	.009	-.224	.108
Item 27	.433	.506	.065	.187	-.122	-.071	-.022

4.3 Information Security Awareness (ISA) Level

Table 11 below provides ISA score levels, where the ISA values were calculated as a percentage of the total number of favourable responses marked as either "Agree" or "Strongly Agree". Furthermore, all favourable responses were calculated as a percentage (a value out of 100) from the total number of responses received.

Table 11 also shows the percentage of favourable (which is in line with information security policy and procedure) knowledge, attitude and behavioural responses for research participants. After reverse scoring was applied to the HAIS-Q, favourable responses were a total of responses that were marked as either 'Strongly Agree', 'Agree' or 'Somewhat Agree', and represented as a percentage of the total number of responses for each information security focus area. This method is adapted from the study by Pattinson et al. (2016).

As a result of the favourable percentage for knowledge, attitude and behaviour, the following rating methods was used to categorise what is bad (requires improvement), reasonable and good security awareness.

- Scores above 80 were regarded as having a **good** awareness of security threats facing the organisation.
- Scores 60 - 79 were regarded as having **reasonable** awareness of security threats.
- Scores below 60 were regarded as areas that **could use improvement**.

Table 10. Percentage of favourable responses

Focus area	Knowledge	Attitude	Behaviour	Average ISA Score
Password Management	88	87	93	**89**
Email Use	72	84	82	**79**
Internet Use	68	86	77	**77**
Total ISA Score	**76**	**86**	**84**	**82**

4.3.1 Total Information Security Awareness (ISA) results per demographic

In the section below, Table 12 combines demographic variables (gender, age, ethnic groups, and education levels) and their respective ISA score levels to uncover several relationships.

Response option "Prefer not to Answer" was omitted in the analysis of gender and race.

In the gender demographics, both Males and Females had a good security awareness. This is seen across the ISA score levels for knowledge, attitude and behaviour. The overall ISA score between Male and Female research participants was only a 1% difference.

The age demographic indicated a good security awareness across all the age categories. As indicated, the older generation (40 and over) performed better in comparison to the younger generation (18 – 39). This result could mean that experience is a key factor for security awareness level. However, the difference between the overall ISA score across all age categories is not significant (3% at most). This is a potential indication that perhaps age does not play a critical role when it comes to security awareness.

The ethnic group demographic is consistent with other demographics too. The security awareness is good across African, White/Caucasian, Asian, Indian and Coloured people. The overall ISA score for all the ethnic groups is above 80%, with 6% difference between the leading and the least ISA score, Asian (88%) and Coloured (88%) and White/Caucasian (82%). This can be explained by the fact that Asian and Coloured research participants have a better security awareness in comparison to White/Caucasian research participants. However, the Asian group was very small so this played a role in scoring a high ISA.

Lastly, the education level demographic shows good security awareness across all the education levels, above 80%. However, as one would have expected, there is a positive relationship between education and the ISA score levels. Research participants with better qualifications boasted better ISA score levels. There is an 8% difference between 'High School or Lower' and the 'Postgraduate and Higher'. This result shows that education is a key factor in security awareness.

Table 11. Demographic variables and affiliated ISA score levels

Demography	Category	Number of respondents	Knowledge	Attitude	Behaviour	ISA Score
Gender	Male	177	81	87	86	85
	Female	145	78	87	86	84
Age	18 – 29	117	78	86	83	82
	30 – 39	125	80	87	86	84
	40 - 49	52	79	89	88	85
	50 – 59	21	80	91	93	88
	60 and over	7	77	90	88	85
Ethnic group/race	African	155	79	87	85	84
	White/Caucasian	96	77	86	84	82
	Asian	2	90	91	82	88
	Indian	19	81	88	89	86
	Coloured	45	84	89	90	88
Level of education	High school or Lower	54	76	82	85	81
	Diploma/college graduate	94	76	84	84	81
	Bachelor degree	87	80	86	85	84
	Postgraduate and Higher	87	85	94	89	89

4.3.2 ISA Score per question with respect to Knowledge, Attitude and Behaviour

The ISA score was calculated based on the HAIS-Q questions with respect to the focus areas, knowledge, attitude and behaviour as indicated in Tables 13, 14 and 15 below. The following paragraphs and tables provide a detailed analysis of how respondents responded to the HAIS-Q questions in comparison to knowledge, attitude and behaviour.

Table 12. Knowledge HAIS-Q

Item ID	Knowledge Questions	ISA Score
HAIS-Q: Q01	It's acceptable to use my social media passwords on my work accounts	77
HAIS-Q: Q02	I am allowed to share my work passwords with colleagues	86
HAIS-Q: Q03	A mixture of letters, numbers and symbols is necessary for work passwords	87
HAIS-Q: Q04	I am allowed to click on any links in emails from people I know	64
HAIS-Q: Q05	I am not permitted to click on a link in an email from an unknown sender	77
HAIS-Q: Q06	I am allowed to open email attachments from unknown senders	73
HAIS-Q: Q07	I am allowed to download any files onto my work computer if they help me to do my job	54
HAIS-Q: Q08	While I am at work, I shouldn't access certain websites	82
HAIS-Q: Q09	I am allowed to enter any information on any website if it helps me do my job	56
	Overall ISA Score	**73**

As indicated in Table 13, the overall ISA score for knowledge-based questions is 73%, which is regarded as a reasonable awareness of security threats. It is an indication that ISA can be improved, specifically focusing on knowledge. The highest ISA score was for the question "**A mixture of letters, numbers and symbols is necessary for work passwords"** at 87%. This ISA score is regarded as good awareness. To emphasise the significance, it is 14% above the average ISA score for knowledge. This is an indication that respondents understand the importance of using a complex password – alphanumeric. One would assume that research participants are likely to be aware that easy passwords can be easily cracked and therefore used to hack into relevant accounts. Following was the question **"I am allowed to share my work passwords with colleagues"** at 86%. This ISA score is an indication that respondents are well aware that it is not safe to share passwords with colleagues. Password sharing could potentially lead to a password breach or being compromised. However, this ISA score can be improved.

The lowest ISA score was for the question **"I am allowed to download any files onto my work computer if they help me to do my job"** at 54%. This is a poor ISA score and it is under the average knowledge ISA score by 19%. This is quite significant, therefore efforts should be put in place to have the ISA improved. Improved by educating end-users on what file types are safe to download. Additionally, this statistic can be used to enhance security controls which prevent end-users from downloading malicious files.

Following was the question **"I am allowed to enter any information on any website if it helps me do my job"** at 56%. This is a poor score with respect to the other knowledge ISA scores and can be improved. Furthermore, it is an indication that respondents are not cautious while providing and entering confidential information into malicious websites. As indicated, they are willing to enter any information on any website given it assists them in completing work they are tasked to do. This is a risk behaviour which could lead to respondents falling into phishing attempts, scams and fraud attempts.

Table 13. Attitude HAIS-Q

Item ID	Attitude Questions	ISA Score
HAIS-Q: Q10	It's safe to use the same password for social media accounts	79
HAIS-Q: Q11	It's a bad idea to share my work passwords, even if a colleague asks for it	86
HAIS-Q: Q12	It's safe to have a work password with just letters	83
HAIS-Q: Q13	It's always safe to click on links in emails from people I know	64
HAIS-Q: Q14	Nothing bad can happen if I click on a link in an email from an unknown sender	87
HAIS-Q: Q15	It's risky to open an email attachment from an unknown sender	88
HAIS-Q: Q16	It can be risky to download files on my work computer	83
HAIS-Q: Q17	Just because I can access a website at work, doesn't mean that it's safe	88
HAIS-Q: Q18	If it helps me to do my job, it doesn't matter what information I put on a website	72
	Overall ISA Score	**81**

As indicated in Table 14, the overall ISA score for attitude-based questions is 81%, which is regarded as a good security awareness.

The highest ISA score for attitude based on HAIS-Q was for the following question **"It's risky to open an email attachment from an unknown sender**" at 88%. This is a good score and it implies that respondents are aware of the risks associated with email attachments from unknown senders. Malicious email attachments from unknown senders can lead to ransomware outbreaks; which could lead to data loss if there are no data backups. The following question "**Just because I can access a website at work, doesn't mean that it's safe**" scored the same ISA score, 88%. This suggests that end users judge or question accessible websites at work. Websites which are accessible on a work network does not necessary imply they are safe to access at all times.

Following is the question "**If it helps me to do my job, it doesn't matter what information I put on a website"** at 72% as well. The ISA score is regarded as good awareness and further indicates that respondents are cautious with the information being entered on the websites, even at the cost of getting the work done, they are willing to ensure that the website is safe to access. Overall, a good attitude towards information security and awareness for both HAIS-Q questions rating 88%.

The attitude-based question with the lowest ISA score is "**It's always safe to click on links in emails from people I know**" at 64%. This is a low ISA score that is 17% below the average score. This score can be improved by providing ISA focusing on email security. In addition, this ISA score indicates a poor attitude towards information security awareness. This poor attitude towards information security awareness is an indication that clicking on any links embedded into an email is deemed safe from the respondents' perspective, even from people they are aware of. Scams and phishing emails can now perfectly impersonate and spoof known email addresses. In this case, 64% of respondents would fall for this trap.

Following was the question "**If it helps me to do my job, it doesn't matter what information I put on a website**" at 72%. This is a reasonable ISA score and can be improved, meaning some respondents are not aware that it is not safe to enter any information on a website. Confidential and sensitive information is to be treated with the utmost security, preventing security risks. Respondents' attitude towards information security was found to be reasonable but still requires significant improvement.

Table 14. Behaviour HAIS-Q

Item ID	Behaviour Questions	ISA Score
HAIS-Q: Q19	I use a different password for my social media and work accounts	88
HAIS-Q: Q20	I share my work passwords with colleagues	87
HAIS-Q: Q21	I use a combination of letters, numbers and symbols in my work passwords	90
HAIS-Q: Q22	I don't always click on links in emails just because they come from someone I know	79
HAIS-Q: Q23	If an email from an unknown sender looks interesting, I click on a link with it	78
HAIS-Q: Q24	I don't open email attachments if the sender is unknown to me	81
HAIS-Q: Q25	I download any files onto my work computer that will help me get the job done	61
HAIS-Q: Q26	When accessing the Internet at work, I visit any websites that I want to	73
HAIS-Q: Q27	I assess the safety of websites before entering information	84
	Overall ISA Score	**80**

As indicated in Table 15, the overall ISA score for behaviour based questions is 80%. This is an indication of good awareness and an indication that respondents' behavioural intentions are risk-averse in their organisations.

The highest ISA score for the HAIS-Q behaviour oriented question is **"I use a combination of letters, numbers and symbols in my work passwords"** at 90%. This is a good ISA score and is indicative of a risk-averse behaviour towards password management.

Following is the question "**I use a different password for my social media and work accounts"** at 88%. This a good ISA score that serves to indicate a risk-averse behaviour towards password management. Moreover, it indicates that 88% (8% above the average the ISA score) of the respondents believe in having different passwords for social media and work accounts. This is a good information security best practice and it improves the overall information security posture in an organisation. Additionally, this is a security-conscious behaviour and further indicates a good understanding of information security awareness.

As indicated in Table 15, the lowest behaviour oriented ISA score was for the question "**I download any files onto my work computer that will help me get the job done**" at 61%. This ISA score is reasonable, it indicates that some people are knowledgeable about appropriate files to keep on a work computer. Furthermore, it is an indication that respondents are security conscious when downloading files and therefore their attitude and behaviour is aligned to information security awareness knowledge. As a result, 61% of the respondents are risk-averse

when downloading any files to their work computer, whereas the other 39% prefer to download any files on a work computer if it assists them to finish the job.

4.4 VARK Inventory

Table 16 summarises the percentage of choosing each option of VARK. This includes double-counting because of the opportunity to choose more than one option in any of the 6 questions in Appendix A.

Table16 excludes those who chose all four options to any question. Respondents who chose all four options were Q1:65 cases, Q2: 21 cases, Q3: 25cases, Q4: cases, Q5: 25 cases and lastly Q6: 13 cases. This is because it would excessively increase figures by the same amount.

Table 15. The percentage of choosing each option

	Percentage who chose this option as all, or part, of their answer						
VARK Question	**V**	**A**	**R**	**K**	**Total**	**Most popular option**	**Least popular**
1	134	84	108	127	454	V	A
2	93	121	78	192	484	K	R
3	105	114	129	167	515	K	V
4	159	59	123	174	515	K	A
5	69	112	86	241	508	K	V
6	141	114	134	90	479	V	K

With reference to Table 16, the below can be deduced:

1. When the research participants are in training which includes a test they are required to pass, the most popular mode of learning is seeing examples – visual. The least popular learning mode is by listening to a presenter – aural.
2. When the research participants have to remember a time when they have to do something new on a computer. The most popular mode of learning is by watching a demonstration – kinaesthetic. The least popular mode of learning is by reading written explanations, for example through a manual or blog – read/write.
3. When the research participants want to learn a new computer program. The most popular mode of learning is by learning how to use it through trial and error – kinaesthetic. The least popular mode of learning is by following the diagrams in the instructions – visual.
4. When the research participants have to learn through a website. The most preferred website to learn from is a website that has components they can click on or interact with - kinaesthetic. The least common website to learn from is a website with audio channels, where they can hear podcasts, radio programs or interviews – aural.
5. The most preferred presenter or instructor is the one who utilises demonstrations or practical sessions – kinaesthetic. The least preferred is an instructor or presenter who utilises diagrams, charts or graphs – visual.
6. The most preferred method of receiving feedback when research participants have completed a test at the end of a training course and would like to receive feedback is by having their results displayed visually – visual. The least preferred method is by using examples from what they have done – kinaesthetic.

Using SPSS, questions 1 to 6 was analysed in order to calculate the frequencies and the percentages.

With regards to "**participating in training that includes a test that you are required to pass**", Table 17 indicates 65 (20.2%) research participants prefer training or learning by means of visual, aural, read/write and kinaesthetic. This is the highest frequency as indicated in Table 15. The lowest frequency is for research participants who prefer training by reading and kinaesthetic, 6 (1.9%) research participants.

Table 16. Learning Styles, Q1

You are participating in training that includes a test you are required to pass		
	Frequency	Percentage
Total	322	100.0
VARK	65	20.2
K	39	12.1
R	33	10.2
V	32	9.9
VK	28	8.7
VRK	18	5.6
VR	17	5.3
VAK	15	4.7
A	15	4.7
VAR	14	4.3
ARK	11	3.4
VA	10	3.1
AK	10	3.1
AR	9	2.8
RK	6	1.9

Table 18 indicates frequencies for "**remember a time when you learned how to do something new on a computer**". Most research participants, 79 (24.5%), prefer learning by kinaesthetic. The least number of research participants, 4 (1.2%), prefer learning by a mixture of visual and reading/writing.

Table 17. Learning Styles, Q2

Remember a time when you learned how to do something new on a computer			
		Frequency	Percentage
	Total	322	100.0
	K	79	24.5
	KA	33	10.2
	A	32	9.9
	KV	32	9.9
	V	24	7.5
	AR	22	6.8
	KAVR	21	6.5
	R	17	5.3
	KR	16	5.0
	KAV	15	4.7
	KAR	9	2.8
	KVR	8	2.5
	AV	8	2.5
	VR	4	1.2
	AVR	2	.6

Table 19 indicates frequencies for the question "**if you want to learn a new computer program**". Most of the research participants, 45 (14%), prefer learning a new program by means of kinaesthetic. The least number of research participants, 11 (3.4%), prefer learning by a mixture of aural and visual.

Table 18. Learning Styles, Q3

If you want to learn a new computer program			
		Frequency	Percentage
Valid	Total	322	100.0
	K	45	14.0
	RK	35	10.9
	RAKV	34	10.6
	A	30	9.3
	R	24	7.5
	AK	23	7.1
	KV	20	6.2
	RKV	20	6.2
	V	18	5.6
	RA	14	4.3
	RAV	12	3.7
	RAK	12	3.7
	RV	12	3.7
	AKV	12	3.7
	AV	11	3.4

Table 20 shows frequencies and percentages for the question "**I like websites that have**" features encapsulated in the VARK inventory modulus. Most of the research participants, 50 (15.5%), prefer websites with kinaesthetic features. The least number of research participants, 2 (0.6%), prefer websites with mixed features that contain visual, read/write and aural.

Table 19. Learning Styles, Q4

I like websites that have			
		Frequency	Percentage
Valid	Total	322	100.0
	K	50	15.5
	V	44	13.7
	KV	34	10.6
	KVR	31	9.6
	KR	28	8.7
	R	28	8.7
	KVRA	25	7.8
	VR	23	7.1
	KVA	13	4.0
	KA	12	3.7
	VA	12	3.7
	A	9	2.8
	KRA	6	1.9
	RA	5	1.6
	VRA	2	.6

Table 21 shows frequencies and percentages for the question "**do you prefer a presenter or instructor who uses**" tools which are encapsulated in the VARK inventory modulus. Most of the research participants, 92 (28.6%), preferred learning through a presenter or instructor who utilises kinaesthetic features. Only one research participant (the least), 1 (0.3%), preferred a presenter or instructor that uses a mixture of aural, read/write and visual features.

Table 20. Learning Styles, Q5

Do you prefer a presenter or instructor who uses			
		Frequency	Percentage
Valid	Total	322	100.0
	K	92	28.6
	KA	46	14.3
	KV	31	9.6
	KAR	29	9.0
	KARV	25	7.8
	KR	25	7.8
	A	17	5.3
	R	13	4.0
	V	12	3.7
	KAV	10	3.1
	KRV	8	2.5
	AR	6	1.9
	RV	4	1.2
	AV	3	.9
	ARV	1	.3

Lastly, Table 22 shows the frequencies and percentage for the question "**you have completed a test at the end of a training course, and you would like to receive feedback**". Most of the research participants, 49 (15.2%), prefer receiving feedback through visual features. The least preferred method of reiving feedback is a mixture of kinaesthetic, aural and reading/writing, 2 (0.6%).

Table 21. Learning Styles, Q6

You have completed a test at the end of the training course, and would like to receive feedback			
		Frequency	Percentage
Valid	Total	322	100.0
	V	49	15.2
	R	46	14.3
	A	43	13.4
	VR	30	9.3
	K	28	8.7
	VA	23	7.1
	AR	20	6.2
	KA	15	4.7
	KR	14	4.3
	VKR	14	4.3
	VK	14	4.3
	VKAR	13	4.0
	VAR	8	2.5
	VKA	3	.9
	KAR	2	.6

4.5 Preferred Learning Styles and Delivery Methods Received

The following section of analysis indicates the findings from the VARK inventory question that was posed to the research participants.

The VARK inventory questions allowed the research participants to select more than one option of V, A, R or K. To calculate the preferred learning styles, the researcher counted the number of each of the letter or a combination of the VARK letters. The highest frequencies of a single or combination of letters was identified to be the most preferred.

To calculate whether ISA learning styles received and preferred matched or not, the method in Table 23 was used. The method was to find any matching style between received and preferred. If matching, 1 was assigned and 0 was assigned for not matching. However, when neither of the letters matched, NA was assigned. The variable NA was assigned to research participants whereby ISA was not offered at their workplace. Table 21 indicates this method used to categorise matching and not matching ISA learning styles, with respect to the VARK inventory.

Table 22. Matching preferred and received learning styles

Preferred learning mode	Provided learning mode by a workplace	Matching or Not Matching
V	K	0
VR	-	NA
V	-	NA
VK	R	0
V	A	0
VARK	K	1
VK	A	0

Furthermore, an overall matching value (YES or NO) was calculated using the rules below, in Table 24.

- Matching calculated from the 6 questions were used. Whereby 1 equals matching, 0 equals not matching and NA equals not applicable as ISA was not offered to the research participant.
- From the six questions, when the numbers of **matches <3** is regarded as not matching overall.
- From the six questions, when the number of **matches >=3** is regarded as matching overall.
- Alternatively, **Total<3** is regarded as not matching and **Total>=3** is regarded as matching.
- NA was kept the same.

Table 23. Overall matching analysis

Matching 001	Matching 002	Matching 003	Matching 004	Matching 005	Matching 006	Total	Matching
0	0	1	0	0	1	2	NO
NA	NA	NA	NA	NA	NA	0	NA
1	1	1	1	1	1	6	YES
1	1	1	1	1	1	6	YES
0	1	1	1	1	1	5	YES
NA	NA	NA	NA	NA	NA	0	NA
NA	NA	NA	NA	NA	NA	0	NA
0	1	0	0	1	1	3	YES
0	0	0	0	0	0	0	NO
1	1	0	0	1	0	3	YES

Table 25 summaries the VARK inventory questions using the survey data for received and preferred learning styles, when research participants are provided with ISA programs at their workplaces. The ISA level figures were calculated using the previously mentioned method in section 4.3.

Table 24. VARK inventory questions & the ISA scores

VARK Questions	ISA score when ISA programs are aligned to user preferences	ISA score when ISA programs are not aligned to user preferences
1	87	81
2	87	82
3	86	82
4	87	82
5	87	81
6	87	83

Table 25 shows the ISA scores for when ISA programs are aligned and not aligned to user preferences. This is indicated with respect to each VARK question. These ISA scores were calculated by using the method generated in Table 24, whereby aligned equalled Yes and not aligned equalled No. After separating the scores, the researcher was able to generate ISA scores per VARK question. As predicted, the ISA scores for ISA programs that are aligned to user preferences are greater than the ISA scores for not aligned.

The following section shows a summary of received and common ISA delivery methods. From the range of text-based, video-based, game-based, and other ISA programs delivery methods.

To calculate the total number of provided ISA delivery methods with respect to their workplaces, a similar method of calculating the most common or preferred learning style was used. In this case, the variables were 1 for text-based, 2 for video-based, 3 for game-based, and 4 for other. As indicated in Table 26, the most common ISA programs delivery method is video-based (171), followed by text-based (154). The least common ISA programs delivery method is game-based (32), followed by 'other' delivery method (14).

Table 25. ISA programs delivery method and the associated ISA score levels

ISA Programs delivery method	Count	ISA level (%)
Text-based	154	85
Video-based	**171**	87
Game-based	32	88
Other	14	**91**

The highest ISA score is achieved when research participants use 'other' methods of delivery methods, at 91%. The 'other' delivery methods are indicated in Table 27 below. Research participants in the survey's open-ended questions provided these options listed as 'other'. Following is the game-based delivery method, at 88. The ISA scores for video-based and text-based are 87 and 85 respectively. They are not too far apart from the second-highest ISA score achieved.

Table 26. ISA programs delivery mode: Other

Other
I'm not sure
Phishing exercises
online learning
Meeting room sessions
Presentations and Workshops with professionals
Workshops, voluntary
Presentations by product experts
Training seminars/workshops
Live presentation
Person comes to train
practical training
seminar
Email

4.6 ISA programs frequency and the ISA score Levels

This section discusses the relationship between ISA programs frequency and the ISA scores and the findings from this relationship. This is achieved by using the SPSS scatter plot to view the relationship between the two variables. The scatter plot is shown in Figure 6.

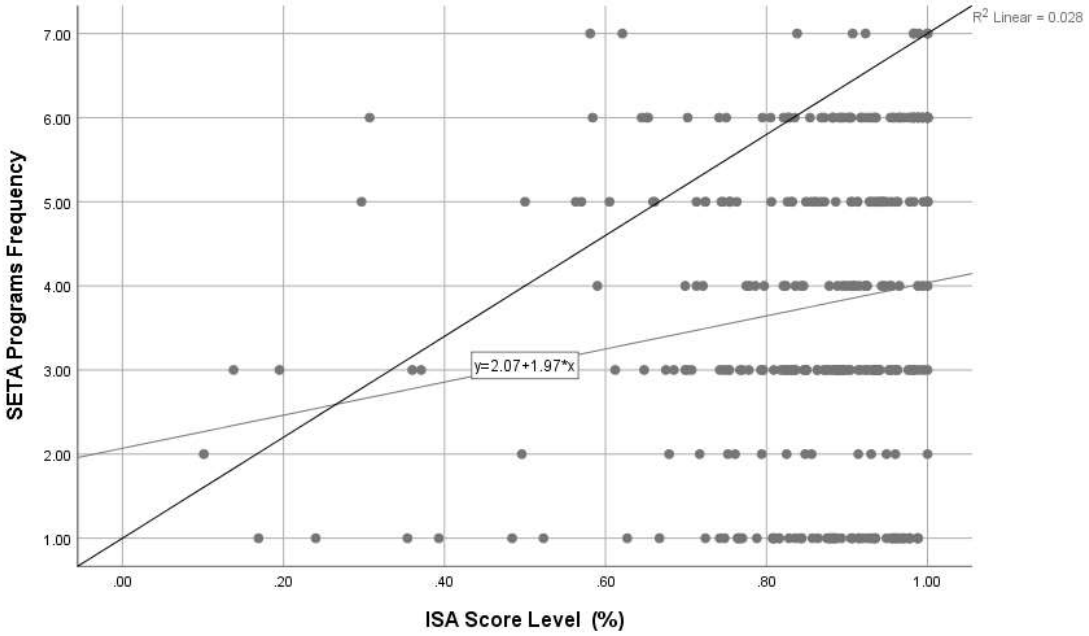

Figure 6. ISA programs frequency and the ISA score

Using the collected data from the online survey, Figure 6 does not indicate a positive nor a negative linear relationship between the ISA programs frequency and the ISA scores – both variables do not increase or decrease together. Moreover, the correlation value r=0.028 is an indication of zero or a very weak correlation between two variables (Kent State university, 2019).

Based on the above-mentioned results, it can be asserted that an increase in ISA programs frequency does not imply a better or higher ISA score. This result is consistent with the previous findings (Pattinson et al., 2019). As a result of this continuous finding, security practitioners can save money and time by focusing on other strategies instead of continuously increasing ISA programs, hoping to improve the organisation's information security posture (Pattinson et al., 2019).

4.7 Pearson Correlation tests and the research propositions

This section of data analysis utilises scatter plots and the Bivariate Pearson Correlation tests to validate the research propositions.

The Bivariate Pearson Correlation test results in a sample correlation coefficient (r) that measures the strength and the direction of a linear relationship between pairs of **continuous variables** (Kent State university, 2019)**.**

The scatter plots and the Bivariate Pearson Correlation tests are generated using SPSS statistics tool.

The data ingested into SPSS belongs to continuous variables. The variables used were ISA scores for knowledge, attitude and behaviour. Moreover, ISA scores for knowledge, attitude and behaviour were divided into end-user preferred (matching) and non-user preferred (non-matching).

As a rule of thumb, it is important that the researcher conforms to the rules and requirements of a statistical test. The rules, pre-checks, and requirements are listed below.

The Bivariate Pearson Correlation objective is to firstly indicate whether a statistically significant linear relationship exists between two continuous variables. Secondly, it indicates the strength or magnitude of a linear relationship – "how close the relationship is to being a perfectly straight line" (Kent State university, 2019). Thirdly, it indicates the direction of the linear relationship – whether it is increasing or decreasing.

The Bivariate Pearson Correlation test has the below data requirements. These data requirements are a pre-requisite and serve as a guide prior to performing a correlation test (Kent State university, 2019).

- Assumption that two or more research variables should be continuous (i.e. interval or ratio variables).
- Cases that have values on both variables.
- There should be a linear relationship between the variables.
- Independent cases – independence of observation:
    - There is no relationship between the values of variables between cases.
    - The Bivariate Pearson Correlation Coefficient and corresponding significance test are not robust when independence is violated.
- Bivariate normality - each pair of variables should be normally distributed.
- The population sample should be a random sample of data, selected from the population.
- Ensure there are no outliers.

In the following sections (4.7.1 – 4.7.4), scatter plots and the Bivariate Pearson Correlation tests are generated. Both the scatter plot and correlation test are used to summarise, validate, and conclude the research propositions.

4.7.1 Scatter Plot and Pearson Correlation Test - Knowledge and Attitude

P_1: Aligning ISA programs to match preferred learning styles and delivery methods is associated with a better impact of knowledge on attitude.

Figure 6, the scatter plot below indicates a slight linear relationship between the knowledge and attitude using the ISA scores, specifically for **matching ISA programs with preferred learning styles**. Similarly, Table 26 shows a Bivariate Pearson Correlation test using knowledge and attitude variables.

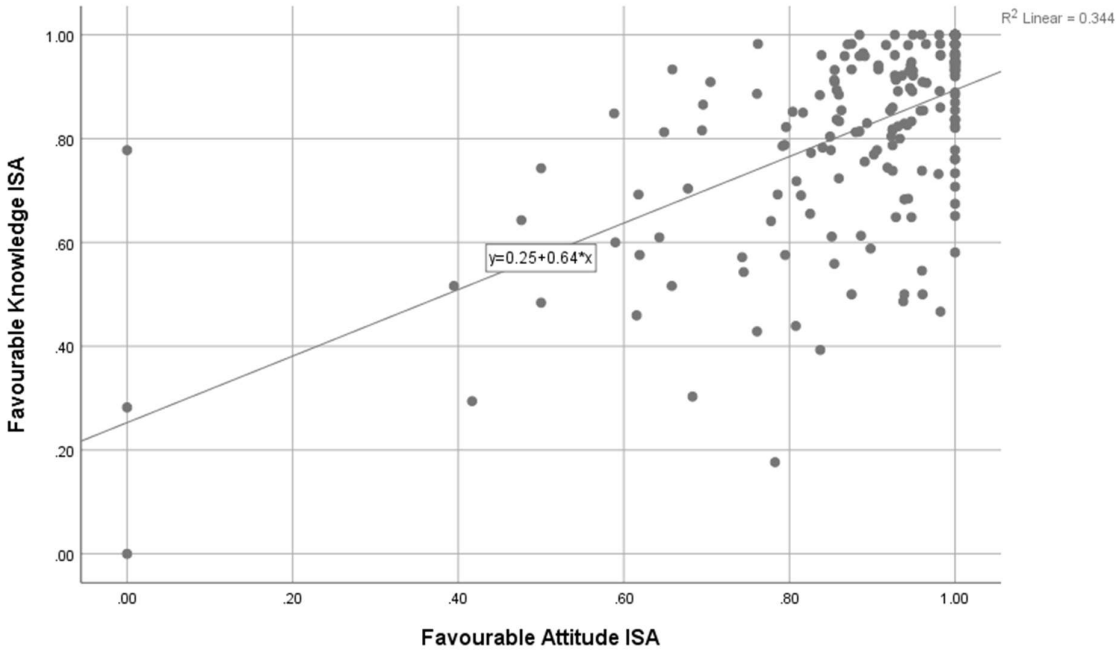

Figure 7. Scatter plot – knowledge and attitude, aligned

Table 27. Bivariate Pearson Correlation test for knowledge and attitude ISA scores, aligned

Pearson Correlation Test - Bivariate			
		Favourable Knowledge ISA	Favourable Attitude ISA
Favourable Knowledge ISA	Pearson Correlation	1	.586**
	Sig. (2-tailed)		.000
	N	194	194
Favourable Attitude ISA	Pearson Correlation	.586**	1
	Sig. (2-tailed)	.000	
	N	194	194
**. Correlation is significant at the 0.01 level (2-tailed).			

Figure 7, the scatter plot below indicates a slight linear relationship between the knowledge and attitude using the ISA scores, specifically for **not matching ISA programs with preferred learning styles**. Similarly, Table 28 shows a Bivariate Pearson Correlation test using knowledge and attitude variables.

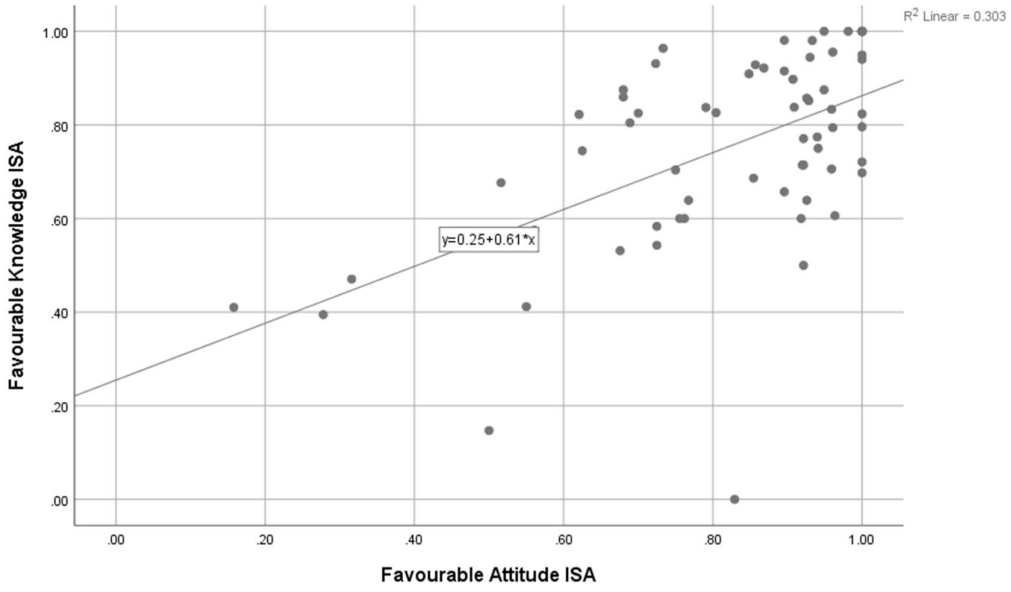

Figure 8. Scatter plot – knowledge and attitude, not aligned

Table 28. Bivariate Pearson Correlation test for knowledge and attitude ISA scores, not aligned

		Favourable Knowledge ISA	Favourable Attitude ISA
Favourable Knowledge ISA	Pearson Correlation	1	.551**
	Sig. (2-tailed)		.000
	N	64	64
Favourable Attitude ISA	Pearson Correlation	.551**	1
	Sig. (2-tailed)	.000	
	N	64	64
**. Correlation is significant at the 0.01 level (2-tailed).			

As indicated in the correlation test tables, SPSS marks a 0.05 significance level with one asterisk (*) and a 0.001 significance level with two asterisks (**). In this case, the significance level is at 0.01(**). Therefore, since the Pearson Correlation Coefficient for knowledge and behaviour are 0.586 (matching) and 0.551 (not matching), which are significant because – p>0.001 for a two-tailed test. In other words, there is a linear relationship between knowledge and attitude when ISA programs are aligned to user-preferred or non-preferred learning styles. However, the correlation coefficient for user preferred ISA learning style is greater (0.586>0.551) than the correlation coefficient of the non-preferred ISA learning style. Therefore, we can deduce and conclude that the learning style mode of ISA programs that is a user-preferred option has a stronger linear relationship, therefore yielding a better information security awareness (ISA score) and posture.

Based on Figure 8 and the Pearson correlation test – Table 29, we can sate the following:

- Regardless of ISA programs' delivery and learning style match, there is a statistically significant linear relationship between information security knowledge and attitude ($p>0.001$).
- The direction of the relationship is positive, which means that these variables (knowledge and attitude) tend to increase together.
- The strength of the association is strong as it falls into the following range ($.5 < | r | ….$).

4.7.2 Scatter Plot and Pearson Correlation Test – Knowledge and Behaviour

P_2: Aligning ISA programs to match preferred learning styles and delivery methods is associated with a better impact of knowledge on end users' behaviour.

Figure 9, the scatter plot below indicates a slight linear relationship between the knowledge and behaviour using the ISA scores, specifically for **matching ISA programs with preferred learning styles**. Similarly, Table 30 shows a Bivariate Pearson Correlation test using knowledge and behaviour variables.

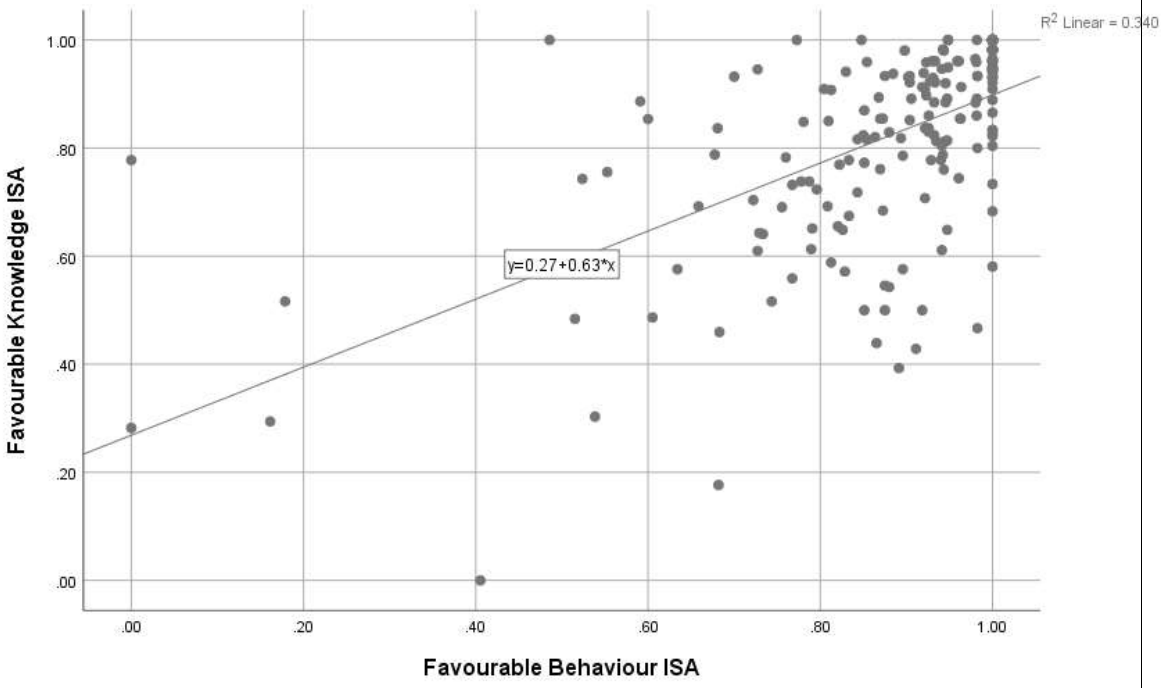

Figure 9. Scatter plot – knowledge and behaviour, aligned

Table 29. Bivariate Correlation test for knowledge and behaviour ISA scores, aligned

		Favourable Knowledge ISA	Favourable Behaviour ISA
Favourable Knowledge ISA	Pearson Correlation	1	.584**
	Sig. (2-tailed)		.000
	N	194	194
Favourable Behaviour ISA	Pearson Correlation	.584**	1
	Sig. (2-tailed)	.000	
	N	194	194
**. Correlation is significant at the 0.01 level (2-tailed).			

Figure 10, the scatter plot below indicates a slight linear relationship between the knowledge and behaviour using the ISA scores, specifically for **not matching ISA programs with preferred learning styles**. Similarly, Table 31 shows a Bivariate Pearson Correlation test using knowledge and behaviour variables.

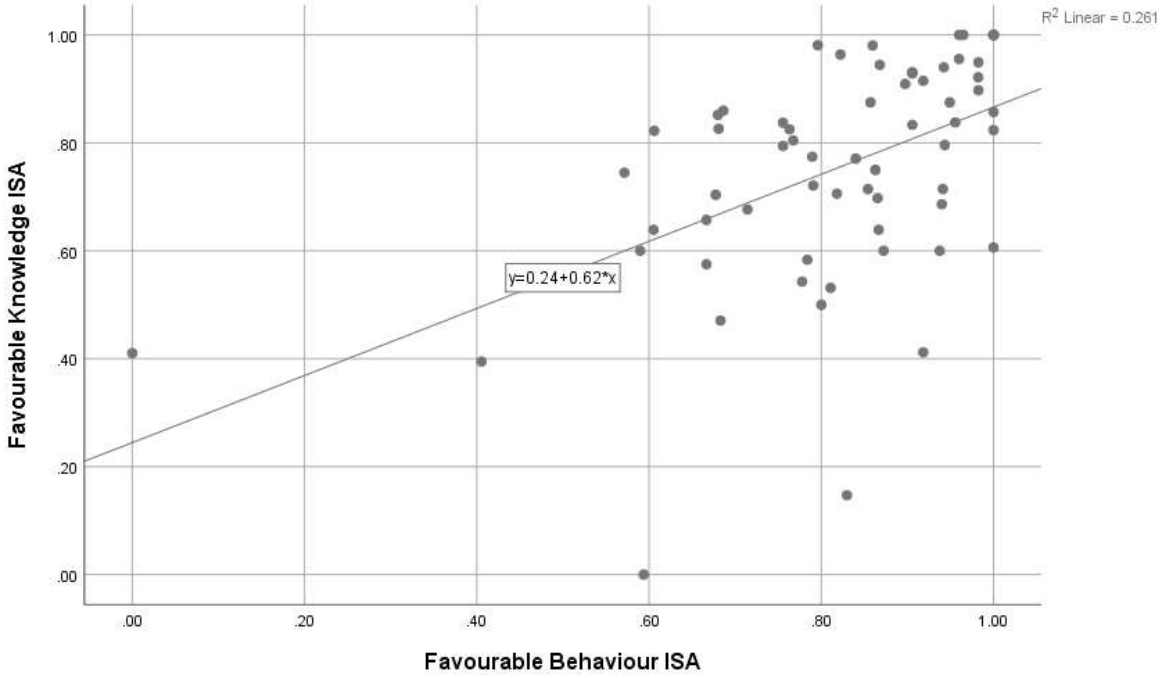

Figure 10. Scatter plot – knowledge and behaviour, not aligned

Table 30. Bivariate Pearson Correlation test for knowledge and behaviour ISA score, not aligned

		Favourable Knowledge ISA	Favourable Behaviour ISA
Favourable Knowledge ISA	Pearson Correlation	1	.511**
	Sig. (2-tailed)		.000
	N	64	64
Favourable Behaviour ISA	Pearson Correlation	.511**	1
	Sig. (2-tailed)	.000	
	N	64	64
**. Correlation is significant at the 0.01 level (2-tailed).			

Since the Pearson Correlation Coefficients for knowledge and behaviour are 0.584 (matching) and 0.511 (not matching), which are significant because of p>0.001 for a two-tailed test. In other words, there is a linear relationship between knowledge and behaviour when ISA programs are aligned to user-preferred or non-preferred learning styles. However, the correlation coefficient for user preferred ISA learning style is greater (0.584>0.511) than the correlation coefficient for user non-preferred ISA learning style. Therefore, we can deduce and conclude that the user preferred learning style mode of ISA has a stronger linear relationship. Therefore, it yields better information security awareness (ISA score) and posture.

Based on the scatter plot – Figure 10 and the correlation test – Table 31, we can sate the following:

- Regardless of ISA programs' delivery and learning style match, there is a statistically significant linear relationship between information security knowledge and behaviour (p>0.001).
- The direction of the relationship is positive, which means that these variables (knowledge and behaviour) tend to increase together.
- The strength of the association is approximately strong as it falls into the following range (.5 < | r | ….).

4.7.3 Scatter Plot and Pearson Correlation Test - Attitude and Behaviour

P3: Aligning ISA programs to match preferred learning styles and delivery methods is associated with a better impact of attitude on end users' behaviour.

Figure 11, the scatter plot below indicates a slight linear relationship between the knowledge and attitude using the ISA scores, specifically for **matching ISA programs with preferred learning styles**. Similarly, Table 32 shows a Bivariate Pearson Correlation test using attitude and behaviour variables.

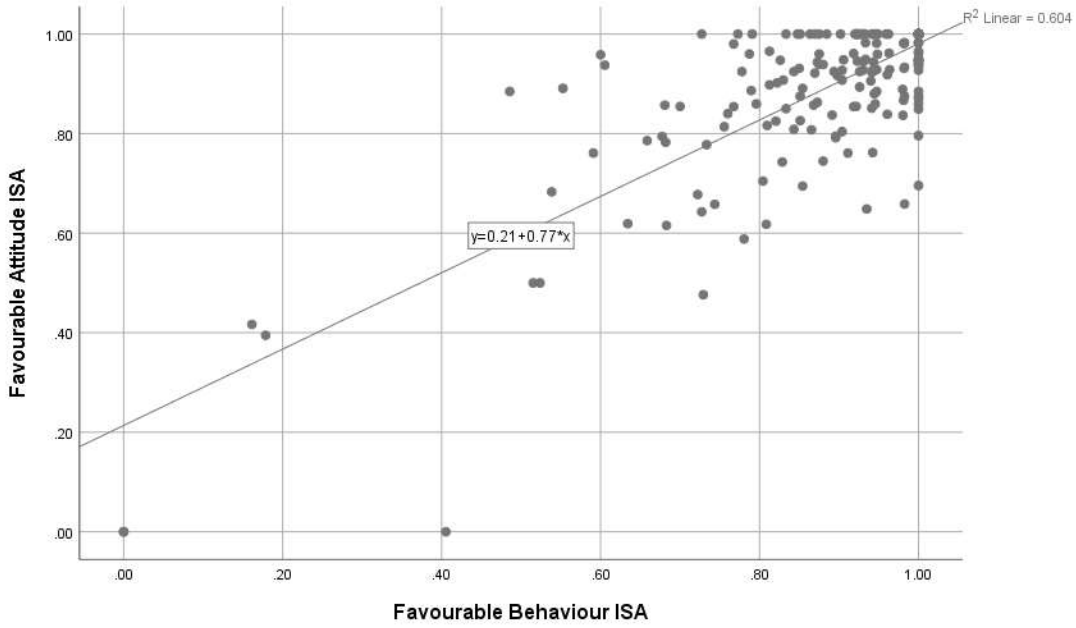

Figure 11. Scatter plot – attitude and behaviour, aligned

Table 31. Bivariate Pearson Correlation for attitude and behaviour of ISA scores, aligned

		Favourable Attitude ISA	Favourable Behaviour ISA
Favourable Attitude ISA	Pearson Correlation	1	.777**
	Sig. (2-tailed)		.000
	N	194	194
Favourable Behaviour ISA	Pearson Correlation	.777**	1
	Sig. (2-tailed)	.000	
	N	194	194
**. Correlation is significant at the 0.01 level (2-tailed).			

Figure 12, the scatter plot below indicates a slight linear relationship between attitude and behaviour using the ISA scores, specifically for **not matching ISA programs with preferred learning styles**. Similarly, Table 33 shows a Bivariate Pearson Correlation test using attitude and behaviour variables.

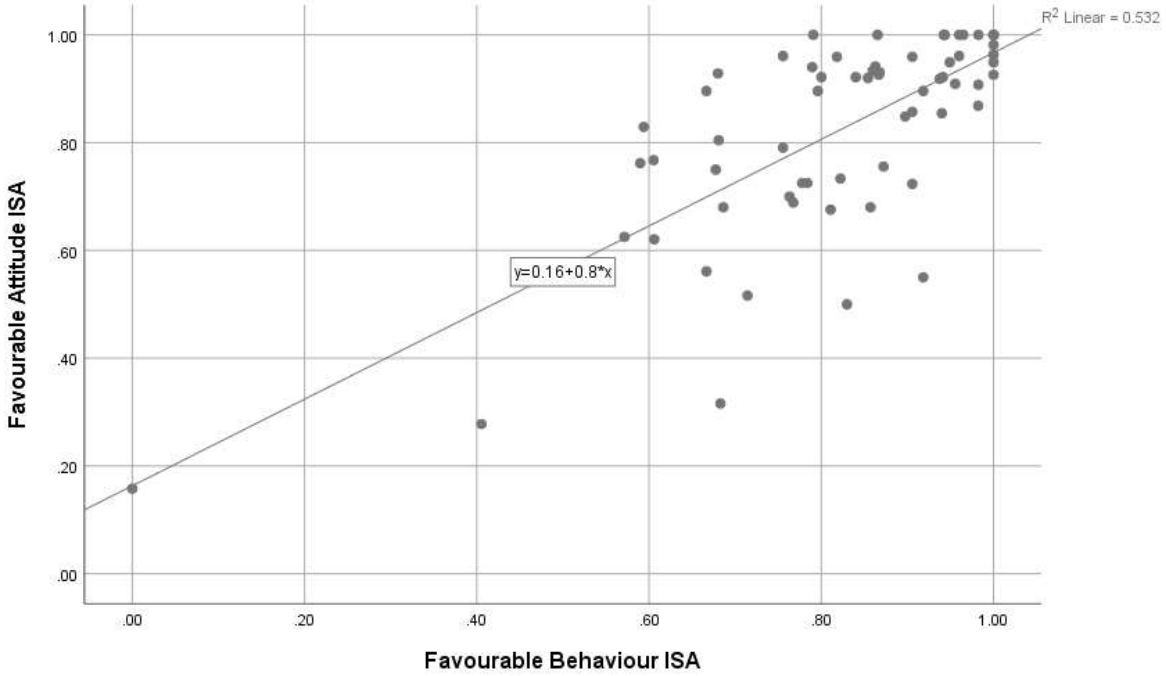

Figure 12. Scatter Plot – attitude and behaviour, not aligned

Table 32. Bivariate Pearson Correlation test for attitude and behaviour of ISA scores, not aligned

		Favourable Attitude ISA	Favourable Behaviour ISA
Favourable Attitude ISA	Pearson Correlation	1	.730**
	Sig. (2-tailed)		.000
	N	64	64
Favourable Behaviour ISA	Pearson Correlation	.730**	1
	Sig. (2-tailed)	.000	
	N	64	64

**. Correlation is significant at the 0.01 level (2-tailed).

Since the Pearson Correlation Coefficient for attitude and behaviour is 0.777 (matching) and 0.730 (non-matching), which is significant because p>0.00 for a two-tailed test. In other words, there is a linear relationship between attitude and behaviour when ISA programs are aligned to user-preferred or non-preferred learning styles. However, the correlation coefficient for matching ISA learning style is greater (0.777>0.730) than the correlation coefficient of the non-matching ISA learning style. Therefore, we can deduce and conclude that the delivery mode of user-preferred ISA programs learning styles has a stronger linear relationship. As a result, there is better information security awareness (ISA score) and posture.

Based on the scatter plot - Figure 12 and the correlation test – Table 33, we can state the following:

- Regardless of ISA programs' delivery and learning style match, there is a statistically significant linear relationship between information security attitude and behaviour (p>0.001).

- The direction of the relationship is positive, which means that these variables (behaviour and attitude) tend to increase together.
- The strength of the association is approximately strong as it falls into the following range (.5 < | r | ….).

4.7.4 Discussion of Findings

As predicted by the KAB model, there is a significant relationship in all cases. As indicated in the research propositions, the scatter plots and the Bivariate Pearson Correlation tests are expected and predicted by the KAB model. There is a significant relationship in all cases – in all the cases, there is a slightly (non-significant) higher correlation coefficient value when delivery matches the provided learning styles.

The afore-mentioned results are consistent with the previous studies. One of the key findings in the study by Pattinson et al. (2018) was the positive influence towards ISA levels when training matched an individual's' learning preferences. However, the study did not indicate a direct comparison of ISA levels between when the training received matched or did not match their learning preference.

In chapter 4, data analysis was completed following the design laid out in section 3, and the findings were discussed.

5. Conclusion

Understanding human behaviour and information security enable the potential to add or extend existing security frameworks and standards (ISO 27000 series, NIST's SP800 or ISACA's COBIT5). This can be achieved by focusing on the human element, which has previously been overlooked. There are security studies which focus on the human aspect, such as thwarting phishing attacks and end-user awareness to combat security risks. However, the proposed KAB model and the findings seek to formalise and convert the model and conclusions into guidelines that could be implemented in real-time to improve information security posture.

This chapter summarises and concludes the research by discussing how research questions and objectives set out in Chapter 1 were addressed and met, respectively. Also, the contributions made and the future research considerations identified through the research.

In Chapter 2, the proposed KAB model depicts the properties of improving security awareness and posture. This is achieved by indicating causal relationships between research constructs. These relationships, also shown in the research propositions, were demonstrated and proven to be correct, empirically. This research revealed the need for properties required to improve information security awareness and posture. The KAB model indicated how these properties can be achieved and adapted in real-world for different types of employees.

In Chapter 3, the research design was discussed. The employed research philosophy, approach, purpose, strategy and the data analysis guided the study to meet the set-out objectives.

In Chapter 4, the effect of aligning ISA programs with user preferred learning styles was shown to be positive. Firstly, the analysis indicated that aligning ISA programs with preferred learning styles is associated with better knowledge and security attitudes. Secondly, aligning ISA programs with preferred learning style is associated with better knowledge and risk-averse behaviour towards security. Thirdly, aligning ISA programs with preferred learning style is associated with a better attitude and risk-averse behaviour towards security.

Additionally, the study tested three propositions through an online survey that collected and analysed data relating to information security awareness through VARK inventory, the delivery modes (text, video and game) and the HAIS-Q to gather ISA score levels. The findings supported and were in line with the propositions. Using Bivariate Pearson correlation tests, it was proven that ISA programs that are aligned to the user-preferred learning style achieve a more excellent ISA score. A higher ISA score is an indication that users have internalised security knowledge, have a better attitude and are risk-averse. A video-based delivery method indicated to be the most common and preferred. However, this delivery method did not yield the highest ISA score. The highest ISA score is achieved through a mixture of delivery methods. This result is consistent with the study by Abawajy (Abawajy, 2014). A higher ISA score indicates a better security awareness, therefore a better security posture.

When ISA programs are adapted to an individual's needs, human error and risky behaviour should be decreased. Additionally, organisational strategies should focus on spending resources on customising content for employees and the organisational context, instead of just increasing ISA programs' frequency.

5.1 Revisiting the Research Questions

In chapter 1, the main research question was posed. To support the main research question, two sub-questions were added. This section revisits the main and sub-questions, ensuring the questions were thoroughly addressed in the study.

Which properties of preferred learning styles influence information security awareness?

This question (first sub-question) was addressed by understanding the learning styles offered to the research participants at their workplaces. Also, the learning styles they prefer when receiving security awareness programs. Using data analysis, the following properties and inferences can be asserted:

Research participants indicated that they receive and prefer a mixture of learning styles. This was shown in the data analysis section.

Research participants with the alignment of user-preferred learning styles and the provided learning styles achieved higher ISA scores at their workplaces. This was depicted in Table 23.

Which properties of information security delivery methods influence information security awareness?

This question (second sub-question) was addressed by understanding the preferred delivery method of security awareness programs. The properties below were identified using data analysis.

The majority of the participants prefer receiving security programs through the video-based delivery method. However, this does not achieve a better ISA score as the case for learning styles. Data analysis results indicated that a better ISA score is achieved when a mixture of delivery methods is utilised.

What effect does ISA programs' alignment with users' preferred learning styles and delivery methods have on security awareness?

Lastly, the main question was addressed by looking into the alignment of both learning styles and delivery methods with security awareness programs.

The KAB model was extended by an additional construct: learning styles and delivery methods. The model depicted the possibility of improving security awareness and organisational security posture by enhancing security knowledge and attitude and improving user behaviour to risk-averse behaviour. This is made possible through the alignment of learning styles and delivery methods with security awareness programs.

Additionally, the empirical data and the Bivariate Pearson Correlation tests proved this correct. The Bivariate Pearson Correlation Coefficients are more significant in all cases where the provided learning styles match the user-preferred learning styles.

5.2 Research Contributions

The study contributes by extending the KAB model to include learning styles and delivery methods. The effectiveness of aligning ISA programs with user preferred learning styles and delivery methods is tested empirically, using a Bivariate Pearson Correlation test. A similar study examined employees in Australia. However, this study is for the South African context.

As a result, we are aware of the learning styles provided and preferred at workplaces in South Africa.

In addition to the above-mentioned, we know that South African employees prefer ISA programs through video delivery method.

The South African organisational employees' security awareness for password management is regarded as a good security awareness (above 80%). It is considered a reasonable security awareness (60 – 79%) for internet and email use. Additionally, attitude and behaviour towards security are rated as good (80%), and security knowledge is regarded as reasonable (73%).

The study indicates areas (through good or poor ISA score performance) where ISA score levels are high and low. This result can be used to plan and improve with better strategies.

5.3 Research Limitations and Recommendations

Since the study only focuses on South Africans (by design), results may not be generalisable to other countries. The existing options for delivery methods, used in this study, may not include a broad enough range that is used in the industry. Separate research should be conducted to examine user-preferred delivery methods used to achieve ISA in organisations.

Instead of relying on self-reported data from surveys, future research can follow a different methodology, such as experimenting. In the experiment, the researcher would provide ISA programs through learning styles aligned and not aligned with research participants' preferences. Then, research participants will undergo HAIS-Q questionnaire testing to capture their ISA score levels. This approach would likely yield a more significant result that is more applicable to the real-world.

6. References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Accenture and Ponemon Institute. (2019). *Ninth Annual Cost of Cybercrime Study Unlocking the Value of Improved Cybersecurity Protection*. 18. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human Computer Studies*, *82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Alshboul, Y., & Steff, K. (2016). Information Security Awareness : Antecedents and Satisfaction Perspective. *Twenty-Second Americas Conference on Information Systems, San Diego*, 2016.

Amankwa, E., Loock, M., & Kritzinger, E. (2016). Enhancing information security education and awareness: Proposed characteristics for a model. *2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec 2015*, 72–77. https://doi.org/10.1109/InfoSec.2015.7435509

Anseel, F., Lievens, F., Schollaert, E., & Choragwicka, B. (2010). Response rates in organizational science, 1995-2008: A meta-analytic review and guidelines for survey researchers. *Journal of Business and Psychology*, *25*(3), 335–349. https://doi.org/10.1007/s10869-010-9157-6

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/J.CHB.2014.05.046

Baranowski, T., Cullen, K. W., Nicklas, T., Thompson, D., & Baranowski, J. (2003). Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts? *Obesity Research*, *11*(S10), 23S-43S. https://doi.org/10.1038/oby.2003.222

Berger, I. E., & Mitchell, A. A. (2002). The Effect of Advertising on Attitude Accessibility, Attitude Confidence, and the Attitude-Behavior Relationship. *Journal of Consumer Research*, *16*(3), 269. https://doi.org/10.1086/209213

Chmura, J. (2017). Forming the Awareness of Employees in the Field of Information Security. *Journal of Positive Management*, *8*(1), 78. https://doi.org/10.12775/JPM.2017.006

Christensen, L. B., Johnson, R. B., & Turner, L. A. (n.d.). *Research Methods, -Design, and Analysis*.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers and Security*, *26*(1), 63–72. https://doi.org/10.1016/j.cose.2006.10.005

Cybersecurity Nexus. (2016). *State of Cybersecurity Implications for 2016 The State of Cybersecurity*.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Dhillon, G., Almusharraf, A., & Samonas, S. (2015). Mismatched understanding of IS security policy: A RepGrid analysis. *2015 Americas Conference on Information Systems, AMCIS 2015*, (2009), 1–12.

Ernst and Young. (2017). Cybersecurity regained: preparing to face cyber attacks. In *20th Global Information Security Survey 2017-18*. Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf

Fin24. (2018). Five massive data breaches affecting South Africans. Retrieved July 31, 2019, from News24 website: https://www.fin24.com/Companies/ICT/five-massive-data-breaches-affecting-south-africans-20180619-2

Foddy, W., & Foddy, W. H. (1994). *Constructing questions for interviews and questionnaires: Theory and practice in social research*. Cambridge university press.

Gholami, S., & Hamzehloei, T. (2013). Hereditary of alpha-1-Antitrypsin deficiency. In *Shiraz E Medical Journal* (Vol. 14). https://doi.org/10.1056/NEJM196802152780701

Gritzalis, D., & Tejay, G. (2013). Cybercrime in the digital economy - Editorial. *Computers and Security*, *38*, 1–2. https://doi.org/10.1016/j.cose.2013.08.002

Haeussinger, F., & Kranz, J. (2017). Antecedents of Information Security Awareness - review, synthesize, and directions for future research. *25th European Conference on Information Systems (ECIS)*, *June 5-10,*.

Holden, M. T., & Lynch, P. (2006). Choosing the Appropriate Methodology: Understanding Research Philosophy. *The Marketing Review*, *4*(4), 397–409. https://doi.org/10.1362/1469347042772428

ITWeb. (2019). City Power hit by ransomware attack | ITWeb. Retrieved July 31, 2019, from ITWeb website: https://www.itweb.co.za/content/GxwQDq1AnVWqlPVo

Kent State university. (2019). SPSS TUTORIALS: PEARSON CORRELATION. Retrieved September 20, 2006, from Kent State University website: https://libguides.library.kent.edu/SPSS/PearsonCorr

Knekta, E., Runyon, C., & Eddy, S. (2019). One size doesn't fit all: Using factor analysis to gather validity evidence when using surveys in your research. *CBE Life Sciences Education*, *18*(1), 1–17. https://doi.org/10.1187/cbe.18-04-0064

Kollmuss, A., & Agyeman, J. (2002). Mind the Gap: Why do people act environmentally and what are the barriers to pro-environmental behavior? *Environmental Education Research*, *8*(3), 239–260. https://doi.org/10.1080/13504620220145401

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5–6), 224–231. https://doi.org/10.1016/J.COSE.2008.05.006

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

Leite, W. L., Svinicki, M., & Shi, Y. (2010). Attempted validation of the scores of the VARK: Learning styles inventory with multitrait-multimethod confirmatory factor analysis models. *Educational and Psychological Measurement*, *70*(2), 323–339. https://doi.org/10.1177/0013164409344507

Lusinga, S., & Kyobe, M. (2015). Towards a Typology for Understanding Mobile Phone Victimisation in South African High Schools. *Inted2015: 9Th International Technology, Education and Development Conference*, 878–893.

Martelli, J., & Greener, S. (2018). *An introduction to Business Research Methods*. Bookboon.

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

Mccusker, K., & Gunaydin, S. (2015). *Research using qualitative , quantitative or mixed methods and choice based on the research*. https://doi.org/10.1177/0267659114559116

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences*, *147*, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers and Security*, *48*, 267–280. https://doi.org/10.1016/j.cose.2014.10.015

Nadeau, M. (2017). *Future cyber security threats and challenges: Are you ready for what's coming?* Retrieved from https://www.csoonline.com/article/3226392/future-cyber-security-threats-and-challenges-are-you-ready-for-whats-coming.html

Orlikowski, W., & Baroudi, J. J. (1991). Studying Information Technology in Organizations : Research Approaches and Assumptions Author (s): Wanda J . Orlikowski and Jack J . Baroudi Published by : INFORMS Stable URL : http://www.jstor.org/stable/23010611 Studying Information Technology in Orga. *Information Systems Research*, *2*(1), 1–28.

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. *Computer & Security*, *66*, 40–51.

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 & Security*, *42*, 165–176. https://doi.org/10.1016/J.COSE.2013.12.003

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The information security awareness of bank employees. *Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016*, (Haisa), 189–198.

Pattinson, M. R., Butavicius, M. A., Parsons, K., McCormac, A., & Jerram, C. (2015).

Examining Attitudes toward Information Security Behaviour using Mixed Methods. *HAISA*, 57–70.

Pattinson, Malcolm, Butavicius, M., Ciccarello, B., & Liilie, M. (2018). Adapting Cyber-Security Training to Your Employees. *Adapting Cyber-Security Training to Your Employees*, 67–71. Human Aspects of Information Security & Assurance (HAISA 2018).

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

PEDIAA. (2017). Difference Between Research Methods and Research Design | Definition, Features, Comparison. Retrieved May 7, 2019, from https://pediaa.com/difference-between-research-methods-and-research-design/

Peyman, H., Sadeghifar, J., Khajavikhan, J., Yasemi, M., Rasool, M., Yaghoubi, M. Y., … Karim, H. (2014). Using VARK approach for assessing preferred learning styles of first year medical sciences students: A survey from Iran. *Journal of Clinical and Diagnostic Research*, *8*(8), 1–4. https://doi.org/10.7860/JCDR/2014/8089.4667

Pinsonneault, A., & Kraemer, K. L. (1993). Survey research methodology in management informationan assessment systems: 10(2), 75(31). doi:1175042. *Journal of Management Information Systems, 10*(2).

PWC. (2015). *2015 INFORMATION SECURITY BREACHES SURVEY*. Retrieved from www.pwc.com.

Rotvold, G. (2008). how to create a security culture in Your Organization. *The Information Management Journal*, *2008*(11/12), 32–38.

Runeson, P. (2014). *A Survey of Unit Testing Practices A Survey of Unit Testing Practices*. https://doi.org/10.1109/MS.2006.91

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

Saunders, M., & Lewis, P. (2012). *Doing Research in Business and Management*. 102–103. https://doi.org/10.1017/CBO9781107415324.004

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (Seventh). Edinburg: Pearson.

Schultz, E. (2005). From the Editor-in-Chief: The Human Factor in Security. *Comput. Secur.*, *24*(6), 425–426. https://doi.org/10.1016/j.cose.2005.07.002

Scrimgeour, J., & Ophoff, J. (2019). *Lessons Learned from an Organizational Information Security Awareness Campaign*. https://doi.org/10.1007/978-3-030-23451-5

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

Sohrabi, N., Solms, R. Von, Furnell, S., Elizabeth, P., & Africa, S. (2016). Information

security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

South African Cyber Security Academic Alliance. (2015). *Welcome to SACSAA* (pp. 1–4). pp. 1–4. Retrieved from http://www.cyberaware.org.za/

South African Government. (2019). Protection of Personal Information Act 4 of 2013 | South African Government. Retrieved March 21, 2019, from Government of South Africa website: https://www.gov.za/documents/protection-personal-information-act

Spears, J., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 503–522.

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

Stone, A. (2018). Solving Cybersecurity's People Problem. Retrieved October 18, 2018, from government technology website: http://www.govtech.com/workforce/Solving-Cybersecuritys-People-Problem.html

SurveyMonkey. (2019). Sample Size Calculator: Understanding Sample Sizes | SurveyMonkey. Retrieved May 12, 2019, from SurveyMonkey website: https://www.surveymonkey.com/mp/sample-size-calculator/

Sutherland, E. (2017). Governance of Cybersecurity – The Case of South Africa. *The African Journal of Information and Communication*, (20), 83–112. https://doi.org/10.23962/10539/23574

Tavakol, M., & Dennick, R. (2011). *Making sense of Cronbach ' s alpha*. 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

Trading Economics. (n.d.). South Africa Employed Persons | 2019 | Data | Chart | Calendar | Forecast. Retrieved May 19, 2019, from Trading Economics website: https://tradingeconomics.com/south-africa/employed-persons

Trček, D., Trobec, R., Pavešić, N., & Tasič, J. F. (2007). Information systems security and human behaviour. *Behaviour & Information Technology*, *26*(2), 113–118. https://doi.org/10.1080/01449290500330299

Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. *20th Americas Conference on Information Systems, AMCIS 2014*, 1–13. Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-84905977874&partnerID=40&md5=355cd1e55d5cbda3d53d82ecc7576f83

Van Kessel, P. (2018). Is cybersecurity about more than protection? Retrieved October 18, 2018, from EY website: https://www.ey.com/en_gl/advisory/global-information-security-survey-2018-2019

VARK Learn Limited. (2014). VARK Modalities. Retrieved February 4, 2019, from VARK Learn Limited website: http://www.vark-learn.com/english/page.asp?p=categories

Ven, A. Van de, Adner, R., Barley, S., Dougherty, D., Fountain, J., Hargadon, A., … Schilling, M. (2017). Increasing benefits & reducing social costs of technological innovations. *Behavioral Science & Policy*, *3*(1), 92–103. https://doi.org/10.1353/bsp.2017.0008

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

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

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research*, *10*(1), 69–80. https://doi.org/10.1675/1524-4695(2008)31

Whitman, M. E., & Mattord, H. J. (2014). Management of information. In *College and Research Libraries* (4th ed., I, Vol. 50). https://doi.org/10.5860/crl_50_05_521

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. https://doi.org/10.33151/ajp.8.3.93

Wood, J. (2004). Cultural change in the governance of security. *International Journal of Phytoremediation*, *21*(1), 31–48. https://doi.org/10.1080/1043946042000181548

Yellow, C. M., & Bell, J. (n.d.). *Cyan Magenta Yellow Black PRINT CMYK PROCESS COLOURS Open UP Study Skills 216 X 135 format*.

Appendix A - Cyber-security Learning Styles Inventory

Item	Response option
Q: 1 You are participant in training that includes a test you are required to pass. You would learn most	Seeing examples (V)
	Listening to the presenter (A)
	Reading written instructions
	Watching a demonstration(K)
Q: 2 Remember a time when you learned how to do something new a computer. You learned best by	Watching a demonstration(K)
	Listening to somebody explaining it and asking questions (A)
	Looking at visual cues, e.g diagrams or charts (V)
	Reading written explanations, e.g. a manual or blog (R)
Q: 3 You want to learn a new computer programme. You would	Read the written instructions that came with the programme (R)
	Talk with people who know about the programme (A)
	Learn how to use it through trial and error (K)
	Follow the diagrams in the instructions (V)
Q: 4 I like websites that have	Things I can click on or interact with (K)
	Interesting design and visual features (V)
	Interesting written descriptions, lists or explanations (R)
	Audio channels where I can hear podcasts, radio programmes or interviews (A)
Q: 5 Do you prefer a presenter or instructor who uses	Demonstrations or practical sessions (K)
	Question and answer sessions or guest discussions (A)
	Handouts, books or readings (R)
	Diagrams, charts or graphs (V)
Q: 6 You have completed a test at the end of a training course and would like to receive feedback. You would like to receive feedback by	Having your results displayed visually, e.g. on graphs or diagrams (V)
	Using examples from what you have done(K)
	Having someone talk you through it (A)
	Using a written description of your results (R)

Appendix B – Survey Approval Letter

Faculty of Commerce
Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: com-faculty@uct.ac.za
Internet: www.uct.ac.za
@Commerce UCT UCT Commerce Faculty Office

21st June 2019

Mr Blaise Ntwali
Department of Information Systems
University of Cape Town

Dear Mr Ntwali

REF: REC 2019/000/055

IMPROVING INFORMATION SECURITY POSTURE BY ALIGNING SETA LEARNING STYLES AND DELIVERY METHODS

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid for 1 year and may be renewed upon application.

Please be aware that you need to notify the Ethics Committee immediately should any aspect of your study regarding the engagement with participants as approved in this application, change. This may include aspects such as changes to the research design, questionnaires, or choice of participants.

The ongoing ethical conduct throughout the duration of the study remains the responsibility of the principal investigator.

We wish you well for your research.

Shandre Swain
Administrative Assistant
University of Cape Town
Commerce Faculty Office
Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695 / 4375
Office Fax: +27 (0)21 650 4369
E-mail: sl.swain@uct.ac.za
Website: www.commerce.uct.ac.za<http://www.commerce.uct.ac.za/>

"Our Mission is to be an outstanding teaching and research university, educating for life and addressing the challenges facing our society."

Appendix C – Survey Introduction Letter

Department of Information Systems

Leslie Commerce Building

Engineering Mall, Upper Campus

OR

Private Bag. Rondebosch 7701

Tel: +27 (0) 21 650 4028 Fax: +27 (0) 21650 2280

Internet: http://www.commerce.uct.ac.za/informationsystems/

Dear participants

Welcome and thank you for your involvement in this short survey. The study aims to explain how the preferred delivery of Information Security Education, Training and Awareness (SETA) and the matching learning styles can improve information security posture in South Africa. Furthermore, the study findings are aimed at improving user behavioural intentions to a risk-averse behaviour by focusing on knowledge and attitude towards information security.

This research has been approved by the Commerce Faculty Ethics in Research Committee. Your participation in this research is voluntary. You can choose to withdraw from the research at any time. The questionnaire will take approximately 5 to 10 minutes to complete. You will not be requested to supply any identifiable information, ensuring the anonymity of your responses.

Thank you for your time and participation. Should you have any questions regarding the research, please feel free to contact the researcher on ntwbla001@myuct.ac.za.

Blaise Ntwali

Masters Student

Department of Information Systems

University of Cape Town

Email:ntwbla001@myuct.ac.za

Dr Jacques Ophoff

Email: Jacques.ophoff@uct.ac.za

Research Supervisor

Department of Information Systems

University of Cape Town

Appendix D – Questionnaire

Start of Block: Welcome Page

Dear participants

Welcome and thank you for your involvement in this short survey. The study investigates how the preferred delivery of information Security Education, Training and Awareness (SETA) and the matching learning styles affect information security posture in South Africa.

This research has been approved by the Commerce Faculty Ethics in Research Committee. Your participation in this research is voluntary. You can choose to withdraw from the research at any time. The questionnaire will take approximately 5 to 10 minutes to complete. You will not be requested to supply any identifiable information, ensuring the anonymity of your responses. Thank you for your time and participation. Should you have any questions regarding the research, please feel free to contact the researcher on ntwbla001@myuct.ac.za.

Requirements for participating and completing this survey, you must:

- Be between the age of 18 and older
- Be employed and living in South Africa

Regards

Blaise Ntwali

Email:ntwbla001@myuct.ac.za

Masters Student

Department of Information Systems

University of Cape Town

Dr Jacques Ophoff

Email: Jacques.ophoff@uct.ac.za

Research Supervisor

Department of Information Systems

University of Cape Town

End of Block: Welcome Page

Start of Block: Test Question

2 Are you currently employed and living in South Africa ?

- ○ Yes (1)
- ○ No (2)

Skip To: End of Block If Are you currently employed and living in South Africa ? = No

End of Block: Test Question

Start of Block: Section A : Demographics

3 What is your current age?

- ○ 18 – 29 (1)
- ○ 30 – 39 (5)
- ○ 40 – 49 (6)
- ○ 50 – 59 (7)
- ○ 60 and over (8)

4 What is your gender?

- ○ Male (1)
- ○ Female (2)
- ○ Prefer not to answer (3)

5 Level of Education:

- ○ High School or Lower (1)
- ○ Diploma/College graduate (2)
- ○ Bachelor Degree (3)
- ○ Postgraduate and Higher (4)

6 Ethnic group/race:

- ○ African (1)
- ○ White/Caucasian (2)
- ○ Asian (3)
- ○ Indian (4)
- ○ Coloured (5)
- ○ Prefer not to answer (6)

7 Which of the following best describes your current primary occupation ? (Please select one)

- ○ Protective Service Occupations (1)
- ○ Healthcare Practitioners and Technical Occupations (4)
- ○ Sales and Related Occupations (5)
- ○ Architecture and Engineering Occupations (6)
- ○ Management Occupations (7)
- ○ Business and Financial Operations Occupations (8)
- ○ Life, Physical, and Social Science Occupations (9)
- ○ Education, Training, and Library Occupations (10)
- ○ Healthcare Support Occupations (11)
- ○ Installation, Maintenance, and Repair Occupations (12)
- ○ Building and Grounds Cleaning and Maintenance Occupations (13)
- ○ Computer and Mathematical Occupations (14)
- ○ Food Preparation and Serving Related Occupations (15)
- ○ Arts, Design, Entertainment, Sports, and Media Occupations (16)
- ○ Personal Care and Service Occupations (17)
- ○ Farming, Fishing, and Forestry Occupations (18)
- ○ Office and Administrative Support Occupations (19)
- ○ Community and Social Service Occupations (20)
- ○ Construction and Extraction Occupations (21)

- ○ Production Occupations (22)
- ○ Legal Occupations (23)
- ○ Transportation and Materials Moving Occupations (24)
- ○ Other (please specify) (25)

_____

End of Block: Section A : Demographics

Start of Block: Section B: Learning Styles

8 Choose the answers that best describe your preference when *learning about using computers for work*. For each statement, please select *more than one* if a single answer does not match your preference.

9 You are participating in training that includes a test that you are required to pass. You would learn from:
(Please select one or more)

- ☐ Seeing examples (1)
- ☐ Listening to the presenter (2)
- ☐ Reading written instructions (3)
- ☐ Watching a demonstration (5)

10 Remember a time when you learned how to do something new on a computer. You learned best by:
(Please select one or more)

- [ ] Watching a demonstration (1)
- [ ] Listening to somebody explaining it and asking questions (2)
- [ ] Looking at visual cues, e.g., diagrams or charts (3)
- [ ] Reading written explanations, e.g., a manual or blog (4)

---

11 If you want to learn a new computer program. You would:
(Please select one or more)

- [ ] Read the written instructions that came with the program (1)
- [ ] Talk with people who know about the program (2)
- [ ] Learn how to use it through trial and error (3)
- [ ] Follow the diagrams in the instructions (4)

---

12 I like websites that have:
(Please select one or more)

- [ ] Things I can click on or interact with (1)
- [ ] Interesting design and visual features (2)
- [ ] Interesting written descriptions, lists or explanations (3)
- [ ] Audio channels where I can hear podcasts, radio programs or interviews (4)

13 Do you prefer a presenter or instructor who uses: (Please select one or more)

- ☐ Demonstrations or practical sessions (1)
- ☐ Questions and answers sessions or guest discussions (2)
- ☐ Handouts, books, or readings (3)
- ☐ Diagrams, charts or graphs (4)

14 You have completed a test at the end of a training course, and would like to receive feedback. You would like to receive feedback by: (Please select one or more)

- ☐ Having your results displayed visually, e.g., on graphs or diagrams (1)
- ☐ Using examples from what you have done (2)
- ☐ Having someone talk you through it (3)
- ☐ Using a written description of your results (4)

End of Block: Section B: Learning Styles

Start of Block: Section C: Information Security Training

15

How frequently does your place of work provide information security education, training or awareness programs?
(Please select one)

- ○ Never (1)
- ○ Every two years (8)
- ○ Annually (9)
- ○ Twice a year (10)
- ○ Every three months (11)
- ○ At least once a month (12)
- ○ Other (please specify) (13)

_____

Display This Question:

If How frequently does your place of work provide information security education, training or aware... != Never

16 What is the method used to deliver security education, training and awareness programs at your place of work?
(Select one or more)

- ☐ Text-based (e.g., infographics, posters, newsletters) (1)
- ☐ Video-based (e.g., e-learning courses, simulations) (2)
- ☐ Game-based (e.g., educational video games) (3)
- ☐ Other (please specify) (4)

_____

Display This Question:

If How frequently does your place of work provide information security education, training or aware... != Never

17 Please indicate whether the following statements apply to the security education, training and awareness programs that you have received in your place of work?(Select one or more)

- ☐ They include speaking and listening (e.g., discussions, seminars) (1)
- ☐ They include reading or writing (e.g., handouts, note-taking) (5)
- ☐ They include visual depiction of information (e.g., diagrams, graphs, charts) (6)
- ☐ They include experience and practice, either simulated or real (e.g., real-life examples, demonstrations, guest lecturers) (7)

End of Block: Section C: Information Security Training

Start of Block: Focus area: Password management, Email and internet use. Knowledge

18 The following statements are about your **knowledge** of how you should use a computer at work.

19 Please indicate your level of agreement with the following statements:

	Strongly agree (2)	Agree (3)	Somewhat agree (4)	Neutral (5)	Somewhat disagree (6)	Disagree (7)	Strongly disagree (8)
It's acceptable to use my social media passwords on my work accounts (1)	○	○	○	○	○	○	○
I am allowed to share my work passwords with colleagues (2)	○	○	○	○	○	○	○
A mixture of letters, numbers and symbols is necessary for work passwords (3)	○	○	○	○	○	○	○

20 Please indicate your level of agreement with the following statements:

	Strongly agree (2)	Agree (3)	Somewhat agree (4)	Neutral (5)	Somewhat disagree (6)	Disagree (7)	Strongly disagree (8)
I am allowed to click on any links in emails from people I know (1)	○	○	○	○	○	○	○
I am not permitted to click on a link in an email from an unknown sender (2)	○	○	○	○	○	○	○
I am allowed to open email attachments from unknown senders (3)	○	○	○	○	○	○	○

21 Please indicate your level of agreement with the following statements:

	Strongly agree (2)	Agree (3)	Somewhat agree (4)	Neutral (5)	Somewhat disagree (6)	Disagree (7)	Strongly disagree (8)
I am allowed to download any files onto my work computer if they help me to do my job (1)	○	○	○	○	○	○	○
While I am at work, I shouldn't access certain websites (3)	○	○	○	○	○	○	○
I am allowed to enter any information on any website if it helps me do my job (5)	○	○	○	○	○	○	○

End of Block: Focus area: Password management, Email and internet use. Knowledge

Start of Block: Section D

Start of Block: Focus area: Password management, Email and internet use. Attitude

22 The following statements are about your **attitude**. You've told us about your knowledge of computer use guidelines. Now please tell us what you think about these guidelines.

23 Please indicate your level of agreement with the following statements:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neutral (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
It's safe to use the same password for social media accounts (4)	○	○	○	○	○	○	○
It's a **bad idea** to share my work passwords, even if a colleague asks for it (5)	○	○	○	○	○	○	○
It's safe to have a work password with just letters (6)	○	○	○	○	○	○	○

24 Please indicate your level of agreement with the following statements:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neutral (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
It's always safe to click on links in emails from people I know (4)	○	○	○	○	○	○	○
Nothing bad can happen if I click on a link in an email from unknown sender (5)	○	○	○	○	○	○	○
It's risky to open an email attachment from an unknown sender (6)	○	○	○	○	○	○	○

25 Please indicate your level of agreement with the following statements:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neutral (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
It can be risky to download files on my work computer (4)	○	○	○	○	○	○	○
Just because I can access a website at work, doesn't mean that it's safe (5)	○	○	○	○	○	○	○
If it helps me to do my job, it doesn't matter what information I put on a website (6)	○	○	○	○	○	○	○

End of Block: Focus area: Password management, Email and internet use. Attitude

Start of Block: Focus area: Password management, Email and internet use. Behaviour

26 The following statements are about your **behaviour**. You've told us what you know, and what you think about computer use guidelines. Now please tell us what you do when using a computer at work.

27 Please indicate your level of agreement with the following statements:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neutral (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
I use a different password for my social media and work accounts (1)	○	○	○	○	○	○	○
I share my work passwords with colleagues (2)	○	○	○	○	○	○	○
I use a combination of letters, numbers and symbols in my work passwords (3)	○	○	○	○	○	○	○

28 Please indicate your level of agreement with the following statements:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neutral (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
I don't always click on links in emails just because they come from someone I know (1)	○	○	○	○	○	○	○
If an email from an unknown sender looks interesting, I click on a link with it (2)	○	○	○	○	○	○	○
I don't open email attachments if the sender is unknown to me (3)	○	○	○	○	○	○	○

29 Please indicate your level of agreement with the following statements:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neutral (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
I download any files onto my work computer that will help me get the job done (1)	○	○	○	○	○	○	○
When accessing the Internet at work, I visit any websites that I want to (2)	○	○	○	○	○	○	○
I assess the safety of websites before entering information (3)	○	○	○	○	○	○	○

End of Block: Focus area: Password management, Email and internet use. Behaviour