Examining the attitudes of employees towards information security and cybersecurity threats in the financial services industry

Moroka William

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2019 - 2020

(Version 2019-2020)

ABSTRACT

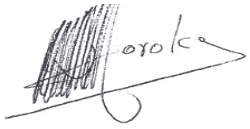
The financial services industry in South Africa is the prime target of cyber-attacks to steal information, money, compromising customer data and disrupting operations. Employees in this industry have been identified as the weakest link and responsible for successful malware attacks mostly distributed via e-mails. Awareness of the recent cyber-threats is a key defence in the protection of employees and systems. The study examined the attitude of employees towards information security and cybersecurity threats in the financial services industry. A questionnaire tested employees on four variables: cyber threats, cybersecurity awareness; cybersecurity behaviour and employee attitude. The responses revealed limited cybersecurity awareness and employees' negative attitude towards policy measures. The findings demonstrate the need for information management systems and cybersecurity training programs across the financial services industry.

KEY WORDS

Cybersecurity, Malicious emails, Internet of Things, Information Security, Malware

DECLARATION

I, Moroka William, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Moroka William Signature: 

Signed at ……Bloemfontein……

On the ……15… day of ……April…… 2020

DEDICATION

I dedicate my research work to my late grandfather, Boedile Moroka. A special feeling of gratitude to my mother, Sejabaledi Moroka whose presence give meaning to my life.

ACKNOWLEDGEMENTS

I would like to thank the following people without whom this research would not have been possible:

- Melba Moroka, for her love, undivided support and patience.
- My children, for always understanding.
- My supervisor: Dr Tweneboah for his advice.
- Johan Hartzer for his support and inspiration.
- Ivor, Reuben and Sjanel for your data collection assistance
- All the participants for their support and cooperation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

Botnet – Robot and Network

CIA – Confidentiality, Integrity and Availability

DDos – Distributed Denial-of-Service

DNS – Domain Name Server

FinTech – Financial Technology

IEC – International Electrotechnical Commission

IoT – Internet of Things

IS – Information Security

ISMS – Information Security Management System

ISO – International Organisation for Standardization

IT – Information Technology

PDCA – Plan-Do-Check-Act

PwC – PricewaterhouseCoopers

RACI – Responsible-Accountable-Consulted and Informed

RegTech – Regulatory Technology

RQ – Research Question

SABRIC – South African Banking Risk Information Centre

SPSS – Statistical Package for Social Sciences

CHAPTER 1. INTRODUCTION

1.1 Purpose of the study

The purpose of this cumulative study is to expand body of knowledge according to different aspects of information security awareness to improve the understanding of cybersecurity knowledge and attitudes of employees towards cybersecurity threats in the financial services industry. The study encompasses three research reports on cyber-crimes, technological transformation in the financial services industry and the current state of cybersecurity within the sector. Therefore the three interrelated researches formulates a series of research questions which is directed at aspects of the topic and enable the study to do extensive review of literature, proposing research models that addresses different gaps in information security.

1.2 Context of the study

The South African banks, investments and insurance companies are the prime targets of cyber-attacks to steal information, money, disrupting operations, destroying critical infrastructure and compromising customer data. According to the South African Banking Risk Information Centre (SABRIC) annual crime stats, South Africa is ranked third globally for the number of cybercrime victims and the report quoted an estimated R2.2 billion loss a year between customers and businesses within the financial services industry (Sabric, 2018).

A separate research conducted by Deloitte Center for Financial Services singled out the massive technological transformation in the financial services industry that is driven by the use of financial technology (FinTech), regulatory technology (RegTech), mobile applications, platforms and other emerging developments as reasons behind increase in cyber-attacks quantity and sophistication (Deloitte, 2018).

The PricewaterhouseCoopers (PwC) report on cybersecurity in the financial services industry highlighted the sector as being ahead of many industries in

terms of prevention and detection of financial crimes through continuous development of software and hardware preventative measures (PwC, 2019). However, cyber-attacks and breaches are becoming a daily occurrence with cyber-attackers using variety of tactics to overcome traditional security measures. Contrary to the PwC report, research indicates that traditional security measures such as firewalls and antivirus software are gradually proving to be inadequate in the evolving threat landscape (Biscoe, 2018). Biscoe (2018) is supported by research and analysis conducted by Kaspersky Lab, a global cybersecurity company that reported an increased malware attacks in South Africa by 22% in the first quarter of 2019 as compared to the same quarter in 2018 (Kaspersky Lab, 2019).

Besides all the statistical context, the study is also influenced by the reported cyber-attacks incidents of the recent years in the industry with the background of technical weaknesses that were exploited. Table 1 provides a summary of these incidents. The summary indicates the timeline of attacks, background and reported losses of the respected organisations within the industry.

Table 1: Timeline of cyber-attacks in the Financial Services industry

Year	Financial institute	Background
2003	**ABSA**	Access to Internet banking profile was gained and reported R530 000 was stolen from customer through e-mails containing spyware.
2010	**LandBank**	Hackers gained access using Land Bank passwords obtained through the help of an insider. There was an unsuccessful attempt to steal R150 million from the bank.
2012	**PostBank**	The bank lost R42 million were Postbank employee used computer of a colleague during Christmas break.
2016	**Standard Bank**	A highly sophisticated and coordinated attack by a Japanese cyber-criminal syndicate that resulted to the bank losing R300 million through ATM fraud.
2017	**Old Mutual**	Unauthorised entry to one of the company systems which led to access to customer information.
2018	**Liberty**	Hackers accessed the organisational e-mail servers and obtained e-mail addresses for both internal staff and customers.

Year	Financial institute	Background
2019	**Standard Bank/ABSA**	Both banks reported a DDoS attack that resulted to delay in transactions and some of their services experience downtime. Value of the loss was not reported by both banks.

The technology aspect of cybersecurity and information security is a well-researched topic, however, the background of the South African attacks on this timeline expose the human factors as one of the key aspects of the losses (Kaspersky Lab, 2019). The cyber-attacks and breaches covered by PwC report underlined that all the attacks take advantage of employees' knowledge and behaviour while posing significant risks to the industry (PwC, 2019). Based on the level of employee knowledge on cybersecurity and information technology, the attackers use low technology techniques to get access to different systems (PwC, 2019).

The use of low technology methods is common in the financial services industry to take advantage of employees to access information assets (Jones and Towse, 2018). These low technology methods influence the study and part of the risk factors exposing employees as a weak link in protecting information assets (Jones and Towse, 2018). These low technology methods are listed in Table 2.

Table 2: Low technology methods common in the financial industry (Jones and Towse, 2018)

METHODS	DESCRIPTIONS
Internal threats	Refers to both current and former employees gaining unauthorised access to confidential data or sensitive information, including infiltrating the organisation's network with mischievous intents. Attackers use existing employees with access to systems for infecting machines with malicious software.
Social engineering	In this method, the attackers pose as internal employees to obtain access to the network. The common technique is used by attackers presenting themselves as IT Security staff asking for a network password.

METHODS	DESCRIPTIONS
Baiting	Attackers access and use information captured about employees to trick them into revealing passwords or access to networks. The common technique is using information of a senior manager to target junior employees.
Unsubscribe buttons	Attackers coax targeted employees into downloading malwares by hiding links to malware sites in e-mails unsubscribe buttons. The common technique is flooding an employee's inbox with promotional e-mails to trigger the need to unsubscribe.
Keyloggers	Software programme designed to secretly monitor and log all keystrokes. The technique records and stores strokes of a keyboard to pick up sensitive data such as passwords and e-mail identities.

The constant use of e-mails as line of communication in the financial services remain a link between the technical aspects of information security and human factors which is a vector to initiate attacks such as malware delivery, impersonations and phishing attacks. The 2019 Mimecast research on the state of e-mail predicted that 59% of organisations in South Africa will suffer a negative business impact from an e-mail borne attack (Mimecast, 2018). The same study further underlined 61% of the organisations used in their sample were hit by cyber-attack and the malicious activity was spread from one infected user to other employees via e-mail.

Human factor plays an important role in cybersecurity. However, cybersecurity has not been given focus in the literature with regards to human factor outcome and researchers have called for more examination in this area. In view of the consequences of cyber-attacks and threats, many employees who lack awareness and knowledge, consequently, are ignorant of the need to protect their organisations against cyber threats (Sabillon, Serra-Ruiz and Cavaller, 2019). Furthermore, the employees' insecure online attitudes and behaviour makes them the weakest link and easy target for exploitation.

The rationale employed in the study is based on a premium South African financial services group that offers a broad spectrum of financial solutions to retail

and corporate customers across key markets in Africa. The employees of this organisation was therefore used as research population to represent the financial services industry. It is against this background that this research focused on the impact of employees' attitudes towards and knowledge of cyber-security threats on organisations in the financial services industry.

1.3 Research problem

The common practice in the financial services industry is to focus on the newest available technology in the market as a way to combat both cybersecurity threats and technological risks. The industry is known for investments in highly sophisticated hardware and software protection against cyber threats. However, the level of investment in risk management processes and the adequacy of employees training is not publicly communicated and researched (PwC, 2019). The implementation of this hardware and software protection system follow strong frameworks and well researched processes. However, the link between the sophistication of this technology and employees as the human factors of the security measure is not given enough attention.

Organisations in the financial services industry invest large amounts of money to ensure high level of data security and security information systems, however, lack of human security culture is the missing link in their cybersecurity efforts (Glaspie and Karwowski, 2017). Different studies in literature emphasise the view that organisations must ensure a mix of technical systems and human behavioural aspects of cybersecurity management in order to establish information security culture (Glaspie and Karwowski, 2017). There is limited studies in literature that examined the connotation between human factors in cybersecurity in the organisation and the technical aspect of information security which opens a gap in their information security management system. This study aims to examine the attitudes of employees through their level of cybersecurity awareness in terms of different cyber threats.

1.4 Research questions

The purpose of this research was to explore the readiness of the South African financial sector for flexible working conditions according to different aspects of information security. Therefore the study encompasses three interrelated topics about cybersecurity awareness, aspects of cyber threats and cybersecurity behaviour to give separate detailed discussion of the findings and their implications to this study. The in-depth analysis of the literature encompasses the following two main questions:

Research Question 1: What is the current state of cybersecurity awareness for employees in the financial services industry?

a) **What is the level of understanding in the aspects of malware, passwords usage, phishing, social engineering and online scam?**

Research Question 2: How does employees' attitudes relate to cybersecurity threats?

The first question creates a synthesised review of the current state of cybersecurity awareness literature with the purpose to provide accumulated knowledge of information security to different levels of management in the financial services industry and reveal potential areas for further research. The sub-question conceptualises how literature defines different aspects of cybersecurity threats while having a closer look at the existing body of knowledge regarding the question and provide a better understanding of individual threats in relation to cyber security awareness. The second research question is important to give insight on employee attitude that can help security managers to identify the best fitting approach to cybersecurity training as well as the effectiveness of different information security strategies.

The researcher takes into consideration the view of the study null hypothesise that employees in the financial services industry have unlimited understanding of the latest cybersecurity threats and their attitudes towards mitigation are positive. The study answered the abovementioned research questions by testing the null hypothesis against the following alternative hypotheses:

- **Hypothesis 1:** Employees in the financial services industry have limited understanding of the latest cybersecurity threats.
- **Hypothesis 2:** Employees' attitudes towards cybersecurity threats influence their intention to comply with the cybersecurity information and training.

1.5 Significance of the study

The study is guided by literature and is conducted within the context of CIA Triad model used in identifying problem areas within the cybersecurity landscape. The CIA Triad model is a security model that highlights core data security objectives and the acronym refers to Confidentiality, Integrity and Availability.

- The protection of **confidentiality** in the financial services industry is dependent on the organisation being able to define access levels of information, access control lists and file encryption (Cherdantseva and Hilton, 2013).
- **Integrity** in the model is an essential component designed to protect data from modification by unauthorised party.
- The final component of the triad is **availability** which is about authentication mechanisms, access channels and ensuring that systems within the organisation function properly for the information they protect.

The CIA Triad model is the component of security used to plan and implement quality security policies within organisations. The three components of security work well together in protecting organisations against external cyber threats, however, employees are identified as the weakest link of the security. The study is looking at knowledge and awareness of employees in the latest cyber threats against the industry. The significance of the study is in identifying human elements that can compromise one or all of the CIA triad principle. The findings of this study will be of great benefit to organisations and employees:

- **Organisations in the Financial Services Industry** – The results of this study will assist organisations in improving security protocols and ensure that employees are compliant to protect the operational ability of the organisations and key customer information (Korpela, 2015). The best security protocols are

comprehensive and holistic by incorporating hardware, software and human measures to avoid potential security threats (Korpela, 2015). The study is intended to be of value to enable the researcher to recommend comprehensive, holistic and the best possible cybersecurity frameworks and models for the financial services industry.

- **Employees in the Financial Services Industry** – The findings of the study will be beneficial to the financial services industry by improving attitude of employees by empowering them to act from a point of knowledge and awareness of the risks (Korpela, 2015). The outcome of the study should improve cybersecurity awareness and attitude of employees to decrease frequency and intensity of threats (Korpela, 2015). The study should contribute to the conversation around the link between human factors and cybersecurity threats.

1.5.1 *Delimitations of the study*

The study has limitations that should be considered when interpreting the results. Data collection procedure was confined to employees working in a premium South African financial services group that offers a broad spectrum of financial solutions to retail and corporate customers across key markets in Africa. To generalise the findings, future research is needed to incorporate employees of other organisations within financial services industry to account for cultural differences. The use of Likert scale on the questionnaire is also a limiting factor for the study when asking attitudes and behavioural questions. According to Theofanidis and Fountouki (2018), many participants avoid selecting the extreme measures like “Strongly Disagree” or “Strongly Agree” and prefer to choose middle measures; which lead to concealing of real attitudes or behaviours of the participants.

1.6 Definition of terms

In this study, there are several terms that need to be defined for purposes of clarity and understanding.

1.6.1 Robot and Network (Botnet)

According to Bertino and Islam (2017), botnet is a network of devices infected by an attacker and it is used to perform tasks such as distributed denial of service attacks and spreading the spam e-mails.

1.6.2 Data Breach

A data breach is the event when network of an organisation is attacked and valuable data is stolen (Bouveret, 2018). Bouveret (2018) further highlighted valuable data in a data breach as personal information, log-in credentials, credit card details and social security numbers in relation to the study.

1.6.3 Distributed Denial of Service (DDoS) attack

DDoS attacks is used by attackers to render a network unavailable to overwhelm the targeted machine with massive requests from multiple devices (Bouveret, 2018). The targeted machine suffers a severely clogged bandwidth and legitimate connections become impossible (Swami, Dave and Ranga, 2019).

1.6.4 Domain Name Server (DNS) attack

A DNS attack is a type of DDoS attack that uses specific kinds of query protocols and available hardware to overwhelm a system with incoming queries (Carter, 2017). A harker manipulates publicly accessible domain names and flood the target with large volumes of data packets or requests (Bouveret, 2018).

1.6.5 Trojan horse (Trojan)

Trojan is a type of malware that is disguised as legitimate software. Trojan is employed by cyber thieves and hackers, who try to gain access to user's systems (Carter, 2017).

1.6.6 Malicious software (Malware)

Malware is a collective name for a number of malicious software variants including viruses, ransomware and spyware. Malware contains code developed by cyber attackers designed to cause extensive damage to data, systems and to gain unauthorised access to a network (Sikorski and Honig, 2012).

1.6.7 Phishing

Phishing is defined as a method of sending a user or multiple users digital correspondence that appears legitimate, but is actually meant to lure potential victims into providing some level of personal information for nefarious purposes (O'Leary, 2019).

1.6.8 Ransomware

Ransomware is the type of malware that prevents or limits users from accessing their system by locking the system's screen or by locking the users' files until a ransom is paid (Carter, 2017).

1.6.9 Spyware

Spyware is malware used by hackers to spy on a user to get access to personal information, bank account details, online activities and anything else that is valuable to the user (Gribble, Levy and Bragin, 2015).

1.7 Assumptions

During the study design process, the researcher balanced various threats to validity and the following assumptions create the best design possible.

a. Training given to participants on the subject matter is adequate

b. Measures used to characterise the participants are valid.

c. The characterisation data provided by the participants is reliable and valid.

1.8 Conclusion

The chapter gave the reader background of the study, key questions and the rationale why the study was undertaken. This includes the research problem of the study and the hypothesis for direction and better understanding of the topic. Definition of key terms was also covered under this chapter.

CHAPTER 2. LITERATURE REVIEW

2.1 Introduction

A better understanding of the literature, ultimately provide scholars with a detailed and structured access to the accumulated knowledge that the study provides (Webster and Watson, 2002). This chapter gives in-depth analysis of the literature review related to the research questions and the hypothesis of this study.

2.2 Definition of topics and background discussion

2.2.1 *Cybersecurity*

Cybersecurity entails larger study areas and complex matters. Cybersecurity as a concept is the insecurity created through cyberspace, including both technical and non-technical practices of making it secure (Cavelty, 2010). This$.5> definition presents cyber securing as a technical issue which is associated with computer science, cryptography or information technology, as presented by many cybersecurity researchers (Cavelty, 2010). The researcher categorises cybersecurity definition into three interlocking discourses, namely: academia, industry and government organisations.

These categories encompass the worms, viruses, different bugs and crime-espionage discourse that involve the issues of cyber attackers, digital spies and military-civil defence discourse which entails the subject vital system security.

There is no uniform perspective of cybersecurity in different industries and thus the researcher considered different perspectives that came to the fore in the literature review. Some of this perspectives are highlighted below:

- **Financial industry perspective**

Cybersecurity from the perspective of financial services industry focuses on tangible guidance for strategic decision-makers (Walls, Perkins and Weiss, 2013). The term cybersecurity at industry level is used in context of security

practices related to the combination of offensive and defensive actions involving systems, information technology and operational technological environment (Walls et al., 2013).

- **Government and national state perspectives**

There is no universally accepted perspective of cybersecurity in different national strategies as some governments regard cybersecurity as overlapping with information security without any definitive conclusion. The definition of cybersecurity from the government perspective focuses more on integrity and availability of information while information security is mainly concerned with confidentiality (Wamala, 2011).

- **Academic definition**

Literature on cybersecurity remains policy-orientated and problem solving while theoretically guided or empirically oriented academic researchers are still relatively rare (Von Solms and Van Niekerk, 2013). Cyber security is part of the umbrella term **information security**. Information security or information technology (IT) security aims to protect all digital and hard copy information assets (MBN, 2020).

The word ***cyber*** is short for **cybernetics**. Cyber is a prefix or adjective which means relating to or characteristic of IT (information technology), computers, and virtual reality. **Cybernetics** is the science of communications and automatic control devices or machines, as well as living things. Cyber originated in the early 1980s as a short form for cybernetics (MBN, 2020).

Cyber security refers to the practice of protecting computer systems, networks, programmes, and data from cyber-attacks or digital attacks (MBN, 2020). For the purpose of this study, cybersecurity is defined as a practice of defending servers, mobile devices, computers, networks and data from malicious attacks (Von Solms and Van Niekerk, 2013). This definition includes network security, application security, information security and end-user education.

2.2.2 *Cyber-Attacks*

A cyber-attack is any type of offensive manoeuvre that targets a computer network or computer information system. Cyber-attacks may also target personal devices, infrastructure, and medical devices. According to *CISCO*, an American multinational technology company, cyber attackers usually aim to destroy, change, or access sensitive information. They may do this to interrupt normal business operations or extort money from people, businesses, governments, and other organisations (Hari and Lakshman, 2016; MBN, 2020).

2.2.3 *Information Security (IS)*

The international standard and code of practice for information security management defines information systems (IS) as protection of information from a wide range of threats in order to ensure continuity in business, minimising risk and maximising return on investments (Hilton, 2013). The concept is also defined as a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types in order to keep information in all its location (Hilton, 2013).

Information security is often used interchangeably with the term cybersecurity due to the substantial overlap between the two concepts. The definition of both concepts in this study clarity how the researcher uses both terms.

2.2.4 *Adversary*

Adversary in the cyberspace is malicious entity or someone with the objective to prevent the users to achieve their intended goals by attempting to discover data illegally, corrupting data that is accessible in the system, deceptive identity or forcing a system shutdown (Huster**,** Chiang, Chadha and Swami, 2018).

There are five common adversaries that are active in the cyberspace. These adversaries are listed in Table 3.

Table 3: Common adversaries in cyberspace (Huster, Chiang, Chadha and Swami, 2018)

ADVERSARY	DESCRIPTION
Cyber-attackers	An individual or a team using technology to commit fraud, malicious activities on cyberspace to steal sensitive data with purpose of profit gaining.
Hackers	An individual or a team that enjoy exploring methods for breaching information security systems and exploiting network weaknesses.
Hacktivists	An individual or team of hackers who attack organisations for ideological gain, social change or political motives.
Industrial Actors	Individuals or institutions with capability to influence the industry with the sole purpose of gaining economic advantage for their organisations.
Insiders	Internal employees with legitimate access to information then perform criminal activity which can be deliberate or an accidental act due to lack of knowledge.

2.2.5 *Vulnerability*

Vulnerability in the cyberspace is linked to weaknesses in the system design that gives attackers unauthorised access to data or allow attackers access to execute malicious commands into the entire organisational systems (Abomhara, 2015). Weaknesses in system design can mean both software and hardware, organisational policies and procedures that guarding the internet of things (IoT) system or users of the systems in a form of knowledge or attitude (Abomhara, 2015). The cyberspace highlights four primary vulnerability types:

Table 4: Four primary vulnerability types (Abomhara, 2015)

VULNERABILITY	CAUSE	DEFINING ATTRIBUTES
System defect	Complexity/Unintended Errors	Coding of software, unintended errors in the design phase and system operation.
Lack of Security	Budget/Funding	Lack of proper funding, the organisation put no proper action to system protection.
Human Factors	Ignorance/Attitude	Lack of proper cybersecurity training and threats awareness
Organisational	Negligence	Inadequate policies, skills, procedures and security processes

2.2.6 *Threat in basic security frameworks*

Threat in the cyberspace is the capability of adversaries (refer to section 2.2.4) and is a possible danger that exploit vulnerability of infrastructure to breach all possible security measures (Kostopoulos, 2017). There are three different types of threats that are common in the basic security frameworks and actively taking place in cyberspace (Kostopoulos, 2017). These threats are described in Table 5.

Table 5: Three types of threats in cyberspace (Kostopoulos, 2017)

TYPE	MOTIVATION	ATTRIBUTES	EXAMPLES
Confidentiality	Profit	Both personal and organisational information	Data Breaches
Integrity	Degradation	Remote operational change	Malware
Availability	Disruption/ Disorder	Distributed botnet attacks	DDoS

2.3 Information Security Management System (ISMS)

The information security management system is achieved by establishing and operating effective information security through constant reviews and improvement of data management that addresses human behaviour and use of technology within an organisation (Soomro, Shah and Ahmed, 2016). The fundamental areas of the organisation that is addressed by ISMS is to counter all adversary related to data vulnerabilities, providing a secured growth while meeting all legal and regulatory requirements (Soomro et al., 2016). The objective of an ISMS is to assist organisations in protecting their assets by means of a set of procedures and guidelines (Soomro et al., 2016). Furthermore, an ISMS provides consistency in ensuring application of security principles and policy implementation. For the purpose of this study, discussions related to an ISMS are based on the ISO/IEC 27001 frameworks and standards. Further aspects are discussed in the sections below.

2.3.1 *ISO/IEC 27001-based Information Security Management System*

The International Organisation for Standardisation (ISO) is an international body for standards that is agreed upon by different national standard organisations and the International Electrotechnical Commission (IEC) comes from the background of publishing the international standards for all electrical, electronic and other related technologies (Disterer, 2013). Both the ISO and IEC cooperate in publishing the information security standard. The ISO and the IEC published ISO/IEC 27000 family of standards as a composition of different information security standards for information security standards, risks and control measures within information management security system (Humphreys and Plate, 2006). The ISO/IEC 27001 within the ISO/IEC 27000 family describes all best practices for developing an ISMS standard. The ISO/IEC 27001 provides both systematic approach and a common framework in the organisation to build a culture of security which ensure the confidentiality, integrity and availability of information (Humphreys, 2016). These standards are common language throughout the

world across industries to manage information security policies and implementation of ISMS.

The standard presents a model called Plan-Do-Check-Act (PDCA), aiming to improve the effectiveness of ISMS adopted by an organisation (Humphreys, 2016). The model is directly linked to the management system and aims to establish key risk areas, implement risk controls and continuously improve the efficiency of ISMS (Susanto and Shobariah, 2016). The four phases of the PDCA cycle are explained in Table 6.

Table 6: The Four phases of PDCA (Susanto and Shobariah, 2016)

PHASE	STRUCTURE	APPLICATION TO ISMS
Phase 1: Plan	• Context of the organisation • Leadership • Planning • Support	It is the phase were ISMS is establish, including policies, organisational objectives, processes and other procedure to manage risk.
Phase 2: Do	Operations	Implementation and operation of the ISMS policies, controls based on the Plan phase.
Phase 3: Check	Performance Evaluation	Under this phase, both monitoring and reviewing of ISMS take effect. Assessment and measurements of performance against established ISMS policies and objectives.
Phase: Act	Continuous Improvement	The last phase is about maintenance and continuous improvement of ISMS by taking corrective measures based on internal ISMS audits and other internal reviews.

The application of the PDCA cycle to an ISMS is illustrated in Figure 1.

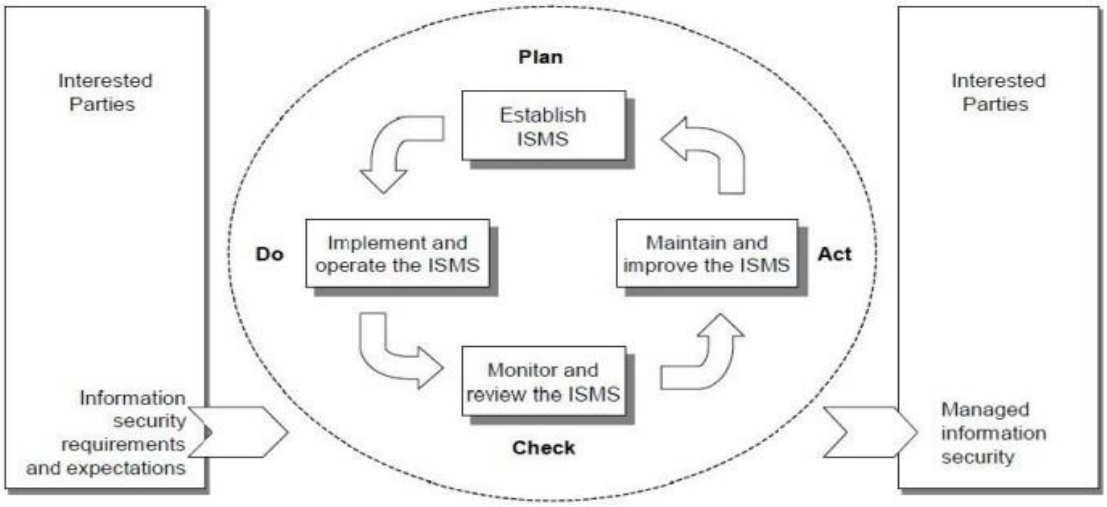


Figure 1: PDCA Model applied to ISMS Processes (Humphreys, 2016)

Figure 1 highlights the level of involvement of different interested parties and shows the continuous improvement of the ISO/IEC 27001 standards (Humphreys, 2016). The commitment of leadership is also demonstrated as an interested party responsible for information security requirements and a stakeholder, who is responsible to manage information security through effective ISMS (Humphreys, 2016; Susanto and Shobariah, 2016).

2.3.2 *ISO/IEC 27001 based Leadership*

The key component for successful ISMS is an effective and committed top management team that is actively involved and has deep knowledge of vulnerability and information security management. The ISO/IEC 27001 provides the leadership focused clause to emphasise the need for ISMS to be supported by senior management (Calder, 2016). The clause sets standards by identifying specific aspects of the ISMS where top management becomes an interested party and demonstrates a level of leadership and commitment (Calder, 2016). Table 7 outlines the different aspects of leadership.

Table 7: ISO/IEC 27001 and ISMS Leadership Aspects (Calder, 2016)

ISO/IEC 27001 : Leadership Aspects	ISMS: Leadership Aspects
Accountability for the effectiveness of the management system;	Pre-built regulation, certification, and standards frameworks to meet ISO 27001, ISO 27701, ISO 22301
Ensuring the policy and objectives are established and are compatible with the context and strategic direction of the organisation;	Create policies, controls, and other information quickly
Ensuring the integration of the management system are embedded into business processes;	See progress and completion of your ISMS at all times
Promoting the use of the process approach and risk-based thinking	Facilitate team collaboration
Ensuring adequate resources are in place;	Visible audit trails with version control management
Engaging, directing and supporting persons to contribute to the effectiveness of the management system	Set automated policy reminders and alerts for review

2.3.3 *Responsible, Accountable, Consulted and Informed (RACI) Matrix for ISO/IEC 27001*

The best-practice approach for a successful implementation of ISMS for an organisation to manage information security is based on how they address the combination of people, processes and technology. Furthermore, the accreditation certification is also based on this combination as an indication that ISMS is aligned with information security best practice of that specific industry (Stoll, 2015). However, the ISO/IEC 27001 Global Report released in 2016 pronounced some of the challenges and highlighted the view that ISMS implementation fails at project level citing unclear roles and responsibilities of key players (Aginsa, Edward and Shalannanda, 2016).

The implementation of ISO/IEC 27001 projects across all sectors is a multi-level venture with key players having different roles and responsibilities. There are four key responsibilities in the RACI Matrix that is used to clarify roles in the running of an ISMS project. These roles are defined as follows (Aginsa, Edward and Shalannanda, 2016):

a) **Responsible** – Refers to all stakeholders responsible for the completion of the task in the project.
b) **Accountable** – Defines all key players responsible for the results of a specific activity. There is a two-way communication under this role.
c) **Consulted** – Refers to stakeholders who is required to be heard in the decision-making process. There is a two-way communication under this role.
d) **Informed** – Designates internal stakeholders that sought to be kept up-to-date on the progress of the project. There is a one-way communication under this role.

Based on the definition of responsibilities, the RACI Matrix was developed using key activities that is outlined under ISO/IEC 27001 implementation checklist using the following key roles: Top management, Project Team, Unit Heads and End-Users (Stoll, 2015). The RACI Matrix is designed with the view that top management and executives already approved the ISMS implementation project (Stoll, 2015).

The RACI Matrix as tool and methodology helps to:

- Define and clarify key responsibilities;
- Help to reduce miscommunication or implementation errors that can put the project at risk of failing.

In the PDCA Model applied to ISMS processes, the RACI Matrix is part of the plan-phase ISMS is established. The RACI Matrix outlined in Table 8 is meant to assist organisations with project implementation the ISO/IEC 27001 standards (Stoll, 2015):

Table 8: RACI Matrix for Project implementation (Stoll, 2015)

Activities	ROLES			
	Top Management	Project Team	Interested Parties/ Process Owners	Users/ Employees
Indentifying the ISMS requirements and interested parties	Accountable	Responsible	Consulted	Consulted
Defining ISMS basic framework	Accountable	Responsible	Consulted	Informed
Development of the risk assessment and treatment methodology	Accountable	Responsible	Consulted	Informed
Performing the risk assessment and defining the risk treatment plan	Accountable	Responsible	Consulted	Consulted
Controls implementation	Informed	Responsible	Accountable	Informed
Training and awareness of personnel	Informed	Responsible	Accountable	Informed
Controls Operation	Informed	Responsible	Accountable/ Responsible	Responsible
Monitorig and Measuring Performance	Informed	Responsible	Accountable/ Responsible	Responsible
Performing Internal Audit	Informed	Accountable/ Responsible	Consulted	Consulted
Performing Management Review	Accountable	Responsible	Consulted	Informed
Addressing nonconformities, corrective measures	Accountable	Responsible	Responsible	Informed

Successful ISMS project implementation depends on top management support mostly at the beginning to identify requirements and basic frameworks (Calder, 2016). The process owners then become accountable for the phases related to controls and measurements to enforce and maintain commitment to the ensure ISMS project. The details of the RACI Matrix about all the responsibilities are therefore detailed in project documents such as budget, schedule of the project and other developed plans for the ISO/IEC 27001 (Calder, 2016).

For the purpose of this study ISO/IEC 27001 specify a management system that bring information security under explicit management control in the financial

services industry. The framework demonstrate clear commitment to information security management and compliance. The ISMS covered in literature provides a management framework of policies and procedures that keeps information in the financial services industry secured (Soomro et al., 2016). The RACI matrix is a useful tool for ISMS project implementation by defining and clarifying roles of different stakeholders within organisations in the financial services industry (Stoll, 2015).

2.4 Theoretical models in Cybersecurity Compliance

2.4.1 *Theoretical model for employees' cybersecurity policy compliance*

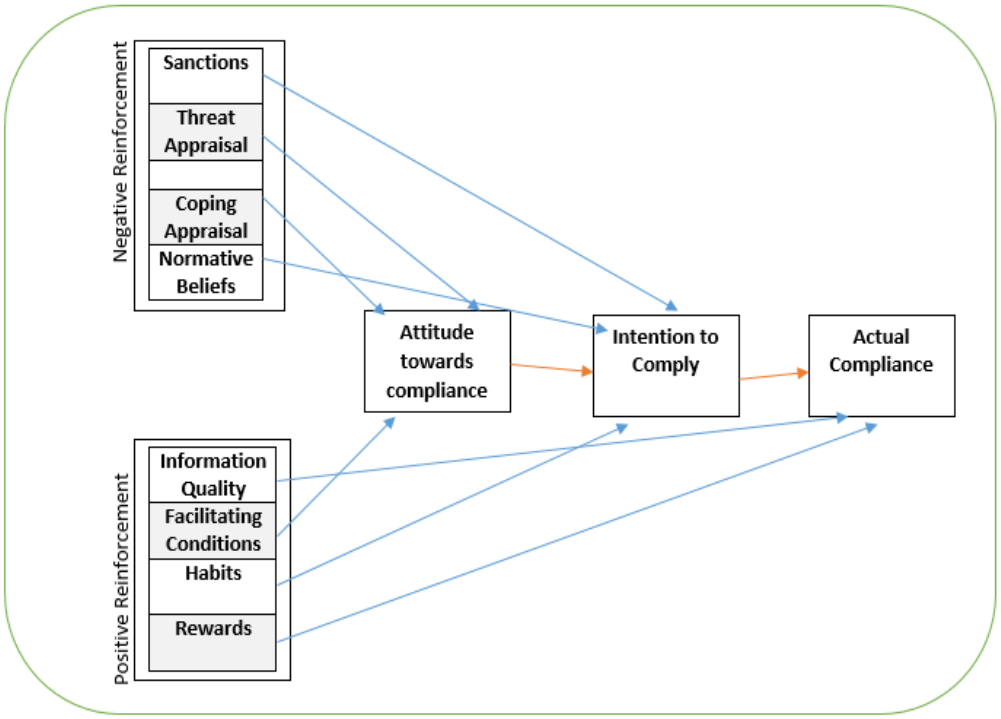


Figure 2: Theoretical model (Pahnila, Siponen and Mahmood**, 2007)**

The theoretical model for employees' cybersecurity policy compliance is derived from a combination of theories supported applied behaviour analysis in a form of positive and negative reinforcement (Pahnila, Siponen and Mahmood, 2007). Positive reinforcements of the model present motivating stimulus for employees after a specific behaviour is displayed, encouraging this behaviour to be repeated in future (Pahnila et al., 2007). The negative reinforcements in the model are

factors that are encouraging a specific behaviour by avoiding a negative stimuli or consequences (Schieltz, Wacker and Romani, 2017). The negative reinforcement as used in the model is different from punishment as it does not aim to discourage a specific behaviour (Schieltz et al., 2017). The theories in the model includes the following:

Table 9: Three theories for policy compliance

THEORY	DESCRIPTION
General Deterrence Theory	The theory is based on the belief that an increase in both certainty and severity of punishment may discourage unsolicited behaviour in the organisation (Bhattacherjee and Shrivastava, 2018). Based on the theory, employees are more likely to be persuaded to comply with cybersecurity policies due to level of enforcement such as legal actions, suspensions or even termination
Protection Motivation Theory	The theory is linked to motivation to employees to respond to threats or malicious behaviours (Vance, Siponen, and Pahnila, 2012). The theory predict and explain factors that motivates employees to change certain behaviours.
Theory of Reasoned Action (TRA)	The theory, according to is used in predicting how employees behave based on pre-existing attitudes, behavioural intentions and explain within human action the relationship between attitudes and behaviours (Montano and Kasprzyk, 2015).

Previous researchers on cybersecurity compliance have criticised the existing information security awareness approaches as lacking theoretical and empirical principles to ensure that employees comply with different risk policies (Pahnila et al., 2007). The model above contains factors that explain cybersecurity compliance with attitude towards compliance, intention to comply and the actual

compliance as key factors of the theory. These key factors are based on the theory of reasoned action (Yzer, 2017).

Attitude in the model as defined by Yzer (2017) refers to both positive and negative feelings towards a specific inducement object while intentions in the model capture the motivational factor that a specific behaviour indicate in how employees are willing to perform. The theory of reasoned action in literature emphasise that the stronger the intention of employee to carry out a behaviour, the more likely the behaviour will be carried (Yzer, 2017). In the model, the stronger the intention to comply with cybersecurity policies, the more likely employees will actually comply with policies. The key components of the TRA model is highlighted in details below:

I. Sanctions

Sanctions as part of the negative reinforcement of the model comes from general deterrence theory. Figure 1 demonstrates that sanctions as a reinforcement affect employees' intention to comply with cybersecurity policies. The general deterrence theory in this case suggests that celerity, severity and certainty of punishment affect employees' decision on whether to comply with implemented risk policies (Bhattacherjee and Shrivastava, 2018). The model does not cover key components of literature under general deterrence theory, namely social disapproval, self-disapproval and impulsivity (Pahnila et al., 2007).

II. Threat appraisal and coping appraisal

Figure 1 demonstrates that **threat appraisal** is part of the negative reinforcement and affects the attitude of employees towards complying with cybersecurity policies and compliance strategies. There are two key dimensions in threat appraisal, namely perceived vulnerability and perceive severity.

- **Perceived vulnerability** is applied to the question of non-compliance with regards to cybersecurity policies by employees and it refers to employees' assessment of whether the organisation is antagonised by cyber-threat. According to Pahnila et al. (2007) there is a view that if employees are

exposed and confronted by to cyber-threat, they will not comply with cybersecurity guidelines.

- **Perceived severity** on the other hand refers to consequences to employees in a case were the organisation was cyber attacked (Arachchilage, Love and Beznosov, 2016). The concept is derived from protection motivation theory and it includes things like identify theft and e-mail hacking (Montano and Kasprzyk, 2015).

Coping appraisal is a negative reinforcement for the cybersecurity policy compliance and affects employee attitudes. According to Pahnila et al. (2007), coping appraisal is a measure with three proportions, namely response efficacy, self-efficacy and response cost.

- **Response efficacy** relates to belief in the perceived benefits of the action.
- **Self-efficacy** emphasises the employees' ability or any level of judgement of their capabilities to cope with any responsibilities at hand.
- **Response costs** are costs which results from employees' behaviours.

III. Normative beliefs

The normative beliefs in the model are linked to the employees' intention to comply with risk management policies. According to Pahnila et al. (2007), normative beliefs in an organisation are a reflection of normative expectations of peers and individual employees create behaviours based on interaction with fellow colleagues. The role of management as the influencer from a social environment may have a persuasive influence on whether employees perform or not perform a specific behaviour. Positive attitudes towards complying with cybersecurity policies and guidelines is more likely to guide employee attitude, leading to a positive attitude towards the risk management rules (Pahnila et al., 2007).

IV. Information quality

Information quality on the model is first of the positive reinforcement and affect the actual compliance with cybersecurity policies. Kang and Namkung (2019)

research identified the two dimensions of information quality as perceived importance of information and perceived usefulness of information. **Perceived importance of information** includes factors such as relevance of information, meaningfulness of data and its significance while **perceived usefulness of information** includes factors such as unambiguity and readability (Kang and Namkung, 2019).

V. Facilitating conditions

The success of any level of policy or guideline document in the organisation depends on employees' acceptance of it. Facilitating conditions play a critical role in the acceptance of risk management guidelines as it meant to make task easy to accomplish. Facilitating condition is one of the positive reinforcements and affect the attitude of employees towards complying with cybersecurity policies. According to Pahnila et al. (2007), facilitating conditions refer to objective factors that employees' agree to make a task accomplish and has positive influence on the intention to comply with cybersecurity policies. In an environment where employees to have systems and hardware to support their facilitating conditions, compliance is more unlikely to take place.

VI. Habits

Habits are unconscious or automatic behaviour, which are different from defined intentions on the model and conscious behaviour (Pahnila et al., 2007). Habits in the model explain the cybersecurity usage and is argued to be influencing actual behaviour of employees in the long run. According to Pahnila et al. (2007), the use of technology in cybersecurity policy compliance can be made habitual through using mandatory initiatives such as rewards or any other form of incentives. Habitual behaviour on the model explains cybersecurity non-compliance.

VII. Rewards

The effective use of rewards in the model is to cultivate interest and increase motivation or performance on general compliance. Rewards in this case include **tangible benefits** such as money and awards or **intangible rewards** such as recognitions. According to Pahnila et al. (2007), employees' attitude and intentions towards actual policy compliance can be impacted using both tangible and intangible rewards.

2.4.2 *CIA Triad security model*

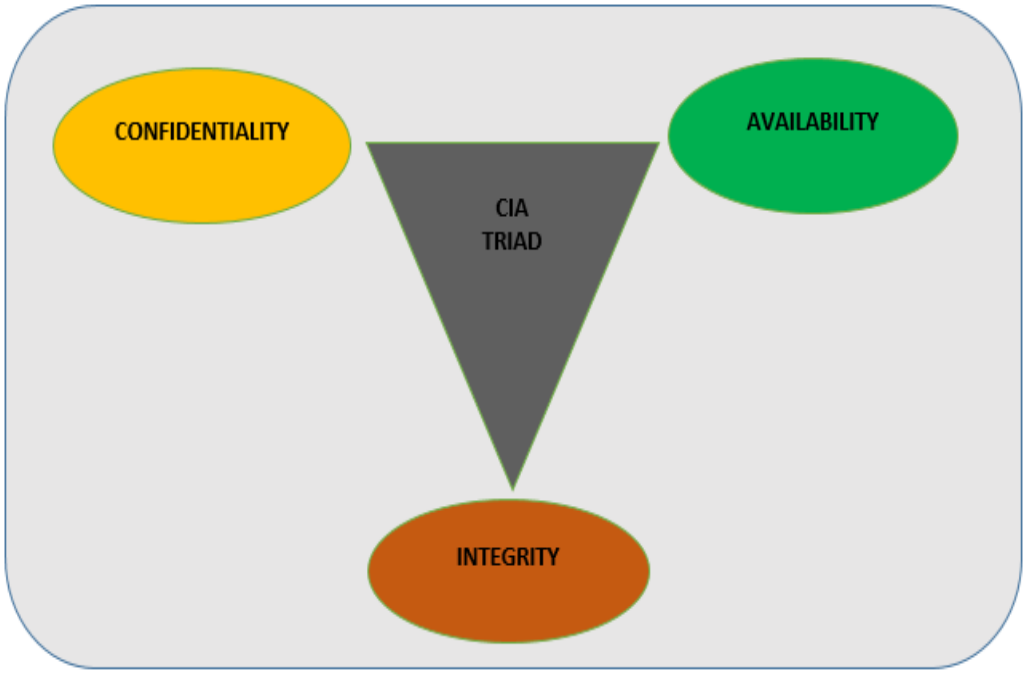


Figure 3: The CIA triad security model (Samonas and Coss, 2014)

The history of the model goes back to the early days of computers when there only a few threats to the protection of information. The early focus for protecting information was linked with reliability of the system because of the rarity of the computers and skills to operate the system (Samonas and Coss, 2014). Information security in the early years was achieved by controlling physical access to the machine from those with computing programming skills. The usage of computers increased over the years with a high level of software development

which shifted the focus from protecting computers to protection of information. The concepts of confidentiality, integrity and availability started to gain importance as part of information security (Samonas and Coss, 2014).

The CIA triad model as presented by Clark and Wilson in 1987 is now known as an imperative part of different security governance standards and codes of practice (Moghaddasi, Sajjadi and Kamkarhaghighi, 2016). The acronym CIA refers to confidentiality, integrity and availability. These aspects are seen as governing principles through which information security is achieved and they are also seen as an integral part of stakeholder expectations in information technology. Organisations use the loss of CIA triad of information system as the basis for classification and qualitative assessment of cybersecurity controls. In the same manner, confidentiality, integrity and availability are also used for privacy rules of electronically saved data. The CIA model is used for cybersecurity development as an obligatory set of controls and principles for the organisation to use as security implementation. Confidentiality, integrity and availability are discussed in more detail below.

i) Confidentiality

The first component of the triad is a security principle that controls access to organisational information and designed to limit access to sensitive information (Pattanavichai, 2018). The principle ensures that access to information, systems and networks are restricted only to users with authority to view and utilise organisational data (Pattanavichai, 2018). Protecting confidentiality includes categorising of data according to type and severity damage that could happen should it fall into the hands of attackers, including training for those, who handle and share sensitive data. This special training must include familiarising all authorised system users with security risk factors and different ways to protect vulnerable data assets (Cernov, 2018). Methods that can be used to protect confidentiality include the use of data encryption, password-related best practices, two-factor authentication, and biometric verification (Cernov, 2018). The two-factor authentication is commonly used for authenticating users to access sensitive data and serve as extra step to log-in processes.

ii) Integrity

The second component of the CIA triad model is meant to assure that all sensitive data with controlled access is trustworthy and accurate. The key principle of maintaining integrity in information security is to ensure consistency, accuracy and trustworthiness of data over its life-cycle. The use of version control to ensure that sensitive data is not altered in transit and security measures like file permissions and user access controls are employed. According to Cernov (2018), the use of other measures to detect data changes such as server crash or environmental failures should be used to prevent unintentional changes or deletion of data.

iii) Availability

The last component of the CIA triad is linked to the actual availability of organisational data. The authentication mechanisms which is linked directly with confidentiality of data, access channels that is designed to protect data must all work properly under this component to ensure availability of data. **Availability** means maintenance of all hardware, performing hardware repairs to ensure functioning operating systems and all necessary upgrading of organisational systems. The fast-adaptive disaster recovery plan and safeguards against data loss which includes back-up in a geographically isolated location.

Extra security equipment and software are used to guard against unreachable data due to malicious attacks. There are different theories that confirmed the view that availability is linked to information security because the effectiveness of security measures is meant to protect system components and ensuring availability of information (Qadir andd Quadri, 2016). Availability as an element of CIA triad model that is considered within information system and it is related to assets such as hardware, software and networks (Moghaddasi et al., 2016). Furthermore, the component includes different organisational systems, established processes, different human factors and information (Moghaddasi et al., 2016).

2.5 Cybersecurity behaviour in the aspects of malware, passwords usage, phishing, social engineering and online scam for employees in the financial services industry

The internal human threats in the financial services industry range from employee attitude to intentional and unintentional threats. **Intentional threats** are the results of harmful decisions that are related to crimes such as espionage, identity theft, purposely damaging property or stealing customers' information (Ernst and Young, 2003). The **unintentional threats** are caused by low cybersecurity awareness and cyber threats and include the accidental violations of information by employees (Ernst and Young, 2003). The study aims to identify cyber threats impacting the financial services industry and targeting the employees through e-mails and other communication channels.

Two cyber threats, namely phishing and ransomware are discussed in the sections below.

2.5.1 *Phishing*

Phishing is one of the most common terms associated with cybersecurity where the attacker creates a replica of an existing web page to fool users in to submitting personal, financial, transaction and password data to what looks like a service provider website (Chawla and Chouhan, 2014). The word phishing is produced from fishing, referring to the act that the attacker appeal users to visit a fake website by sending fake e-mails (Chawla and Chouhan, 2014).

Three types of phishing attacks/techniques are used. These phishing attacks are:

- **Deceptive phishing** – the technique is associated with social engineering schemes which is depending on forged email claims that emerge to originate from a legitimate organisation (Chawla and Chouhan, 2014). The phisher embedded the link within the e-mail with the attempt to redirect users to fake websites to fraudulently access data from the victim.

- **Malware-based phishing** – the technique involves technical ploy schemes that rely on malicious code or malware after user click on a link rooted in the e-mail or detecting security holes in the user computer to access victims' online credentials.

- **Clone phishing** – It is the kind of phishing assault that genuine and beforehand conveyed an e-mail hold within a connection or connection has had its substance which is used to make a practically cloned e-mail (Dakpa and Augustine, 2017). The connection inside the e-mail is oust with a malevolent form and after that sent from an e-mail delivery mock to seem to originate from the first user. The system is utilised to turn from a previously machine and pick up a grip on different computers, abusing the faith in people connected with the induced association because both sides accepted the first e-mail (Dakpa and Augustine, 2017).

- **Spear phishing** – the malware virus targets a particular group of people or organisations that has been named skewer phishing with attackers collecting entire information relating to their objective of accomplishment (Dakpa and Augustine, 2017).

2.5.2 *Ransomware*

Ransomware outlines the malware as the type that restricts users from accessing their system either by locking the system screen or by locking the users' files in the system unless a ransom is paid (Tailor and Patel, 2017). The study further highlights that modern ransomware families categorised as crypto-ransomware encrypt certain file types on infected systems and force the users to pay the ransom through online payment methods to get the decrypt key (Tailor and Patel, 2017).

2.6 Employee attitudes in relation to cyber threats

Organisations in the financial services industry are known for vigilance in the cybersecurity execution. Executing consistently in a highly regulated industry requires both training and resources. Despite all the significant budgetary expenditure in systems to protect organisations against cyber-attacks, literature highlight very little comparative investment in human factors and security culture (Alavi, Islam, Jahankhani and Al-Nemrat, 2013). Alavi et al. (2013) further argue that employees' attitudes can result in undesirable behaviour as a direct reflection of the culture in terms of information security or cybersecurity. The information security cultures model gives a theoretical perspective on understanding the background that leads to different attitudes of employees in both cybersecurity awareness and compliance.

2.6.1 *Cybersecurity culture*

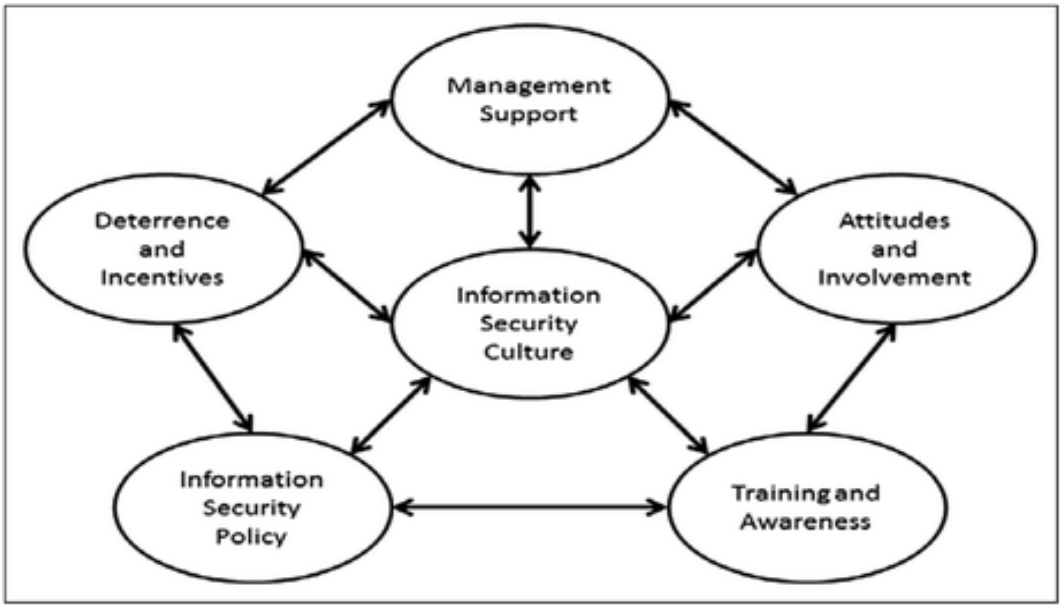


Figure 4: Factors that influences Cybersecurity Cultures (Da Veiga and Eloff, 2010)

Figure 4 synthesises the role and impact of employee attitudes a cybersecurity culture. The components in the model are discussed to demonstrate a clear correlation between cybersecurity culture and employee behaviour around cybersecurity risk management. The study conducted by Da Veiga and Eloff

(2010) emphasised the effectiveness of any counter measure to cyber-threats as a scope of technical and non-technical controls. The technical controls refer to sophisticated hardware and effective software that the industry apply. The following section covers non-technical controls that impact countermeasure cybersecurity.

I. Information security policy

The focus of information security is to measure the shift from technology to human factors. Different studies have investigated the influence and effect that information security policies have on the overall information security culture. According to Van Niekerk and Von Solms (2010), organisations in sectors such as the financial services industry are required to have information security policies in place as per regulatory authority. In relation to employee behaviour, the policies set mandatory guidelines to influence favourable organisational behaviour when using the systems or working on customer related data. The security policies are created to communicate security protocols, assign and clarify roles and responsibilities while providing employees with guidance for acceptable usage to ensure security behaviours in line with expectations (Van Niekerk and Von Solms, 2010).

According to Glaspie and Karwowski (2017), when policies in relation to security are complex, ambiguous, complicated, vague or difficult for employees to understand, attitudes towards compliance are negatively impacted. The role of organisations in dealing with cyber threats is to ensure that information security policies are understandable, relevant and accessible to all employees.

II. Attitudes and Involvement

The fight to protect the organisations from information theft and cyber-crime devote a great deal of attention to improve existing information security infrastructure. The focus on technical solution to cybersecurity often fails to acknowledge that for system to be effective, employee engagement and understanding of their utility is therefore required (Ifinedo, 2014). Positive employee attitudes about information security compliance and their involvement

in the process are regarded as another factor that impacts on the information security culture in an organisation. Research has shown that employee experience and involvement influence their perceptions about or attitudes towards information security (Safa, Von Solms and Furnell (2016). Furthermore, employees' attitudes towards organisational compliance and the perceptions of other members in the workplace greatly affect secure behaviour (Safa et al. 2016).

III. Deterrence and incentives

Information security policies within organisations contain language that informs the end-users about the consequences of non-compliance, which is formal deterrence against negative employee behaviour. There are different studies in literature that discuss the link between an employees' willingness towards security policy compliance and their perceived benefits or cost of compliance versus non-compliance (Glaspie and Karwowski, 2017). Safa et al. (2016) reveal that organisations with higher severity in punishments for non-compliance are more likely to have a strong information security culture in line to guard against cybersecurity crimes and threats.

The study conducted by Glaspie and Karwowski (2017) indicates that rewards or incentives contributes to the information security culture, however, not all incentives positively influence performance in the information security culture. Rewards according to Glaspie and Karwowski (2017) can negatively affect compliance intention if perceived benefits of non-compliance are greater than the perceived incentive from the organisation. Therefore, regardless of deterrence or incentives, adherence to information security policy is a major factor in cultivating an information security culture (Glaspie and Karwowski, 2017).

IV. Training and awareness

Different studies refer to the training and awareness factor as foundational elements of cybersecurity. A proper and well-executed training and awareness programme in an organisation provides employees with savvy knowledge that is required for compliance requirements, risk management strategies and data management (Adams and Makramalla, 2015). The opposite of it is negative and

unaware employees that are more likely to expose the organisation to different levels of cyber threats. The investment in resources towards building a strong cybersecuring skills across all levels of employees of the organisation as key in building strong information security culture (Adams and Makramalla, 2015). The investment in both hardware and software mean less as a countermeasure in an organisation were employees are unaware or untrained as attackers focus more on human factors (Badie and Lashkari, 2012). Inadequate skills and awareness is the source of negative attitude that leads to both intentional and unintentional errors that is a high liability in organisational risk management (Badie and Lashkari, 2012). Employees with adequate skills are known to exhibits positive attitudes towards cybersecurity measures and cyber-threat concepts that eliminates human errors (Parsons, McCormac, Pattinson, Butavicius and Jerram, 2014).

Lack of cybersecurity awareness from employee perspective contributes to development of an attitude that results to cyber-attacks caused by human behaviours. Organisations have the responsibility to build effective and customised awareness programmes that benefit employees in understanding the importance of data protection, data management and occurrence of threats against them (Bada, Sasse and Nurse, 2019). This study further emphasised the importance of constant review of training contents, the use of language and specific jargon that is relevant to the business objective or industry standard (Bada, Sasse and Nurse, 2019). Different personality types also play a role in how employees react to cyber-threats and sanctions in a form of consequences from non-compliance. Adopting a comprehensive cybersecurity training and awareness programme is regarded as a key factor in fostering high level of information security culture in all organisations (Safa et al., 2016).

V. **Management support**

There are limited research and studies on the role of management support in the cyber space, however, this factor is critical in cultivating a cybersecurity culture. Consistency by organisational management in supporting culture building initiatives is regarded as key contributor to a successful implementation of information security efforts (Singh, Gupta and Ojha, 2014). Management support

includes sufficient budgets on building cybersecurity culture, the right technology to deal with system risk and investment in human capital to deal organisational need. Furthermore, the support includes management advocating and delivering clear message on information security policies and setting goals for the entire organisation (Singh, Gupta and Ojha, 2014).

Management support is the level were policies, strategies and cybersecurity guidelines are developed. Leadership emphasis drives cybersecurity focus while correlation between management support and security awareness strengthen security culture (Singh, Gupta and Ojha, 2014). The study further highlighted the role of management support in an environment where employees' jobs are highly dependent upon other employees as critical in emphasising security awareness and training programmes as these employees tend to police each other. In such a case, management needs to monitor security policy and attitudes for compliance. The role management can play in affecting compliance attitude by cross training set-up, sharing of cybersecurity knowledge and other security collaboration (Safa et al., 2016). It is the role of management to build effective organisational structure to support culture. The structure will then ensure that security functions are aligned to protect the organisation. Failure to build effective structure can result to negative employee attitudes as policies and programs can be seen as interference to their task function, not a support factor (Flores, Antonsen and Ekstedt, 2014).

2.7 Conclusion

The findings from reviewing literature reveal limited literatures on the specifics of this study. The results of different studies on the attitude of employees and cybersecurity threats are inconclusive and often contradictory. There is no significant work that has considered to examine the link between attitude of employees and cybersecurity threats which made it difficult to draw appropriate theoretical framework for the study from literature that consider both attitude of employees towards information security and cybersecurity threats. The direction of the literature review is extracted from key areas of literature that relate to employees attitudes and cybersecurity threats.

CHAPTER 3. RESEARCH METHODOLOGY

The purpose of this chapter is to discuss the research design and methodology used to conduct this research. As stated in chapter 1, a descriptive research design was deemed suitable for this study as it has been found to be useful in identifying variable and hypothetical constructs which can be further investigated through other means of research and gives the researcher the possibility to observe the phenomenon in a completely natural and unchanged environment. The research design indicates the procedures involved in conducting the research and covers sampling, data analysis, validity and ethical considerations of the study. A description of the data collection techniques employed to gather information is also set out in this chapter.

3.1 Research approach

The main purpose of this quantitative research is to describe and then explain the phenomena through numerical presentation of data or manipulation of observations (Sukamolson, 2010). This quantitative study focused on examining the level of cybersecurity awareness and the attitude of employees in the financial services industry and further give the researcher the prospect to further clarify the problem at hand. The researcher chose quantitative research to have a clear understanding of cybersecurity awareness and attitude of employees by utilising questionnaires. Closed ended questions in the questionnaire would assist the researcher to gather experiences, perception and opinion from the study participants (Bryman, 2015).

The quantitative research method was also chosen because the researcher wanted to avoid personal bias of the study by allowing respondents to fill online questionnaires independently. The quantitative study is also known for enabling the researcher to draw comparisons, facilitate large amounts of information and results are limited owing to numerical descriptions. In choosing the quantitative study, the researcher was aware of some of the disadvantages of the method compared to other research methods (Sukamolson, 2010). Developing standard questions can lead to false representation as the researcher is able to influence

the participants to reflect his view of the situation (Sukamolson, 2010). For the purpose of getting accurate feedback of the study, the researcher covered facts in the questionnaire around the subject more broadly to get different views of the participants.

3.2 Research design

The researcher followed the survey research design and attempted to assess the situation in the financial services industry in relation to cybersecurity knowledge and awareness by gathering data through questionnaires to prove the correlation between cyber threats and the attitude of employees having e-mails. The 2017 study by Creswell defined descriptive research as a study designed to depict the participants in an accurate way. More simply put, descriptive research is all about describing people who take part in the study (Creswell, 2017). The design is therefore in line with the research problem and why the researcher is conducting the study.

3.3 Data collection methods

Primary data is defined as original materials such as attitudes, perceptions, knowledge, experiences and behaviours on which the research is based (Gibbs, 2018). This is known as first-hand testimony or direct evidence concerning a topic under consideration. They present information in its original form, neither interpreted nor condensed nor evaluated by other writers (Gibbs, 2018). The advantage of using primary data is that researchers collect information for the specific purposes of their study. In essence, the questions the researchers ask are tailored to draw out the data that promote the study.

3.4 Population and sample

3.4.1 *Sampling*

Sampling is either probability or non-probability and these types are different, based on randomisation (Bryman, 2015). Sampling is therefore a process to

select a group of people using a sampling frame with the primary aim of conducting research. This quantitative research used sampling to make assumptions about the population from gathered data using a sampling frame with the purpose of getting the effect of the problem. There are different strategies for sampling, depending on the goal of the researcher. For the purpose of this study, the researcher looked at generalising the results beyond those in the study.

3.4.2 *Population*

The population of the study is all employees made of all Senior Provincial Managers, Regional Managers, Area Managers and branch managers in one of the financial services organisations in South Africa. Subjects of the study was recruited by e-mail and links was also distributed through the organisation's e-learning portal. The total population is 480 and web-log indicated that 321 visited the portal with 228 completing the survey. All participants who didn't answer all questions were excluded, which resulted to a total of 3 exclusions (Barends and de Vries, 2019). Furthermore, an average response time for a completed questionnaire was recorded as 12 minutes, 1 questionnaire was excluded because of a noticeable short response of 3 minutes (Barends and de Vries, 2019).

A sample population in relation to the study is a group of individual units with a commonality and is determined by the error percentage the researcher is willing to tolerate (Bryman, 2015). The final sample of the study consisted of n = 224 complete questionnaires meeting the exclusion criteria. There was no significant difference between first and the last third of the data, therefore a non-response bias could be ruled out (Dong and Peng, 2013). The data shows a varied sample population of the organisation with detailed illustration of the demographics summarised in Table 12.

3.4.3 *Sample and sampling method*

The researcher used non-probability sampling and preferred using convenience sampling when determining the sample size. Convenience sampling was chosen

in this study because of the time frame of the research and the convenient accessibility (Gibbs, 2018). The researcher preferred a method that is fast, inexpensive and easy to use since the participants are situated in different departments. The study avoided using other methods owing to protocols involved in those methods being time consuming. The sample selected by the researcher is accessible and within close proximity to the researcher. Table 1 below highlight the profile of participants of the study:

Table 10: Profile of respondents

Description of respondent type	**Number to be sampled**
Senior Provincial Managers	5
Regional Managers	5
Area Managers	44
Branch Managers	170
TOTAL number of respondents	224

3.5 The research instrument

The researcher chose to use survey questionnaires as a data collection tool because of its effectiveness and its popularity as a means of collecting data. The standard psychometric scale development procedures were conducted as part of developing research instrument (Kyriazos and Stalikas, 2018). Existing literature was carefully reviewed and practical validated scales were adopted. A pre-testing approach and practical validated scales were adopted by the study to provide the best reliability scores of the results (Nicewander, 2018). The pre-tests were used for checking and eliminating any complexity, indistinctness and confusion within the items, as well as the general mechanics of the questionnaire to ensure initial reliability of the scales (Nicewander, 2018).

The survey questionnaires were designed with research questions, relevant literature and objectives of the study in mind (Li, Vedula, Hadar, Parkin, Lau and Dickersin, 2015). The questionnaire designed consists of close-ended questions

that are based on the pre-coded Lickert interval scale (Li *et al*., 2015). The researcher adopted this scale because it has been used extensively over the years as a tool to measure opinions, beliefs and attitudes; it is also user friendly. There was minor adjustment as a result of pre-testing, the final research instrument consisted of a set of 26 clear and understandable items with distinguishable constructs. The Lickert interval scale is presented as follows (Hayes, 2014):

1	2	3	4	5
Strongly Disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly Agree**

3.6 Procedure for data collection

Quantitative research methods emphasise objective measurements and the statistical, mathematical or numerical analysis of data collected through polls, questionnaires and surveys by manipulating pre-existing statistical data using computational techniques (Babbie, 2010). The study population is a total of 480 employees with e-mail from one of the financial services organisations in South Africa. The researcher made use of questionnaires distributed through e-mails as data collection method. The following procedures was followed to collect data for the study (Nardi 2018):

- The data gathering procedure started after the researcher received a letter of approval to conduct the needed data.
- The questionnaire to be used was then tested for its reliability and validity before it is distributed to target population and measures were employed to abide by the ethical principles in the conduct of the research.
- The respondents was informed about the nature of the study to ensure freedom of choice and provide an avenue for the respondents to voluntarily consent or decline participation in the study.
- The researcher distributed the questionnaires to the respondents and questionnaires was answered at their own convenience.

- The respondents was given enough time to answer the questionnaires and allowed to ask questions or seek clarification.
- The responses was collected by the researcher to compile and seal for analysis.

3.7 Data analysis and interpretation

The research will use descriptive statistical analysis as a form of analysis for an uncomplicated display of patterns and differentiation of results set. Descriptive data analysis are best used in this study as the researcher need summary of the results to gain insights of responses in a way that patterns develops from the data (Antonius, 2012). The descriptive analysis is meant to assist the researcher to determine the outcomes from analysis and affect interpretations of the data. Statistical Software Package for Social Science (SPSS) was used a software for representation of sophisticated statistical analysis. SPSS is a valid tool for this study as findings are readily displayed from various aspects of the analysis and the system can be custom programmed to either replicate results or adapt them if required for use (Antonius, 2012).

3.8 Limitations of the study

The condition or any influence uncontrollable to the researcher and restrictions placed on research conclusions or methodology may be regarded as study limitations (Shipman, 2014). The following limitations of this study were therefore identified as factors that the researcher had no control over:

- Limitations of the study is that a formal pilot was not conducted owing to time constraints. This is a weakness of the study and a more formal pilot study would have improved the validity. There were difficulties in checking the accuracy of the responses; a high number of responses were neutral. By using a mixed research method, the researcher might have probed and gained more insight by utilising interviews instead of questionnaires only.

3.9 Validity and reliability

Validity concerns for what instruments measures and how well it does so while reliability concerns the faith that one can have in the data obtained from the use of an instrument, that is, the degree to which any measuring tool controls for random error (Mohajan, 2017). The study incorporates reflective and formative measurement scales. According to Heale and Twycross (2015), formative constructs cannot be assessed using the same reliability and validity tests as reflective constructs, the evaluation was therefore done separately.

3.9.1 *External validity*

External validity is referred to as the validity of applying the conclusions of a scientific study outside the context of that study (Onwuegbuzie, 2000). The researcher adopted a probability sampling to counter and avoid any level of selection biases by ensuring that everyone in a population has an equal chance of being selected for a study sample (Andrade, 2018). The researcher was aware of the importance of general experiences during the entire data collection process and enough time was allocated for participants to complete questionnaires. Therefore, the study is externally valid as the sample closely mirrored the population that was being studied, sample shared similar characteristics to the population such as the ratio of males to females, age and other demographics (Heale and Twycross 2015).

3.9.2 *Internal validity*

Internal validity establish the trustworthy of the study by making it possible to eliminate alternative explanations for the findings (Andrade, 2018). The study followed a rigorous procedures in collection of data and maintain a low chances of confounding in the study. Data collection procedures for the study was guided by literature to avoid confounding and random selection of participants was used to avoid any level bias (Onwuegbuzie, 2000).

3.9.3 *Reliability*

Reliability is defined as a way of assessing the quality of the measurement procedure used to collect data in a study (Onwuegbuzie, 2000). The study questionnaire will be distributed electronically in a form of a link to participants to avoid researcher error in the process. Before going into the field, the study instrument was pre-tested to ensure reliability of the scales and clear unambiguousness of the questions. Furthermore, the internal consistency reliability was tested by enabling portal to save uncompleted questionnaires to cater for environmental changes of the participants because the survey can be saved and complete at a later stage (Andrade, 2018).

3.10 Demographic profile of respondents

The respondents of the study is a professional employees of an established financial services organisation with daily access to e-mails and the use of the internet. The minimum qualification for all participants is Grade 12 certificate as requirement by the organisation with a fairly prolific computer skills. Below is a demographic profile of the population:

Table 11: Demographic profile of the population

Occupational levels	Male				Female				Age Average (Years)
	African	Coloured	Indians	White	African	Coloured	Indians	White	
Provincial Managers	6	0	0	0	2	0	0	0	41
Regional Managers	4	0	0	0	3	1	1	1	37
Area Managers	22	4	0	4	36	4	15	8	34
Branch Managers	126	38	6	11	145	9	14	20	31

3.11 Ethical considerations

There are ethical principles that the researcher was aware of and followed religiously throughout the course of the study. Different studies highlight the importance of participants of the research not suffering any physical harm,

discomfort and pain, loss of privacy or embarrassment because of the study (Zimbardo, 2017). Participants were informed of the following (Zimbardo, 2017):

- Purpose of the research was clearly explained and outlined.
- All possible risks participants may face due to the study.
- Benefits accruing to them as a result of participating in the study.
- Their independence in making participation decisions without fear of any negative results or consequences.

All ethical standards were considered by the researcher and all participants were informed of the ethical standards. All participants completed consent forms to ensure that they participated willingly.

CHAPTER 4. PRESENTATION AND DISCUSSION OF RESULTS

4.1 Introduction

This chapter gives a presentation of the results by describing the data analysis and discussion of research findings related to research questions that guided the study. Data analysis were conducted to examining the attitude of employees towards information security and cybersecurity threats in the financial services industry. This data was collected through a self-administered questionnaires, which was completed by 224 (*n = 224)* employees in the financial services industry, a 74% response rate for the study. A total of 225 responses to distributed questionnaires were received, however, only 224 responses met the required inclusion criteria and were usable for the study.

The method of data analysis and presentation used in the study is descriptive statistical analysis to identify both the frequencies and percentages to answer all of the questions in the questionnaire. The 224 respondents who met the inclusion criteria did not answer all the questions, therefore, the percentages reported will correspond with total number of respondents answering the individual questions and the not applicable percentage will include all questions that were not answered. The only questionnaire deemed unusable, the responded did not complete the questionnaire in that two subsections of the questionnaire were not attempted. The questionnaire included three sections and data generated will be presented as follows:

- The demographic data such as age, level of education and experience is included in the first section of the questionnaire.
- The second section comprises of questions related to cyber-threats, cybersecurity awareness and cybersecurity behaviour.
- The third section of the questionnaire comprises of questions related employee attitude on cybersecurity.

4.2 Demographic profile of respondents

Table 11 and table 12 display means, standard deviations, standard errors and correlation coefficients for the LScU and ATScT as a function of gender, race, education and work experience.

Table 12: Means, standard deviations, standard errors and correlation coefficients on the limited understanding of cybersecurity (LScU) according to gender, race, education and work experience

Variable	Sample size *n*	Mean	SD	Standard Error	Correlation Coefficient
Total	***224***	***3.82***	***0.97***	***0.21***	***0.253***
Gender	**224**	**3.86**	**1.02**	**0.1**	**0.264**
Male	86	3.8	1.1	0.12	0.289
Female	138	3.92	0.95	0.08	0.242
Race	**224**	**3.83**	**0.96**	**0.2**	**0.25**
African	184	3.89	1.04	0.08	0.267
Coloured	25	3.71	0.77	0.16	0.207
Indian	5	3.7	0.98	0.23	0.264
White	10	4	1.05	0.33	0.263
Education	**224**	**3.84**	**0.94**	**0.29**	**0.245**
Matric/ Grade 12	120	3.93	0.94	0.09	0.239
Diploma	55	3.94	1.05	0.14	0.266
Degree	12	3.77	0.83	0.23	0.22
Post Graduate	14	3.43	1.39	0.78	0.405
Other	21	3.69	1.08	0.23	0.292
Not Applicable	2	4.25	0.35	0.25	0.082
Experience	**224**	**3.76**	**0.96**	**0.24**	**0.255**
1 to 4 years	67	3.57	1.03	0.12	0.289
5- 10 years	92	4.13	0.95	0.1	0.23
11-15 years	42	3.92	0.93	0.14	0.237
16-20 years	9	3.69	1.34	0.48	0.363
20+ years	11	3.76	1.02	0.32	0.271
Not Applicable	3	3.5	0.5	0.29	1.43

Table 11 shows the demographic output for all answers to the questionnaire from the entire sample of participants (n = 224). Demographic relationships in the study was not part of the purpose, however, this set of data proposed to describe demographic outputs of the sample and assess any level of influence on the

findings. The demographic data presented on the table consist of gender, race, level of education and work experience. A visual inspection of the table disclose that 62% of the participants self-reported being females while 82% of the total participants happen to be Africans. Furthermore, the length of working experience and level of education was tabulated with respondents asked to choose the relevant options with 71% of the participants below 10 years working experience in the management role and 54% have only matric as their level of education. The results show strong relationships between gender, race, education level and work experience towards understanding cybersecurity. The results on Table 1 show a correlation coefficients of 0.257. This means that the level of understanding cybersecurity is influenced by the gender, race, education level and work experience.

Similarly attitude is strongly influenced by gender, race, education level and work experience. There is a significantly strong correlation between gender, race, education level and work experience at 0.498 as shown in Table 2.

Table 13: Means, standard deviations, standard errors and correlation coefficients according to attitude towards cybersecurity threats (ATScT)

Variable	Sample size *n*	Mean	SD	Standard Error	Correlation Coefficient
Total	***224***	***2.47***	***1.23***	***0.52***	***0.498***
Gender	**224**	**2.54**	**1.27**	**1.13**	**0.5**
Male	86	2.4	1.27	0.14	0.529
Female	138	2.68	1.26	0.11	0.47
Race	**225**	**2.63**	**1.25**	**0.33**	**0.475**
African	184	2.57	1.29	0.1	0.502
Coloured	25	2.54	1.16	0.23	0.456
Indian	5	2.6	1.4	0.63	0.538
White	10	2.8	1.14	0.36	0.407
Education	**224**	**2.65**	**1.26**	**0.33**	**0.475**
Matric/ Grade12	120	2.59	1.24	0.11	0.479
Diploma	55	2.54	1.19	0.16	0.469
Degree	12	2.38	1.26	0.36	0.529
Post Graduate	14	2.11	1.29	0.34	0.611
Other	21	3	1.36	0.3	0.453
Not Applicable	2	3.25	1.19	0.75	0.366
Experience	**224**	**2.4**	**1.15**	**0.29**	**0.479**
1to 4 years	67	2.72	1.19	0.14	0.438
5- 10 years	92	2.67	1.34	0.14	0.501
11- 15 years	42	2.46	1.24	0.19	0.504
16- 20 years	9	1.72	1	0.33	0.581
20+ years	11	2.05	1.08	0.33	0.527
Not Applicable	3	2.83	1.08	0.62	0.82

There is a positive relationships established between understanding and attitudes towards cybersecurity, it can be concluded that that there is significant positive connection between understanding cybersecurity and understanding of the same.

4.3 Limited understanding of cybersecurity (LScU)

The 5 point Likert scale from one to five where 1= strongly disagree, 2= disagree, 3= neither agree nor disagree, 4= agree and 5= strongly agree was used to rate participants responses. The questions used to measure employee understanding were related to understanding of cyber-threats and if employees in the financial services industry understand the different malware and the latest cyber-attack trends. Furthermore, the other set of questions were on cybersecurity awareness examine if employees in the industry are skilled and informed to deal with cybersecurity threats. High scores indicate that employees have limited understanding of cybersecurity while low scores are indicative of high understanding.

Table 14: Scale items for all questions relating to limited understanding of cybersecurity and attitude towards cybersecurity threats and responses (%)

Cyber Threats

No.	Item	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
7	I am confident in my organisation overall security posture	41.3	40.9	12.4	4.4	0.9
8	I am aware of all different malwares and the latest cyber-attack trends	28.4	40	24	4.9	2.7
9	I am skilled and informed to deal with different cyber attacks	32.4	37.3	19.1	8.4	2.7
10	Willing to open e-mail attachments from strangers	3.6	4	8.1	14.8	69.5
11	Interesting subject line causes the opening of an e-mail	10.9	11.8	15.8	15.4	46.2

Cybersecurity Awareness

No.		Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
	I am aware and equipped enough to deal with the following Cyber-Threats:					
12	Phishing attacks	38.7	35.1	15.6	5.3	5.3
13	Ransomware	22.9	33.2	25.1	9.4	9.4
14	Trojan horse	19.1	24.2	34.9	9.8	12.1
15	Robot and Network (Botnet)	17.9	31.8	29.6	10.3	10.3

The overall confidence of employees in the organisational security posture was tabulated in item 7 and item 8 of the questionnaire. The respondents were given option to tick the relevant option provided and both questions achieved a 100% response rate. The respondents reported 82.2% and 68.4% respectively on either strongly disagreeing or disagreeing with tabulated questions on both items of the questionnaire. Item 9 of the questionnaire tabled a question around employees' skills to deal with cyber-attacks and 67.7% of the respondents reported no skill in dealing with cyber-attacks.

There is two studies in literature that highlighted the requirement organisation in sectors like the financial services industry are required to have information security policy in place as per regulatory authority and the policy must set mandatory guidelines to influence favourable organisational behaviour when employees use the systems (Van Niekerk and Von Solms, 2010) (Glaspie and Karwowski, 2017). It is further reported that when policies in relation to security are complex, ambiguous, complicated, vague or difficult for employees to understand, attitudes towards compliance are negatively impacted (Glaspie and Karwowski, 2017). The role of organisation in dealing with cyber threats is to ensure that information security policies are understandable, relevant and accessible to all employees. The results highlight limited understanding of cyber-threats which has direct correlation with lack of proper cybersecurity mitigation policies.

Participants were also asked to indicate their level of awareness in dealing with individual cyber-threats in item 12 to item 15. The participants demonstrated a level of consistency by strongly disagreeing and disagreeing with the statement that they are aware and equipped enough to deal with cyber-threats. All participants responded to the question on phishing attacks with 73.8% showing limited understanding and awareness to deal with this type of cyber-threat. Only 222 participant responded to question on ransomware and 81.2% of participants showed either limited understanding on this type of cyber-threat or they were uncertain about their level of knowledge. The last two items under this section was questions on Trojan and Botnet with participants showing a level of consistency with results highlighting limited level of understanding and uncertainty.

An international study by Tailor and Patel (2017) outlined the timeline and evolution of ransomware as the type of malware were attackers capitalise on limited knowledge of the end-user. The table above highlighted limited understanding of cyber-threats by participants and the continuous improvement in sophistication of this type of malware pose a high risk of intentional and unintentional threats to the financial services industry. The unintentional threats in the organisations are caused by low cybersecurity awareness and cyber threats, and include the accidental violations of information by employees (Ernst and Young, 2003). The definitions of different malwares in literature review demonstrate the level of risk that is modelled by lack of knowledge and awareness of cyber-threats.

4.4 Attitudes towards cybersecurity threats (ATScT)

Similarly, the Likert scale from 1- 5 was used to rate participants responses where 1= strongly disagree; 2= disagree; 3= neither agree nor disagree; 4= agree and 5= strongly agree. The questions used to qualify employee attitude were: I don't have enough time to read all security information and updates; all cybersecurity trainings are complex and technical to understand. Based on these questions, high scores indicate that employee attitudes are negative towards cybersecurity threats while lower scores indicate a positive attitude.

Table 15: Scale items for all questions relating to cybersecurity behaviour, employee attitude and responses (%)

Cybersecurity Behaviour:

No.	Item	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
16	Not interested reading Social Engineering issues	12.4	20.9	30.7	15.6	20.4
17	Not a target of social engineering attacks due to my role size	10	12.7	24.5	22.3	30.5
18	Unwilling to respond to e-mail messages to friendly and non-threatening strangers	25.8	22.6	20.3	12	19.4
19	I use work e-mail to subscribe to external websites and memberships	2.3	3.2	6.4	12.3	75.8
20	I receive e-mails from potential customers with attachments and links	8.7	16.4	14.2	17.4	43.4
21	My work e-mail account is linked with my social media accounts	1.4	0.5	5.6	6.9	85.6

Employee Attitude on Cybersecurity:

No.	Item	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
22	I do not need to worry about cyber-attack because my employer is having a strong IT team	13.8	10.7	16.1	17	42.4
23	All cybersecurity trainings are complex and technical to understand	15.2	21	23.2	21	19.8
24	I am competent enough to deal with cyber-attacks and threats	18.2	36.8	27.3	10.5	7.3
25	I have easy access information security policy	13.8	10.7	16.1	17	42.4
26	I don’t have enough time to read all security information and updates.	15.2	21	23.2	21	19.6

The participants were asked to indicate their level of agreement or disagreement with the statements on this section of the questionnaire. The two key items on employee attitude towards cybersecurity had 223 participants (99.5%) responding to both questions. The tables above give an overall feedback on behaviour of employees in the financial services which has a direct correlation with employee attitude towards cybersecurity. The high score of 40.8% from participants indicated that employees has negative attitude towards cybersecurity threats. According to a study in literature, positive employee attitudes about cybersecurity compliance and their involvement in the process is regarded as another factor that impacts the information security culture in an organisation.

The theoretical model for employees' cybersecurity policy compliance demonstrate that threat appraisal is part of the negative reinforcement and affects attitude of employees towards complying with cybersecurity policies and compliance strategies (Pahnila et al., 2007). The participants (23.2%) have demonstrated the level of uncertainty in their responds about the complexity and technicality to understand the cybersecurity concepts, a behaviour that is explained in literature using the theoretical model for employees' cybersecurity policy compliance.

The questionnaire included a section with set of statements on employees' behaviour around cybersecurity measures. The responses on this set of statements is important to understand some of the behaviours that lead to a specific attitude by employees. The Da Veiga and Eloff (2010) study emphasise the effectiveness of any counter measure to cyber-threats as a scope of technical and non-technical controls. The study cited the focus of cybersecurity measure as the shift from technology to human factors such as management support, incentive, training and awareness. The level of responses on employees gives an indication of information security culture in the industry. The overall response of participants on all items under this section of the questionnaire appear to be negative, which is consistent with the findings on employees' attitude towards cybersecurity.

4.5 Summary of the results/findings

4.5.1 *Limited understanding of cybersecurity*

The responses in general show that employees have limited cybersecurity awareness and limited knowledge of the recent cyber-threats trends. The scores on the two questions reveal that 69% of the employees disagree and highly disagree that they are skilled and that they are aware of cybersecurity. The scores also revealed a mean of 3.82 with a standard deviation of 0.97 and a standard error of 0.21. The 95% confidence level shows an average of 4 which leads to the P-value being less than the alpha, therefore, the null hypothesis is rejected.

4.5.2 *Attitudes towards cybersecurity threats (ATScT)*

In general, the responses show that employees are showing negative attitude towards cybersecurity based on their responses on the two key questions asked on attitude. The high scores indicate negative attitude with an average of 25% stuck on neither agree nor disagree while 40.8% disagreed we both statements. The mean score was low at 2.47 with a standard deviation of 1.23 and a standard error of 0.53. The 95% correlation coefficient level shows an average of 2.75 which leads to the P-value being less than the alpha, therefore, the null hypothesis is reject in favour of the alternative hypothesis.

Table 16: One-Sample Test of the study

One-Sample Test						
Item No: 7 - 26	test value = 0					
	t	df	sig. (2-tailed)	Mean difference	95% confidence interval of the difference	
					lower	upper
I am confident in my organisation overall security posture	71,389	224	,000	4,173	4,06	4,29
I am aware of all different malware and the latest cyber-attack trends	59,619	224	,000	3,867	3,74	3,99
I am skilled and informed to deal with different cyber attacks	55,943	224	,000	3,884	3,75	4,02
Willing to open e-mail attachments from strangers	22,581	222	,000	1,574	1,44	1,71
Interesting subject line causes the opening of an e-mail	23,673	220	,000	2,258	2,07	2,45
Phishing attacks	53,407	224	,000	3,964	3,82	4,11
Ransomware	43,231	222	,000	3,507	3,35	3,67
Trojan horse	39,149	214	,000	3,284	3,12	3,45
Robot and network (Botnet)	42,162	222	,000	3,368	3,21	3,53
Not interested reading social engineering issues	33,523	224	,000	2,893	2,72	3,06
Not a target of social engineering attacks due to my role size	28,211	219	,000	2,495	2,32	2,67
Unwilling to respond to e-mail messages to friendly and non-threatening strangers	32,834	216	,000	3,235	3,04	3,43
I use work e-mail to subscribe to external websites and memberships	23,174	218	,000	1,438	1,32	1,56
I receive e-mails from potential customers with attachments and links	24,438	218	,000	2,297	2,11	2,48
My work e-mail account is linked with my social media accounts	26,102	215	,000	1,250	1,16	1,34
I do not need to worry about cyber-attack because my employer is having a strong it team	24,239	223	,000	2,366	2,17	2,56
All cybersecurity trainings are complex and technical to understand	32,357	223	,000	2,911	2,73	3,09
I am competent enough to deal with cyber- attacks and threats	45,926	219	,000	3,482	3,33	3,63
I have easy access information security policy	37,960	221	,000	3,387	3,21	3,56
I don't have enough time to read all security information and updates.	28,200	223	,000	2,250	2,09	2,41

4.6 Conclusion

The statistical analysis for the study, the interpretation of the results were presented in table format and discussed in this chapter. Different studies from literature were used to emphasise areas of the findings and indicate similar finding in literature. The data collected from 224 respondents from the financial services industry revealed a limited cybersecurity awareness and limited knowledge of the recent cyber-threats trends. This limited knowledge found to be present within the financial services industry is a level of vulnerability that attackers exploit regularly and indicates the need for CIA triad and ISO/IEC 27000 frameworks to address the shortcomings. The following chapter will conclude the study by discussing the findings in relation to research questions, make practical recommendations and suggestions for further studies.

CHAPTER 5. CONCLUSIONS and RECOMMENDATIONS

5.1 Introduction

This chapter will summarises the conclusions of the study by integrating the analysed findings about the hypothesis and answer both research questions. The conclusions will include a brief discussion presented according to individual research questions, the rationale of the findings and synopsis of the literature review findings. The answers to these research questions makes it possible to give recommendations for different stakeholders identified in the study and suggested areas for further research.

5.2 Conclusions regarding state of cybersecurity awareness for employees in the financial services industry.

In order to establish the nature of employee attitude towards cybersecurity and cyber-threats, two unknown elements were investigated. The first ultimate question the study aimed to answer was to understand the level of cybersecurity awareness in the industry. This question is fundamental to the study to understand the efforts of employees in educating themselves and the level in which they see organisation putting in reliable security measures. The sub-question looked at the level of understanding on the most common cybersecurity-threats to provide a base to answer the main question. The question examined details such as common cyber-threats which can be action using common communication system such as e-mails. The responses to the main question and sub-question were documented in section 4.3 of the analysis.

The study shows a limited cybersecurity awareness as reported in section 4.3 as average of 82.2% of the respondents either disagreed or strongly disagreed with all statements tabulated. The result is in contrary to the PwC report on cybersecurity in the financial services industry that suggested the higher digital walls alone will not protect organisation from cyber-attacks (PwC, 2019). The report highlighted employees' knowledge and awareness on areas such as social engineering techniques as important and recommended that organisation must consider cybersecurity awareness programmes. The Deloitte (2018) report put

emphasis on the evolving technology, risk and compliances that is exposed that the finding of the study.

The study confirmed also that the overwhelming majority of the employees in the financial services industry are not cyber-savvy when it comes to basic cyber-threats. This was confirmed by an average of 68.4% respondents who highlighted limited knowledge common cyber-threats such as phishing attacks, ransomware, Trojan and botnet. The finding is in harmony with Mimecast report on the state of e-mail security in South Africa that reported a 63% increase in impersonation fraud and 84% in e-mail based spoofing. The Mimecast research was not performed in the context of South African financial services industry, however, it illustrate the same conclusion as research focused on e-mail users across industries.

In answering the research question, the study found that the current state of cybersecurity awareness is limited in the financial services industry and the level of understanding on aspects of password usage, phishing, social engineering and online scam is low. There has been limited researches on attitude of employees towards cybersecurity that the study can compare. However, there are different frameworks and models in literature that the study identified to address the shortcomings of the findings. The application of ISO/IEC 27001 framework provide cybersecurity guidelines and structure on implementing awareness training (Disterer, 2013). The CIA triad model designate areas of the organisations and critical elements of the security system that is exposed to cyber-attacks (Cherdantseva and Hilton, 2013).

5.3 Conclusions regarding employee attitude towards cybersecurity threats

The other fundamental question that the study aim to answer was to look at employee behaviour towards basic security practices and the general attitude towards cyber-threats. The study shows two contrasting indicators to the behaviour of employees in the financial services industry. There is a high number of respondents (30.7%) who were either uncertain or disagreeing (33.3%) with

the statement that employees are not interested in reading about Social Engineering issues. On the contrary, there is 52.8% of the respondents who do believe to be the target of cyber-attacks because of their role within the organisation. This findings are not supported by Ernst and Young (2003) research that confirmed that unintentional threats are caused by limited cybersecurity awareness and threats, including the accidental violations of information by employees.

The study shows a reckless attitude by employees in terms of e-mail usage as analysed in section 4.5.2 with 69.4% of respondents having limited access to information security policy. The Da Veiga and Eloff (2010) study on cybersecurity culture covered under literature review underlined the non-technical controls that impact countermeasures on cybersecurity. This non-technical controls such as information security policy, employee attitude and awareness are identified as areas that hinder the promotion of cybersecurity culture within the organisation. (Da Veiga and Eloff, 2010). The application of ISO/IEC 27001 framework provide cybersecurity guidelines and structure on implementing of information technology policies with an organisation (Disterer, 2013).The implementation of ISMS as outlined by the ISO/IEC 27001 framework will systematically and sensibly protecting the confidentiality, availability and integrity of data from vulnerabilities.

In answering the research question, the study found that there is level of reckless in e-mail usage and policy compliance that can be linked to negative attitude of employees towards cybersecurity. There is limited studies in literature that the current study can build on, however, there is existing model to improve some of the findings. The Da Veiga and Eloff (2010) study presents a model on factors that can influences cybersecurity cultures within the organisation. This model will contribute in assisting organisations within the financial services industry to create positive cyber-savvy culture and improve the level of risk policy compliance (Da Veiga and Eloff, 2010). The key objectives of financial services industry is to ensure that the confidentiality of information is protected while maintaining strong integrity controls. Successful implementation of this model will assist the industry to maintain this key objectives.

5.4 Recommendations

The financial services industry is experiencing a constant cyber-attacks with a high magnitude and level of sophistication. In order to reduce the impact of this cyber-attacks, the study make recommendations based on the industry and discoveries made through the analysis. The following recommendations are based on the two identified stakeholders and some of the key findings in literature review:

5.4.1 *Organisations in the Financial Services Industry*

Recommendation 1: Implementation of Information Security Management Systems across the industry.

The financial services industry needs to develop a framework that can guide their information security measures. The participating employees in this study demonstrated a level of reckless in their conducts within cyberspace and there is limited knowledge and awareness in terms of the latest cyber-threats. There is no clear and obvious link between human factors and technological aspects of cyber security. Furthermore, it is acknowledged in literature that employees are often the weakest link in cyber security measures. The ISMS framework is critical in creating common focus between the human and technological aspect of the organisation through adequate risk assessment and risk management.

The ISO/IEC 27001 offer the PCDA model for the organisation as a guide to implement ISMS and ensure continuous improvement of the processes. PCDA model is directly linked to the management system with the aim to establish key risk areas for organisations individually, implement risk controls and continuously improve the efficiency of ISMS (Susanto and Shobariah, 2016). The ISMS assists organisation within the financial industry to evolve their security controls mechanisms as their risks, culture and resources change. Organisation can build their own ISMS framework or acquire ready-made product from the market.

Recommendation 2: Implement Cybersecurity awareness and training program for employees.

The implementation of awareness and training program in the financial industry that is in line with ISO/IEC framework will protect the industry by reducing errors, promoting positive attitude towards risk policies and enhance overall organisational security. Informed and trained employees will improve compliance and help with employee morale. Pahnila et al. (2007) introduced a theoretical model that organisation can adopt as a guiding theory to build effective training program. The model presents motivating stimulus for employees after a specific behaviour is displayed, encouraging this behaviour to be repeated in future (Pahnila et al., 2007). The negative reinforcements in the model are factors that are encouraging a specific behaviour by avoiding a negative stimuli or consequences (Schieltz, Wacker and Romani, 2017).

There is an element of human error in the study that can be directed to lack of threats awareness, limited knowledge of malwares and attitudes cyber security processes in an industry with highly sophisticated software and hardware protection (Pollock, 2017).The PricewaterhouseCoopers research confirmed that cyber security awareness and training will not ensure adequate protection against cyber threats, however, their survey has shown that organisations with a well-crafted awareness training have less cyber related events compared to their counterparts (PwC, 2019). The volume, sophistication and diversity of attacks requires employees with a high level of information technology awareness and the right disposition in cyber threats (Modina, 2015).

5.4.2 *Employees in the Financial Services Industry*

Recommendation 1: Participation in cybersecurity programs

There is studies in literature on cybersecurity training and awareness that recommends mandatory compliance training for all employees. The success of this kind of measure depends on employees and management compliance relationship. The respondents of the study highlighted a level of ignorance from the side of employees in how e-mail access is utilised. Recommendations is for employees to play a role in creating cybersecurity by participating in policy formulation, reporting of incidents and continuously educating themselves on recent cyber trends. Pahnila et al. (2007) explain the importance of consistency

and habits in cybersecurity measures as being the actual influence in employee behaviour in a long run.

5.5 Suggestions for further research

a) **The attitude of Executives towards cybersecurity awareness in the financial services industry**

This study has exposed a limited cybersecurity awareness and knowledge from the side of employees. The study needs to be done to scrutinise the level of executive knowledge and attitude towards cybersecurity. This study will further assist to analyse the challenging areas of cybersecurity by comparing the findings of both studies.

b) **The impact of culture on cybersecurity policy implementation and compliance**

Further study needs to be done to if there is correlation between cultures and how organisation within the financial services industry can combat with the rising threat that is posed by cyber-attacks. Issues of culture in a country that still lag behind in technological development is still important in both strategy formulation and creation of information management systems

5.6 Conclusion

In conclusion, this study set out to examine the attitudes of employees towards information security and cybersecurity threats in the financial services industry. The cyber-attacks in the industry target organisations through confidentiality, integrity and availability as the three main areas of information security. These area of information security are either exposed or protected by employee information security awareness, which has direct impact on human behaviour such as attitude (Ani, He and Tiwari, 2019). Based on this areas of information security, this chapter concluded the study by answering research questions and give recommendation based on reviewed literature.

REFERENCES

Abomhara, M. (2015). Cybersecurity and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cybersecurity and Mobility*, *4*(1): 65-88. River Publishers.

Adams, M., and Makramalla, M. (2015). Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1). Talent First Network (Carleton University).

Aginsa, A., Edward, I. Y. M., and Shalannanda, W. (2016). Enhanced information security management system framework design using ISO 27001 and Zachman framework-A study case of XYZ company. In *2016 2nd International Conference on Wireless and Telematics (ICWT)* (pp. 62-66). IEEE.

Alavi, R., Islam, S., Jahankhani, H. and Al-Nemrat, A. (2013). Analyzing human factors for an effective information security management system. *International Journal of Secure Software Engineering (IJSSE)*, *4*(1), 50-74. IGI Global.

Amoroso, E. G. and Amoroso, M. E. (2017). *From CIA to APT: An Introduction to Cybersecurity*. Independently published.

Andrade, C. (2018). Internal, external, and ecological validity in research design, conduct, and evaluation. *Indian journal of psychological medicine*, *40*(5), 498. Medknow Publications.

Antonius, R. (2012). *Interpreting quantitative data with IBM SPSS statistics*. Sage Publications.

Arachchilage, N. A. G., Love, S., and Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185-197. Elsevier B.V.

Bada, M., Sasse, A. M., and Nurse, J. R. (2019). Cybersecurity awareness campaigns: Why do they fail to change behaviour? Elsevier B.V.

Badie, N., and Lashkari, A. H. (2012). A new evaluation criteria for effective security awareness in computer risk management based on AHP. *Journal of Basic and Applied Scientific Research*, *2*(9), 9331-9347. Textroad Publication.

Barends, A. J., and de Vries, R. E. (2019). Noncompliant responding: Comparing exclusion criteria in MTurk personality research to improve data quality. *Personality and individual differences*, *143*, 84-89.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24-31. Elsevier B.V.

Bertino, E., and Islam, N. (2017). Botnets and internet of things security. *Computer*, (2): 76-79. IEEE

Bhattacherjee, A., and Shrivastava, U. (2018). The effects of ICT use and ICT Laws on corruption: A general deterrence theory perspective. *Government Information Quarterly*, *35*(4), 703-712. Elsevier B.V.

Bouveret, A. (2018). *Cyber risk for the financial sector: a framework for quantitative assessment*. International Monetary Fund. IMF Working Paper.

Bryman, A. (2015). *Social research methods*. New York: Oxford University Press.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality--Based Beliefs and Information Security Awareness. *MIS Quarterly,* Vol. 34, No. 3, pp. 523–527. Information Systems Research Center

Calder, A. (2016). Nine Steps to Success: An ISO27001: 2013 Implementation Overview. IT Governance Ltd.

Carter, W. (2017). Forces Shaping the Cyber Threat Landscape for Financial Institutions. Swift Institute Working Paper No. 2016-004.

Cernov, A. M. (2018). Security in Computer Networks. *International Journal of Information Security and Cybercrime (IJISC)*, *7*(1), 45-52. RAISA.

Chawla, M., and Chouhan, S. S. (2014). A survey of phishing attack techniques. *International Journal of Computer Applications*, *93*(3).

Cherdantseva, Y., and Hilton, J. (2013). A reference model of information assurance and security. In *2013 International Conference on Availability, Reliability and Security* (pp. 546-555). IEEE.

Creswell, J. W. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Deloitte (2018). Taking cyber risk management to the next level, [online] Available: https://www2.deloitte.com/tr/en/pages/risk/articles/cyber-risk-management-financial-services-industry.html [Accessed 21 August 2019].

Dong, Y., & Peng, C. Y. J. (2013). Principled missing data methods for researchers. *SpringerPlus*, *2*(1), 222.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Scientific Research Publishing.

Flores, W. R., Antonsen, E., and Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral

information security governance and national culture. *Computers and security*, *43*, 90-110. Elsevier B.V.

Gibbs, G. R. (2018). *Analyzing qualitative data* (Vol. 6). Sage.
Glaspie, H. W., and Karwowski, W. (2017). Human factors in information security culture: a literature review. In: *International Conference on Applied Human Factors and Ergonomics* (pp. 269-280). Springer, Cham.

Hari, A., and Lakshman, T. V. (2016). The internet blockchain: A distributed, tamper-resistant transaction framework for the internet. In: *Proceedings of the 15th ACM Workshop on Hot Topics in Networks* (pp. 204-210). ACM.

Hayes, J. (2014). *The theory and practice of change management*. Macmillan

Heale, R., and Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-based nursing*, *18*(3), 66-67.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Artech House.

Humphreys, T., and Plate, A. (2006). *Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001*. BSi Business Information.

Huster, T. P., Chiang, C. Y. J., Chadha, R., and Swami, A. (2018). Towards the development of robust deep neural networks in adversarial settings. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)* (pp. 419-424). IEEE.

Jones, H. S., and Towse, J. (2018). Examinations of Email Fraud Susceptibility: Perspectives from Academic Research and Industry Practice. In: *Psychological and Behavioral Examinations in Cybersecurity* (pp. 80-97). IGI Global.

Kang, J. W., and Namkung, Y. (2019). The information quality and source credibility matter in customers' evaluation toward food O2O commerce. *International Journal of Hospitality Management*, *78*, 189-198. Elsevier B.V.

Kaspersky Lab (2019). Threat Intelligence, [online] Available https://www.kaspersky.co.za/enterprise-security/cybersecurity-services [Accessed 21 August 2019].

Korpela, K. (2015). Improving cybersecurity awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, *24*(1-3), 72-77. Taylor and Francis.

Kostopoulos, G. (2017). *Cyberspace and cybersecurity*. Auerbach Publications.

Kyriazos, T. A. and Stalikas, A. (2018). Applied psychometrics: The steps of scale development and standardization process. *Psychology*, *9*(11), 2531-2560.

Li, T., Vedula, S.S., Hadar, N., Parkin, C., Lau, J. and Dickersin, K. (2015). Innovations in data collection, management, and archiving for systematic reviews. *Annals of internal medicine*, *162*(4), pp. 287-294. American College of Physicians (United States)

Market Business News (MBN) (2020). [Online] Available: https://marketbusinessnews.com/financial-glossary/cyber-security-definition/ [Accessed 15 April 2020].

Mimecast (2019). Secure Email Gateway, [online] Available https://www.mimecast.com/solutions/email-security/ [Accessed 21 August 2019].

Modina, M. (2015). Internal Rating Systems: A Critical Vision. In: *Credit Rating and Bank-Firm Relationships* (pp. 48-70). Palgrave Macmillan

Moghaddasi, H., Sajjadi, S., and Kamkarhaghighi, M. (2016). Reasons in support of data security and data security management as two independent concepts: a new model. *The Open Medical Informatics Journal*, *10*, 4. CrossMark

Mohajan, H. K. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University. Economic Series*, *17*(4), 59-82. CEEOL Publishers

Montano, D. E., and Kasprzyk, D. (2015). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. *Health behavior: Theory, research and practice*, *70*(4), 231. Jossey – Bass

Muijs, D. (2010). *Doing quantitative research in education with SPSS*. Sage.

Nardi, P. M. (2018). *Doing survey research: A guide to quantitative methods*. Routledge.

Nicewander, W. A. (2018). Conditional reliability coefficients for test scores. *Psychological Methods*, *23*(2), 351.

O'Leary, D. E. (2019). What Phishing E-mails Reveal: An Exploratory Analysis of Phishing Attempts Using Text Analyzes. *Journal of Information Systems*. AAA Digital Library.

Onwuegbuzie, A. J. (2000). Expanding the Framework of Internal and External Validity in Quantitative Research. APA PsycNet

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., and Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management and Computer Security*. Emerald Group Publishing Limited

Pattanavichai, S. (2018). Design Network Model for Information Security Management Standard depend on ISO 27001. *GSTF Journal on Computing*, *5*(4). IT Governance Publishing

Pollock, T. (2017). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). Digital Commons

PwC (2019). Building a united front on financial crimes in the financial services sector, [online] Available https://www.pwc.co.za/en/press-room/cyber-security.html [Accessed 21 August 2019].

Qadir, S., and Quadri, S. M. K. (2016). Information availability: An insight into the most important attribute of information security. *Journal of Information Security*, *7*(3), 185-194. Scientific Research Publishing

Sabillon, R., Serra-Ruiz, J., and Cavaller, V. (2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology (JCIT)*, *21*(3), 26-39. IGI Global

Sabric (2018). SABRIC ANNUAL CRIME STATS, [online] Available https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2018/ [Accessed 21 August 2019].

Safa, N. S., Von Solms, R., and Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and security*, *56*, 70-82. Elsevier B.V.

Sikorski, M., and Honig, A. (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software*. No Starch Press.

Singh, A. N., Gupta, M. P., and Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*. Emerald Group Publishing Limited

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. Elsevier

Stoll, M. (2015). An Information Security Model for Implementing the New ISO 27001. In *Handbook of Research on Emerging Developments in Data Privacy* (pp. 216-238). IGI Global.

Sukamolson, S. (2010). Fundamentals of quantitative research. *Language Institute, Chulalongkorn University*. Academia Publishing

Susanto, A., and Shobariah, E. (2016). Assessment of ISMS based on standard ISO/IEC 27001: 2013 at DISKOMINFO Depok City. In *2016 4th International Conference on Cyber and IT Service Management* (pp. 1-6). IEEE.

Swami, R., Dave, M., and Ranga, V. (2019). Software-defined Networking-based DDoS Defense Mechanisms. *ACM Computing Surveys (CSUR)*, *52*(2), 28. ACM Digital Library

Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., and Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581. Elsevier B.V.

Theofanidis, D., and Fountouki, A. (2018). Limitations and delimitations in the research process. *Perioperative nursing*,*7*(3), 155-163.

Van Niekerk, J. F., and Von Solms, R. (2010). Information security culture: A management perspective. *Computers and security*, *29*(4), 476-486. Elsevier B.V.

Van Puyvelde, D., and Brantly, A. F. (2019). *Cybersecurity: politics, governance and conflict in cyberspace*. John Wiley and Sons.

Vance, A., Siponen, M., and Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information and Management*, *49*(3-4), 190-198. Elsevier B.V.

Von Solms, R., and Van Niekerk, J. (2013). From information security to cybersecurity. *Computers and security*, *38*, 97-102. Elsevier B.V.

Yzer, M. (2017). Theory of reasoned action and theory of planned behavior. *The International Encyclopedia of Media Effects*, 1-7. SAGE Journals

Zimbardo, P. G. (2017). On the ethics of intervention in human psychological research: With special reference to the Stanford prison experiment. Routledge

APPENDIX A - QUESTIONNAIRE

Research Study

Letter of Information

(Re: Surveys/Questionnaires)

Good day

Survey link: http://omfhrl02.za.omlac.net/mod/feedback/edit.php?id=8335

Title of the study: Examining the attitude of employees towards information security and cybersecurity threats in the financial services industry.

Student: Moroka William, 2288660

Supervisor(s): Dr George Tweneboah

You are invited to participate in the abovementioned survey as part of my research project required in order to fulfil my **Master of Management in Digital Business** (MMDB) qualification at **WITS Business School.** The survey should take you approximately 10 minutes to complete. You do not have to answer any questions that you do not want to answer.

Purpose of the Study: This research is a quantitative method study to improve the understanding of cybersecurity knowledge and attitudes of employees towards cybersecurity threats in the financial services industry.

The information that you will share will remain strictly confidential and will be used solely for the purposes of this research. The only people who will have access to the research data are the researcher, the study supervisor and Wits Business School. Your answers to close-ended questions may be used verbatim in presentations and publications, but neither you nor your organisation will be identified. Results will be published in pooled (aggregate) format. Anonymity is guaranteed since you are not being asked to provide your name or any personal identification.

If you have any questions or concerns about the research, please feel free to contact the researcher via email William.moroka@omfinance.co.za and/or my supervisor Dr George Tweneboah on george.tweneboah@wits.ac.za.

Should you experience any difficulties accessing the link above, please contact Sjanel Vosloo on email Sjanel.Vosloo@omfinance.co.za.

Your support and participation will be highly appreciated.

Moroka William

24 January 2020

Section A: Biographical Details

1. Gender:

☐ **Male** ☐ **Female**

2. Age:

Up to 20 Years	☐
21 - 30 Years	☐
30 - 40 Years	☐
41 50 Years	☐
51 - 60 Years	☐
61 – 65 Years	☐

3. Race

☐ **African**
☐ **Coloured**
☐ **Indian**
☐ **White**
☐ **Other** Specify……

4. Qualification:

☐ **Matric/Grade 12**
☐ **Diploma**
☐ **Degree**
☐ **Postgraduate Qualification**
☐ **Other** Specify……

5. Experience:

☐ **B1 - 4 years**
☐ **5 - 10 years**
☐ **11 - 15 years**
☐ **16 - 20 years**
☐ **Above 20 years**

SECTION B

Cyber Threats

No.	Item	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
7	I am confident in my organisation overall security posture	1	2	3	4	5
8	I am aware of all different malwares and the latest cyber-attack trends	1	2	3	4	5
9	I am skilled and informed to deal with different cyber attacks	1	2	3	4	5
10	Willing to open e-mail attachments from strangers	1	2	3	4	5
11	Interesting subject line causes the opening of an e-mail	1	2	3	4	5

Cybersecurity Awareness

No.	I am aware and equipped enough to deal with the following	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
12	Phishing attacks	1	2	3	4	5
13	Ransomware	1	2	3	4	5
14	Trojan horse	1	2	3	4	5
15	**Robot and Network (Botnet)**	1	2	3	4	5

SECTION C

Cybersecurity Behaviour:

No.	Item	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
16	Not interested reading Social Engineering issues	1	2	3	4	5
17	Not a target of social engineering attacks due to my role size	1	2	3	4	5
18	Unwilling to respond to e-mail messages to friendly and non-threatening strangers	1	2	3	4	5
19	I use work e-mail to subscribe to external websites and memberships	1	2	3	4	5
20	I receive e-mails from potential customers with attachments and links	1	2	3	4	5
21	My work e-mail account is linked with my social media accounts	1	2	3	4	5

Employee Attitude on Cybersecurity:

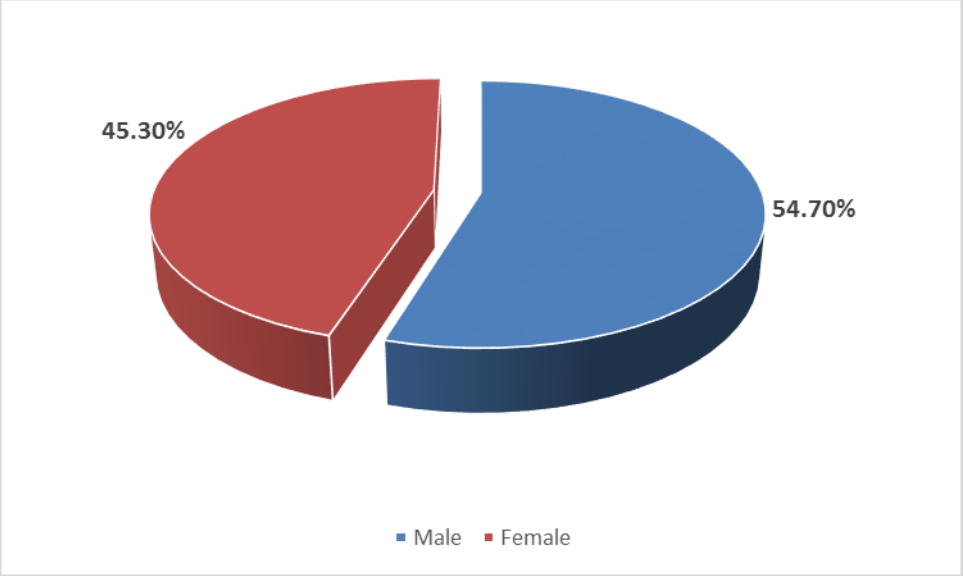
No.	Item	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
22	I do not need to worry about cyber-attack because my employer is having a strong IT team	1	2	3	4	5
23	All cybersecurity trainings are complex and technical to understand	1	2	3	4	5
24	I am competent enough to deal with cyber-attacks and threats	1	2	3	4	5
25	I have easy access information security policy	1	2	3	4	5
26	I don't have enough time to read all security information and updates.	1	2	3	4	5

APPENDIX B – DEMOGRAPHIC PROFILE

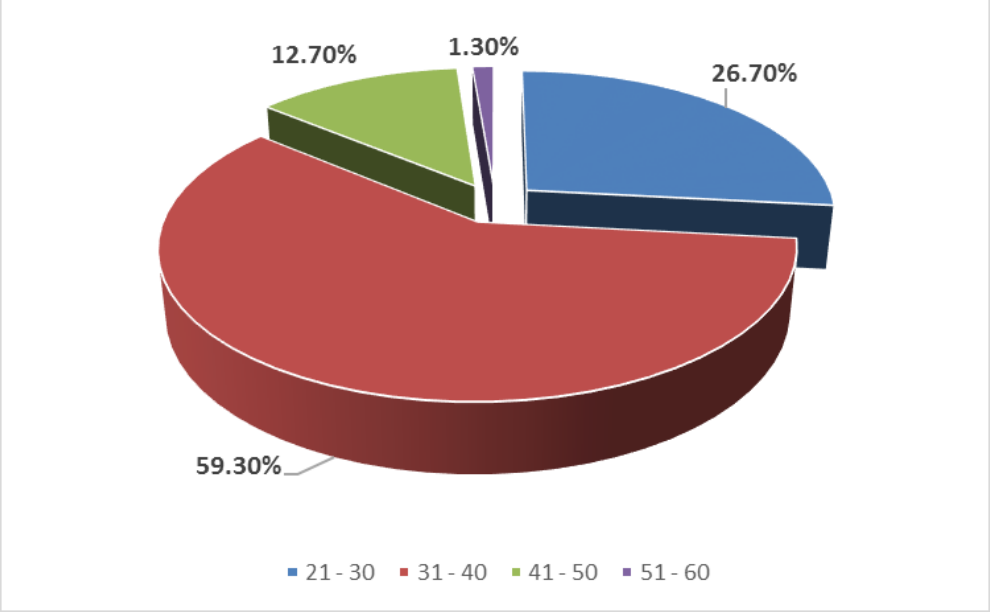
POPULATION DEMOGRAPHIC PROFILE

The following information was solicited from the population: gender, age, race, qualification and work experience. The demographic profile of respondents is presented in the following sub-sections.

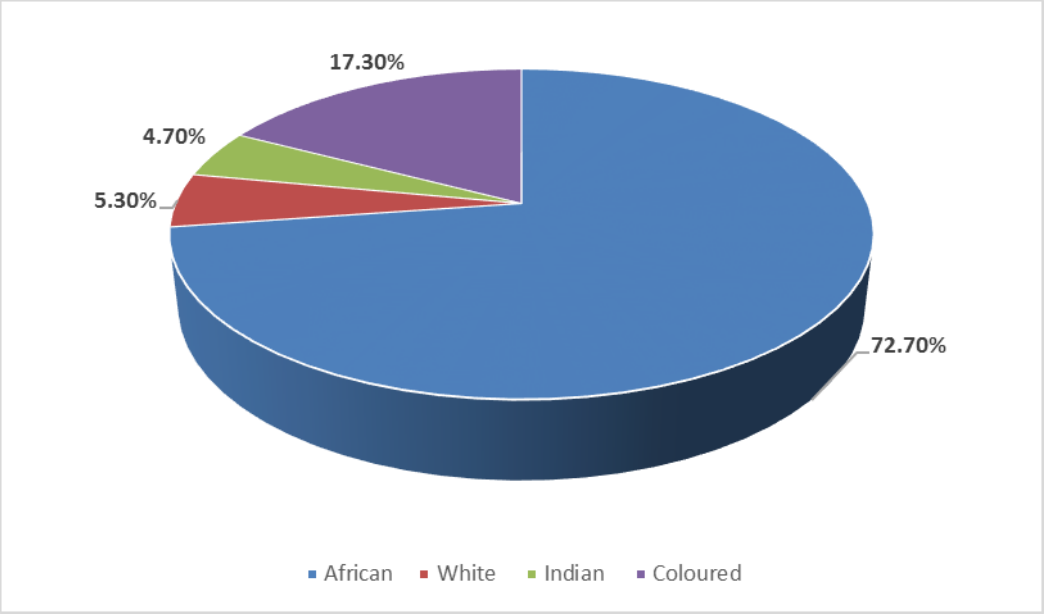
Gender



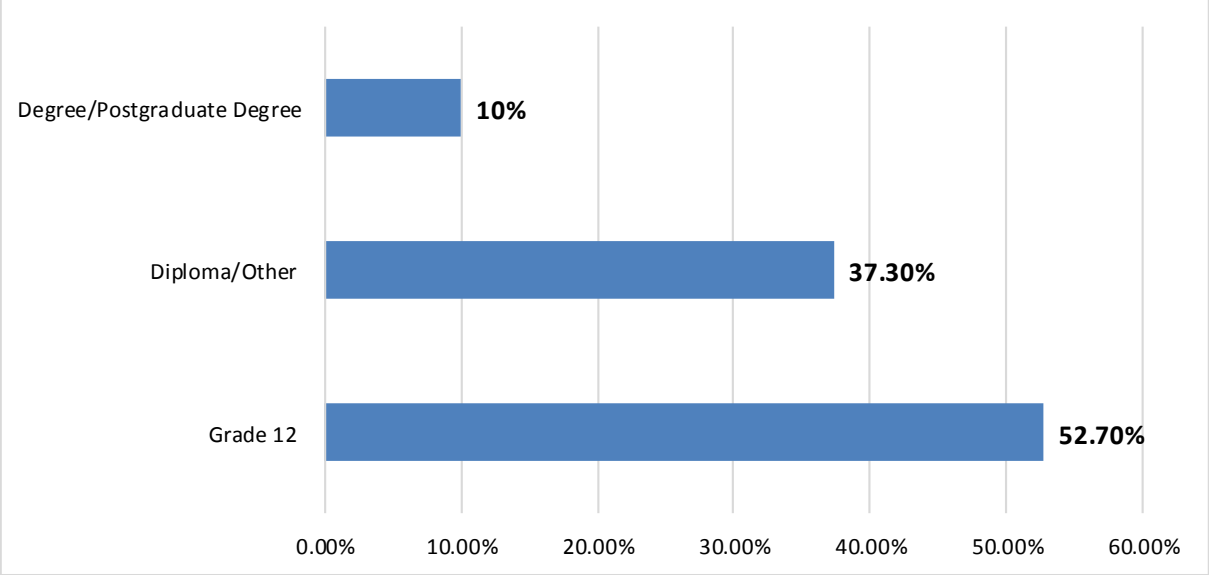
Age



Race

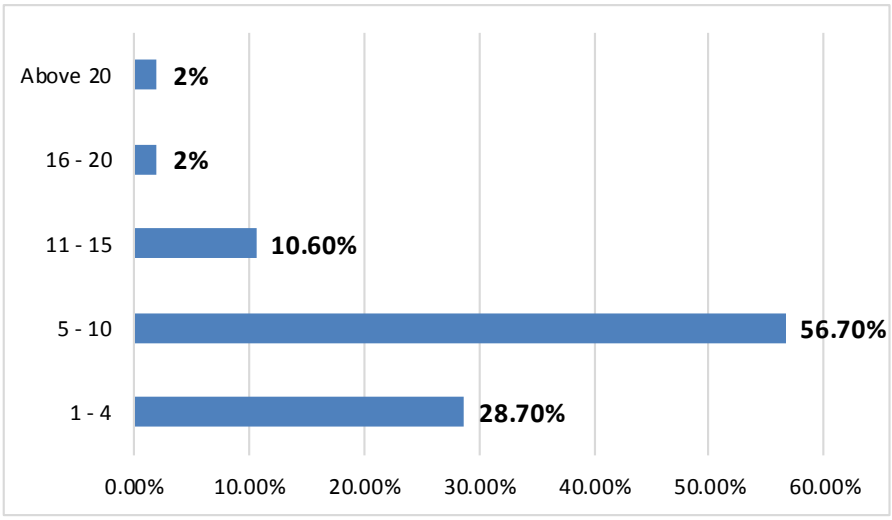


Qualification



.

Work Experience


Above 20
2%
16 - 20
2%
11 - 15
10.60%
5 - 10
56.70%
1 - 4
28.70%
0.00%
10.00%
20.00%
30.00%
40.00%
50.00%
60.00%

APPENDIX C - ANALYSIS

Variable	Sample size *n*	Mean	SD	Standard Error	Correlation Coefficient
Total	**224**	**3.82**	**0.97**	**0.21**	**0.253**
Gender	**224**	**3.86**	**1.02**	**0.10**	**0.264**
Male	86	3.80	1.10	0.12	0.289
Female	138	3.92	0.95	0.08	0.242
Race	**225**	**3.83**	**0.96**	**0.2**	**0.250**
African	184	3.89	1.04	0.08	0.267
Coloured	25	3.71	0.77	0.16	0.207
Indian	5	3.70	0.98	0.23	0.264
White	10	4.00	1.05	0.33	0.263
Education	**224**	**3.84**	**0.94**	**0.29**	**0.245**
Matric/ Grade 12	120	3.93	0.94	0.09	0.239
Diploma	55	3.94	1.05	0.14	0.266
Degree	12	3.77	0.83	0.23	0.220
Post-Graduate	14	3.43	1.39	0.78	0.405
Other	21	3.69	1.08	0.23	0.292
Not Applicable	2	4.25	0.35	0.25	0.082
Experience	**224**	**3.76**	**0.96**	**0.24**	**0.255**
1to 4 years	67	3.57	1.03	0.12	0.289
5- 10 years	92	4.13	0.95	0.10	0.230
11-15 years	42	3.92	0.93	0.14	0.237
16-20 years	9	3.69	1.34	0.48	0.363
20+ years	11	3.76	1.02	0.32	0.271
Not Applicable	3	3.50	0.50	0.29	1.43

Table 2: Means, standard deviations, standard errors and correlation coefficients according to attitude towards cybersecurity threats (ATScT)

Variable	Sample size *n*	Mean	SD	Standard Error	Correlation Coefficient
Total	**224**	**2.47**	**1.23**	**0.52**	**0.498**
Gender	**224**	**2.54**	**1.27**	**1.13**	**0.500**
Male	86	2.40	1.27	0.14	0.529
Female	138	2.68	1.26	0.11	0.470
Race	**225**	**2.63**	**1.25**	**0.33**	**0.475**
African	184	2.57	1.29	0.10	0.502
Colored	25	2.54	1.16	0.23	0.456
Indian	5	2.60	1.40	0.63	0.538
White	10	2.80	1.14	0.36	0.407
Education	**224**	**2.65**	**1.26**	**0.33**	**0.475**
Matric/ Grade12	120	2.59	1.24	0.11	0.479
Diploma	55	2.54	1.19	0.16	0.469
Degree	12	2.38	1.26	0.36	0.529
Post-Graduate	14	2.11	1.29	0.34	0.611
Other	21	3.00	1.36	0.30	0.453
Not Applicable	2	3.25	1.19	0.75	0.366
Experience	**224**	**2.40**	**1.15**	**0.29**	**0.479**
1 to 4 years	67	2.72	1.19	0.14	0.438
5 - 10 years	92	2.67	1.34	0.14	0.501
11 - 15 years	42	2.46	1.24	0.19	0.504
16 - 20 years	9	1.72	1.00	0.33	0.581
20+ years	11	2.05	1.08	0.33	0.527
Not Applicable	3	2.83	1.08	0.62	0.82

Table 3: Scale items for all questions relating to limited understanding of cybersecurity and attitude towards cybersecurity threats and responses (%)

Index	Item	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
1	I am confident in my organisation overall security posture	41.3	40.9	12.4	4.4	0.9
2	I am aware of all different malwares and the latest cyber-attack trends	28.4	40	24	4.9	2.7
3	I am skilled and informed to deal with different cyber attacks	32.4	37.3	19.1	8.4	2.7
4	Willing to open e-mail attachments from strangers	3.6	4	8.1	14.8	69.5
5	Interesting subject line causes the opening of an e-mail	10.9	11.8	15.8	15.4	46.2
6	Phishing attacks	38.7	35.1	15.6	5.3	5.3
7	Ransomware	22.9	33.2	25.1	9.4	9.4
8	Trojan horse	19.1	24.2	34.9	9.8	12.1
9	Robot and network (botnet)	17.9	31.8	29.6	10.3	10.3
10	Not interested reading social engineering issues	12.4	20.9	30.7	15.6	20.4
11	Not a target of social engineering attacks due to my role size	10	12.7	24.5	22.3	30.5
12	Unwilling to respond to e-mail messages to friendly and non-threatening strangers	25.8	22.6	20.3	12	19.4
13	I use work e-mail to subscribe to external	2.3	3.2	6.4	12.3	75.8

Index	Item	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
	websites and memberships					
14	I receive e-mails from potential customers with attachments and links	8.7	16.4	14.2	17.4	43.4
15	My work e-mail account is linked with my social media accounts	1.4	0.5	5.6	6.9	85.6
16	I do not need to worry about cyber-attack because my employer is having a strong it team	13.8	10.7	16.1	17	42.4
17	All cybersecurity trainings are complex and technical to understand	15.2	21	23.2	21	19.8
18	I am competent enough to deal with cyber-attacks and threats	18.2	36.8	27.3	10.5	7.3
19	I have easy access information security policy	13.8	10.7	16.1	17	42.4
20	I don't have enough time to read all security information and updates.	15.2	21	23.2	21	19.6

One-Sample Test						
	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I am confident in my organisation overall security posture	71,389	224	,000	4,173	4,06	4,29
I am aware of all different malware and the latest cyber-attack trends	59,619	224	,000	3,867	3,74	3,99
I am skilled and informed to deal with different cyber attacks	55,943	224	,000	3,884	3,75	4,02
Willing to open e-mail attachments from strangers	22,581	222	,000	1,574	1,44	1,71
Interesting subject line causes the opening of an e-mail	23,673	220	,000	2,258	2,07	2,45
Phishing attacks	53,407	224	,000	3,964	3,82	4,11
Ransomware	43,231	222	,000	3,507	3,35	3,67
Trojan horse	39,149	214	,000	3,284	3,12	3,45
Robot and network (botnet)	42,162	222	,000	3,368	3,21	3,53
Not interested reading social engineering issues	33,523	224	,000	2,893	2,72	3,06
Not a target of social engineering attacks due to my role size	28,211	219	,000	2,495	2,32	2,67
Unwilling to respond to e-mail messages to friendly and non-threatening strangers	32,834	216	,000	3,235	3,04	3,43
I use work e-mail to subscribe to external websites and memberships	23,174	218	,000	1,438	1,32	1,56
I receive e-mails from potential customers with attachments and links	24,438	218	,000	2,297	2,11	2,48
My work e-mail account is linked with my social media accounts	26,102	215	,000	1,250	1,16	1,34
I do not need to worry about cyber-attack because my	24,239	223	,000	2,366	2,17	2,56

employer is having a strong it team						
All cybersecurity trainings are complex and technical to understand	32,357	223	,000	2,911	2,73	3,09
I am competent enough to deal with cyber- attacks and threats	45,926	219	,000	3,482	3,33	3,63
I have easy access information security policy	37,960	221	,000	3,387	3,21	3,56
I don't have enough time to read all security information and updates	28,200	223	,000	2,250	2,09	2,41

APPENDIX D – ETHICS CERTIFICATE

UNIVERSITY OF THE WITWATERSRAND JOHANNESBURG

SCHOOL OF GRADUATE SCHOOL OF BUSINESS ADMINISTRATION ETHICS COMMITTEE
CONSTITUTED UNDER THE UNIVERSITY HUMAN RESEARCH ETHICS COMMITTEE (NON-MEDICAL)

CLEARANCE CERTIFICATE **PROTOCOL NUMBER: WBS/BA2288660/139**

PROJECT TITLE Employees attitude towards information security and cybersecurity threats in the South African financial services industry

INVESTIGATOR	Mr William Moroka
SCHOOL/DEPARTMENT OF INVESTIGATOR	MM (Digital Business)
DATE CONSIDERED	31 October 2019
DECISION OF THE COMMITTEE	Approved unconditionally
RISK LEVEL	MINIMAL RISK
EXPIRY DATE	28 FEBRUARY 2021

ISSUE DATE OF CERTIFICATE 17 February 2020 **CHAIRPERSON** _____
(Dr MDJ Matshabaphala)

cc: Supervisor: Dr Tweneboah

DECLARATION OF INVESTIGATOR

To be completed in duplicate and **ONE COPY** returned to the Chairperson of the School/Department ethics committee.

I fully understand the conditions under which I am are authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I/we undertake to resubmit the protocol to the Committee.

_____ 18_/__02___/__2020_____
Signature **Date**

PLEASE QUOTE THE PROTOCOL NUMBER ON ALL ENQUIRIES

APPENDIX E – PERMISSION LETTER

OLDMUTUAL

Old Mutual Finance (RF) (Pty) Ltd
Mutualpark, Jan Smuts Drive, Pinelands 7405. PO Box 453, Cape Town 8000, South Africa.
Tel +27 (0)860 445 445, Fax +27 (0)21 503 4298. Email omfinance@oldmutual.com, www.oldmutual.co.za

24 October 2019

Wits Business School Research Ethical Team

Request to collect data for research

This letter serves to confirm that William Moroka, Student No. 2288660 is presently conducting research for the Wits Business School. The research proposal entitled ***Employees attitude towards information security and cybersecurity threats in the South African financial services industry*** was approved by WBS Research Panel as he needs to collect data on his research title.

Your assistance will be greatly appreciated

Kind Regards

William Moroka

0820440034

I, Danie Malan, Director, Old Mutual Finance, hereby give permission to William Moroka to conduct the survey.

Signature **Date** 25/10/2019