Research Report Title: Insights derived from information security behaviour of employees in the South African banking industry.

Student name: Thembi Dhladhla 534351

Supervisor name: Dr Kebashnee Moodley

School of Business Sciences,
Faculty of Commerce, Law and Management,
University of the Witwatersrand

Acknowledgement

A heartfelt thanks to the Almighty God for making this journey possible and for never giving up on me, my flaws and all.

My sincere gratitude to my supervisor Dr. Kebashnee Moodley for your guidance, kindness and unwavering support. I cannot thank you enough for your ongoing encouragement and for believing in me.

Mama Sponono Esther Dhladhla, my angel in heaven. Words cannot express how I feel reaching this moment without you to witness it, thank you for everything. I love you till eternity.

I extend deep gratitude to my husband, my children and my siblings, my in-laws for your love, patience and support. I appreciate your understanding when I could not spend time with you because I had a deadline to meet, and for the hours I was away from you, I locked myself in the study room working on the thesis. A big thank you for allowing me to take time away from our family to further my studies. I am blessed beyond measure to have such an amazing family.

I thank the financial institution that allowed me to conduct my research study, for allowing your employees to freely take part in this study. Thank you to all respondents who took the time to answer the questionnaire and shared valuable insights. Thanks to my leadership, my colleagues and friends who cheered me on till the end.

Table of Contents

Abstract

An increase in malicious, accidental, and intentional information security incidents caused by employees necessitate further research to get insights on how to detect and prevent internal attacks (Ponemon, 2021). The South African banking industry employees either choose to comply or are non-compliant to the principles of the information security policy. It is imperative to understand what factors motivate bank employees to comply and what encourages them to be non-compliant. Additionally, the study sought to understand the impact of the information security behaviour of employees on the bank. To achieve this purpose, a quantitative method was utilised in the form of an online questionnaire which was distributed to 383 bank employees. 223 valid responses were analysed using the IBM SPSS tool. The data analysis was first done by using descriptive statistics. It was followed by conducting Cronbach's alpha test of reliability or internal consistency of the scale items used. This informs how closely related the questions in the Likert scale is related as a group. Pearson correlation and multiple regression analysis was used to assess the interrelationship between the independent and dependent variables. The researcher coined a hybrid theoretical framework named the Composite Information Security Behaviour Framework (CISB) which consists of Protective Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Deterrence Theory (DT), Reactance Theory (RT) and Techniques of Neutralisation (TN). The CISB framework was able to predict 52% of the information security behaviours of bank employees in contrast to using individual information security behaviour theories on their own to predict compliant and non-compliant security behaviour. Pearson correlation indicated that the Protective Motivation Theory (PMT) and Theory of Planned Behaviour were the information security theories that most influenced positively and significantly the compliant security behaviour of bank employees. This study contributes to the body of knowledge, it explored the information security relationship employees have with information security policies and found the influences on their chosen security behaviour be it compliance or non-compliance. The contribution is to the existing research literature on the underpinning theories which are Techniques of Neutralisation, Reactance Theory, Deterrence Theory, Theory of Planned Behaviour, and Protective Motivation Theory particularly in the South African banking industry. Subsequently, with an improved understanding of the information security behaviours, the bank can implement measures to support and assist their employees with understanding the impact of their information security behaviour and create a mutually beneficial information security ecosystem for the bank and its employees.

Chapter 1: Introduction

1.1. Introduction

The purpose of the study is to explore and acquire an understanding of motivating factors and influences such as positive attitude, self-efficacy, swiftness of punishment, certainty of punishment of compliant and non-compliant security behaviour of bank employees concerning the information security policies implemented by a South African bank. The motivating factors are taken from the information security behaviour theories which are used to predict the behaviour of people (AlGhamdi, Win, & Vlahu-Gjorgievska, 2022).

The banking industry is highly regulated, as the International Organisation of Standardisation (ISO/IEC, 2013) require that organisations put stringent controls and policies to ensure the Infosec triad which is availability, integrity and confidentiality remains intact (ISO/IEC, 2013; Lundgren and Moller, 2019). South Africa as one of the developing countries in Africa, has had to transform how it does business to remain relevant and competitive. The banking industry in SA embarked on a journey to transform and digitise its platforms which has introduced challenges both for the bank and its customers (Phiri, Lavhengwa, & Segooa, 2024). Crime syndicates are targeting bank employees and working with some of them to steal customer data and money (BASA, 2024). The SA government has implemented and enforced the POPI Act to protect customers and their personal data from 1 July 2021 (Presidency, 2013) . The PWC Biennial Global Economic Crime Survey indicates that South Africa has a higher economic crime rate in comparison to the global average rate of economic crime for year 2020 (PwC's Global Economic Crime Survey, 2020). South Africa is one of the top ten countries globally to be susceptible to information security and cybercrime breaches (Phiri, Lavhengwa, & Segooa, 2024). This made it ideal for the researcher to investigate the study from a developing country that is growing its digital presence with a mixed population consisting of poor people some being risk inclined because of lack of education and rich people some being risk averse in terms of information security behaviour because they were exposed to training and education (Gwebu, Wang, & Hu, 2019). The easy access of the study population made it ideal for the researcher to investigate SA and not any other country.

In the South African (SA) context, the South African Reserve Bank (SARB) issues what is termed the Guidance Notes that necessitates the banks to assess the adequacy and robustness of their processes and policies and match them to international best practices

(SARB, 2024). As a result, the different banks create and implement bank-specific information security policies as guiding principles for their employees to safeguard themselves and bank systems.

The information security policies and standards also divulge acceptable employee conduct, use of bank assets and forbidden conduct. Each bank has the liberty to create its information security policies and standards as per requirements from SARB based on international best practices (SARB, 2023) . Information security is a set of activities and principles that ensures that sensitive data is protected against unauthorised usage (Ashenden, 2018). It also seeks to uphold the integrity of the data by safeguarding it so that it is not tampered with while stored or in transmission. Thus, employees are the most critical stakeholders in ensuring that the safeguarding measures are implemented operationally in organisations (Alzahrani, 2021). Previous studies have suggested motivating factors that influence employees to comply with information security policies (Ali, et al., 2021; Alzahrani, 2021; Bulgurcu, et al., 2010). Others have discussed based on behaviour theories, reasons for non-compliance security behaviour (Gwebu, et al., 2019; Hu and Xu., 2019; Lowry, et al., 2015; Warkentin, et al., 2011).

The study has reviewed prior research that focused on employee behaviour and investigated some of the information security behaviour theories used to predict employee information security behaviour. This chapter will touch on the background of the study, and the problem statement which are the motivating factors that encourage an employee to comply or deviate from policy requirements. It goes on to provide an overview of the purpose and the intended contribution of the study to the body of knowledge. In the next section, we discuss the background of the current study.

1.2. Background

Organisations create and maintain information security policy documents containing guidelines of acceptable security behaviour and what is deemed as unacceptable behaviour in and outside of work by the organisation. An employee shows compliant behaviour towards information security policies and standards when they conduct themselves in a manner that agrees with what the policy and standards dictate as acceptable behaviour and use of the organisation's technology, data, and the entire network (Ali, et al., 2021). Non-compliance or deviant security behaviour from an employee contradicts what has been defined as acceptable security behaviour by the policies and standards (Ali, et al., 2021). Additionally, it

is behaviour that puts the organisation and the employee at risk of being harmed. The organisations require employees to adhere to the guiding principles of the policies and when this occurs the employer predicts that the number of security vulnerabilities in the form of theft and fraud amongst many others can be lowered (Cram, et al., 2020).

In the Information Security domain, organisations encounter security threats that emanate internally or externally. Internally, the source of the threats are employees, and they are described as internal threat agents (Khan, et al., 2021). Externally they are from hackers and are referred to as external threat agents (Khan, et al., 2021). The current study focuses on internal threat agents, bank employees from one of the major banks in SA because employees in any organisation are the most important stakeholder in ensuring that the detection, monitoring, and preventative measures are successfully implemented operationally in organisations and become effective in protecting the bank and their employees (Alzahrani, 2021). Employees have also been found to be the contributors in data breaches resulting in loss of confidential data from banks (Ponemon, 2023). Internal threat agents, based on their intentions and motivations can maliciously or accidentally through their information security behaviour cause harm to the organisation (Khan, et al., 2021).

There are two types of information security behaviours that employees can perform, namely intentional/malicious behaviour and accidental/non-malicious behaviour. The current study sought to understand what motivates bank employees to either comply or not comply with the statutes of information security policies with a focus on employee intentional/malicious information security behaviour. The information security behaviour theories were mostly used in quantitative studies, only a few studies used the qualitative approach. The decision to use the quantitative approach in the current study was based on most previous studies that have used the same approach (Ajzen, 1991; Alzahrani, 2021, Ashenden, 2018; Box and Pottas, 2014; Bulgurcu, et al., 2010; Cheng, et al., 2013; Cram, et al., 2020; Hu and Xu, 2018; Musarurwa, et al., 2018; Muhammad, et al., 2017).

Prior research has used different behaviour theories to understand peoples' compliant and non-compliant behaviour. These studies have been carried out in different contexts such as healthcare, education, and banks in developing and developed countries (Riahi & Islam, 2023) (Fasae, 2024) (Ali & Dominic, 2024) (Tenzin, McGill, & Dixon, 2024) (Smith, 2023). Considering the complexity of human behaviour and the context of the different studies,

contradicting results and in some cases similar results were observed. In each study either one or two behaviour theories were used to do the investigation. The researchers agreed that the behaviour theories complement each other, where one concept of a theory would seem weaker, then the other of a different theory would come across as being stronger. A study carried out in Pakistan found the Deterrence Theory did not have any influence on their employee's compliance however it found that because of the country's religious beliefs, the Theory of Planned Behaviour seemed to have had a positive influence on compliance (Muhammad, et al., 2017). This then required a balance and complimentary usage of the theories to cover all possible behaviour avenues for the investigation in the SA context, being a developing country that seeks to address the injustices of the past by providing equal opportunities of employment to a diverse nation which has different beliefs, norms and educational disparity.

The banks are a stable contributor to the economy of South Africa. The banking sector serves as a reliable pillar in bolstering the nation's economy. The researcher delved into existing knowledge, aiming to expand upon it while specifically addressing the South African context and its distinctive factors (SARB, 2023).

The figures depicted in Figure 1.1 and Figure 1.2 below, as presented by the South African Reserve Bank (SARB), highlight the continued profitability of banks. Nevertheless, the cumulative profits are influenced by rising credit losses, stemming from job losses in various sectors (SARB, 2023). Consequently, bank clients are facing challenges in servicing their debts (SARB, 2023).

The following figures provide stats on the profitability and capital ratio in the banking sector.

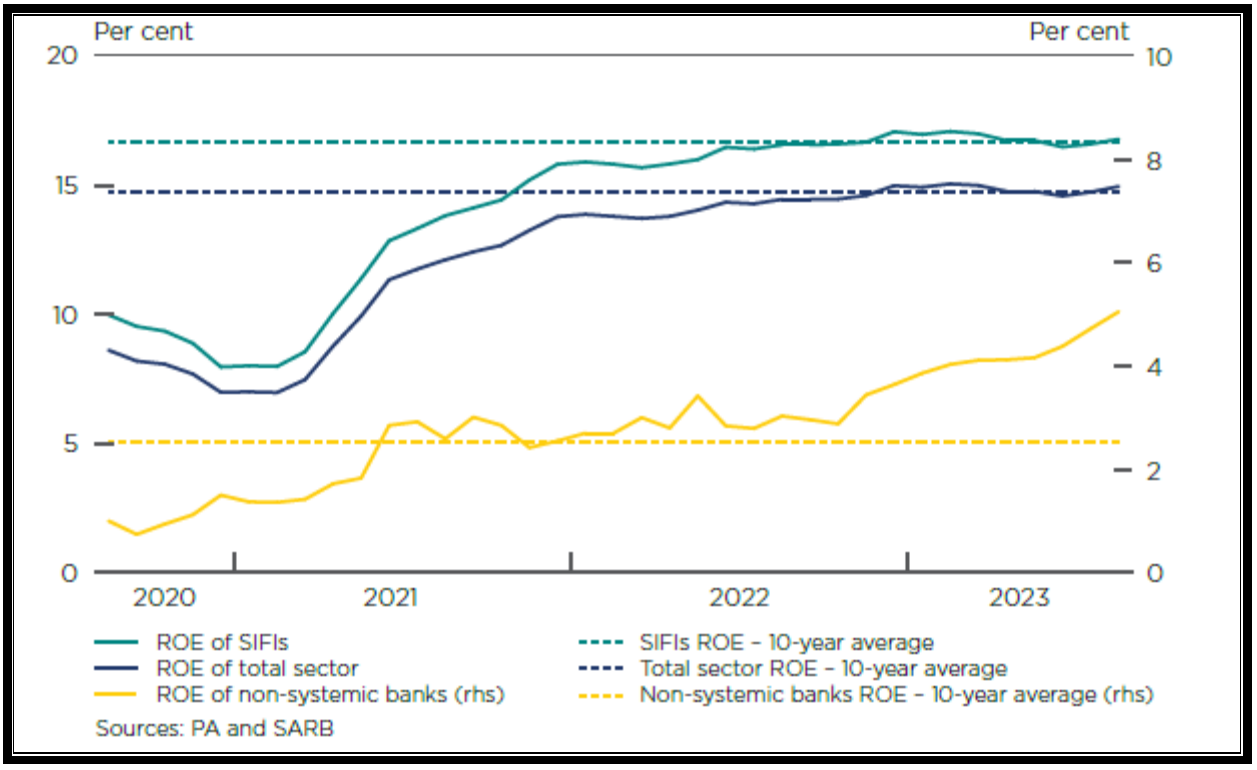


Figure1.1: Banking Sector Profitability

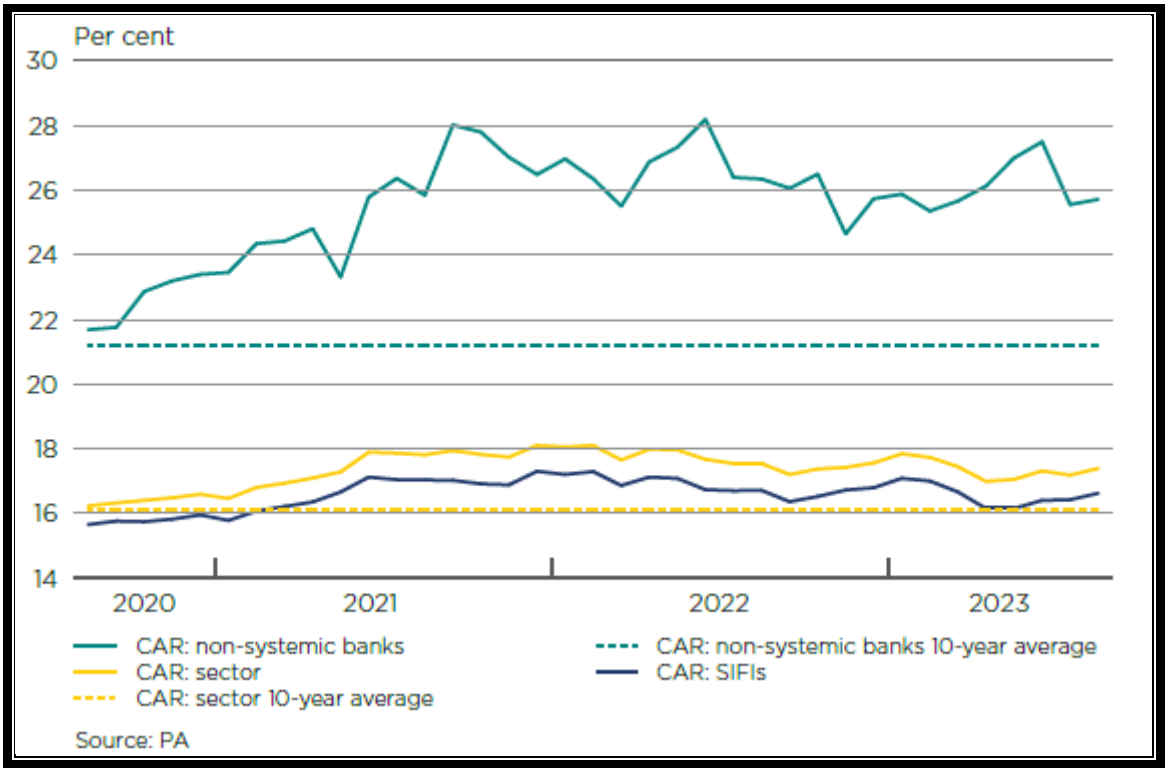


Figure1.2: Banking Sector Capital Adequacy Ratio

The above is another reason why the South African banking industry is the ideal sector for the study to have investigated the information security behaviour of employees.

1.3. Problem Statement

The escalation in accidental, malicious and intentional information security internal occurrences, presented the banking sector in South Africa as an ideal prospect for exploring the factors influencing the information security behaviours of employees because many of their information security behaviours contributed to the problem seen in the 10% growth year on year of the compromised customer records leading to financial loss and reputational damage for the banks (Gorskie, et al., 2019; Penomon, 2021). Globally, the banking or financial industry is still the second highest sector with most expensive data breach at a cost of $ 5.90 million in 2023 and $ 5.97 million in 2022 per breach (Ponemon, 2023). Bank employee's information security non-compliant behaviour was identified as the initial attack vector or the malicious insider root cause with the highest cost of $ 4.9 million (Ponemon, 2023). The customer 52% and employee 40% personal identifiable information was the costliest to have been compromised among all data types. There is a need for more understanding of the motivations and influences that lead to compliant and non-compliant information security behaviours of bank employees (Nakitende, Rafay, & Waseem, 2024). The current study looked to get better comprehension based on employee feedback on the information security behaviours of current employees at a bank, to get a view on the reasons that cause employees to comply or be non-compliant with the information security policy. Prior research has indicated that South Africa has become the playing test ground for external security attacks (Monzon, 2021). With the rise in external attacks in the form of crime syndicates, bank employees choose to become accomplices in the crimes and are significantly contributed to data loss both maliciously and accidentally (Ponemon, 2021).

The information security policies for instance state that, an employee should not commit fraud, theft or click on links that may compromise their system logon credentials making it difficult for organisations to discern an attack from a legitimate activity when authentication happens with employee credentials (Pieterse, 2021). An IBM report (2020) stated that "breaches caused by malicious employees are often more costly for an organisation than other types of breaches. The average cost of such 8 cyber incidents, across sectors, is $4.37 million. In comparison, the average cost of data breaches caused by system glitches is $3.38 million and human error $3.33 million" (Wass, 2020). Information security threats introduced

by employees are costly and have increased over the years (Ponemon, 2021). Employees who are the source of these threats from within the organisation are described as internal threat agents, to distinguish them from external threat agents such as hackers or people not employed by the organisation (Pereira & Santos, 2015). The challenge of internal threat agents requires attention as internal threats are difficult to detect because they use valid login credentials of an employee. The total cost of compromised records has increased by 10% from the previous year to 2021 (Ponemon, 2021). The cost of a data breach went up from 3.86 million to 4.24 million dollars (Ponemon, 2021). Thus, it is of great importance to investigate the compliant and non-compliant behaviours of employees, especially with access to personal data. The access and use of data can bring about a lot of risks as data is the second most important asset of an organisation after its employees (Hobson, 2019).

1.4. Research Questions

Research questions were meant to answer the questions raised because of a problem or a challenge under investigation. Data collected from respondents is supposed to answer the research question once it is analysed and the findings presented. Research questions assist in narrowing down the scope of the phenomenon under study by providing what to mainly focus on (Creswell, 2014). The main research question:

What insights regarding compliance and non-compliance can be gathered from information security behaviour of employees in the South African banking industry?

The research questions that assisted in unearthing the required information are as follows:

- What are the motivating factors that encourage bank employees to comply with information security policies?
- What factors influence deviant/non-compliant behaviour of information security policies by bank employees?
- What impact does the information security behaviour of employees have on the bank?

This section shared the study's research questions as the guiding principles, in the next section, the research objectives are discussed to give an overview of what the current study is trying to achieve.

1.5. Research Objectives

Research objectives are what the researcher aimed to acquire as the findings of the investigation. They are a guide on which data was collected, analysed, and reported on (Blumberg, et al., 2014). The main research objective is:

To determine insights that can be obtained regarding compliant and non-compliant information security behaviour of employees and the impact the behaviour has in the South African banking industry.

The study had the following objectives:

- To determine motivating factors that encourage bank employees to comply with information security policies.
- To determine what factors influence non-compliant security behaviour of information security policies by bank employees.
- To determine the impact the information security behaviour of employees has on the bank.

1.6. Significance of The Study

This study contributes to the body of knowledge by having explored the security relationship employees have with information security policies and to find the influences on their chosen information security behaviour be it compliance or non-compliance. The researcher utilised the underpinning theories which are Techniques of Neutralisation, Reactance Theory, Deterrence Theory, Theory of Planned Behaviour, and Protective Motivation Theory. The researcher invented the Composite Information Security Behaviour Framework (CISB) which showed the relationship amongst the constructs that were under investigation and predicted the information security behaviour of 52% of the respondents. Particularly in the banking industry, the intention was to better understand the influences and motivators of their employee' security behaviour that result in both compliance and non-compliance to information security policies.

The study focused on South Africa (SA) as a country, in the engagement of the literature review, many studies were encountered that focused on employees' information security behaviour (Cram, et al., 2020; Hooper and Blunt, 2020; Liang and Xue, 2010; Lowry, et al.,

2014; Shamsudin, et al., 2019). However, the researcher had not come across a study that was conducted exploring specifically the banking industry in SA, albeit acknowledging that information security studies in other different industries and contexts have been investigated in SA (Gwebu, et al., 2019; Vroom and Solms, 2004). Additionally, the banking industry is one of the most rigorously regulated industries to ensure that customers, employees, and their data are protected from unauthorised usage (Van Wyk, et al., 2016). The following section shares the limitations of the study.

1.7. Delimitations

The study focused on one major bank in SA. In the banking sector the information security policies and standards are applied to all employees, the banking industry prescribes to regulations from governing bodies that require banks to proactively introduce and improve their security policies. The respondents of the study were people currently employed in a South African bank. The bank was selected because it has a virtual and physical footprint in servicing their customers and they each have employees of about 25,000 in SA.

The study was undertaken in South Africa to understand the unique and numerous challenges facing bank employees coming from all spheres of life, cultures, attitudes, and beliefs. The researcher did acknowledge that the collection and analysis of primary data would require time, an online questionnaire was used to collect the data. This ensured the elimination of travelling costs. The section above discussed the delimitations of the study.

1.8. Conclusion

This chapter highlighted the purpose of the study as well as the intended contribution of the study. The researcher highlighted the research questions and objectives that may have assisted in identifying factors that motivate complaint behaviour and negatively influence non-compliant behaviour together with a combination of theories. These theories will be discussed in detail in Chapter 2, the literature review.

An exploratory study took place using a questionnaire. It was conducted amongst bank employees in SA whose main work functions related to Information Technology (IT) and those who were not technology-inclined non-IT. This will be discussed in more detail in Chapter 3, Research Methodology. Finally, the study may help the bank to identify and understand what

is causing the internal threats and attacks to occur which result in financial, data loss and reputational damage.

Chapter 2: Literature Review

2.1. Introduction

Information security compliance and non-compliant behaviour of employees is an area that continues to attract attention from researchers (Kuppusamya, et al., 2020). Organisations endeavour to protect their assets, and employees against threats (D'Arcy & Lowry, 2019). Compliant behaviour can be defined as an employee's conduct and practising the guidelines specified in the organisation's information security policies and standards (Kuo, et al., 2020). This means an employee is behaving by what has been deemed as proper security conduct. Non-compliant or deviant behaviour goes against the principles and rules of the information security policies (Kuo, et al., 2020). There is an increase in malicious, accidental, and intentional security incidents caused by employees that call for further research to get insights on how to detect and prevent internal attacks (Ponemon, 2021). Employees' deviant information security behaviour can expose customer and employee data, resources, and systems to malicious attacks; however, information security behaviour that adheres to the principles of the security policy will protect it (Cram, et al., 2020). The following diagram depicts the research questions and how they all are linking to the information security behaviour of an employee.

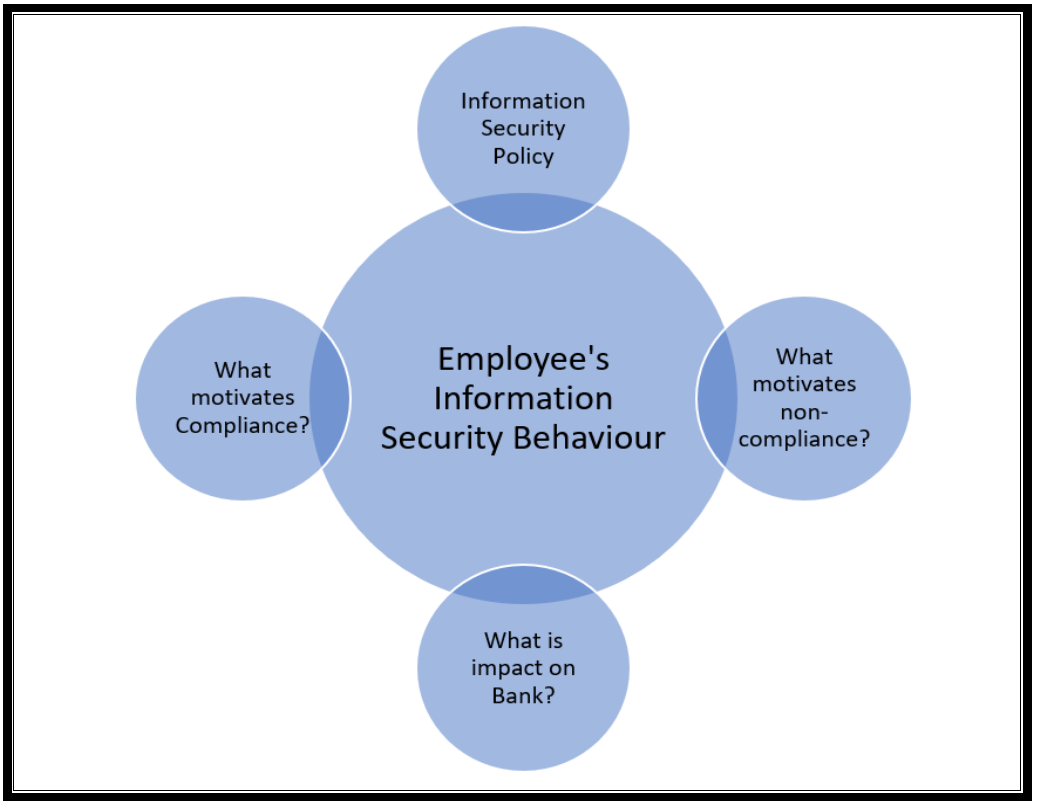


Figure 2.1: How employee behaviour links to research objectives.

The proposed exploration was motivated by previous studies beginning with one from a South African context, related towards information security behavioural compliance (Gwebu, et al., 2019). It looked at possible issues arose from auditing employees' information security behaviour. The study found that security breaches caused by employees far exceeded those that were successfully exploited by external hackers based on results from an information security industry survey (Briney, 2001). Also, it confirmed the key role employees played in the success of a company, notwithstanding that they remained the weakest link (Vroom & Solms, 2004).

The results of a similar study showed that the cognitive drivers of employees' information security behaviour were related to compliance and non-compliance with information security policy (D'Arcy & Lowry, 2019). Theories of planned behaviour (TPB) and rational choice (RCT) were integrated with affective factors to investigate the drivers to comply or not comply. The results showed that compliance was influenced by a combination of stable beliefs, daily work events and behaviours (D'Arcy & Lowry, 2019). Information security behaviour continues to be of interest to investigate factors influencing the information security behaviour of IT employees in the banking sector. A study conducted by Hooper and Blunt (2020) was based on the Protective Motivation Theory (PMT) but borrowed some constructs from the Deterrence Theory (DT) and the Theory of Reasoned Action (TRA). The results from this study showed that reasons influencing the behaviour of an IT employee may not necessarily apply to that of a normal employee who is not IT-inclined. It also found that IT employees are mostly aware of their way around the systems, and access levels which necessitate them to be more stringent in being compliant (Hooper & Blunt, 2020). The previous literature investigated employee security behaviours, and what influenced compliance and motivated deviance from information security policies. A mixture of underpinning theories was used to propel these studies. Similarly, the current study sought to investigate the information security behavioural factors of bank employees to understand why compliant or non-compliant behaviour occurs. The motivating reasons for these behaviours can provide insights to better understand and possibly create in future studies preventative and detective controls to minimise insider threats because of non-compliance to information security policy. The threats can be defined as those risks and vulnerabilities that are emanating from within an organisation, executed by its employees. Many theories have investigated security behaviour and have been found to encourage employees to act according to the principles and

guidelines of the information security policy. Findings of the studies will be discussed in detail in the next section looking into the various security behaviour theories. According to Kuppusamya, et al. (2020), the two most dominant studied theories are the Theory of Planned Behaviour (TPB) and Protective Motivation Theory (PMT). Other theories that moderately influenced employee behaviour towards information security policy compliance or noncompliance are the Deterrence Theory (DT) and Techniques of Neutralisation (NT). The least studied behaviour compliance theory is the Psychological Reactance Theory (RT) The following section will provide details of the most dominant, moderately used and least used security-compliant theories as part of the information security domain.

2.2. Information Security

Information Security (InfoSec) is a domain that focuses on ensuring that data as an asset in its static form and while in transit is kept confidential, has its integrity preserved and is always available for use (Alzahrani, 2021). Similarly, the IT infrastructure must be protected. Its focus has evolved from thwarting viruses and worms to detecting, monitoring, and preventing internal and external attacks on organisations (Dlamini, et al., 2009). This section provides discussions about information security based on compliant and non-compliant behaviour, its findings and how these findings could assist the researcher in bridging the gap that currently exists amongst employees' behaviour in the banking sector. The discussion starts with an overview of theories related to compliant behaviour.

2.2.1. Information Security Compliant Behaviour

This section provides the details of theories applicable to compliant behaviour.

2.2.1.1. Theory of Planned Behaviour

The theory of Planned Behaviour is based on an earlier theory referred to as the Theory of Reasoned Action (TRA). This theory specified that a human's behaviour can be explained by the attitude they have and principles that a person deems as norms (Ajzen & Fishbein, 1980). A decade later, the results of another study attested to the findings of TRA however introduced a component that assists in predicting human behaviour, the ability of a human to choose their behaviour according to their own free will (Ajzen, 1991). This then infers the notion that employees are in control of their choices and behaviour in the workplace. In the year 2002, TPB was extended and named the Extended Theory of Planned Behaviour ETPB,

it introduced an additional component alluding to the behavioural history of a person being another indicator for predicting a person's behavioural intention (Ajzen, 2002).

The ETPB was at the time declared as one of the behaviour theories that are rigorous and inclusive, this was supplemented by dissecting the “norms” into two categories namely the moral and descriptive norms (Ajzen, 2011). Various other studies have utilised ETPB to study human behaviour in education, tourism, health, government and in banks which mostly focused on customer behaviour (Ajzen, 2011; Box and Pottas, 2014; Hina, et al., 2019). Engagement with literature has thus far produced one study that focused on bank manager’s behaviour in Pakistan delving into religion as an influencer of ethical behaviour using the ETPB (Muhammad, et al., 2017).

The results of this study suggested that some components of ETPB positively influenced the manager's behaviour, particularly the moral norm and the belief that managers had of being in control of their choices and actions. The manager's behavioural history or past, be it compliance or noncompliance was not found to influence their current behaviour and intentions at the bank. This study building on others before it, persuaded us to investigate ETPB to evaluate if bank employees are showing indications of any ETPB components in complying or deviating from information security policies and standards. This theory is therefore applicable to the current study. A previous study defined positive attitude as having good and constructive feelings about yourself and your actions; and being optimistic about your view of the world despite unpleasant circumstances (Bulgurcu, et al., 2010). An employee's attitude can be altered by various things and a few outside of their control for instance, knowledge, culture, good and bad experiences. Therefore, the theory can be understood to imply that a positive attitude can be a catalyst in encouraging an employee to comply with information security policy principles and a negative attitude can influence security behaviour that is contrary to the principles of the information security policy (Hina, et al., 2019). Another different study agreed with the findings relating to a positive attitude, that suggested that employed users report higher levels of fear and protection motivation than personal users. The theoretical crux of an effective fear appeal is that it must be personally relevant to stimulate fear; the study showed that concrete fear appeals help stimulate fear and the desired protective response (Schuetz, Lowry, Pienta, & Thatcher, 2020)

Locus of control in the context of positive attitude can be defined as an employee's opinion on whether they have been empowered with knowledge to act better (self-efficacy). This then implies that an employee may comply if they understand and have been trained on compliant security behaviours, with this knowledge they can act better. Additionally, without the knowledge, they would not know and are likely to deviate and when they do, it would have been out of their control because they did not know better. Employees have been found to willingly comply with information security policy when information security training is increased, improved and provided continuously (AlGhamdi, Win, & Vlahu-Gjorgievska, 2022).In the current study, the researcher sought to determine if a positive attitude influences an employee to adhere to the information security policy principles. Additionally, the researcher sought to determine if continuous information security training and being knowledgeable influence compliance positively.

Concept 1a: Positive attitude influences compliance with information security policies.

Concept 1b: Information Security Training and Awareness positively influences compliance with information security policies.

2.2.1.2. Protective Motivation Theory

PMT's fear factor has been used to discourage security behaviour that deviates from the information security policy (Shamsudin, et al., 2019). This theory is among a handful that has been studied rigorously and used in studies investigating how people behave and the influences of those behaviours (Boss, et al., 2015; Johnston, et al., 2015; Liang and Xue., 2010; Moody, et al.,). It articulates the agitation and fright that encompasses an employee when the consequences of perceived threat, the likelihood of the punishment occurring and perceived threat vulnerability cause more problems as compared to the peace of mind that comes with adopting protective measures from PMT (Shamsudin, et al., 2019).

There have been numerous studies that explored PMT and agree with the results of the "fear appeal manipulation positively moderates fear, threat and protection motivation" (Boss, et al., 2015; Moody, et al., 2018; Shamsudin, et al., 2018). One study used the Protective Motivation Theory PMT and found that the threat appraisal and coping appraisal positively influence the security behaviour of employees (Boss, et al., 2015). PMT has contributed immensely to social behaviour literature, it has been explored extensively however the researcher will use

the concepts from the theory in the South African context to get a better understanding of bank employees' information security behaviour.

Threat appraisal is described as the probability of a threat occurring should an employee opt to be non-compliant towards information security policies (Boss, et al., 2015). The coping appraisal can be defined as an employee choosing for themselves an effective action from the information security policy on how to deal with the threat should it materialise. In this case, the employee would be compliant. However, if the employee chooses an ineffective behaviour, then they are opting to be non-compliant (Boss, et al., 2015). The coping appraisal is further dissected into two categories, self-efficacy and response efficacy. Self-efficacy is a conviction that one has about themselves on how they will positively handle any arising threats (Boss, et al., 2015; Leering, et al., 2022). On the other hand, response efficacy is the belief by the employee that should they behave according to what has been prescribed by the information security policy, the threat can be prevented or appropriately handled (Boss, et al., 2015; Leering, et al., 2022).

Considering the two concepts from PMT the self-efficacy and response-efficacy, the researcher investigated if self-efficacy can positively influence security behaviour. Additionally, sought to determine if response efficacy positively influences an employee's information security behaviour. Thus, the PMT theory applied to the current study and was explored as one of the underpinning theories.

Concept 2a: Self-efficacy positively influences the security behaviour of an employee.

Concept 2b: Response efficacy positively influences the security behaviour of an employee.

The above factors were deemed to influence the compliant security behaviour of employees. In the next section, the factors that were deemed to be motivators for non-compliance behaviours will be discussed in more detail.

2.2.2. Information Security Non-Compliant Behaviour

Non-compliant or deviant behaviour goes against the principles and rules of the information security policies (Kuo, et al., 2020). The factors and theories that may influence this behaviour will be provided in this section.

2.2.2.1. Techniques of Neutralisation

The famous techniques that employees would use to justify their actions to themselves, and others include absolving themselves of the responsibility of the deviant act, denial of the harm they have caused by their actions, denial of victim by refusing to acknowledge the impact their actions have on others, condemnation of condemners and the appeal to higher loyalties (Skyes and Matza, 2010).

Denial of responsibility is when an employee believes that they have no other choice except to be non-compliant with the security policy. They believe that the deviation is not their fault, and they are a victim of their circumstance meaning the deviation is beyond their control.
Denial of injury occurs when an employee accepts that their non-compliant behaviour is unacceptable as stated in the security policy however, they justify their deviation as having not harmed anyone and that their actions were harmless.

Denial of victims is a belief and acknowledgement that their non-compliant security behaviour caused harm however they justify their actions by claiming that the affected person or organisation deserved what happened to them.

Condemnation of condemners happens when an employee blames colleagues, management or the bank for their non-compliant security behaviour because they think that everyone is non-compliant and everyone deviates from the security policies and standards.

Appeal to higher loyalties is a belief by an employee that their non-compliant security behaviour was necessary and is a benefit to others. An example would be when an employee shared customer data with unauthorised third parties because they threatened to kidnap their child. Essentially the justification is that for the protection of the child, customer data must be stolen.

Techniques of Neutralisation (TN) have been accentuated as the dominant yardstick of deviant behaviour (Siponen and Vance, 2010; Pei-Lee, et al., 2015). Our study investigated to determine if the information security behaviour of bank employees is positively influenced by the Techniques of Neutralisation. We hypothesise that the concepts, of denial of responsibility, denial of injury, denial of victim, condemnation of the condemners and appeal

to higher loyalties positively influence non-compliance to information security behaviour of bank employees.

Concept 3a: Denial of responsibility positively influences non-compliance behaviour.

Concept 3b: Denial of Injury positively influences non-compliance behaviour.

Concept 3c: Denial of victim positively influences non-compliance behaviour.

Concept 3d: Condemnation of the condemners positively influences non-compliance behaviour.

Concept 3e: Appeal to higher loyalties positively influences non-compliance behaviour.

2.2.2.2. Deterrence Theory (DT)

Research by Yazdanmehr et al. has explained the Deterrence Theory as one that delves into what the employee views as punishment, the likelihood of that punishment occurring, the certainty of that punishment occurring and how quick the organisation would be in implementing the punishment to the employee (Yazdanmehr, et al., 2020). The theory indicates that if an employee perceives the certainty and severity of punishment as being higher, then that may deter the employee from deviating from a security policy. Also, if the punishment is enforced swiftly, that adds another aspect that can stop the employee from breaching policy (D'Arcy, et al., 2009).

Deterrence Theory has been investigated moderately and the results from many DT studies are aligned in that they agree that the higher the severity, certainty, and celerity of the punishment, the less likely an employee will deviate (D'Arcy, et al., 2009; Hu and Xu, 2018; Straub, 1990). The results of these studies indicated that severity, certainty, and celerity were positive moderators of Deterrence Theory. DT has been included as part of the discussion in this study being one of the top two moderately studied theories looking at employee information security compliance behaviour. It was applied in the current study to investigate the SA context, to get an understanding and to compare to other studies that confirmed that the higher the severity, certainty, and celerity of the perceived punishment due to not behaving in accordance with stipulations of the information security policies then the less likely that the employee will deviate (D'Arcy, et al., 2009; Hu and Xu, 2018; Straub, 1990). Another research has indicated that cultural differences may be one reason for inconsistent findings hence calling for cross-cultural research on deterrence in information security. It was suggested that moral belief seem to have bigger influence on intentions to be non-compliant however there is acknowledgement that there is no specific understanding of which moral

belief influence the behavior therefore needing further investigations to examine moral theories and the effect they have on security behaviour of an employee. (Vance, Siponen, & Straub, 2020)

Many studies used Deterrence Theory to explain the compliant behaviour of employees, however, the results of those studies were inconsistent and contradicting (D'Arcy and Herath, 2011; Guo,2013). Consequently, it was argued that Deterrence Theory is more suitable for predicting non-compliance behaviour (D'Arcy, et al., 2009; D'Arcy and Herath, 2011; Gwebu, et al., 2019).

In this study, the researcher investigated if certainty, severity, and swiftness of punishment have a positive influence on non-compliant security behaviour of employees.

Concept 4a: Swiftness of punishment has a positive influence on non-compliant security behaviour.

Concept 4b: Certainty of punishment has a positive influence on non-compliant security behaviour.

Concept 4c: Severity of punishment has a positive influence on non-compliant security behaviour.

2.2.2.3. Psychological Reactance

Theory Reactance Theory has been described as embedded in the notion of "reacting or responding" to a hostile situation in the form of security policies and guidelines that are threatening to take away what has been deemed as "normal behaviour" or freedom to act by employees (Lowry & Moody, 2014).

Prior studies alluded to the fact that employees perceiving information security policies, guidelines, and regulations as violating their freedom to act in a way they want to act (Cram, et al., 2020). Instead, these policies are dictating to them what and how they ought to behave which infringes on their rights (Lowry, et al., 2015). The feeling of infringement is experienced by employees on certain activities that they could previously perform before the implementation of security policies, such as bringing a USB that is not encrypted and inserting it into a work device or a sudden introduction of a policy that prevents employees from accepting gifts or financial rewards given to them by clients if the employees had become accustomed to doing so before policy implementation (Lowry & Moody, 2014).

Other research investigating the impact of organisational justice on employees has found that if employees perceive the distribution of justice by the organisation and leadership as not being fair or they perceive the application of punishment and consequences to not be consistently applied to all offenders then that may trigger a retaliation or psychological reactance which can be used as justification not to adhere to security policies and judicial requirements and regulations (Lowry & Moody, 2014).

Evidence shared from other studies points to employees having confirmed that passive leadership style and behaviour of colleagues who get away with security policy defiance (Siponen & Kajava, 1998), security behaviour oppression of their colleagues 24 (Sittenthaler, et al., 2015) are some of the contributing factors in their non-compliant security behaviour (Gwebu, et al., 2019; Yazdanmehr, et al., 2020). Reactance Theory is one of the least investigated theories however, some studies that have used it to investigate compliance have shared similar findings, pointing to it being a predictor of non-compliance behaviour (Hu and Xu,2018; Kajtazi, et al., 2018; Lowry, et al., 2015).

The researcher investigated if psychological reactance positively influences the non-compliance behaviour of employees.

Concept 5: Reactance positively influences non-compliance behaviour. The researcher discussed in the previous section; the different theories used to study security behaviour. The next section will discuss the new theoretical framework.

2.3. Composite Information Security Behaviour Framework (CISB)

The CISB framework, figure 2.1 may have assisted in investigating the motivating factors of compliant and non-compliant information security behaviours amongst bank employees. The framework merged various information security behaviour theories to capture an understanding of the influences and motivators that encourage employees to either comply with information security policies or not comply. These theories combined rich concepts that gave us profound insights into how bank employees relate to information security policies.

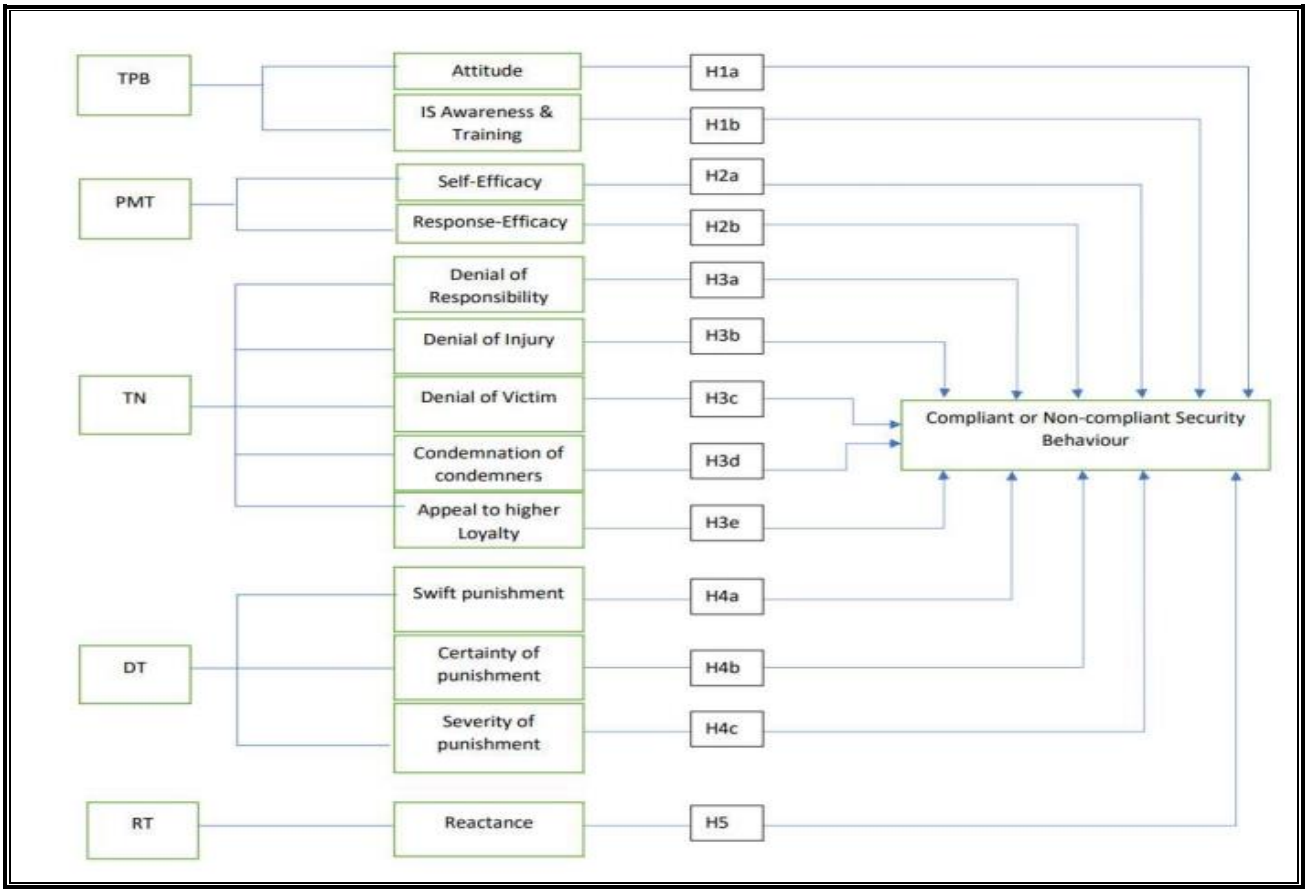


Figure 2.2: Composite Information Security Behaviour Framework (Adapted from Ajzen, 1991; Boss, et al., 2015; Lowry, et al., 2015; Warkentin, et all., 2011)

Key: PMT – Protective Motivation Theory

TPB – Theory of Planned Behaviour

TN – Techniques of Neutralisation

DT – Deterrence Theory

RT – Psychological Reactance Theory

2.4. Literature Review Conclusion

This chapter discussed the principles of Information Security. It also brought to our attention different theories that were used to understand compliance and non-compliant information security behaviour from employees. The concepts from these theories were used to form concepts that were investigated in the current research. The composite information security behaviour framework CISB was used as a guide to lead the investigation.

Chapter 3: Research Methodology

3.1. Introduction

The methodology assists in sharing information on how the research data will be collected and the analysis process that is involved. It also gives context on how trustworthy and reliable the data is.

3.2. Research Design

The research design is a process that defines how data will be collected, its analysis and the presentation of results based on the interpretation made from the analysis (Creswell & Plano Clark, 2007). It is an enabler in answering research questions and objectives (Grey, 2014). This study used an exploratory research design because the focus was not on finding a conclusive single answer or solution for the research (Saunders, et al., 2007). However, it was to investigate and have a better understanding of bank employee's information security behaviour, their attitudes, and influencers on how they conduct themselves towards information security policies. The fundamental aim of the study was to get insights that can assist in explaining why compliant or non-compliant behaviours occur in the banking sector and the motivating factors thereof. The research design informed the type of approach that was adopted in the study, the next section provides more information on the selected approach.

3.3. Research Approach

The research paradigm that was used in the current study is positivism. The positivism paradigm produced explanations and their associated reasons (Alharahsheh & Pius, 2020). It also provides information on causal relationships of the phenomenon under study. The observation of reality can be identified, understood, and measured (Saunders, et al., 2007). In this paradigm, the research objective does not interfere or influence the data (Saunders, et al., 2007).

The goal of this paradigm in the study was to understand the relationship of bank employees with information security policies which may be deduced based on their security behaviour when they either comply or deviate from the information security policies. The study adopted a deductive approach with a quantitative research method. Deductive research may describe,

generate, or improve the theoretical framework at any time throughout the research process (Conaty, 2021).

Additionally, this type of research approach is flexible and drifts to and from between the inductive and deductive approaches. It seeks to systematically consolidate the two approaches to advance studies in social sciences (Conaty, 2021). Using the deductive reasoning approach, the researcher remained objective and let facts emanate from the data that could explain the security behaviour of bank employees. The discussion above focused on the research paradigm, and deductive reasoning and the following section discusses the population and sample size.

3.4. Respondents

A sample is a specific group of people taking part in research, which are referred to as respondents. They are selected from the research population (Casteel & Bridier, 2021). The respondents in a sample are the research stakeholders whom data will be collected from. The sample for this study was bank employees which were people with active employment contracts working at a bank. The online research questionnaire was distributed to 383 employees. Valid responses received were from 223 employees from different clusters or departments working in IT and Non-IT roles. The data was analysed using the IBM SPSS tool. The data analysis was first done by using descriptive statistics. It was followed by inferential analysing using Pearson Correlation, Cronbach Alpha and Multiple Regression analysis.

The sample size had been selected considering the total number of SA employees about an average of 25 000, the large sample was used to alleviate margin of error that may result from a less representative sample, this ensured that we have accurate, representative, and meaningful findings.

The current study sought to achieve a confidence level of 95%. This is the percentage of times that the different samples would produce this result (Qualtrics, 2022). Thus, the goal is for the study to be generalised and repeated that the confidence level would give us 9 out of 10times, the results within the confidence margin (Qualtrics, 2022). The above discussed the respondents for the study. The next section discusses the details of how data was analysed.

3.5. Data Analysis

The independent variable is the object that acts on the dependent variable. The dependent variable is the phenomenon that researchers measure to understand the degree to which the independent variable causes an effect (Saunders, Lewis, & Thornhill, 2007). The study has the independent variables extracted from the different behaviour theories such as positive attitude, self-efficacy, response efficacy, severity of punishment, certainty of punishment, swiftness of punishment, awareness & training, reactance, denial of injury, condemnation of condemners, denial to victim, denial of responsibility and appeal to higher loyalties. The dependant variable defined as the bank employee's information security behaviour.

Data was analysed using IBM SPSS. The tool provides powerful functions such as generating powerful insights from responses to questions (Arkkelin, 2014). It also has a visualisation designer that enables the researcher to create charts and boxplots from the survey and questionnaire data (Arkkelin, 2014). It is agile and easily customisable to provide data that can depict trends, manipulate survey variables and report on them (Arkkelin, 2014). Research needs to be rigorous, reliable, and trustworthy for it to be considered research of good quality (Saunders, et al., 2007).

This study used inferential statistics to source the data on employee behaviour using the research questions. Cronbach alpha, Linear regression analysis and Pearson correlation were used for this study because of their concise, clear and statistical prowess in clarifying the impact of one variable on another providing the illuminating insights on the security behaviour of bank employees.

Cronbach alpha represented by symbol α determines the consistency, or precision of the items being measured in the questionnaire (Barbera, Naibert, Komperda, & Pentecost, 2021). It is suggested that the values of Cronbach alpha are as follows, if $\alpha \geq .9$ then the results are excellent. If $\alpha \geq .8$ the results are good. If $\alpha \geq .7$ the results are acceptable. If $\alpha \geq .6$ then results are questionable and if $\alpha \geq .5$ the results are poor (Cho & Kim, 2015).

Pearson correlation assisted to correlate factors with each other to determine the possible behaviour of an employee about information security policy compliance or non-compliance. Pearson correlation coefficient, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation (Oliveira, Moral, Zocchi, Demetrio, & Hinde, 2020).

Linear regression examined the impact on the bank when employee's security behaviour launches vulnerabilities into the bank that have potential to harm and cause financial & reputational damage. Regression analysis was used to get the insights, it is a statistical method that can predict independent variable's impact on the dependent variable (Abdel, Alamro, & Alamro, 2020).

3.6. Data Instrument

The concepts used in the instrument were all adapted from previous studies, some having originated from other domains outside of the information security realm. This was done to increase the reliability of concepts and results. The concepts were used to construct questions addressing each of the security behaviour theories and their associated concepts. Likert scales were used in quantitative research questionnaires, they are deemed suitable for social science or behavioural research. The Likert scale consisted of five equal intervals with a neutral midpoint. An example of the scale is strongly agree, agree, neutral, strongly disagree, disagree (Hinkin 1998)

	Theory	**Author**	**Year**	**Domain**
1.	Theory of Planned Behaviour	Ajzen	1985	Psychology
2.	Protection motivation theory	Rogers	1975	Psychology
3.	Deterrence Theory	Gibbs	1975	Criminology
4.	Techniques of Neutralisation	Sykes and Matza	1957	Criminology
5	Psychological Reactance Theory	Brehm	1966	Psychology

Figure 1: Origins and domains of the security behaviour theories

3.7. Data Collection

An anonymous online questionnaire mainly with closed ended questions, using the Qualtrics tool was shared via email with employees. The purpose for posing the closed ended was to acquire focused quantitative feedback that relates to the information security behaviour theories. The reason for sourcing minimum personal information was that we wanted the respondents to answer questions freely without feeling that they could be identified and

subsequently victimised for their actions and feedback. The online questionnaire was distributed to 383 bank employees who have IT and non-IT roles. Respondents included permanent (full-time employees) and contractors (part-time employees) who had valid employment contracts.

Microsoft Outlook and SAP systems were used to check and verify that the roles of respondents were in different clusters, had different levels of seniority in the bank and had clear job names that could be categorised as an IT or a non-IT role (a role only focused on business tasks outside of Group Technology). The sample size was selected based on the total population number of SA based employees which are an average of 25 000. The questionnaire was sent to all 383 bank employees across all 9 provinces of South African, from internship, graduate program, junior staff to senior and executives level roles.

The bank head office is in Johannesburg in Gauteng province, all other bank buildings are spread around the different 9 provinces including rural and urban areas. The sample size of 383, of the 383 only 223 provided valid responses. There were 155 (70%) of 223 employees with IT roles and 68 (30%) of 223 had non-IT roles. The questionnaire was active for 2 months. A total of 223 responses were valid with the remaining 160 of 383 responses that we not valid because the respondents answered 30% or less of the questionnaire and then submitted with 70% of the questions missing responses. All of the 160 responses that were not valid had selected a non-IT role as their primary role, however, they selected different business clusters or departments in the bank for instance Marketing, Retail/Branch, Legal and HR. Each employee could answer the questionnaire only once.

3.8 Threats to Internal and External Validity

Validity is related to making the study credible and the findings believable because they were not altered, disturbed, or influenced by any factor (Casteel & Bridier, 2021). This section will provide more information on the concept of validity as well as the threats to internal and external validity.

3.8.1 Validity

Threats to validity for this study were anticipated looking at the single group of current bank employees and will not include employees from other non-financial organisations. The

researcher will verify that the respondents are bank employees by sending the consent form to the work email address. The employees are protected by the POPI Act, in that their private work email contents will remain confidential and accessible to only them therefore the manager would not know exactly which employee participated in the study and would not have merit to constitute any disciplinary due to how the “evidence” that is the consent form would have been obtained without agreement or valid business justification by the manager to access an employee’s work emails (The RSA Presidency, 2013).

3.8.2. Threats to Internal Validity

Numerous threats to internal validity exist. These are made up of dismissal incidences which may have a negative impact if employees observe their colleagues being dismissed a week or few days before they participate in the study (Cram, et al., 2020); respondents may alter their responses because of fear of getting into trouble with the potential of being dismissed and if they are in doubt of whether their participation and the information, they provide will be kept confidential or not. Even though the dismissal of colleagues is not directly related to study however it has the potential to affect the respondents of the study emotionally and mentally causing them not to disclose information. Respondents will be assured upfront as part of the consent form that their responses will not be made accessible to their managers. Maturation is another category of potential threat to the study if only newly employed people participate in the study (Cram, et al., 2020). In many cases new employees still want to impress their managers and colleagues, they follow rules, policies, and standards. The employees who have experience working in the bank and who have seen the implementation of the security policies and their evolution may or may not have the same experience as new employees. The number of years a person has been working in the bank being exposed and required to adhere to policies and standards has a potential of producing different results depending on the work experience of the respondent. This will be eliminated by ensuring that the respondents have a good representation of the population of bank employees. Current bank employees regardless of the number of their service will be offered an equal opportunity to willingly take part in the study to share their experiences. Also, should insights reveal that there is a great number of respondents recently employed, interviews will continue to be distributed to more bank employees for feedback. The question of length of service will be asked, with an estimate time frame recorded as an answer; for example, 1 to 3 years then 4 to 6 years and 7 or more years.

3.8.3 Threats to External Validity

External validity or transferability occurs when findings of an investigation cannot be transferred or is not applicable to other studies that are also investigating security behaviour of employees (Yazdanmehr, et al., 2020). In this study the sample population are bank employees, and the context is defined as employees only currently working for Nedbank, a South African bank. Bank employees may suddenly change their security behaviours because they are aware that there is a researcher conducting a study about security behaviours of bank employees (Casteel & Bridier, 2021). There is a possibility of respondents significantly improving how they behave, when employees do that, it is termed the Hawthorne effect (D'Arcy & Lowry, 2019). An attempt to prevent this will be made by the researcher, respondents will be assured that the study is not about judging anyone, but it is about understanding the influences and reasons of both positive and negative security behaviours. Their honest feedback will not be shared with their line managers or their employer.

Sampling bias can negatively affect external validity if the sample is not representative of everyone who is a current bank employee (Casteel & Bridier, 2021). The sample must be inclusive of all current bank employees at Nedbank regardless of which department they work for and must also be inclusive of both IT and Non-IT employees. We will also capture the years of service of the employee. Ethical conduct is a must have when research is performed, so it can be done safely, and honest feedback provided. We seek to produce research of high quality hence ethics are critical to uphold. The next section elaborates on vital ethical considerations for a successful study.

3.9. Ethics Consideration

Research ethics share required conduct that is expected from researcher. Research that has high scientific quality tends to be research that has high ethics (Rosenthal, 1994).

This study undertook to follow good ethics in how the study is conducted and the treatments of respondents. This study commits to respecting human dignity in the way we going to collect and report on data. The researcher commits to being honest and informing the respondents of the aims and objectives of the study, what the study is about, who will have

access to the data, how it will be processed, used and the ramifications of their participation in the study.

A consent form will be shared for respondents to fill in, with the liberty to withdraw from participating anytime they wish to. The researcher ensured that the respondents are guaranteed privacy and anonymity by not sharing their details and responses with their managers. Protecting the respondent's freedom to speak or not speak and their integrity. The study did not put respondents in any harm. There was no reward paid for taking part in answering the interview questions, participation is done willingly without any prejudice. Any information that can be used to identify respondents was protected and kept confidential. The collected data was used only for its intended purpose and was not distributed to any third parties. Data will be stored in an encrypted database, only accessible to the researcher and supervisor.

It will not be stored longer than required, when discarded that will be done safely, deleted completely with no backups kept for later use. Prior to the study being conducted, permission for ethical clearance was submitted to the Ethics Committee at Wits University. Permission was granted, only then did the study commence.

3.10. Research Methodology Conclusion

In Chapter 3 , the use of the positivism paradigm was discussed to explore the current study. The goal of this paradigm in the study was to understand the relationship of bank employees with the information security policy based on the security behaviour they choose to either comply with or deviate from the principles of the information security policy. The study adopted a deductive approach with a quantitative research method. The chapter also discussed the threats to internal and external validity along with the ethics considerations. The next section discusses results and the insights coming from the data.

Chapter 4: Results

4.1. Introduction

This chapter shares the findings from data that were obtained from the questionnaire that was distributed to bank employees. The respondents work in both IT and non-IT roles, belonging to various clusters or departments of the bank. The survey collected minimal information that could identify the respondents, this was done to encourage honest and unbiased feedback on employees' behaviour.

The data was analysed using Statistical Package for the Social Sciences (SPSS). The analysis began with findings related to the demographics of the respondents, to depict the representative nature of the data by including all types of bank employees. It then presents the descriptive statistics sharing comprehensive insights about the security behaviour of the employees, then Pearson correlation, Cronbach alpha and multiple regression to understand the relationship between dependent and independent variables. The study concludes the results by summarising the hypothesis and indicating whether the results supported or rejected the hypothesis.

4.2. Demographics

4.2.1. Individual factors

Individual factors indicate the work role of the respondent, whether it is IT-focused or business-aligned. The questionnaire was distributed to 383 bank employees, and a total of 233 employees completed the questionnaire with valid responses. There were 160 of 383 questionnaires that had invalid responses and were excluded from the analysis.

Out of the 223 respondents, 155 have IT roles and 68 have business or non-IT roles. This is displayed in Tables 4.1 to 4.3 below. The information about job roles or titles enabled the researcher to make a distinction between business (non-IT) and IT roles. This was obtained from Microsoft Outlook, which the bank uses to show employee roles and titles. Microsoft Outlook, one of the bank's official communication tools, was used to send the questionnaire to the participants of the study.

Table 4.1 IT and non-IT respondents

IT or Non-IT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	IT role	155	69.5	69.5	69.5
	Non-IT role	68	30.5	30.5	100.0
	Total	223	100.0	100.0	

Table 4.2 Employee Department or Cluster

Department

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	RBB	25	11.2	11.2	11.2
	Group Finance	5	2.2	2.2	13.5
	Group Technology	165	74.0	74.0	87.4
	Other (Specify)	15	6.7	6.7	94.2
	Balance Sheet Management	1	.4	.4	94.6
	Legal	1	.4	.4	95.1
	CIB	10	4.5	4.5	99.6
	Audit	1	.4	.4	100.0
	Total	223	100.0	100.0	

Table 4.3 Primary Role of Employee

Primary Role

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Executive	10	4.5	4.5	4.5
	Senior Manager	23	10.3	10.3	14.8
	Middle Manager	37	16.6	16.6	31.4
	Other (Specify)	44	19.7	19.7	51.1
	Junior Manager	26	11.7	11.7	62.8
	General Staff Member	83	37.2	37.2	100.0
	Total	223	100.0	100.0	

Some respondents provided their specific role names instead of categorising themselves using the management classification used above such as junior, middle or executive or senior management. Table 4.4 below details other roles that the respondents hold in the bank.

Table 4.4: Break-down of other roles

Specify Other Role

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		180	80.7	80.7	80.7
	Client Advisor	1	.4	.4	81.2
	Administrator	1	.4	.4	81.6
	Analyst	1	.4	.4	82.1
	Analyst Programmer / Designer	1	.4	.4	82.5
	Business Analyst	1	.4	.4	83.0
	Consultant	1	.4	.4	83.4
	Engineer	1	.4	.4	83.9
	HR Officer	1	.4	.4	84.3
	Information Security Administrator	1	.4	.4	84.8
	Infrastructure Project Manager	1	.4	.4	85.2
	IT Security Administrator	1	.4	.4	85.7
	IT servvice desk IT support engineer	1	.4	.4	86.1
	IT Technical Support Specialist	1	.4	.4	86.5
	Junior BI Developer	1	.4	.4	87.0
	Management consultant	1	.4	.4	87.4
	Operations Analyst	3	1.3	1.3	88.8
	Process Engineer	1	.4	.4	89.2
	Project Coordinator	2	.9	.9	90.1
	Project Manager	4	1.8	1.8	91.9
	security administrator	2	.9	.9	92.8
	Security administrator	1	.4	.4	93.3
	Security Administrator	1	.4	.4	93.7
	Security Administrator 1 (Access)	2	.9	.9	94.6
	Security Administrator II	1	.4	.4	95.1
	Senior Program Manager	1	.4	.4	95.5
	service consultant	1	.4	.4	96.0
	Software Architect	1	.4	.4	96.4
	Specific Technology Specialist	1	.4	.4	96.9
	System Engineer	1	.4	.4	97.3
	Systems Analyst / Designer	1	.4	.4	97.8
	Systems Engineer - IT	1	.4	.4	98.2
	Systems Engineer Specialist	2	.9	.9	99.1
	technician	1	.4	.4	99.6
	Technician	1	.4	.4	100.0
	Total	223	100.0	100.0	

4.2.2. Employee work experience

The respondents indicated their years of work experience in the banking sector. Table 4.5 below shared findings that revealed 13% of respondents had been working for 2 to 5 years, 23% for 6 to 10 years, 39% had work experience of 11 to 20 years and employees with work experience exceeding 20 years represented 22% of the respondents.

Table 1.5: Work Experience of Employee

Work Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 2 years	3	1.3	1.3	1.3
	2 to 5 years	31	13.9	13.9	15.2
	6 to 10 years	53	23.8	23.8	39.0
	11 to 20 years	87	39.0	39.0	78.0
	More than 20 years	49	22.0	22.0	100.0
	Total	223	100.0	100.0	

The above table provided information on the demographic and representativeness of the respondents in the study so we can have insights into which roles the respondents held, the number of their working experience in the bank and their level of seniority. In the next section, we will discuss the descriptive statics.

4.3. Descriptive statistics

4.3.1. Introduction

The researcher used descriptive statistics to summarise, organise and present the data in a meaningful and comprehensive manner. The study sought to understand and acquire insights to better understand trends and patterns that could possibly explain the influencing factors to comply or be non-compliant to information security behaviour. Each of the information security behaviour theories has elements used in a Likert scale that investigated whether the bank employee would comply or choose non-compliance security behaviour with the information security policy principles and guidelines.

4.3.2. Theory of Planned Behaviour (TPB)

The questionnaire consisted of 10 elements of TPB, 5 investigating the employee's attitude towards the Information Security Policy. The other 5 tested the employee's views concerning Information Security Awareness and Training. It is important to note that some responses of the elements are missing as responses were not provided for those elements. The detailed statistics and distribution of responses are indicated in Table 4.6 below.

Table 4.6: Types of attitudes towards information security policy

Statistics

		Positive Attitude	Conflicted Attitude	ISP is Important Attitude	ISP Restricts Employees Attitude	I Don't Care about ISP Attitude
N	Valid	223	219	218	218	216
	Missing	0	4	5	5	7

4.3.2.1. TPB Employee attitude - positive attitude towards information security policy

This question was asked to get an understanding of the employee's attitude, whether their attitude is a positive one towards the Information Security Policy or not. Data findings in Table 4.7 below, indicate that 164 (74%) out of 223 employees strongly agreed and 52 (23%) agreed that as bank employees, they have a positive attitude toward the Information Security Policy. Only a total of 3 (1%) out of 223 employees strongly disagreed that their attitude towards the Information Security Policy is a positive one. There were 4 respondents (2%), who neither agreed nor disagreed with having a positive attitude. In summary, the data in Table 4.7 below indicate that 97% of respondents see themselves as having a positive attitude towards information security policy.

Table 4.7: Positive Attitude

Positive Attitude

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*164*	*73.5*	*73.5*	*73.5*
	Agree	*52*	*23.3*	*23.3*	*96.9*
	Neutral	*4*	*1.8*	*1.8*	*98.7*
	Disagree	*0*	*.0*	*.0*	*98.7*
	Strongly Disagree	*3*	*1.3*	*1.3*	*100.0*
	Total	*223*	*100*	*100*	

4.3.2.2. TPB Employee attitude – conflicted towards information security policy

Respondents were asked to indicate their attitude towards the Information Security Policy in terms of whether it is conflicted or not towards the Information Security policy. A total of 15 (7%) of 223 employees, agreed and strongly agreed respectively regarding being in a conflicted relationship with the Information Security Policy. Employees who strongly disagreed represented (65%) of the respondents, meaning 145 of 223 employees strongly disagreed and 42(18%) of 223 were conflicted towards the Information Security Policy. The remainder 17 (8%) respondents neither agreed nor disagreed with being conflicted. This element of TPB's conflicted attitude had 4 missing responses, which represented 2% out of 223 of the population. In summary, the data in Table 4.8 below indicates that 84% of respondents disagreed that they have a conflicted attitude toward the information security policy.

Table 4.8: Employee's conflicted attitude towards information security policy

Conflicted Attitude					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*8*	*3.6*	*3.7*	*3.7*
	Agree	*7*	*3.1*	*3.2*	*6.8*
	Neutral	*17*	*7.6*	*7.8*	*14.6*
	Disagree	*42*	*18.8*	*19.2*	*33,8*
	Strongly Disagree	*145*	*65.0*	*66.2*	*100*
	Total	*219*	*98.2*	*100.0*	
	Missing System	*4*	*1.8*		
	Total	*223*	*100.0*		

4.3.2.3. TPB Employee attitude - information security policy safeguards bank and employees

This question was asked to employees about their thoughts on the purpose of the Information Security Policy. The question was posed to get an understanding of whether the employees agree or disagree with the statement that the Information Security Policy is key to protecting the bank and its employees. Table 4.9 depicts a total of 163 (73%) strongly agreed and 46 (21%) agreed of 223 employees; that the Information Security Policy is key in safeguarding the bank and its employees. A total of 5 (1%) of 223 employees strongly disagreed and 2 (1%)

disagreed that the Information Security policy is important in protecting the bank and its employees. Only 2 respondents (1%) neither agreed nor disagreed. A total of 5 (2%) of the 223 employees did not submit an answer to this question. In summary, a total of 95% of respondents agreed that the purpose of the information security policy is to protect the bank and its employees.

Table 4.9: Information Security Policy is Important to safeguard the bank

Information Security Policy is Important Attitude

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*163*	*73.1*	*74.8*	*74.8*
	Agree	*46*	*20.6*	*21.1*	*95.9*
	Neutral	*2*	*.9*	*.9*	*96.8*
	Disagree	*2*	*.9*	*.9*	*97.7*
	Strongly Disagree	*5*	*2.2*	*2.3*	*100.0*
	Total	*218*	*97.8*	*100.0*	
	Missing System	*5*	*2.2*		
	Total	*223*	*100.0*		

4.3.2.4. TPB Employee attitude – information security policy controls and restricts unnecessarily

This question was aimed at understanding employees whether they feel restricted or controlled using the Information Security policy. Bank employees, 124 (56%) of 223 strongly disagreed and 48 (22%) of 223 disagreed with the notion that the Information Security policy is a mechanism used to exert control and restrictions on employees unnecessarily. A representation of 12 (5%) of 223 employees, strongly agreed that the bank controls and restricts employees using the policy. A further 6%, representing 14 of 223 respondents agreed that the policy is used to unnecessarily control and restrict employees. Table 4.10 shows a total of 20 (9%) of 223 employees chose to neither agree nor disagree with the statement. Of the 223 responses, there were 5 missing values from the responses, representing 2% of the data (100%). In summary, 78% of respondents disagreed that the Information Security policy is a mechanism used to exert control and restrictions on employees unnecessarily.

Table 4.10: Information Security Policy Restricts Employees

Information Security Policy Restricts Employee Attitude					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*12*	*5.4*	*5.5*	*5.5*
	Agree	*14*	*6.3*	*6.4*	*11.9*
	Neutral	*20*	*9.0*	*9.2*	*21.1*
	Disagree	*48*	*21.5*	*22.0*	*43.1*
	Strongly Disagree	*124*	*55.6*	*56.9*	*100.0*
	Total	*218*	*97.8*	*100.0*	
	Missing System	*5*	*2.2*		
	Total	*223*	*100.0*		

4.3.2.5. TPB Employee attitude towards information security policy

The purpose of this question was to understand the employees' thoughts on the principles of the Information Security policy and whether it influences them to comply or not comply. A total of 216 (97%) responses were received, 148 (66%) of 223 strongly disagreed and 48 (22%) of 223 disagreed that they do not consider the Information Security policy to be important and its principles do not deter them from non-compliance. Only 7 (3%) of the 223 employees strongly agreed and 4 (2%) employees agreed that the Information Security policy is not important as it does not deter them from being non-compliant. There were 9 out of 223 respondents representing 4% who neither agreed nor disagreed. Responses not submitted or missing were 7 (3%) from 223 employees. Table 4.11 shares a summary indicating that 5% of respondents agreed that they have a negative attitude towards the security policy and 88% disagreed that they have a negative attitude about the security policy. They indicated that the information security policy does deter non-compliant behaviour.

Table 4.11: Employees have a negative attitude about information security policy

I Don't Care about Information Security Policy Attitude

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	7	3.1	3.2	3.2
	Agree	4	1.8	1.9	5.1
	Neutral	9	4.0	4.2	9.3
	Disagree	48	21.5	22.2	31.5
	Strongly Disagree	148	66.4	68.5	100.0
	Total	216	96.9	100.0	
	Missing System	7	3.1		
	Total	223	100.0		

4.3.2.6. TPB Awareness and training

This question was asked to get a view from employees if there is a need for the bank to invest in more Information Security training. Table 4.12 depicts that a total of 222 (99%) out of 223 responded to the question. There were 101(45%) of 223 employees strongly agreed, and another 93 (42%) of 223 agreed with the need to have additional training in the organisation. Only 5 (2%) of the 223 employees strongly disagreed and 9 (4%) disagreed with additional Information Security training being created and offered to employees. There was 1 (0.4%) of 223 missing value that was not submitted by a respondent. About 14 (6%) respondents neither agreed nor disagreed with a question. In summary, 87% of respondents agree that there is a need to increase information security training and awareness.

Table 4.12: Increase information security training and awareness

Increase Information Security Awareness and Training					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	101	45.3	45.5	45.5
	Agree	93	41.7	41.9	87.4
	Neutral	14	6.3	6.3	93.7
	Disagree	9	4.0	4.1	97.7
	Strongly Disagree	5	2.2	2.3	100.0
	Total	222	99.6	100	
	Missing System	1	.4		
	Total	223	100.0		

Furthermore, employees were asked whether they felt they had sufficient knowledge about the principles of Information Security. Table 4.13 shows that a total of 4 (2%) out of 233 employees strongly disagreed and 9 (4%) disagreed they do not have adequate information regarding Information Security and its policies. Of employees who agreed 121 (54%) of 223 and a further 20% representing 45 employees strongly agreed that they are empowered with Information Security knowledge. Only 2 (1%) of the 223 respondents did not submit responses to this question. A total of 42 (19%) neither agreed nor disagreed with the question. In summary, 74% of respondents agree that they possess sufficient knowledge about the security policy.

Table 4.13: Employee has sufficient knowledge of information security policy

I Have Sufficient Knowledge of Information Security Policy					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*45*	*20.2*	*20.4*	*20.4*
	Agree	*121*	*54.3*	*54.8*	*75.1*
	Neutral	*42*	*18.8*	*19.0*	*94.1*
	Disagree	*9*	*4.0*	*4.1*	*98.2*
	Strongly Disagree	*4*	*1.8*	*1.8*	*100.0*
	Total	*221*	*99.1*	*100.0*	
	Missing System	*2*	*.9*		
	Total	*223*	*100.0*		

4.3.2.7. TPB Awareness and training – information security content is communicated

The question was asked to understand if Information Security content and learning material is shared and whether it is being used or not. Respondents totalling 59 (27%) and 10 (5%) of 223 employees respectively indicated that the Information Security Policy is communicated on various platforms however they do not have time to read it. The highest group of respondents 79 (36%) of 223 collectively agreed and strongly agreed that the Information Security material is available across organisational platforms, and they confirmed that they

read it. They were 73 (33%) of 223 who neither agreed nor disagreed with the statement of the content and material being available and communicated. Only 2 (1%) of 223 responses had missing values for them, meaning no response was received. Table 4.14 gives a summary, 36% of respondents confirmed that information security training is available, and they read it, and 35% indicated that the training is available however they do not read it. A total of 33 % neither agreed to read it or not read it.

Table 4.14: Availability of information security online training

Online Training is Available I Don't Read

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*10*	*4.5*	*4.5*	*4.5*
	Agree	*59*	*26.5*	*26.7*	*31.2*
	Neutral	*73*	*32.7*	*33.0*	*64.3*
	Disagree	*57*	*25.6*	*25.8*	*90.1*
	Strongly Disagree	*22*	*9.9*	*10.0*	*100.0*
	Total	*221*	*99.1*	*100.0*	
	Missing System	*2*	*.9*		
	Total	*223*	*100.0*		

4.3.2.8. TPB Awareness and training – information security content is not visible and accessible

The question investigated whether employees have not seen the security policy being communicated on various bank communication platforms or done Information Security training and have no access to content and learning material. Table 4.15 depicts that bank Employees disagreed with this statement, 101 (45%) of 223 employees strongly disagreed and 94 (42%) of 223 employees disagreed that Information Security content and material is not available, visible and accessible. There were 6 (3%) and 9 (4%) of 223 (100%) employees who strongly agreed and agreed respectively that they have not seen the security policy on the bank's various communication platforms nor done any Information Security training. Only 2 (1%) employees did not submit their responses back. There were 11 (5%) respondents who

neither agreed nor disagreed with a question. In summary, 87% disagreed that they have no access to information security learning material.

Table 4.15: Online security training not available

Online Security Training is Not Available					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*6*	*2.7*	*2.7*	*2.7*
	Agree	*9*	*4.0*	*4.1*	*6.8*
	Neutral	*11*	*4.9*	*5.0*	*11.8*
	Disagree	*94*	*42.2*	*42.5*	*54.3*
	Strongly Disagree	*101*	*45.3*	*45.7*	*100.0*
	Total	*221*	*99.1*	*100.0*	
	Missing System	*2*	*.9*		
	Total	*223*	*100.0*		

4.3.2.9. TPB Awareness and training – The information security training program requires improvement

The purpose of this question was to get recommendations from the employees to suggest whether the Information Security training program requires improvement or is effective as is. Table 4.16 gives a view indicating that most respondents agreed that the Information Security training program requires improvement for it to be effective. A total of 89 (40%) agreed and 49 (22%) strongly agreed with the statement. Those who neither agreed nor disagreed were 44, making 20% representation of total respondents. Missing responses were 2 in total at 1%. A total of 11 (5%) of 223 respondents strongly disagreed that the Information Security program requires improvement. In summary, 62% of respondents agreed that the information security training program needs to be improved. Only 18% disagreed and they stated that the training program is effective as is.

Table 4.16: Improve information security awareness and training programme

Improve Security Training and Awareness Training

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	49	22.0	22.2	22.2
	Agree	88	39.9	40.3	64.2
	Neutral	44	19.7	19.9	82.4
	Disagree	28	12.6	12.7	95.0
	Strongly Disagree	11	4.9	5.0	100.0
	Total	221	99.1	100.0	
	Missing System	2	.9		
	Total	223	100.0		

The next section discusses the descriptive statics for the factors of the Protective Motivation Theory which are self-efficacy and response efficacy.

4.3.3. Protective Motivation Theory (PMT)

The elements of PMT investigated self-efficacy and response efficacy. Self-efficacy refers to an employee's confidence in their ability to complete a task or achieve a goal. Response efficacy refers to an employee's belief as to whether the recommended action step from the Information Security policy will avoid the threat.

4.3.3.1. PMT Self-efficacy – willingness to comply with information security policy

The question aimed to understand employee's level of willingness to comply with the Information Security policy based on the importance of the policy to the bank and employees. Table 4.17 indicates that a total of 122 (55%) employees strongly agreed and 94 (42%) agreed of 223 that they willingly comply with Information Security policies because they understand its importance. Only 3 (1%) out of 223 employees disagreed, indicating that they were not willing to comply with the Information Security Policy. There were 4 (2%) of respondents of 223 that neither agreed nor disagreed with the question. In summary, 97% agreed that they willingly comply with the security policy because they understand its importance. Only 1% disagreed, they do not willingly comply with the security policy, and they do not understand its importance. Only 2% did not agree or disagree.

Table 4.17: Self-efficacy employee's willingness to be compliant

PMT_Self_Efficacy_I_Willingly_Comply					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*122*	*54.7*	*54.7*	*54.7*
	Agree	*94*	*42.2*	*42.2*	*96.9*
	Neutral	*4*	*1.8*	*1.8*	*98.7*
	Disagree	*2*	*.9*	*.9*	*99.6*
	Strongly Disagree	*1*	*.4*	*.4*	*100.0*
	Total	*223*	*100*	*100*	

4.3.3.2. PMT Self-efficacy – intention to continue using an information security policy

The question aimed to understand the intention of the employee on their willingness to continue using the existing and any updated policies provided they get assistance from the bank should they get stuck. Table 4.18 indicates that many employees, 119 (53%) agreed and 92 (41%) of the 223 strongly agreed that they will continue to use Information Security policies if they get assistance when they need help. A single employee (0.4%) declined to continue to use the Information Security policy even when help was provided to them. Only 11 (5%) of 223 employees neither agreed nor disagreed with the statement. In summary, 94% of respondents indicated that they would continue to use the information security policy provided they get help from the bank should they face challenges. The 5% of employees neither agreed nor disagreed.

Table 4.18: Self-efficacy employee's willingness to use security policy with guidance

PMT_Self_Efficacy_Will_Use_ISP_If_Guidance_Is_Provided					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*92*	*41.3*	*41.3*	*41.3*
	Agree	*119*	*53.4*	*53.4*	*94.6*
	Neutral	*11*	*4.9*	*4.9*	*99.6*
	Disagree	*1*	*.4*	*.4*	*100.0*
	Strongly Disagree	*0*	*0*	*0*	*100.0*
	Total	*223*	*100*	*100*	

4.3.3.3. PMT Response efficacy – having an information security policy keeps security breaches down

The purpose of this question was to get insights from employees on whether they think having and adhering to the principles of the Information Security policy alleviates the number of security breaches in the bank. Table 4.19 shows us that of 223 employees, 111 (50%) strongly agreed and 86 (39%) agreed that information Security breaches can be alleviated if employees comply with the principles of the policies. About 13 (6%) employees disagreed with the statement. There were 13 (6%) of 223 respondents who neither agreed nor disagreed with a question. In summary, 89% of respondents agreed that adhering to principles of information security policy reduces the number of security breaches in banks. About 6% disagreed and another 6% were neutral.

Table 4.19: Response efficacy – information security policies ensure low-security incidents

PMT_Response_Efficacy_BreachesAreDown_ISP_Available

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*111*	*49.8*	*49.8*	*49.8*
	Agree	*86*	*38.6*	*38.6*	*88.3*
	Neutral	*13*	*5.8*	*5.8*	*94.2*
	Disagree	*11*	*4.9*	*4.9*	*99.1*
	Strongly Disagree	*2*	*.9*	*.9*	*100.0*
	Total	*223*	*100*	*100*	

4.3.3.4. PMT Response efficacy – complying with information security policy keeps security breaches down

This question investigated whether an employee thought that by complying with Information Security policy, they could contribute to keeping security breaches down. Table 4.20 indicates that there were 127 (57%) employees who strongly agreed and 77 (35%) who agreed of 223 that their compliance can keep security breaches down. Only 9 (4%) of 223 employees

disagreed with the question. A total of 10 (5%) respondents neither agreed nor disagreed with the question. In summary, 92% of respondents agreed that complying with the information security policy can contribute to keeping security breaches down.

Table 4.20: Response efficacy – complying with security policy results in low-security breaches

PMT_Response_Efficacy_Complying_ISP_KeepsBreachesDown					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*127*	*57.0*	*57.0*	*57.0*
	Agree	*77*	*34.5*	*34.5*	*91.5*
	Neutral	*10*	*4.5*	*4.5*	*96.0*
	Disagree	*9*	*4.0*	*4.0*	*100.0*
	Strongly Disagree	*0*	*0*	*0*	*100.0*
	Total	*223*	*100*	*100*	

4.3.3.5. PMT Response efficacy – if all comply, information security threats can be minimised

This question sought to determine the views of the employee on their contribution and the contribution of their colleagues, whether it can minimise the security threats if there is compliance from everyone. Table 4.21 depicts that 144 (65%) of 223 employees described that they strongly agreed and 69 (31%) that it requires a collective compliance effort to minimise the information security threats. Only 3 (1%) employees disagreed that everyone has a part to play in reducing the security threats. A total of 7 (3%) respondents neither agreed nor disagreed with the question. In summary, a total of 96% of respondents agreed that their individual and collective compliant contribution can minimise security breaches.

Table 4.21: Response-efficacy security breaches remain low when all employees comply

PMT_Response_Efficacy_If_We All_Comply_ISP_KeepsBreachesDown					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*144*	*64.6*	*64.6*	*64.6*
	Agree	*69*	*30.9*	*30.9*	*95.5*
	Neutral	*7*	*3.1*	*3.1*	*98.7*
	Disagree	*1*	*.4*	*.4*	*99.1*
	Strongly Disagree	*2*	*.9*	*.9*	*100.0*
	Total	*223*	*100*	*100*	

4.3.3.6. PMT Response efficacy – if some comply, information security threats cannot be eroded

The question was posed to investigate if the employees thought that inconsistent compliance could contribute to perpetuating the existence of information security threats or not. Table 4.22 shows that the study found 91 (41%) strongly agreed and 98 (44%) of 223 employees agreed respectively that inconsistent compliance will not assist in completely eradicating the security threats. Only 14 (7%) of 223 employees disagreed that inconsistencies perpetuate the existence of vulnerabilities in the bank. There were 20 (9%) of 223 employees who neither agreed nor disagreed. In summary, a total of 85% of respondents agree that inconsistent compliance with the information security policy perpetuates the existence of security threats.

Table 4.22: Response-efficacy security breaches increase when some employees deviate

PMT_Response_Efficacy_If_Some_Dont_Comply_ISP_Breaches_Increase					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*91*	*40.8*	*40.8*	*40.8*
	Agree	*98*	*43.9*	*43.9*	*84.8*
	Neutral	*20*	*9.0*	*9.0*	*93.7*
	Disagree	*8*	*3.6*	*3.6*	*97.3*
	Strongly Disagree	*6*	*2.7*	*2.7*	*100.0*
	Total	*223*	*100*	*100*	

4.3.4. Techniques of Neutralisation (TN)

TN investigated employee's views on their responsibility based on the information security behaviour they chose and how that behaviour may if at all affect the bank, customers and colleagues. It sought to understand if employees deemed their behaviour to be acceptable or harmful potentially to themselves and the bank. Employees were also queried on their views on the punishment for non-compliant security behaviour and how they react to those who rebuke them about their behaviour.

4.3.4.1. TN - No consequences for non-compliant behaviour

This question was posed to understand possible reasons why the employee does not adhere to Information Security policies. Table 4.23 shows that there were 142 (63%) strongly disagreed and 35 (16%) agreed of 223 respondents that they do not adhere to security policies because the bank does not hold people who deviate accountable for their actions. Only 4 (2%) of 223 respondents agreed that they do not adhere to security policies because the is no consequence management implemented by the bank. There were 13 (6%) employees who neither agreed nor disagreed with the statement. A total of 29 (13%) respondents did not submit their responses. In summary, 80% of respondents disagreed that there is no punishment for non-compliant security behaviour. Only 2% agreed.

Table 4.23: Accountability – no punishment for non-compliant security behaviour

TN_Responsibility_Bank_DoesNot_Hold_Employee_Accountable

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*2*	*.9*	*1.0*	*1.0*
	Agree	*2*	*.9*	*1.0*	*2.1*
	Neutral	*13*	*5.8*	*6.7*	*8.8*
	Disagree	*35*	*15.7*	*18.0*	*26.8*
	Strongly Disagree	*142*	*63.7*	*73.2*	*100.0*
	Total	*194*	*87.0*	*100*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.2. TN – Employee ignorance or lack of knowledge

This question was asked to get a view from employees on whether they do not read the Information Security policies and because they do not read it, they cannot be held responsible for what they do not know. Table 4.24 shows us that the majority 120 (54%) and 32 (15%) disagreed that they do not read the security policies and a total of 9 (4%) of 223 employees agreed that they do not read the security policies and therefore they cannot be held responsible for information they do not know. About 33 (14%) out of 223 employees neither agreed nor disagreed. There were 29 (13%) missing responses that were not submitted for this question. In summary, a total of 68% of respondents disagreed that they did not read the information security policy. Only 4% agree that they did not read the information security policy and cannot be held responsible for its contents.

Table 4.24: The bank cannot hold employees who did not read the security policy accountable

TN_Responsibility_Bank_Can't_Hold_Employee_Accountable

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*4*	*1.8*	*2.1*	*2.1*
	Agree	*5*	*2.2*	*2.6*	*4.6*
	Neutral	*33*	*14.8*	*17.0*	*21.6*
	Disagree	*32*	*14.3*	*16.5*	*38.1*
	Strongly Disagree	*120*	*53.8*	*61.9*	*100.0*
	Total	*194*	*87.0*	*100.0*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.3. TN – Employees are victims of the bank

The question was asked to determine whether employees are of the view that they are being put in a difficult position by the bank for being exposed to critical and sensitive customer data and working with money they do not have in their personal capacity. A representation of 44% which is 99 employees strongly disagreed and 31 (14%) of 223 disagreed with the statement. A total of 20 (9%) of 223 employees agreed and 11 (5%) strongly agreed that the bank is putting them in a difficult situation. Another 33 (14%) of 223 of employees neither agreed nor

disagreed. A total of 29 (13%) of respondents did not submit their responses to the question. In summary, 58% of respondents disagreed that they are being put in a difficult position by the bank and being exposed to sensitive customer data and money they do not have. Only 14% agreed that they were in a challenging situation that exposed them to sensitive customer data.

Table 4.25: The bank exposes employees to sensitive data and money

TN_Responsibility_Employees_Are_Victims_Exposed_Critical_Data					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*11*	*4.9*	*5.7*	*5.7*
	Agree	*20*	*9.0*	*10.3*	*16.0*
	Neutral	*33*	*14.8*	*17.0*	*33.0*
	Disagree	*31*	*13.9*	*16.0*	*49.0*
	Strongly Disagree	*99*	*44.4*	*51.0*	*100*
	Total	*194*	*87.0*	*100*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.4. TN – Employees claim a deviant behaviour as a mistake

This query was posed to understand employees' views of what they would say if they were caught doing unacceptable behaviour. Table 4.26 indicates that of 223 responses, 46 (21%) strongly disagreed and 24 (11%) disagreed that they would first claim to be innocent and if that does not work then they admit to deviant behaviour being a mistake. Of the respondents who agreed that they would plead innocence till admission of an error 46 (21%) of 223. There were 29 (13%) responses that were missing. A total of 78 (35%) of respondents submitted neutral responses to the question. In summary, a total of 32% disagreed that they would claim to be innocent or admit to having made a mistake if they were caught performing unacceptable information security behaviour.

Table 4.26: The employee pleads innocence or mistake for non-compliance

TN_Responsibility_Employees_Plead_Innocence_ClaimAs_Mistake					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*8*	*3.6*	*4.1*	*4.1*
	Agree	*38*	*17.0*	*19.6*	*23.7*
	Neutral	*78*	*35.0*	*40.2*	*63.9*
	Disagree	*24*	*10.8*	*12.4*	*76.3*
	Strongly Disagree	*46*	*20.6*	*23.7*	*100.0*
	Total	*194*	*87.0*	*100*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.5. TN – Employee unwarranted responsibility

This question aimed to get insights into employees' views, whether they think it is not their responsibility to protect the bank and its employees, therefore how they behave should not matter. Table 4.27 indicates that 148 (66%) respondents strongly disagreed and 20 (9%) of 223 disagreed that they have no part to play in protecting the bank, customers and employees. There were 14 (6,3%) strongly agreed and 6 (3%) agreed of the 223 employees that it is not their responsibility to protect the bank, customers and employees. In total, there were 29 (13%) of 223 missing responses that were not submitted for this question. About 6 (3%) respondents neither agreed nor disagreed with the question. In summary, a total of 75% disagreed that it is not their responsibility to protect the bank and its resources. Only 9% agreed that it is not their responsibility to protect the bank and its resources.

Table 4.27: It is not the responsibility of the employee to protect the bank

TN_Responsibility_Not_Employee's_ResponsibilityTo_Protect_Bank					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*14*	*6.3*	*7.2*	*7.2*
	Agree	*6*	*2.7*	*3.1*	*10.3*
	Neutral	*6*	*2.7*	*3.1*	*13.4*
	Disagree	*20*	*9.0*	*10.3*	*23.7*
	Strongly Disagree	*148*	*66.4*	*76.3*	*100.0*
	Total	*194*	*87.0*	*100*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.6. TN – Effects of employee's security behaviour financial theft

The purpose of the question was to understand if employees believe that they can be involved in theft and whether that theft has no effect on the bank. Table 4.28 indicates that of 223 respondents, 149 (67%) strongly disagreed and 32 (14%) disagreed with the behaviour of theft. A total of 12 (5%) of 223 agreed that theft has no negative impact on the bank. There were 29 (13%) of 223 missing responses that were not submitted for this question. Only 1 (0.4%) respondent neither agreed nor disagreed with a question. In summary, a total of 12% of respondents agreed that they can steal from the bank and that the theft will have no impact on the bank. Many respondents 81% of them disagreed that it is acceptable for them to steal from banks.

Table 4.28: Impact of security behaviour - an employee can steal from the bank

TN_Behaviour_Employees_Can_Steal_From_Bank

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*6*	*2.7*	*3.1*	*3.1*
	Agree	*6*	*2.7*	*3.1*	*6.2*
	Neutral	*1*	*.4*	*.5*	*6.7*
	Disagree	*32*	*14.3*	*16.5*	*23.2*
	Strongly Disagree	*149*	*66.8*	*76.8*	*100.0*
	Total	*194*	*87.0*	*100*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.7. TN – Effects of employee's security behaviour data theft

The question was posed to understand the reasons behind disclosing customer data to third parties, the theft from customers was done with the understanding that the bank will compensate the customer for the loss. Table 4.29 depicts that a total of 223 responses were collected, 151 (68%) strongly disagreed and 26 (12%) disagreed of 223 that it is okay to steal data about wealthy customers to sell to third parties. Only 13 (6%) of 223 agreed that it was okay to steal because the bank compensates the customers for the theft. There were 29 (13%)

of 223 missing responses for this question. About 4 (2%) responded neither agreed nor disagreed with a question. In summary, 80% of respondents disagreed that they have disclosed customer data to third parties. Only 6% agree that they have disclosed customer data to third parties with the understanding that the bank will compensate the customer for their loss.

Table 4.29: Impact of security behaviour - employee can steal customer data

TN_Behaviour_Employees_Can_Steal_Customer_Data

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*8*	*3.6*	*4.1*	*4.1*
	Agree	*5*	*2.2*	*2.6*	*6.7*
	Neutral	*4*	*1.8*	*2.1*	*8.8*
	Disagree	*26*	*11.7*	*13.4*	*22.2*
	Strongly Disagree	*151*	*67.7*	*77.8*	*100.0*
	Total	*194*	*87.0*	*100*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.8. TN – Effects of employee's security behaviour damage or loss of bank property

This question acquired information on the views of the employees on whether they deliberately lose bank assets given to them for work purposes and to find out if they believe that the behaviour does not affect the bank at all. Table 4.30 shows that many employees, 144 (65%) strongly disagreed and 32 (14%) disagreed of 223 that damaging or deliberately losing bank property is acceptable behaviour. A total of 12 (5%) agreed that this is acceptable behaviour and it does not affect the bank at all. There were 29 (13%) of 223 missing responses that were not submitted for this question. A total of 6 (3%) respondents neither agreed nor disagreed with the question. In summary, 79% of respondents disagreed that they lost bank assets on purpose and disagreed that that kind of behaviour does not affect the bank. Only 5% agreed to have deliberately lost bank assets and indicated that the non-compliant security behaviour does not affect the bank.

Table 4.30: Impact of security behaviour - abuse of resources does not affect bank

TN_Behaviour_Employees_Abuse_Property_and _Bank_Resources					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*5*	*2.2*	*2.6*	*2.6*
	Agree	*7*	*3.1*	*3.6*	*6.2*
	Neutral	*6*	*2.7*	*3.1*	*9.3*
	Disagree	*32*	*14.3*	*16.5*	*25.8*
	Strongly Disagree	*144*	*64.6*	*74.2*	*100*
	Total	*194*	*87.0*	*100*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.9. TN – Effects of employee's security behaviour

This question was asked to get an understanding of the reasons for non-compliance from employees. Table 4.31 displays that about 145 (65%) strongly disagreed and 31 (14%) disagreed of 223 that because their colleagues comply with the policy subsequently, they would deviate from the security policy. Additionally, they disagreed that deviation had no negative impact on the bank. Only 14 (6%) of 223 employees agreed and thought if they deviated while everyone complied, that would have no negative impact on the bank. There were 29 (13%) missing responses that were not submitted for this question. A total of 4 (2%) respondents neither agreed nor disagreed with the question. In summary, a total of 79% of respondents disagreed that they are non-compliant because their colleagues are compliant. Only 6% agreed that they have engaged in non-compliant security behaviour because their colleagues were compliant.

Table 4.31: Impact of security behaviour and introducing harm to the bank

TN_Behaviour_AllOthersComply_Idon'tComply_No_Harm					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*7*	*3.1*	*3.6*	*3.6*
	Agree	*7*	*3.1*	*3.6*	*7.2*
	Neutral	*4*	*1.8*	*2.1*	*9.3*

	Disagree	*31*	*13.9*	*16.0*	*25.3*
	Strongly Disagree	*145*	*65.0*	*74.7*	*100*
	Total	*194*	*87.0*	*100.0*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.10. TN – Effects of employee's security behaviour, sometimes I comply sometimes I do not

This question was posed to get a view of inconsistent compliance and non-compliance and why the employee believed that their behaviour does not negatively affect the bank. Table 4.32 shows a representation of 61% which is 137 of 223 employees strongly disagreed and 42 (19%) disagreed that they display inconsistent security behaviour, meaning they sometimes comply and sometimes they do not. Only a total of 11 (5%) of 223 employees strongly agreed and agreed that they sometimes comply and at times they do not. There were 29 (13%) missing responses that were not submitted for this question. A total of 4 (2%) respondents neither agreed nor disagreed with the question. In summary, a total of 80% of the respondents disagreed that they are inconsistent with their compliance with the information security policy and that the behaviour does not affect the bank. Only 5% admitted to being inconsistent with complying with the information security policy.

Table 4.32: Impact of security behaviour when employee complies

TN_Behaviour_I_Don't_Comply_OnAllPrinciples_Icomply_OnSome

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*5*	*2.2*	*2.6*	*2.6*
	Agree	*6*	*2.7*	*3.1*	*5.7*
	Neutral	*4*	*1.8*	*2.1*	*7.7*
	Disagree	*42*	*18.8*	*21.6*	*29.3*
	Strongly Disagree	*137*	*61.4*	*70.6*	*100.0*
	Total	*194*	*87.0*	*100.0*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.11. TN – Effects of employee's security behaviour, introducing vulnerabilities is harmful behaviour

The question sought to get an understanding from employees whether they perceive their actions of introducing vulnerabilities to the bank by being non-compliant with Information Security policy as being harmful or perceive it as acceptable behaviour that has no negative effect on their employer. Table 4.33 shows that there were 139 (62%) of 223 strongly disagreed and 32 disagreed that they had been rewarded by criminals for extracting data from the bank and sharing it with them. About 14 (7%) of 223 employees agreed. A total of 35 (15%) of 223 employees did not submit responses to this question. There were 3 (1%) employees that neither agreed nor disagreed with the question. In summary, a total of 76% of respondents disagreed that they had been rewarded by criminals to steal data from the bank. Only 7% agreed to have received a reward for stealing customer data from the bank and they perceive that behaviour as being acceptable.

Table 4.33: Impact of security behaviour - employee got rewarded for stealing data

TN_Internal_Vulnerabilities_GotRewarded_Stealing_Data

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*6*	*2.7*	*3.2*	*3.2*
	Agree	*8*	*3.6*	*4.3*	*7.4*
	Neutral	*3*	*1.3*	*1.6*	*9.0*
	Disagree	*32*	*14.3*	*17.0*	*26.0*
	Strongly Disagree	*139*	*62.3*	*73.9*	*100.0*
	Total	*188*	*84.3*	*100.0*	
	Missing System	*35*	*15.7*		
	Total	*223*	*100.0*		

4.3.4.12. TN – Effects of employee's security behaviour when password sharing

The question was asked to get insights into the prevalence or scarcity of password sharing amongst colleagues. Table 4.34 shows that many 134 (60%) strongly disagreed and 29 (13%) agreed of 223 that practising the non-compliant behaviour of password sharing. A total of 18 (8%) of the 223 respondents agreed to have shared passwords with their colleagues because there were too many passwords for the different systems to remember. There were 35 (15%)

of 223 respondents who did not submit feedback for this question. Some 7 (3%) of 223 respondents neither agreed nor disagreed with the statement. In summary, a total of 73% disagreed that they engage in non-compliant behaviour by sharing passwords. Only 8% admitted to sharing passwords with colleagues.

Table 4.34: Impact of security behaviour - we share passwords among employees

TN_Internal_Vulnerabilities_Employees_Sharing_Password

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*7*	*3.1*	*3.7*	*3.7*
	Agree	*11*	*4.9*	*5.9*	*9.6*
	Neutral	*7*	*3.1*	*3.7*	*13.3*
	Disagree	*29*	*13.0*	*15.4*	*28.7*
	Strongly Disagree	*134*	*60.1*	*71.3*	*100.0*
	Total	*188*	*84.3*	*100.0*	
	Missing System	*35*	*15.7*		
	Total	*223*	*100.0*		

4.3.4.13. TN - Effects of employee security behaviour, we have always done it this way

The purpose of the question was to determine if employee's perception of having taken part in deviant behaviour introduced a risk that could have been exploited and whether they were willing to change their behaviour and comply. Table 4.35 shows that more than half of the respondents, 160 of the 223 employees strongly disagreed that they were non-compliant and that they were unwilling to change their behaviour. Only a total of 21 (9%) of 223 agreed that they have always been non-compliant, no risk was ever exploited because of their actions therefore there was no need to change non-compliant behaviour. About 7 (3%) of 223 neither agreed nor disagreed with a question. There were 35 (16%) responses that were not submitted for this question. In summary, a total of 71% disagreed that they engaged in non-compliant security behaviour. Only 9 % admitted to having engaged in non-compliant security behaviour and they are not willing to change their behaviour.

Table 4.35: Impact of security behaviour – non-compliance introduces vulnerabilities

TN_Internal_Vulnerabilities_Sensitive_Data_Not_Protected					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*9*	*4.0*	*4.8*	*4.8*
	Agree	*12*	*5.4*	*6.4*	*11.2*
	Neutral	*7*	*3.1*	*3.7*	*14.9*
	Disagree	*32*	*14.3*	*17.0*	*31.9*
	Strongly Disagree	*128*	*57.4*	*68.1*	*100.0*
	Total	*188*	*84.3*	*100.0*	
	Missing System	*35*	*15.7*		
	Total	*223*	*100.0*		

4.3.4.14. TN - Effects of employee's security behaviour – compromised password

The question aimed to understand if employees exposed their sensitive information to others having justification that it was written down but hidden away. Table 4.36 shows those who strongly disagreed were 103 (46%) and 32 (14%) agreed with 223 of the responses received. Responses from 40 (18%) of 223 employees agreed that they engage in non-compliant behaviour of writing passwords down and hiding them away so the passwords cannot be seen by others. There were 35 (16%) who did not submit responses to this question. A total of 13 (6%) respondents neither agreed nor disagreed with the question. In summary, a total of 60% disagreed that they had engaged in non-compliant security behaviour by writing down sensitive information. 18% of respondents admitted to having been non-compliant by writing down sensitive information that can be exposed and exploited.

Table 4.36: Impact of security behaviour - employees write passwords in plain text

TN_Internal_Vulnerabilities_I_Write_Passwords_DownOnPaper					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*8*	*3.6*	*4.3*	*4.3*
	Agree	*32*	*14.3*	*17.0*	*21.3*
	Neutral	*13*	*5.8*	*6.9*	*28.2*
	Disagree	*32*	*14.3*	*17.0*	*45.2*
	Strongly Disagree	*103*	*46.2*	*54.8*	*100.0*
	Total	*188*	*84.3*	*100.0*	

	Missing System	*35*	*15.7*
	Total	*223*	*100.0*

4.3.4.15. TN – Condemnation, privileges because of influential co-workers

The question sought to understand if employees are encouraged to behave non-compliantly because they observed a colleague in a position of power deviating from the Information Security Policy. The researcher sought to understand if employees were content with this behaviour from others or judged their colleagues for deviation. Table 4.37 indicates that there were 136 (61%) of 223 respondents either strongly disagreed or disagreed that they had been non-compliant after observing a colleague deviating from the principles of Information Security policy. A total of 42 (18%) neither agreed nor disagreed with the question. Only 14 (6%) of 223 agreed that they deviated from Information Security policy after having observed a colleague or manager do the same. Further, they condemned their colleague or manager for pretending to be better by reprimanding the employee (subordinate) if the employee (subordinate) did something wrong. There were 31 (14%) of 223 that did not submit answers to this question. In summary, a total of 61% of respondents disagreed that they engaged in non-compliant security behaviour because they saw a colleague in a position of power deviating from information security policy. Only 6% agreed that they engaged in non-compliant behaviour because they observed the same behaviour from a person in a position of power.

Table 4.37: Condemnation - management encourages non-compliant security behaviour

TN_Condemning_Others_Managers_Promote_WrongDoing

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*7*	*3.1*	*3.6*	*3.6*
	Agree	*7*	*3.1*	*3.6*	*7.3*
	Neutral	*42*	*18.8*	*21.9*	*29.2*
	Disagree	*36*	*16.1*	*18.8*	*48.0*
	Strongly Disagree	*100*	*44.8*	*52.1*	*100.0*
	Total	*192*	*86.1*	*100.0*	
	Missing System	*31*	*13.9*		
	Total	*223*	*100.0*		

4.3.4.16. TN – Condemnation, we are all deviating

This question was asked to get an understanding from employees on whether non-compliant behaviour is not hidden amongst themselves, it is known and embraced by everyone in the bank. Table 4.38 shows that there were respondents 92 (41%) strongly disagreed and 40 (18%) disagreed of 223 that non-compliant behaviour is known and embraced by all employees in the bank. Those who neither agreed nor disagreed were 43 (19%). Only 17 (5%) agreed that non-compliance behaviour is performed by all employees, they also agreed that it is a known factor and is embraced by all therefore no employee should be acting innocent. There were 31 (14%) of 223 missing responses that were not submitted for this question. In summary, 59% of respondents disagreed that non-compliant behaviour is embraced by all employees in the bank. Only 8% agreed that non-compliant security behaviour is done and known by all employees.

Table 4.38: Condemnation - deviant security behaviour is a norm

TN_Condemning_Others_Everyone_Does_Not_Comply_Well_Known_Secrete

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*6*	*2.7*	*3.1*	*3.1*
	Agree	*11*	*4.9*	*5.7*	*8.9*
	Neutral	*43*	*19.3*	*22.4*	*31.3*
	Disagree	*40*	*17.9*	*20.8*	*52.1*
	Strongly Disagree	*92*	*41.3*	*47.9*	*100.0*
	Total	*192*	*86.1*	*100.0*	
	Missing System	*31*	*13.9*		
	Total	*223*	*100.0*		

4.3.4.17. TN – Condemnation, targets encourage fraud

The question was asked to investigate if employees perceive the bank and its initiatives such as target incentives to be at cause for the fraud committed by employees. Table 4.39 shows that about 123 (55%) respondents strongly disagreed and 29 (13%) disagreed of 223 that the bank or its initiatives are at fault for the non-compliant behaviour of employees committing fraud. Only 11 (5%) respondents out of 223 agreed that the bank is responsible for the fraud

committed by its employees because of the severe pressure they are put under to achieve targets. Only 30 (14%) of 223 employees did not submit a response to this question. A total of 30 (14%) respondents neither agreed nor disagreed with the question. In summary, a total of 68% disagreed that target incentives are the cause of employees committing fraud. Only 5% agreed.

Table 4.39: Condemnation - work pressure and financial targets cause non-compliance

TN_Condemning_Others_Financial_Target_Pressure_Cause_Theft					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*6*	*2.7*	*3.1*	*3.1*
	Agree	*5*	*2.2*	*2.6*	*5.7*
	Neutral	*30*	*13.5*	*15.5*	*21.2*
	Disagree	*29*	*13.0*	*15.0*	*36.2*
	Strongly Disagree	*123*	*55.2*	*63.7*	*100.0*
	Total	*193*	*86.5*	*100.0*	
	Missing System	*30*	*13.5*		
	Total	*223*	*100.0*		

4.3.4.18. TN – Appeal to higher loyalties, non-compliant behaviour is a norm

This question sought to understand from employees if it is a norm in the bank to display non-compliant behaviour to the principles of Information Security policies. Table 4.40 shows that 150 (67%) strongly disagreed and 32 (14%) disagreed with 223 that it is normal to deviate from the principles of the security policies. Only 5 (2%) of 223 employees agreed that it is normal practice to display non-compliant behaviour in the bank. About 7 (3%) of 223 neither agreed nor disagreed. There were 29 (13%) employees who did not submit an answer to this question. In summary, a total of 81% disagreed with the notion that it is a norm in the bank to display non-compliant security behaviour. Only 2% agreed that it is a norm.

Table 4.40: Non-compliance a norm due to lack of punishment

TN_Punishment_Non-compliance_IsANorm_Punishment_IsNot_Enforced					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*4*	*1.8*	*2.1*	*2.1*
	Agree	*1*	*.4*	*.5*	*2.6*
	Neutral	*7*	*3.1*	*3.6*	*6.2*
	Disagree	*32*	*143*	*16.5*	*22,7*
	Strongly Disagree	*150*	*67.3*	*77.3*	*100.0*
	Total	*194*	*87.0*	*100.0*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.19. TN – Appeal to higher loyalties, religious beliefs motivate deviant behaviour

The question aimed to understand if employees perceived themselves to be influenced by the choice of their religious beliefs and the discrimination that comes because of that choice encourages adherence or deviance from Information Security Policy principles. Table 4.41 indicates that a total of 6 (2%) of the 223 employees agreed that their religious beliefs and the discrimination because of their beliefs encouraged them to deviate. Furthermore, 156 (70%) strongly agreed and 31 (14%) agreed of 223 that their choice of religious beliefs or discrimination had motivated them to be non-compliant. Only 1 (0.4%) of 223 neither agreed nor disagreed with a question. There were 29 (13%) responses not submitted for this question. In summary, 2% of respondents agreed that their religious beliefs and the discrimination that comes with that caused them to engage in non-compliant behaviour. Many 84% disagreed that their religious beliefs caused them to deviate from the information security policy.

Table 4.41: Religious beliefs influence non-compliance to security policy

TN_Punishment_Religious_Beliefs_Cause_Non-compliance					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*3*	*1.3*	*1.5*	*1.5*
	Agree	*3*	*1.3*	*1.5*	*3.1*
	Neutral	*1*	*.4*	*.5*	*3.6*
	Disagree	*31*	*13.9*	*16.0*	*19.6*
	Strongly Disagree	*156*	*70.0*	*80.4*	*100.0*
	Total	*194*	*87.0*	*100.0*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

4.3.4.20. TN – Appeal to higher loyalties, employee or upbringing motivate deviance

The purpose of the question was to understand if employees view their privileged or disadvantaged background and the discrimination based on their upbringing as encouraging them to be non-compliant with Information Security policies. Table 4.42 depicts that there were 140 (63%) strongly disagreed and 32 (14%) disagreed of 223 employees that they were non-compliant because of their background and how they are treated based on that. A total of 10 (4%) of 223 employees agreed that they deviate from the principles of acceptable behaviour because of their background. There were 29 (13%) of 223 responses not submitted for this question. About 12 (5%) respondents neither agreed nor disagreed with a question. In summary, a total of 77% disagreed that their poor or rich background encouraged them to engage in non-compliant security behaviour. Only 4% agreed that their background had a role to play in their security behaviour.

Table 4.42: Rich or Poor background influences non-compliant security behaviour

TN_Punishment_Background_Cause_Non-compliance					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*5*	*2.2*	*2.6*	*2.6*
	Agree	*5*	*2.2*	*2.6*	*5.2*
	Neutral	*12*	*5.4*	*6.2*	*11.3*

Disagree	*32*	*14.3*	*16.5*	*27.8*
Strongly Disagree	*140*	*62.8*	*72.2*	*100.0*
Total	*194*	*87.0*	*100.0*	
Missing System	*29*	*13.0*		
Total	*223*	*100.0*		

4.3.4.21. TN – Appeal to higher loyalties, based on instruction

This question was asked to understand if employees display non-compliant behaviour if they were to perceive that they got instruction to be non-compliant, regardless of the punishment for the deviation and the Information Security policy principles indicating that they must only engage in acceptable behaviour. Table 4.43 displays a total of 145 (65%) strongly disagreed and 29 (13%) disagreed of the 223 received responses that they have deviated because they were told to behave in that way contradicting what the Information Security policy indicates. A few 7 (3%) of 223 employees agreed that they have deviated because they were told to do so regardless of the principles of the policy requiring adherence. Again 29 employees did not submit an answer for this question. A total of 13 (6%) neither agreed nor disagreed with the statement. In summary, 78% disagreed that they engaged in non-compliant security behaviour because they were instructed to do so. Only 3% agreed that they had been non-compliant because they got an instruction to do so.

Table 4.43: Non-compliance security behaviour was an instruction from management

TN_Punishment_I_ShouldNot_Punished_for_Wrong_Instruction

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*4*	*1.8*	*2.1*	*2.1*
	Agree	*3*	*1.3*	*1.5*	*3.6*
	Neutral	*13*	*5.8*	*6.7*	*10.3*
	Disagree	*29*	*13.0*	*14.9*	*25.2*
	Strongly Disagree	*145*	*65.0*	*74.7*	*100.0*
	Total	*194*	*87.0*	*100.0*	
	Missing System	*29*	*13.0*		
	Total	*223*	*100.0*		

Above we discussed the Techniques of Neutralisation which covered various justifications that employees tell themselves and others when they commit unacceptable security behaviour. In the next section, the Deterrence Theory will be discussed.

4.3.5. Deterrence Theory (DT)

The Deterrence Theory consists of factors that can be used to deter non-compliant security behaviour. We investigated to find out if it influenced the bank employees. Factors of the Deterrence Theory are swiftness of punishment where the study sought to understand how quick consequences are applied in the bank when there is deviant security behaviour. The second factor is certainty of punishment, the study investigated how likely the punishment will be implemented by the bank should there be non-compliance to the security policy. The third one is the severity of punishment where the study investigated if the employees are deterred by server consequences for unacceptable behaviour or if they are encouraged to deviate due to lenient punishment for non-conformance to the security policy.

4.3.5.1. DT – Swiftness of punishment

This question was asked to get employee's views on how quick punishment is implemented for non-compliant behaviour. Table 4.44 explains that there were 57 (26%) respondents who strongly agreed and 91 (41%) of the 223 employees agreed that they complied with Information Security policy principles because if there was deviance, they were aware that some of the deviant behaviour warranted immediate dismissal. There were 21 respondents who neither agreed nor disagreed with the question. There were 18 (8%) of 223 respondents who disagreed with a question. A total of 36 (16%) of 223 employees did not answer this question. In summary, a total of 67% agreed they comply with information security policy because they know that deviating from its principles will warrant immediate consequences. Only 8% disagreed.

Table 4.44: Swift Punishment - Deviant security behaviour results in immediate dismissal

DT_Swift_Punishment_Immediately_Dismissed_Non-compliance				
	Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*

Valid	*Strongly Agree*	*57*	*25.6*	*30.5*	*30.5*
	Agree	*91*	*40.8*	*48.7*	*79.1*
	Neutral	*21*	*9.4*	*11.2*	*90.4*
	Disagree	*1*	*.4*	*.5*	*90.9*
	Strongly Disagree	*17*	*7.6*	*9.1*	*100.0*
	Total	*187*	*83.9*	*100.0*	
	Missing System	*36*	*16.1*		
	Total	*223*	*100.0*		

4.3.5.2. DT – Swiftness of punishment

This question was posed to understand if employees were aware that there is no tolerance for non-compliance and that should there be any they would be punished immediately. Table 4.45 depicts many respondents 41 (18%) strongly agreed and 78 (35%) of 223 employees agreed that they were aware that non-compliant information security behaviour will be met by immediate consequences. There were 21 (10%) of 223 responses that did not agree with punishment being implemented immediately after deviation. A total of 47 (21%) of the 223 neither agreed nor disagreed with the swiftness of punishment. There were 36 (16%) of 223 missing responses that were not submitted for this question. In summary, 53% of respondents agreed that the bank has no tolerance for non-compliant security behaviour and that punishment will be swift. Only 10% did not agree.

Table 4.45: Swift punishment - deviant security behaviour is punished immediately

DT_Swift_Punishment_Immediate_Punishment_Non-compliance					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*41*	*18.4*	*21.9*	*21.9*
	Agree	*78*	*35.0*	*41.7*	*63.3*
	Neutral	*47*	*21.1*	*25.1*	*88.8*
	Disagree	*11*	*4.9*	*5.9*	*94.7*
	Strongly Disagree	*10*	*4.5*	*5.3*	*100.0*
	Total	*187*	*83.9*	*100.0*	
	Missing System	*36*	*16.1*		
	Total	*223*	*100.0*		

4.3.5.3. DT – Certainty of punishment

This question was asked to understand if employees are aware that non-compliant security behaviour will certainly yield consequences or punishment. Table 4.46 relay that many employees 55 (25%) strongly agreed and 103 (46%) agreed of the total 223 employees that certainty of punishment discourages non-compliance. There were 9 (4%) of 223 that disagreed with a question. Only 20 (9%) of 223 employees neither agreed nor disagreed with the statement. There were 36 (16%) from the 223 answers that were not submitted for this question. In summary, a total of 71% of respondents agreed that they are aware that if they engage in non-compliant security behaviour they will certainly be punished by the bank. Only 4% of respondents disagreed.

Table 4.46: Certainty of punishment - deviant security behaviour is certainly punished

DT_Certainty_Punishment_Guaranteed_Non-compliance

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*55*	*24.7*	*29.4*	*29.4*
	Agree	*103*	*46.2*	*55.1*	*84.5*
	Neutral	*20*	*9.0*	*10.7*	*95.2*
	Disagree	*1*	*.4*	*.5*	*95.7*
	Strongly Disagree	*8*	*3.6*	*4.3*	*100.0*
	Total	*187*	*83.9*	*100.0*	
	Missing System	*36*	*16.1*		
	Total	*223*	*100.0*		

4.3.5.4. DT – Certainty of punishment, non-compliance

This question was asked to understand if employees perceive that non-compliance behaviour is encouraged by knowing that there will be no punishment to the employee for the deviant behaviour. Table 4.47 communicates that there were 83 (37%) of 223 strongly disagreed and 37 (17%) disagreed that knowing certainly that there will be no punishment for non-compliant behaviour encourages it. About 27 (12%) employees agreed and 12 (5%) strongly agreed of 223 that no punishment for deviant behaviour encourages it to occur. About 28 (13%) of 223 neither agreed nor disagreed with a question. A total of 36 (16%) of 223 responses were not

submitted for this question. In summary, a total of 54% of respondents disagreed that non-compliance security behaviour is encouraged by knowing that there will be no punishment.

Table 4.47: Certainty of punishment - deviant security behaviour is not certainly punished

DT_Certainty_Punishment_Non-compliance_Not_Certaintly_Punished					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*12*	*5.4*	*6.4*	*6.4*
	Agree	*27*	*12.1*	*14.4*	*20.9*
	Neutral	*28*	*12.6*	*15.0*	*35.8*
	Disagree	*37*	*16.6*	*19.8*	*55.6*
	Strongly Disagree	*83*	*37.2*	*44.4*	*100.0*
	Total	*187*	*83.9*	*100.0*	
	Missing System	*36*	*16.1*		
	Total	*223*	*100.0*		

4.3.5.5. DT – Severity of punishment, and harsh consequences encourage non-compliance

This question was to determine if employees comply with the Information Security Policy because they are aware that if they do not the consequence for non-compliance will be harsh. Table 4.48 shares that a majority, 52 (23%) strongly agreed and 84 (38%) of 223 employees agreed that harsh consequences encourage compliance with the principles of the security policies. Only 18 (9%) respondents out of 223 disagreed that harsh punishment motivates compliant behaviour from employees. There were 36 (16%) of 223 missing responses that were not submitted for this question. A total of 33 (15%) neither agreed nor disagreed with the statement that harsh consequences enforced by the bank encourage compliant behaviour. In summary, a total of 61% agreed that they comply with information security policy because if they do not the punishment will be harsh. Only 11% of employees disagreed.

Table 4.48: Severity -harsh punishment encourages compliant security behaviour

DT_Severity_Harsh_Punishment_Non-compliance				
	Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*

Valid	*Strongly Agree*	*52*	*23.3*	*27.8*	*27.8*
	Agree	*84*	*37.7*	*44.9*	*72.7*
	Neutral	*33*	*14.8*	*17.6*	*90.4*
	Disagree	*8*	*3.6*	*4.3*	*94.7*
	Strongly Disagree	*10*	*4.5*	*5.3*	*100.0*
	Total	*187*	*83.9*	*100.0*	
	Missing System	*36*	*16.1*		
	Total	*223*	*100.0*		

4.3.5.6. DT – Severity of punishment, and lenient consequences encourage non-compliance

The purpose of the question was to understand if employees thought that lenient punishment for Information Security deviant behaviour is encouraging non-compliant behaviour. Table 4.49 shows that there were 90 (40%) of those strongly disagreed and 44 (20%) agreed of 223 employees that lenient consequences encourage non-compliance to the security principles of the policy. There were 31 (14%) of 223 respondents who neither agreed nor disagreed with the question. Only a total of 22 (10%) respondents out of 223 thought that deviance was motivated by lenient consequences. Missing responses were 36 (16%) from 223 employees. In summary, 60% of respondents disagreed that lenient consequences encourage non-compliant security behaviour. Only 10% agreed.

Table 4.49: Severity - lenient punishment encourages non-compliant security behaviour

DT_Severity_Lenient_Punishment_Non-compliance					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*7*	*3.1*	*3.7*	*3.7*
	Agree	*15*	*6.7*	*8.0*	*11.8*
	Neutral	*31*	*13.9*	*16.6*	*28.3*
	Disagree	*44*	*19.7*	*23.5*	*51.8*
	Strongly Disagree	*90*	*40.4*	*48.1*	*100.0*
	Total	*187*	*83.9*	*100.0*	
	Missing System	*36*	*16.1*		
	Total	*223*	*100.0*		

Above we discussed the factors of the Deterrence Theory. In the next section, the Reactance Theory is discussed.

4.3.6. Psychological Reactance Theory (RT)

Reactance Theory investigates how employees react to the principles and the guidelines of the information security policy.

4.3.6.1. RT – Employee's reaction to information security policy

This question was asked to get an understanding from employees if they perceive the Information Security Policy to infringe on their freedom to act and hence, they are motivated to be non-compliant in retaliation. Table 4.50 details that there were 70 (31%) employees strongly disagreed and 47 (21%) of 223 employees disagreed that they are attitude is defensive and as a result, they are motivated to be non-compliant. A total of 48 (22%) of 223 employees neither agreed nor disagreed with the question. About 21 (10%) of a total of 223 employees agreed and strongly agreed that they participate in non-compliant security behaviour because they view the security policies as infringing on their ability to decide how to behave according to the principles of the security policies. There were 37 (17%) of 223 responses that were not submitted for this question. In summary, 52% of respondents disagreed that the information security policies infringe on their freedom to act. Only 10% of employees agreed.

Table 4.50: Reactance – information security policy infringes on the freedom to act

RT_Non-compliance_Infringe_On_Freedom_Act

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*6*	*2.7*	*3.2*	*3.2*
	Agree	*15*	*6.7*	*8.1*	*11.3*
	Neutral	*48*	*21.5*	*25.8*	*37.1*
	Disagree	*47*	*21.1*	*25.3*	*62.4*
	Strongly Disagree	*70*	*31.4*	*37.6*	*100.0*
	Total	*186*	*83.4*	*100.0*	
	Missing System	*37*	*16.6*		
	Total	*223*	*100.0*		

4.3.6.2. RT – Employee's reaction to information security policy

This question was to investigate employees whether react positively to the principles of the Information Security Policies and whether they are happy to comply with them. Table 4.51 portrays a total of 98 (44%) strongly agreed and 68 (31%) of 223 employees agreed that they are happy that the Information Security policy must be enforced, and they comply with it because the purpose of the policy is to protect all employees and the bank. Furthermore, a total of 37 (17%) of 223 people did not submit an answer to this question. Only 10 (5%) of 223 employees strongly disagreed and disagreed that they reacted positively to the principles of the security policy. There were 10 (5%) of 223 that neither agreed nor disagreed with a question. In summary, 75% of respondents agreed that they are positive and are happy to comply with the information security policy. Only 5% of employees disagreed.

Table 4.51: Reactance - positive attitude encourages compliance with security

RT_ISP_Protects_BankEmpoyees_and_Bank					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*98*	*43.9*	*52.7*	*52.7*
	Agree	*68*	*30.5*	*36.6*	*89.2*
	Neutral	*10*	*4.5*	*5.4*	*94.6*
	Disagree	*4*	*1.8*	*2.2*	*96.8*
	Strongly Disagree	*6*	*2.7*	*3.2*	*100.0*
	Total	*186*	*83.4*	*100.0*	
	Missing System	*37*	*16.6*		
	Total	*223*	*100.0*		

4.3.6.3. RT – Employee's reaction to information security policy

This question aimed to understand employees whether they view the Information Security Policy as a useless restriction that does not benefit them or the bank. Table 4.52 shows that most respondents with a total of 136 (61%) strongly disagreed and 28 (13%) of 223 disagreed that the principles of the policy did not benefit them or the bank and did not see the policy as a restriction Only 39 (18%) respondents did not submit their responses to the question. About

2 (1%) of 223 respondents strongly agreed and 6 (3%) agreed that the security policy is a restriction, and it does not benefit either the bank or its employees. There were 12 (5%) respondents who neither agreed nor disagreed with a question. In summary, 74% of respondents disagreed that the information security policy is a useless restriction.

Table 4.52: Reactance - security policy is not important

RT_ISP_Is_Useless_RedTape_Does_Not_Benefit_BankEmpoyees					
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	*Strongly Agree*	*2*	*.9*	*1.1*	*1.1*
	Agree	*6*	*2.7*	*3.3*	*4.3*
	Neutral	*12*	*5.4*	*6.5*	*10.9*
	Disagree	*28*	*12.6*	*15.2*	*26.1*
	Strongly Disagree	*136*	*61.0*	*73.9*	*100.0*
	Total	*184*	*82.5*	*100.0*	
	Missing System	*39*	*17.5*		
	Total	*223*	*100.0*		

4.6.3.4 Discussing the summary of descriptive statistics

- There were 216 of 223 bank employees who advised that they have a positive attitude towards the information security policy.
- The study received feedback from 209 of 223 bank employees indicating that the information security policy protects the bank and its employees.
- 172 of 223 employees disagreed and stated that the information security policy does not restrict the employees from doing what they want to do. The security policy is not a useless mechanism used to control employees.
- A total of 166 of 223 bank employees indicated that they have sufficient knowledge about the information security policy.
- There were 195 of 223 employees who disagreed that the information security policy training material was not available. They indicated that the material is available and easily accessible to employees.
- The study found that 216 of 223 bank employees indicated that they willingly comply with the information security policy.

- There were 197 of 223 bank employees who agreed to the question that compliance with the information security policy ensures that there are low incidents of security breaches.
- The feedback received showed that there were 177 of 223 bank employees who disagreed with the question that there was no punishment for non-compliance to information security policy. They also disagreed that data theft has no negative impact on the bank.

The above descriptive statistics shared insights into important aspects of compliance and non-compliance to information security policy according to the behaviour of bank employees. In the next section, we will discuss the Cronbach alpha and the reliability of our items/factors.

4.4. Inferential Statistics

This study used inferential statistics to answer the research questions. Cronbach alpha, Linear regression analysis and Pearson correlation were used for this study because of their concise, clear and statistical prowess in explaining the impact of one variable on another enabling the researcher to acquire insights on the security behaviour of bank employees.

4.4.1. Cronbach Alpha

Cronbach Alpha is one of the most used mechanisms that calculate reliability in organisational and social sciences (Cronbach, 1951). In essence, reliability defines the consistency, or precision of the items being measured in the questionnaire (Barbera, Naibert, Komperda, & Pentecost, 2021).

Cronbach alpha defines the reliability of the average or sum of questions being measured by the multiple items or concepts in our questionnaire, when this occurs, it refers to the measure as calculating the “internal consistency” reliability (Bonett & Wright, 2015).
In the table below, we share findings of the different factors borrowed from the security behaviour theories.

Abbreviations

TPB – Theory of Planned Behaviour
PMT – Protective Motivation Theory

TN – Techniques of Neutralisation

DT – Deterrence Theory

RT – Reactance Theory

It is suggested that the values of Cronbach alpha are as follows, if α ≥ .9 then the results are excellent. If α ≥ .8 the results are good. If α ≥ .7 the results are acceptable. If α ≥ .6 then results are questionable and if α ≥ .5 the results are poor (Cho & Kim, 2015).

Table 4.54: Results of Cronbach Alpha

Factor	Findings	Cronbach Alpha
TPB Attitude	TPB is a predictor of a positive attitude towards ISP.	= .752
TPB Awareness and Training	TPB is not a significant predictor of employees having no knowledge or training of ISP	= .261
PMT Self Efficacy	Self-efficacy is not a predictor of an employee's willingness to comply with the ISP	= .431
PMT Response Efficacy	Response Efficacy is a significant predictor of employees' views on their ability to avoid security threats based on principles in the ISP.	= .879
TN Denial of Responsibility	Denial of responsibility is not a predictor of an employee's non-conformance to ISP	= .676
TN Denial of Injury	Denial of Injury is a significant predictor of non-conformance to ISP	= .960

TN Denial of Victim	Denial of victim is a significant predictor of employee's non-conformance to ISP	= .848
TN Condemnation of Condemners	Condemnation of colleagues is a predictor of an employee's non-conformance to ISP	= .792
TN Appeal to Higher Loyalty	Appeal to higher loyalty is a significant predictor of employee's non-conformance to ISP	= .887
DT Swiftness of Punishment	The swiftness of punishment is not a predictor of an employee's non-conformance to ISP	= .666
DT Certainty of Punishment	Certainty of punishment is not a predictor of non-conformance to ISP	= .145
DT Severity of Punishment	The severity of punishment is not a predictor of an employee's non-conformance to ISP	= .163
RT Reactance	RT is not a predictor of employee's non-conformance to ISP	= .518

The results from above table indicated that the constructs Employee Attitude, Response Efficacy, Denial of Injury, Denial of Victim, Condemnation of Condemners, Appeal to higher loyalty were found to be significant predictors of non-conformance to information security policy $\alpha \geq .7$. The constructs Awareness and Training, Self-Efficacy, Denial of responsibility, Swiftness of punishment, Certainty of punishment, Severity to punishment and Reactance are

not a predictor of an employee's non-conformance to information security policy with Cronbach alpha of ≥ .6. The next section will discuss the Pearson correlation.

4.4.2. Pearson Correlation

We sought to find factors that correlate with each other to determine the possible behaviour of an employee about information security policy compliance or non-compliance. The employee's positive or negative attitude was used and contrasted against the other information security behaviour theory factors to get an understanding if a correlation exists or not.

4.4.2.1. TN – Theory of Planned Behaviour

It was found from the results that people who had positive attitudes indicated that there is a need for continuous improvement and will be receptive to additional ISP training.

The factors that made up the Theory of Planned Behaviour (TPB) were:

- ***Attitude***
- ***Training and awareness program***

Pearson correlation coefficient in next table, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation (Oliveira, Moral, Zocchi, Demetrio, & Hinde, 2020).

Table 4.55: Correlation coefficient for Theory of Planned Behaviour factor

Factor	Findings	Correlation coefficient
Attitude and Training	There is a significant positive relationship between positive attitude and being receptive to getting more training.	r (220) = .133, p = .047
Attitude and Increase in Training	There is a significant positive relationship between the attitude and the need to increase ISP training and	r (219) = .334, p < .001

	awareness for the program to be effective.	

The Theory of Planned Behaviour had two factors training and awareness and attitude. The results found that there is a significant positive relationship between positive attitude and training & awareness factors. Results of the current study indicated that both factors had a correlation of $P < 0.05$ which means there is a significant positive relationship between having a positive attitude towards the information security policy and willingness to get more in-depth training on principles of information security policy. Next is the Protective Motivation Theory.

4.4.2.2. PMT – Protective Motivation Theory

An investigation was conducted to verify if attitude has a relationship or not with factors or concepts of the Protective Motivation Theory which is:

- ***Self-Efficacy***
- ***Response Efficacy***

Consider the Pearson correlation coefficient in table below, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation (Oliveira, Moral, Zocchi, Demetrio, & Hinde, 2020).

Table 4.56: Correlation coefficient for Protective Motivation Theory concepts – Self-efficacy

Factors	***Findings***	**Correlation coefficient**
Attitude and Self-efficacy This is willingly complying with Information Security Policy (ISP)	There are significant positive relationships between the employee's attitude and factors relating to their self-efficacy, the willingness to comply with ISP.	r (220) = .193, p = .004
Attitude and Self-efficacy	There is a significant positive relationship	r (220) = .141, p = .035

This is willingly using principles of Information Security Policy to get information security assistance from the bank.	between the employee's attitude and factors relating to their self-efficacy, and the willingness to use ISP principles.	

Above table shows that the Protective Motivation Theory (PMT) had self-efficacy and response efficacy as factors. Both the factors correlated with $P < 0.05$ meaning that there is a significant positive relationship between the employee's attitude and factors relating to their self-efficacy and response-efficacy. Next we are presented with results of Protective Motivation Theory – response efficacy.

Consider Pearson correlation coefficient for below table, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation (Oliveira, Moral, Zocchi, Demetrio, & Hinde, 2020).

Table 4.57: Correlation coefficient for Protective Motivation Theory – response efficacy

Factor	***Findings***	***Correlation coefficient***
Attitude and Response-efficacy Information security breaches can be reduced with Information Security Policy.	There is a significant positive relationship between the employee's attitude and factors relating to their response to efficacy and the ability to reduce security breaches by having ISP.	r (220) = .190, p = .004
Attitude and Response-efficacy Complying with the Information Security Policy contributes to reducing security breaches.	There is a significant positive relationship between the employee's attitude and factors relating to their response efficacy, the ability of an employee to contribute	r (220) = .198, p = .003

	to the reduction of breaches by complying with ISP.	

The results above show that both the factors correlated with $P < 0.05$ meaning that there is a significant positive relationship between the employee's attitude and factors relating to their response efficacy and the ability to reduce security breaches by having information security policy in the organisation. Moreover, there is a significant positive relationship between the employee's attitude and factors relating to their response efficacy, the ability of an employee to contribute to the reduction of breaches by complying with information security policy. Next, we discuss the Neutralisation techniques.

4.4.2.3. TN – Techniques of Neutralisation

Five original methods explain the techniques starting with the denial of responsibility, denial of injury, denial of victim, condemnation of condemners and the appeal to higher loyalties (Skyes and Matza, 2010). These techniques were used in our study to predict the compliant or non-compliant security behaviour of bank employees. Literature has provided evidence that before humans choose a security behaviour, they would reason and justify to themselves why they choose either to comply or deviate from the principles of the information security policy (Siponen and Vance, 2010; Pei-Lee, et al., 2015). Most of these justifications fall within one of the factors covered by the Techniques of Neutralisation.

Consider Pearson correlation coefficient for below table of Techniques of Neutralisation, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation (Oliveira, Moral, Zocchi, Demetrio, & Hinde, 2020).

The Techniques of Neutralisation were under investigation namely denial of responsibility, denial of injury, denial of victim, condemnation of the condemners, and appeal to higher loyalties. Each has sub-concepts as follows:

Table 4.58: Correlation coefficient for Techniques of Neutralisation sub-concepts

	Sub-factors	Correlation coefficient
Denial of Responsibility	Q1. The bank does not hold deviant employees accountable for their actions. Q2. The bank cannot hold deviant employees accountable if they don't read the Information Security Policy. Q3. The bank exposes employees to customer-sensitive information and money. Q4. The employees are not responsible for protecting the bank and its customers.	P >.05 indicates that there is no significant relationship between an employee's attitude and the mentioned questions in the preceding column.
	Q5. The employees will first plead innocence or claim deviant action as a mistake	There is a negative correlation between employees' attitudes and their denying responsibility r (192) = -175, p = .015
Denial of Injury	Q1. Employees can abuse bank property. Q2. Employees comply with some principles and don't deviate from other principles of the security policy.	P > .05 indicating that there is no relationship between an employee's attitude and two questions on denial of injury on the preceding left column
	Q3. Employees can steal from the bank, and no one will notice. Q4. My colleagues comply but I don't comply with information security policy.	There is a significant negative correlation between employees' attitudes and the claim that banks deserve deviant behaviour from employees. The coefficient correlation showed respectively that r (192) = -15, p = .02 and r (192) = -18, p = 01

Denial of Victim	Q1. Employees were rewarded by the syndicate for stealing customer data. Q2. Employees not protecting sensitive data. Q3. Employees write passwords down.	P > .05 indicating that there is no relationship between an employee's attitude and two questions on denial of the victim on the preceding left column
	Q4. Employees share passwords amongst themselves.	There is a significant negative correlation between employees' attitudes and the statement that they introduce vulnerabilities to the bank by sharing passwords. The coefficient correlation indicates that r (186) = -15, p = .03
Condemnation of the Condemners	Q1. All my colleagues don't comply, and neither am I complying. Q2. Targets put pressure on employees, hence we don't comply.	P > .05 indicating that there is no relationship between an employee's attitude and condemnation questions on the preceding left column
	Q3. Managers promote wrongdoing.	There is a significant negative correlation between employees' attitudes, and people in authority promoting wrongdoing at work r (190) = -.19, p = .007
Appeal to Higher Loyalties	Q1. Employee's background caused them to be non-compliant. Q2. Employees acted on instruction when they deviated from the principles of the information security policy.	P > .05 indicating that there is no relationship between an employee's attitude and choosing deviant behaviour claiming that social norms are less important than their needs as stated in the preceding left column

	Q3. Employee's religious beliefs caused them to be non-compliant.	There is a significant negative correlation between employees' attitudes, and appeal to higher loyalties r (192) = -.14, p = .04

The results in above table showed that P > 0.05 which means that all Techniques of Neutralisation factors were found to have a significant negative correlation between employees' attitude or information security behaviour and factors of TN. This indicated that the bank employees are not influenced by Techniques of Neutralisation. Next we delve into Deterrence Theory.

4.4.2.4. DT – Deterrence Theory

This theory investigated the swiftness, certainty, and severity of punishment if they would influence people to comply with information security policy. A correlation was performed to investigate the employees' attitudes and check if swiftness, certainty, and severity of punishment have a linear relationship or not.

4.4.2.4.1. DT has these concepts and sub-factors.

- ***Swiftness of Punishment***
  - An employee who is non-compliant with the information security policy will be dismissed immediately.
  - An employee who chooses to deviate from the security policy will be punished immediately after the act is performed.

- ***Severity of Punishment***
  - Employees who are non-compliant with the information security policy experience harsh punishment.
  - Employees who deviate from the security policy experience a lenient punishment for non-conformance.

- ***Certainty of Punishment***
  - Employees who deviate from the security policy will be punished for their chosen actions.

Consider the Pearson correlation coefficient for below table with results of deterrence theory, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation (Oliveira, Moral, Zocchi, Demetrio, & Hinde, 2020).

Table 4.59: Correlation coefficient for Deterrence Theory factors

Factors	***Findings***	***Correlation coefficient***
Swiftness of punishment ***Severity of punishment*** ***Certainty of punishment***	There is no significant relationship considering an employee's positive attitude and the swiftness, severity and certainty of punishment for non-compliance. This means an employee who has a positive attitude (willingly chooses to comply with information security policy) is not influenced by the factors of the Deterrence Theory to deviate from the security policy.	P > .05

The above able depicts the Deterrence Theory (DT) investigation which found factors of DT to have P > .05 and r = 0 meaning there was no significant relationship considering an employee's positive attitude and the swiftness, severity and certainty of punishment for non-compliance. Next, the Reactance Theory is discussed.

4.4.2.5. RT – Reactance Theory.

The theory delved into understanding whether bank employees may consider the information security policy as interfering with their freedom to act. We have one main factor called Reactance and three sub-factors.

- ***Reactance***
  - Employees choose deviant behaviour because information security infringes on bank employees' freedom to act.

Note the Pearson correlation coefficient in below table, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation (Oliveira, Moral, Zocchi, Demetrio, & Hinde, 2020).

Table 4.60: Correlation coefficient of Reactance Theory – infringes on the freedom to act.

Factor	***Findings***	***Correlation coefficient***
Reactance Employees choose deviant behaviour because information security infringes on bank employees' freedom to act.	There is no significant correlation between employee's positive attitude and the Reactance Theory factor checking for views on interfering with the freedom to act by bank employees	r (184) = -.03, p = .60

The results in table above indicated that there was no positive correlation between employee's attitude and how they reacted when they think of the information security policy as restricting them from doing what they want to do. Next results of whether the information security policy is a red tape or not are presented.

Consider the Pearson correlation coefficient in table below, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation (Oliveira, Moral, Zocchi, Demetrio, & Hinde, 2020).

Table 4.61: Correlation coefficient of Reactance Theory – security policy not important.

Factor	***Findings***	***Correlation coefficient***

Reactance Information security policy is a useless red tape, it does not benefit the bank or its employees hence I choose to be non-compliant.	There is no significant correlation or association between employee's positive attitude and the Reactance Theory factor checking for views on whether information security policy is a useless red tape	r (182) = -.07, p = .31

The above table shows there is no significant correlation between employee's positive attitude and the Reactance Theory. Next, the correlation of Reactance Theory – security policy protects the bank is discussed.

Consider the Pearson correlation coefficient in table below, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation (Oliveira, Moral, Zocchi, Demetrio, & Hinde, 2020).

- Information security policy protects the bank and its vital resources, employees are happy to comply.

Table 4.62: Correlation coefficient for Reactance Theory – security policy protects the bank.

Factor	***Findings***	***Correlation coefficient***
Reactance Information security policy protects the bank and its vital resources, employees are happy to comply.	There is a significant positive correlation between employee's positive attitude and their views confirming that information security policy protects the bank and its employees hence bank employees are happy to	r (184) = .15, p = .03

	comply with the principles of the security policy	

Above table shows there is a significant positive correlation between employee's positive attitude and their views confirming that information security policy protects the bank and its employees. Next discussion delves into the Linear Regression Analysis.

4.4.3. Linear Regression Analysis

We investigated and sought to get an understanding of the impact on the bank when employees introduce security vulnerabilities. Regression analysis was used to get the insights, it is a statistical method that can be used to predict one (independent) variable's impact on another called, the dependent variable (Abdel, Alamro, & Alamro, 2020). The initial tests investigated the security behaviour theories individually to evaluate the relationships between the variables. Interpreting the linear regression coefficient in tables below, r allocates the value between -1 and 1, a value of 0 means there is no correlation, value of 1 means a positive correlation and -1 interpreted as negative correlation. If the p-value is greater than 0.05, then the independent variables does not show a statistically significant relationship with the dependent variable. If p-value is less than 0.05 then the variables show a significant relationship with each other.

Table 4.63: Individual Information Security Theories

Factors	R	R Square	Sig	Explanation
RT	.167	.028	.165	Reactance Theory positively impacts attitude or security behaviour R = .167, however, the significance of the influence is very low P > 0.05. RT could only predict 28% of the bank employee's security behaviour.
DT	.106	.011	.916	Deterrence Theory positively impacts attitude or security behaviour R = .106, however, the significance of the influence is very low P > 0.05. DT could only predict 11% of the bank employee's security behaviour.
TN	.445	.198	.012	Techniques of Neutralisation positively impact attitude R = .445 however the significance of the influence is high P

				< 0.05. TN could only predict 20% of the bank employee's security behaviour.
PMT	.355	.126	<.001	Protective Motivation Theory positively impacts attitude or security behaviour R = .355 and the influence in determining the security behaviour is highly significant P < 0.05. PMT could only predict 13% of bank employee's security behaviour.
TPB	.556	.310	<.001	The theory of Planned Behaviour positively impacts attitude or security behaviour R = .556 and the influence in predicting the security behaviour is highly significant P < 0.05. TPB could only predict 31% of bank employee's security behaviour.

The above information security behaviour theories all impact the attitude however the significance of the impact very low.

Table 4.64: Composite Information Security Behaviour Framework

Factors	R	R Square	Sig	Explanation
RT, DT, TN, PMT, TPB	.719	.517	<.001	The composite framework produced results that indicate that the model is more predictive of the security behaviour of employees R = .719 The composite framework positively impacts the attitude of the employee, and the influence on the attitude is highly significant P < .001 All the factors of the composite framework can predict 52% of bank employee's positive attitude or compliant security behaviour because R square = .517

The table above shows results of the Composite Information Security Behaviour Framework. The information security behaviour theories when used as a composite framework are more effective in predicting employee behaviour and the impact of the behaviour on the bank. The value of R = .719 is high proving its statistical and predictive power to anticipate the employee's compliant information security behaviour. The employee's compliant attitude was positively impacted, and the influence of that impact was found to be significantly high $P < 0.05$. Bank employees are highly likely to be compliant with the principles of the information security policy when the factors of the composite framework are used in conjunction to predict the security behaviour of employees.

The below table covers all the hypotheses that the study presents from the different information security behaviour theories. Table 4.65. gives a summary of the hypothesis of the current study and details whether the results supported the hypothesis or not.

Table 4.65: Summary of hypothesis testing

Hypothesis	Description	Findings
H1a	A positive attitude influences compliance with information security policies.	Supported
H1b	Information Security Training and Awareness positively influence compliance with information security policies.	Supported
H2a	Self-efficacy positively influences the security behaviour of an employee.	Unsupported
H2b	Response efficacy positively influences the security behaviour of an employee.	Supported
H3a	Denial of responsibility positively influences non-compliance behaviour.	Unsupported
H3b	Denial of Injury positively influences non-compliance behaviour.	Supported

H3c	Denial of victim positively influences non-compliance behaviour.	Supported
H3d	Condemnation of the condemners positively influences non-compliance behaviour.	Supported
H3e	Appeal to higher loyalties positively influences non-compliance behaviour.	Supported
H4a	The swiftness of punishment has a positive influence on non-compliant security behaviour.	Unsupported
H4b	Certainty of punishment has a positive influence on non-compliant security behaviour.	Unsupported
H4c	The severity of punishment has a positive influence on non-compliant security behaviour.	Unsupported
H5	Reactance positively influences non-compliance behaviour.	Unsupported

4.5 Conclusion

We discussed above the descriptive statistics imparting comprehensive insights about the security behaviour of the employees. We then delved into Pearson correlation, Cronbach alpha and multiple regression to understand the relationship between dependent and independent variables. The study concluded the results by summarising the hypothesis and indicating whether the results supported or rejected the hypothesis. The next chapter discusses the findings and the insights revealed by answering the research questions.

Chapter 5: Discussion of Results

Introduction

The purpose of this section is to present findings about the research questions and hypotheses. Importantly it is to highlight the contribution to literature and the effectiveness of the Composite Information Security Framework (CISB) it has on predicting the information security behaviour of bank employees to comply or be non-compliant to the information security policy. These are explained in more detail below.

5.1. Research Question One

What are the motivating factors that encourage bank employees to comply with information security policies?

The Pearson correlation coefficient (r) defines the strength and relationship of quantitative variables. If r is greater than 0.5 it means the relationship is strong. If r is less than 0.5 it indicates a weak relationship. If r is 0 it means, there is no association between the variables. This study used Pearson correlation to calculate the relationship that exists between variables that encourage bank employees to comply with information security policy. The researcher first investigated the Theory of Planned Behaviour. Table 4.55 had two factors training and awareness and attitude. The results found that there is a significant positive relationship between positive attitude and training & awareness factors. Results of the current study indicate that both factors had a correlation of $P < 0.05$ which means there is a significant positive relationship between having a positive attitude towards the information security policy and willingness to get more in-depth training on principles of information security policy. This is in accordance with research by Bulgurcu et al. (2010) that defined a positive attitude as one that is optimistic and encourages compliant security behaviour. A positive attitude is one where a person feels in control regardless of external factors, only a few factors such as knowledge, beliefs and culture may affect an attitude. Thus, the Theory of Planned Behaviour defines a positive attitude as one that can be a promoter of compliance with the information security policy guidelines (Hina, et al., 2019). Hadlington (2017) also agrees that a positive attitude towards cybersecurity in business was negatively related to risky cybersecurity behaviours. “The results present a further step in understanding the individual differences that may govern good cybersecurity practices, highlighting the need to focus directly on more effective training and awareness mechanisms” (Hadlington, 2017, p. 2).

5.1.1. The Protective Motivation Theory (PMT) had self-efficacy and response efficacy as factors. Both the factors correlated with $P < 0.05$ meaning that there is a significant positive relationship between the employee's attitude and factors relating to their self-efficacy and response-efficacy Table 4.56 and 4.57. Results from current study agrees with past research study that found that the appraisal of coping mechanisms which are response cost and self-efficacy has significant influence on protective behaviour intentions (Ma, 2022). Similar studies (Herath & Rao, 2009; Herath et al., 2014; Siponen et al., 2010) have examined the impact of response cost and self-efficacy on IS policy compliance intention as well as users' behavioural intentions to use email authentication systems. It found that the Chinese security employees have a positive attitude towards their self-efficacy and response efficacy to protect themselves against any security threats.

5.1.2. The study then investigated the Techniques of Neutralisation (TN) which consists of factors denial of injury, denial of responsibility, denial of victim, condemning the condemners and appeal to higher loyalty. The results showed that $P > 0.05$ which means that all Techniques of Neutralisation factors in Table 4.58 were found to have a significant negative correlation between employees' attitude or security behaviour and factors of TN. This indicates that the bank employees are not influenced by Techniques of Neutralisation to justify to themselves and others their reasons for non-compliant security behaviour. These results contradict previous research that defines Techniques of Neutralisation as the dominant predictor and influencer of deviant behaviour (Siponen and Vance, 2010; Pei-Lee, et al., 2015). The results from the study conducted about bank employees did not support that the denial of responsibility, denial of injury, denial of victim, condemnation of condemners and the appeal to higher loyalties influenced the security behaviour of the respondents.

5.1.3. The Deterrence Theory (DT) investigation found factors of DT in Table 4.59 to have $P > .05$ meaning there was no significant relationship considering an employee's positive attitude and the swiftness, severity and certainty of punishment for non-compliance. This means that bank employees willingly comply with the information security policies and standards, and the Deterrence Theory had not influenced their security behaviour to comply. These contradicts findings by Straub (Straub, 1990) that states that

Deterrence Theory is a determinant of discouraging non-compliant security behaviour (Straub, 1990). Similarly, (Foth, 2016) shared that the Deterrence Theory plays a major role in ensuring a reduction of security incidents in an organisation.

Investigations that used the Composite Information Security Behaviour Framework (CISB), the PMT and TPB were found to be the information security theories that most influenced positively the compliant security behaviour of bank employees.

5.2. Research Question Two

What factors influence deviant/non-compliant behaviour of information security policies by bank employees?

5.2.1. The Cronbach alpha investigated the internal consistency of the variables. If the alpha is 0.6 or lower, it is not a predictor of compliance, if it is 0.7 it is a predictor of compliance however if alpha is 0.8 and above it is a significant predictor of compliance to security policy. Some factors from the Composite Information Security Framework showed an influence on the security behaviour of employees. The factor Attitude in Table 4.64 was found to be a predictor in compliance security behaviour = .752 which means that if a bank employee has a positive attitude towards the information security policy, they are likely to comply with its principles. The response efficacy in Table 4.64 emerged as a significant predictor of compliant information security behaviour = .879, this indicates that the bank employees believe that what is being recommended by the principles of the information security policy does assist them in avoiding risks thus influencing them to comply with the security policy. These results from current study are consistent and in agreement with findings of prior researched discussed in point 5.1 above by (Hina, et al., 2019) stating that a positive attitude encourages compliance to information security policy and negative attitude encourages non-compliance.

5.2.2. Denial of injury and denial of the victim are significant predictors of non-compliant security behaviour. Denial of injury in Table 4.64 produced results of alpha = .960, this means that the security behaviour of bank employees is significantly influenced by employees' justification to themselves that their behaviour does not harm the bank leading to bank employees not complying with the principles of the information

security policy. The denial of the victim factor produced an alpha result of = .848, this means that bank employees' security behaviour is significantly influencing non-compliance to principles of information security policy and the employees deny that their security behaviour is causing any harm to the bank. The appeal to higher loyalties factor was found to be a significant predictor in non-compliant security behaviour with alpha results of = .887, this indicates that bank employees are significantly influenced to be non-compliant to principles of security policy should they have reasons that they feel justify their deviant security behaviour especially if those reasons benefit the employee and others (deviating from the policy for the greater good of self and others). Lastly, the condemnation of the condemners was found to fairly predict non-conformance to information security policy with alpha results of =.792, this means some bank employees are influenced to be non-compliant to principles of information security policy because they believe other employees particularly those in position of influence and power allow other employees to deviate hence they are also justified to engage in unacceptable behaviour that contradicts the security policy. Deterrence Theory studies are aligned in that they agree that the higher the severity, certainty, and celerity of the punishment, the less likely an employee will deviate (D'Arcy, et al., 2009; Hu and Xu, 2018; Straub, 1990). The results of these studies indicate that severity, certainty, and celerity are positive moderators of Deterrence Theory. Many studies used Deterrence Theory to explain the compliant behaviour of employees, however, the results of those studies were inconsistent and contradicting with the current results of this study and contradicted these studies (D'Arcy and Herath, 2011; Guo,2013). Subsequently, it was argued that Deterrence Theory is more suitable for predicting non-compliance behaviour (D'Arcy, et al., 2009; D'Arcy and Herath, 2011; Gwebu, et al., 2019), the results of our study are agreement with results of these studies by (D'Arcy, et al., 2009; D'Arcy and Herath, 2011; Gwebu, et al., 2019).

5.3. Research Question Three

What impact does the security behaviour of employees have on the bank?

5.3.1. Multiple Regression analysis was used to acquire insights into the impact that the security behaviour of the employee has on the bank. We used an employee's attitude

and calculated the variance of the different information security theories individually, then the measure was done using the Composite Information Security Framework (CISB). This was to determine the impact of the employee's attitude to the bank.

Individual Information Security Theories, Table 4.4.3.1 above provides the details of the results. All the information security theories had a positive impact on the employee's attitude. Techniques of Neutralisation (TN), Protective Motivation Theory (PMT) and Theory of Planned Behaviour (TPB) all were important in that the impact was found significant however all three theories could only predict a very low percentage of the employee's security behaviour.

Composite Information Security Behaviour Framework, Table 4.4.3.2 above indicated that the information security behaviour theories when used as a composite framework are more effective in predicting employee behaviour and the impact of the behaviour on the bank. The value of R = .719 is high proving its statistical and predictive power to anticipate the employee's compliant security behaviour.

The employee's compliant attitude was positively impacted, and the influence of that impact was found to be significantly high $P < 0.05$. Bank employees are highly likely to be compliant with the principles of the information security policy when the factors of the composite framework are used in conjunction to predict the security behaviour of employees in contrast to using stand-alone information security behaviour theories.

The results of the study predicted that the information security behaviour of 52% of the bank employees is influenced to be compliant with the information security policy and the compliance impacts the bank positively. This means that the bank has some work to do in training, monitoring, enforcing and thoroughly addressing the non-compliance of the rest of its employees.

The study used factors namely Attitude, Information Security Policy (ISP) protects the bank, ISP restricts employees, ISP knowledge, ISP training not available, Employee willingly comply to ISP, ISP ensure low-security incidents, No/lack of punishment for non-compliance and Theft had no impact to the bank to understand the information

security behaviour of bank employees. Table 5.1 presents results from the current study compared to results from prior research that are either similar or different to our findings.

Table 5.1: Results of Current vs Prior Research

Factor	Results from the current study	Results from prior studies
Positive attitude	216 (97%) Agreed 3 (1%) Disagreed 4 (2%) neither agreed nor disagreed Bank employees agreed that they identified themselves as having a positive attitude towards the information security policy.	Findings suggest that employed users report higher levels of fear and protection motivation than personal users. The theoretical crux of an effective fear appeal is that it must be personally relevant to stimulate fear; the study showed that concrete fear appeals help stimulate fear and the desired protective response (Schuetz, Lowry, Pienta, & Thatcher, 2020)
ISP protects the bank	209 (94%) Agreed 7 (3%) Disagreed 7 (3%) neither agreed nor disagreed 209 bank employees agreed that the information security policy protects the bank and its employees.	Organisational culture shapes the information security culture. When security policy becomes the responsibility of all employees and monitoring of security behaviour occurs then compliance increases. When there is an increase in compliance with the information security policy then the organisation is protected. (Saxena, et al., 2020)
ISP restricts employees	26 (11%) Agreed 172 (78%) Disagreed 25 (11%) neither agreed nor disagreed	The study found that security behaviour measurements and assessments must be identified and enforced to positively change a person's attitude towards compliance and must

	Results indicated that 172 employees disagreed that the information security policy restricts employees from doing what they want.	consider a person's role, seniority and department to customise it to be effective. The study indicated that the information security policy is important and encourages compliance (D'arcy & Herath, 2011)
ISP knowledge	166 (74%) Agreed 13 (6%) Disagreed 44 (20%) neither agreed nor disagreed Information security policy and its principles enable employees to choose to comply, 166 employees agreed with that.	Lack of information and knowledge is one of the many root causes of information security breaches. When people acquire knowledge, it provides an opportunity for them to make an informed choice of their behaviour (Gwebu, Wang, & Hu, 2020)
ISP training not available	15 (7%) Agreed 195 (87%) Disagreed 13 (6%) neither agreed nor disagreed 195 employees disagreed that information security policy training is not made available to all in the bank.	The study highlighted the importance of an information security program and how it can be used as a mechanism for altering employee behaviour and deterring non-compliance (AlGhamdi, Win, & Vlahu-Gjorgievska, 2022)
Employees willingly comply with ISP	216 (97%) Agreed 3 (1%) Disagreed 4 (2%) neither agreed nor disagreed	Employees have been found to willingly comply with security policy when information security training is increased. (AlGhamdi, Win, & Vlahu-Gjorgievska, 2022)

	Results depicted 216 employees who agreed that they comply with the information security policy willingly.	
ISP ensure low-security incidents	197 (89%) Agreed 13 (6%) Disagreed 13 (5%) neither agreed nor disagreed 197 employees agreed that the information security policy ensures low-security incidents in the bank.	The study found Deterrence Theory having assisted with lowering information security breaches. (Vance, Siponen, & Straub, 2020)
No punishment for non-compliance to ISP	4 (2%) Agreed 177 (80%) Disagreed 42 (18%) neither agreed nor disagreed Results show that 177 employees disagreed that there is no punishment for non-compliance with the information security policy.	Research has indicated that cultural differences may be one reason for inconsistent findings hence calling for cross-cultural research on deterrence in information security. The study formulated a model including deterrence, moral beliefs, shame, and neutralization techniques (Vance, Siponen, & Straub, 2020)
No impact to the bank of security behaviour data theft	13 (6%) Agreed 177 (80%) Disagreed 33 (14%) neither agreed nor disagreed	The research examined the role of organizational punishment and organizational norms in impacting employees' resistance towards the ISS policies (Merhi & Ahluwalia, 2019)

	All 177 employees disagreed that there is no impact on the bank if their security behaviour is non-compliant with the information security policy.	

5.4. Limitations and future consideration

This study only focused on people who currently have valid employment contracts. In future, the study can extend to those who have previously worked for the bank. Having the experience of working at the bank, the former bank employees may share valuable insights on what they observed, their security behaviour when they were employees of the bank and what influenced them to comply with the information security policy.

The study did not receive feedback from some people working in retail branches as it anticipated, there were manual responses received from some employees that asked not to take part in the study due to them fearing their manager would find out about them taking part and discipline them. The study did not include employees from the other 3 major banks in SA, permission to explore the study was received only from one of the big four major banks.

The future study can include employees from various banks who have both physical and online presence. It would be interesting to investigate and find out whether the operating model of the bank may have an impact on the security behaviour of their employees or not. The future study can do a comparative study against this study, it would compare information security behaviours of employees across the South African banks and contrast the behaviour and possibly get the influences of those behaviours.

5.5. Contribution of Study

The study has contributed to the information security behaviour theories by developing the Composite Information Security Behaviour Framework (CISB) that was utilised to investigate the factors influencing the information security behaviour of bank employees and the impact of that compliant or non-compliant behaviour to the bank. The results of the study predicted that the information security behaviour of 52% of the bank employees that provided responses to the questionnaire is influenced to be compliant with the information security policy and the

compliance impacts the bank positively. Based on the results, we can suppose that the bank has work to do on the 48% of their employees to possibly train, educate and help them understand the benefits of complying to the information security policy.

5.6. Conclusion

The study was conducted at a major South African bank with population of 25 000, the sample size of 383 employees and received 223 valid responses. The respondents had entry, junior, senior and executive level positions. The questionnaire was distributed to both IT and non-IT employees working in all 9 provinces of South Africa, working in rural and urban areas. The research gap was identified after observing an increase in malicious, accidental, and intentional information security incidents caused by employees which necessitated further research to get insights on how to detect and prevent internal attacks.

The research gap was explored using the main research question which probed what insights regarding compliance and non-compliance can be gathered from information security behaviour of employees in the South African banking industry? The research objectives were to determine the motivating factors that influence employees to comply or be non-compliant to information security policy. Additionally, the study investigated the impact of the employee's information security behaviour on the bank.

The key findings that stemmed from the study were the researcher invented a hybrid theoretical framework named the Composite Information Security Behaviour Framework (CISB) which consists of Protective Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Deterrence Theory (DT), Reactance Theory (RT) and Techniques of Neutralisation (TN). The CISB framework was able to predict 52% of the security behaviours of bank employees in contrast to using individual information security behaviour theories on their own to predict compliant and non-compliant behaviour. Pearson correlation indicated that the Protective Motivation Theory (PMT) and Theory of Planned Behaviour were the information security theories that most influenced positively and significantly the compliant information security behaviour of bank employees.

The nature of operations in the banking industry requires that the banks implement measures that govern acceptable and unacceptable security behaviour of employees. Information

Security Policies are therefore critical in ensuring that there is a smooth running of business and that risks are identified, quantified, contained, and mitigated. Moreover, it is of utmost importance that employees together with banks collaborate and protect themselves and their customers against information security threats that can be exploited emanating from within the bank.

References

Abdel, M., Alamro, A., & Alamro, A. (2020). Factors affecting intention to use e-banking in JordanAbdel Latef M. Anouze and Ahmed S. Alamro. *International Journal of Bank Marketing, 38*, 86-112.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organisational Behaviour and Human Decision Processes, 50*, 179-211.

Ajzen, I. (2002). Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behaviour. *Journal of Applied Social Pyschology, 32*, 665-683.

Ajzen, I. (2011). The Theory of Planned Behaviour: Reactions and Reflections. *Journal of Psychology and Health, 26*, 1113-1127.

Ajzen, I., & Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior. New Jersey: Prentice-Hall, Englewood Cliffs.

AlGhamdi, S., Win, K., & Vlahu-Gjorgievska. (2022). Employee's intentions towards complying with information security controls in Saudi Arabia's public organisation. *Goverment Information Quarterly*.

Alharahsheh, H., & Pius, A. (2020). A Review of Key Paradigms: Positivism VS Interpretivism. *Global Academic Journal of Humanities and Social Sciences, 2*, 1-2.

Ali, R., & Dominic, P. (2024). Investigation of information security policy violations among oil and gas employees: A security-related stress and avoidance coping perspective. *Journal of Information Science*, 254-272.

Ali, R., Dominic, P., Ali, S., Rehman, M., & Sohail, A. (2021). Information Security Behaviour and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Journal of Applied Science, 11*, 2 - 38.

Alzahrani, L. (2021). Factors Impacting Users' Compliance with Information Security Policies: An Empirical Study. *International Journal of Advanced Computer Science and Applications, 12*, 437-446.

Arkkelin, D. (2014). Using SPSS to Understand Research and Data Analysis. *Journal of Psychology Curricular , 1*, 3-25.

Ashenden, D. (2018). In their Own Words: Employee Attitudes Towards Information Security . *Journal of Information and Computer Security, 26*, 327-337.

Attride-Stirling, J. (2001). Thematic Networks: An Analytical Tool for Qualitative Research. *Qualitative Research, 1*, 385-405.

Barbera, J., Naibert, N., Komperda, R., & Pentecost, T. (2021). Clarity on Cronbach's Alpha Use. *Journal of Chemical Education, 98*, 257-258.

BASA. (2024, April 10). *The Banking Association of South Africa*. Retrieved from Bank Crime: https://www.banking.org.za/consumer-information/bank-crime/

Blumberg, B., Cooper, D., & Schindler, P. (2014). *Business Research Methods.* New York: McGraw-Hill Education Publication.

Bonett, D., & Wright, T. (2015). Cronbach's alpha reliability: Interval estimation, hyphothesis testing, and sample size planning. *Journal of Organizational Behavior, 36*, 3-15.

Boss, S., Galletta, D., Lowry, P., Moody, G., & Polak, P. (2015). What do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly , 39*, 837 - 864.

Box, D., & Pottas, D. (2014). A Model for Information Security Compliant Behavior in the Healthcare Context. *Journal of Procedia Technology, 16*, 1462-1470.

Braun V, C. V. (2006). Using Thematic Analysis in Psychology. *Journal of Qualitative Research in Psychology, 3*, 77-101.

Briney, A. (2001). Information Security Industry Survey. USA: Information Security Magazine.

Bulgurcu, B., Cavusoglu, H., & Benbasant, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. *MIS Quarterly, 3*, 523-548.

Casteel, A., & Bridier, N. (2021). Describing Population and Samples in Doctoral Student Research. *Journal of Doctoral Studies Vol. 16*, 339 - 362.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violations of IS security policy in organisations: an intergrated model based social control and deterrence theory. *Computers and Security*, 447 - 458.

Cho, E., & Kim, S. (2015). Cronbach's Coefficient Alpha: Well Known but Poorly Understood. . *Organizational Research Methods*, 207-230.

Clarke, V., & Braun, V. (2017). Thematic Analysis. *Journal of Positive Psychology, 12*, 297-298.

Conaty, F. (2021). Abduction as a Methodological Approach to Case Study Research in Management Accounting - An Illustrative Case. *Journal of Accounting, Finance & Governance Review, 27*, 3 - 18.

Cram, A., Proudfoot, J., & D Arcy, J. (2020). Maximizing Employee Compliance with CyberSecurity Policies. *MIS Quarterly Vol. 19 No. 3*, 183 - 198.

Cram, A., Proudfoot, J., & D'Arcy, J. (2020). Maximizing Employee Compliance with Cyber Security Policies. *MIS Quarterly , 19*, 183 - 198.

Cram, W., D'Arcy, J., & Proudfoot, J. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 525 - 541.

Creswell, J. (2014). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* housand Oaks, California: SAGE Publications.

Creswell, J., & Plano Clark, V. (2007). *Designing and Conducting Mixed Methods .* Thousand Oaks, California: SAGE Publications.

Creswell, J., & Plano Clark, V. (2007). *Designing and Conducting Mixed Methods Research.* Thousand Oaks, California: SAGE Publications.

Cronbach, l. (1951). Coefficient Alpha and the Internal Structure of Tests. *Psychometrika, 16*, 297-334.

D'Arcy, J., & Herath, T. (2011). A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings. *Journal of Information Systems, 20*, 643-658.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature:Making sense of the disparate findings. *Earopean Journal of Information Systems*, 643 - 658.

D'Arcy, J., & Lowry, P. (2019). Cognitive-affective Drivers of Employee's Daily Compliance with Information Security Policies: A Multilevel, longitudinal Study. *Journal of Information Systems , 29*, 43 - 69.

D'Arcy, J., & Lowry, P. (2019). Cognitive-affective Drivers of Employee's Daily Compliance with Information Security Policies: A Multilevel, longitudinal Study. *Information Systems Journal, 29*, 43 - 69.

D'Arcy, J., & Lowry, P. (2019). Cognitive-affective Drivers of Employee's Daily Compliance with Information Security Policies: A Multilevel, longitudinal Study. *Journal of Information Systems , 29*, 43 - 69.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and its Impact on Information Security misuse: A Deterrence Approach. *Information System Research*, 79 - 99.

Denzin, N., & Lincoln, Y. (2000). *Handbook of Qualitative Research.* London: SAGE .

Dhladhla, T. (2022, November). Insights derived from information security behaviour of employees in the South African banking industry. *Research Proposal*. Johannesburg, Gauteng, South Africa.

Dlamini, M., Eloff, J., & Eloff, J. (2009). Information Security: The moving target. *Journal of Computer & Security, 11*, 1-10.

Fasae, F. (2024). Human and Technology Components in Data/Information Security. *Journal of Computer Science and Information Technology*, 93-107.

Foth, M. (2016). Factors Influencing Intentions to Comply with Data Protection in Hospitals: Based on Gender Differences in Behaviour and Deterrence. *European Journal of Information Systems*.

Francis, J., Johnston, M., Robertson, C., Glidewell, L., Entwhistle, V., Eccles, M., & Grimshaw, J. (2010). What is an Adequate Sample Size? Operationalising Data

Saturation for Theory-Driven Interview Studies. *Journal of Psychology and Health, 25*, 1229-1245.

Grey, D. (2014). *Doing Research in the Real World.* Thousand Oaks, California: SAGE Publications.

Gwebu, K., Wang, J., & Hu, M. (2019). Information Security Policy Noncompliance: An Integrative Social Influence Model. *Journal of Information Systems Vol. 30 No. 2*, 220 - 269.

Gwebu, K., Wang, J., & Hu, M. (2020). Information security noncompliance: An integrative social influence model . *Journal of Information Systems*, 220 - 269.

Hadlington, L. (2017). Human Factors in Cybersecurity, Examining the Link between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity and Risky Cybersecurity Behaviours. *Heliyon*.

Hina, S., Selvam, D., & Lowry, P. (2019). Institutional Governance and Protection Motivation: Theoretical Insights into Shaping Employee's Security Compliance Behaviour in Higher Education Institutions in a Developing World. *Journal of Computers and Security, 87*, 2-15.

Hobson, K. (2019, December 12). *Forbes*. Retrieved from Forbes.com: https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2019/12/12/five-reasons-employees-are-your-companys-no-1-asset/?sh=4b2407c92563

Hooper, V., & Blunt, C. (2020). Factors Influencing the Information Security Policy Behaviour of IT Employees. *Journal of Behaviour & Information Technology, 39*(8), 862 - 874.

Hu, Q., & Xu, Z. (2018). The Role of Rational Calculus in Controlling Individual Propensity toward Information Security Policy Noncompliance Behaviour. (pp. 3688 - 3697). Hawaii: Proceedings of 51st Hawaii International Conference on Systems Sciences.

ISO/IEC, 2. (2013). *ISO 7001:2007*. Retrieved June 22, 2022, from https://www.sis.se/api/document/preview/918727/

Kajtazi, M., Cavusoglu, H., & Benbasant, I. (2018). Escalation of Commitment an an Antecedent to Non-compliance with Information Security Policy. *Journal of Information and Computer Security, 26*, 171-193.

Khan, N., Houghton, R., & Sharples, S. (2021). Understanding Factors that Infuence Unintentional Insider Threat: A Framework to Counteract Unintentional Risks. *Journal of cognition, Technology & Work* , 2-16.

Kiger, M., & Varpio, L. (2020). Thematic Analysis of Qualitative Data: AMEE Guide No 131. *International Journal of Education in Health Sciences*, 2- 10.

Kuo, K.-M., Talley, P., & Huang, C.-H. (2020). Meta-Analysis of the Deterrence Theory in Security Compliant and Security-Risk Behaviours. *Journal of Computers and Security, 96*, 3-12.

Kuppusamya, P., Samy, G., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B., & Perumal, S. (2020). Systematic Literature Review of Information Security Compliance Behaviour Theories. *Journal of Physics: Conference Series, 1551*.

Lowry, P., & Moody, G. (2014). Proposing the Control Reactance Compliance Model CRCM to explain Opposing Motivations to Comply with Organisational Information Security Policies. *Journal of Information Systems Vol. 25 No. 5*, 433 - 463.

Lowry, P., Posey, C., Bennett, R., & Roberts, T. (2015). Leveraging Fairness and Reactive Theories to Deter Reactive Computer Abuse following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust. *Journal of Information Systems Vol. 25 No. 3*, 193-201.

Lowry, P., Posey, C., Roberts, T., & Bennett, R. (2014). Is your Banker Leaking your Personal Information? The Roles of Ethics and Individual-level Cultural Characteristics in Predicting Organisational Computer Abuse. *Journal of Business Ethics , 121*, 385-401.

Lundgren, B., & Moller, N. (2019). Defining Information Security. *Journal of Science, Engineering and Ethics, 25*, 419-441.

Ma, X. (2022). IS Professionals' Information Security Behaviors in Chinese IT organizations for Information Security Protection. *Journal of Information Processing and Management*.

Majid, U. (2018). Research Fundamentals: Study Design, Population and Sample Size. *Journal of Undergraduate Research in Natural and Clinical Sciences and Technology Vol. 2 No. 1*, 1 - 7.

Merhi, M., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to information systems security. *Journal of Computers in Human Behaviour* , 37- 46.

Monzon, L. (2021). *Is South Africa a Playground for Cybercriminals?* Retrieved June 4, 2022, from https://www.itnewsafrica.com/2021/10/is-south-africa-a-playground-for-cybercriminals/

Moody, G., Siponen, M., Pahnila, & Seppo. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly Vol. 42 No. 1*, 285 - 311.

Muhammad, K., Zarkada, A., & Ramayan, T. (2017). The Moderating Effect of Religiosity on Ethical Behavioural Intentions: An application of the Extended Theory of Planned Behaviour to Pakistani Bank Employees. *Personnel Review, 46*, 1-24.

Nakitende, M., Rafay, A., & Waseem, M. (2024). *Frauds in Business Organizations: A Comprehensive Overview.* USA: IGI Global.

Oliveira, T., Moral, R., Zocchi, S., Demetrio, C., & Hinde, J. (2020). Icc: an R package to estimate the concordance correlation, Pearson correlation and accuracy over time. *PeerJ*.

O'Neill, M., Booth, S., & Lamb, J. (2018). Using NVivo for Literature Reviews: The Eight Step Pedagogy (N7+1). *Journal of Qualitative Report, 23*, 21-39.

Pereira, T., & Santos, H. (2015). *Human Aspects of Information Security, Privacy, and Trust* (ISBN : 978-3-319-20375-1 ed.). Switzerland: Springer International.

Phiri, J., Lavhengwa, T., & Segooa, M. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *The South African Journal of Information Management*.

Pieterse, H. (2021). The Cyber Threat Landscape in South Africa: A 10-year review. *The African Journal of Information and Communication , 28*, 1-21.

Ponemon. (2023). *Cost of a Data Breach Report 2023.* New York: IBM.

Ponemon, I. (2021). *Cost of a Data Breach 2021 Report.* Michigan: IBM Security.

Presidency, R. (2013). *Protection of Personal Information Act.* Cape Town: Goverment Gazette.

PwC's Global Economic Crime Survey. (2020, January 17). Retrieved from Global Economic Crime and Fraud Survey: https://www.corruptionwatch.org.za/wpcontent/uploads/2020/06/global-economic-crime-survey-20201.pdf

Qualtrics. (2022). Determining the Sample Size: How to Make Sure You Get the Right Sample Size. United Kingdom: Qualtrics.

Riahi, E., & Islam, M. (2023). Employees' information security awareness (ISA) in public organisations: insights from cross-cultural studies in Sweden, France, and Tunisia. *Journal of Behaviour & Information Technology*, 1-23.

Rosenthal, R. (1994). Science and Ethics in Conducting, Analyzing and Reporting Psychological Research. *Americal Psychological Society Vol. 5 No. 3*, 127 - 134.

SARB. (2023, November 29). Retrieved from South African Reserve Bank Financial Stability Review Second Edition: https://www.resbank.co.za/content/dam/sarb/publications/reviews/finstab-review/2023/financial-stability-review/second-edition-2023-financial-stability-review/Second%20Edition%202023%20Financial%20Stability%20Review1.pdf

SARB. (2024, April 24). *Exchange Control Circular No. 4/2024*. Retrieved from The South African Reserve Bank: https://www.resbank.co.za/en/home/what-we-do/financial-surveillance/financial-surveillance-documents

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students.* Essex: Pitman Publishing.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K., & Burnap, P. (2020). Impact and key challenges of insider threats on organisation and critical businesses. *Electronics*.

Schuetz, S., Lowry, P., Pienta, D., & Thatcher, J. (2020). Effectiveness of Abstract versus Concrete Fear Appeals in Information Security. *Journal of Management Information Systems INFORMATION SYSTEMS* , 723 - 757.

Seidman, I. (2013). *Interviewing as Qualitative Research: A Guide for Researchers in Education & the Social Sciences* (ISBN: 978-0-8077-7 ed.). New York: Teachers College Press.

Shamsudin, N., Yatin, S., Nazim, N., Talib, A., Sopiee, M., & Shaari, F. (2019). Information Security Behaviours among Employees. *Journal of Academic Research in Business and Social Sciences*, 560 - 571.

Siponen, M., & Kajava, J. (1998). Ontology of Organisational IT Security Awareness - From Theoretical Foundation to Practical Framework. (pp. 327 - 331). Stanford, CA, USA: 17th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises Proceedings .

Sittenthaler, S., Traut-Mattausch, E., & Jonas, E. (2015). Observing the Restriction of Another Person: Vicarious Reactance and the Role Self-Construal and Culture. *Journal Frontiers in Psychology Vol.6 No. 1052*, 1 - 13.

Smith, K. J. (2023). Bad Employees: Examining Deviant Security Behaviors. *Journal of Computer Information Systems*, 17-30.

Straub, D. (1990). Effective IS Security: An Emperical Study. *Journal of Information Systems Research* .

Sykes, G., & Matza, D. (2010). *Encyclopedia of Criminological Theory.* Thousand Oaks: SAGE Publications.Inc.

Tenzin, S., McGill, T., & Dixon, M. (2024). An Investigation of the Factors That Influence Information Security Culture in Government Organizations in Bhutan. *Journal of Global Information Technology Management*, 37-62.

The RSA Presidency. (2013). *Protection of Personal Information Act.* Cape Town: Goverment Gazette.

Van Wyk, A., Ganz, N., Mothibe, P., & Machaba, S. (2016). King IV - Steering Point. A summary of the King IV Report on Corporate Governance South Africa. Johannesburg, Gauteng, South Africa.

Vance, A., Siponen, M., & Straub, D. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Journal of Information and Management*.

Vroom, C., & Solms, v. R. (2004). Towards Information Security Behavioral Compliance . *Journal of Computers & Security, 23*, 191 -198.

Warkentin, M., Willison, R., & Johnston, A. (2011). The Role of Perceptions of Organizational Injustice and Techniques of Neutralization in Forming Computer Abuse Intentions.

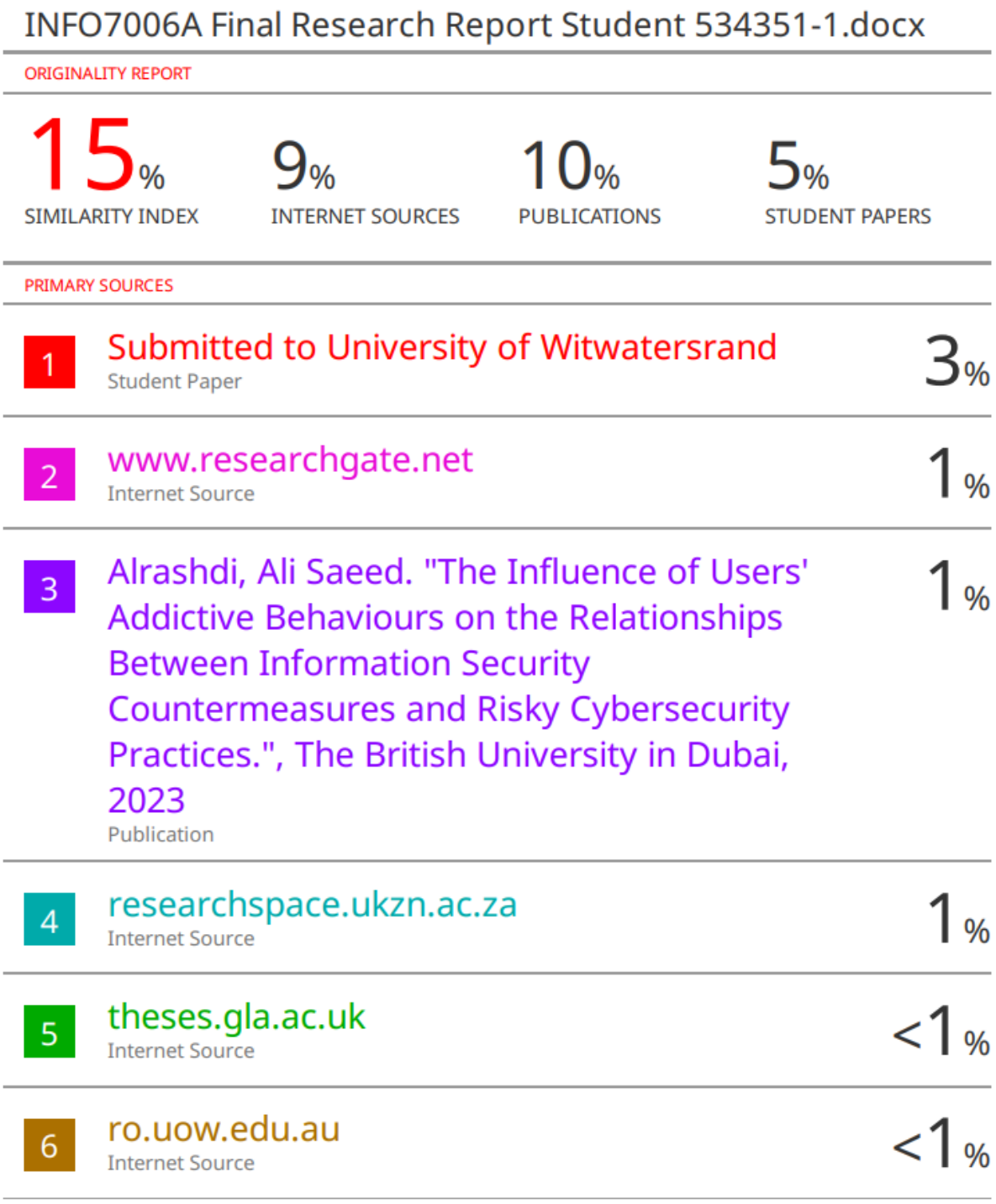
Wass. (2020). Internet crime; Data integrity; Banks; Mental health; Threats; Computer security; Human Error Employees,. United Kingdom, Charlottesville: SNL Financial LC.

Wire Feed. (2019). Mobile Commerce; Security Portfolios; Banking; Financial Services; Fraud. Switzerland, Lausanne: African Press Organization - APO.

Yazdanmehr, A., Wang, J., & Yang, Z. (2020). Peers matter: The Moderating Role of Social Influence on Information Security Policy Compliance. *Journal of Information Systems Vol. 30 No. 5*, 791 - 844.

Appendices

Appendix A: Plagiarism Report



INFO7006A Final Research Report Student 534351-1.docx

ORIGINALITY REPORT

15%	9%	10%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Witwatersrand Student Paper	3%
2	www.researchgate.net Internet Source	1%
3	Alrashdi, Ali Saeed. "The Influence of Users' Addictive Behaviours on the Relationships Between Information Security Countermeasures and Risky Cybersecurity Practices.", The British University in Dubai, 2023 Publication	1%
4	researchspace.ukzn.ac.za Internet Source	1%
5	theses.gla.ac.uk Internet Source	<1%
6	ro.uow.edu.au Internet Source	<1%

Appendix B: Student Form

5

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

Faculty of Commerce, Law and Management

Candidate's Declaration

Name of Candidate:	Thembi Dhladhla
Person Number:	534351
Degree:	MCom Information Systems
Supervisor / Co-Supervisor:	Dr Kebashnee Moodley
School:	School of Business Sciences
Title of Thesis/Dissertation/ Research Report:	Insights derived from information security behaviour of employees in the South African banking industry.

Candidate's Declaration:

i. I hereby submit my PhD Thesis/Masters dissertation for examination (circle applicable).

ii. I confirm that my signed declaration in terms of Rule G9.7 is included in each copy of the thesis/ dissertation.

iii. I have checked all copies of my thesis/ dissertation and declare that no pages are missing or poorly reproduced.

iv. I hereby submit a CD/USB containing a PDF version of my submission for examination and _____ bound copies.

Candidate's Signature: C.T Dhladhla **Date:** 20 Dec 2023

Appendix C: Supervisor Form

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

APPENDIX 2

UNIVERSITY CLEARANCE CERTIFICATE[5]

Name: Constance Thembi Dhladhla candidate for the degree of Mcom Information Systems has today submitted her/his thesis/dissertation/research report/project for examination.

		YES	NO
a)	Has this thesis/dissertation/research report/project been submitted with the consent of the supervisor?	X	
b)	To the best of your knowledge are you able to confirm that the candidate has acknowledged all information used in the thesis, dissertation or research report/project?	X	
c)	To the best of your knowledge are you able to confirm that the candidate has not used any confidential information without the required permission in the thesis, dissertation or research report/project? If **No**, please provide an explanation in the supervisor's report.	X	
d)	Did the candidate's research involve any engagement with people, animals, or the environment?	X	
e)	If **Yes**, did the candidate obtain ethical clearance by the relevant, approved ethics committee of the University before the research was conducted?	X	

f) If **Yes**, please state the ethics certificate number

Protocol Number: CBUSE2057

(If **No**, the degree may not be awarded.)

Name of Supervisor Dr Kebashnee Moodley
Signature of the Supervisor
Date 20 December 2023

Appendix D: Research Questionnaire

Section A: Demographic information

This section seeks to understand more about you.

Q1. What is your primary role in your company?

- ○ Executive
- ○ Senior Manager
- ○ Middle Manager
- ○ Junior Manager
- ○ General Staff Member
- ○ Other (Specify)

Q2. In which department do you work?

- ○ RBB
- ○ CIB
- ○ Group Finance
- ○ Group Technology
- ○ Balance Sheet Management
- ○ Legal
- ○ Audit
- ○ Other (Specify)

Q3. Would you classify your primary role as IT (information technology) or Non-IT?

- ○ IT role
- ○ Non-IT role

Q4. How many years have you been working in the banking industry?

- ○ Less than 2 years
- ○ 2 to 5 years
- ○ 6 to 10 years
- ○ 11 to 20 years
- ○ More than 20 years

Section B: Information Security Compliant Behaviour

This sections seeks to understand the employees' motivating factors that influence compliance with information security policy.

Q5. To determine employee's attitude towards Information Security Policy, please select a statement that describes your attitude with the information security policy from the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. I have a positive attitude towards information security policy, it is vital in helping me understand what is acceptable security behaviour. It also shares information on how to use the bank devices and IT system	○	○	○	○	○
2. I have a conflicted attitude towards information security policy. It does not help employees or the bank in any way.	○	○	○	○	○
3. Information security policy is key to ensuring that I safeguard myself and the bank assets from being abused.	○	○	○	○	○
4. Information Security policy is used as a mechanism to unnecessarily control and restrict what I can do.	○	○	○	○	○
5. I do not care about information security policy, It does not help nor does it deter me from doing anything.	○	○	○	○	○

Q6. To determine employees' views concerning Security Awareness and Training, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. There is need to increase security awareness by offering additional security awareness and training	○	○	○	○	○
2. I possess sufficient knowledge on information security policy.	○	○	○	○	○
3. Various online training material is communicated however, I do not have the time to read them.	○	○	○	○	○
4. I have not seen a communication nor have I done any online training and assessment.	○	○	○	○	○
5. There is a need to improve the entire information security awareness and training program so it can be effective.	○	○	○	○	○

Q7. To determine employees' views on self-efficacy. Self-efficacy refers to an individual's confidence in their ability to complete a task or achieve a goal. Please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. I comply with the information security policy on my own as I understand the importance of security policies.	○	○	○	○	○
2. I intend to continue using the information security policy measures, provided I get guidance when I get stuck.	○	○	○	○	○

Q8. To determine employees' views on response-efficacy. Response-efficacy refers to a person's beliefs as to whether the recommended action step will actually avoid the threat. Please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. Having information security policy in our organisation keeps security breaches down.	○	○	○	○	○
2. Complying to information security policy keeps the security breaches down.	○	○	○	○	○
3. Information security threats can be significantly minimised if we all comply with the principles in the policy.	○	○	○	○	○
4. Information security threats cannot be completely eroded if some of us do not comply with the principles in the policy	○	○	○	○	○

Section C: Information Security Non-compliant Behaviour

This sections seeks to understand the employees' motivating factors that influence non-compliance to information security policy.

Q9. To determine employee's views on their responsibility towards the bank and information security policy, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. I sometimes do not adhere to the information security policy, the bank does not hold employees responsible for non-compliant behaviour therefore it is not my fault.	○	○	○	○	○
2. Employees do not read the information security policy, therefore, the bank cannot hold them accountable for what they do not know.	○	○	○	○	○
3. The employees are the victims, they are exposed to critical data and money that they do not have.	○	○	○	○	○
4. Mistakes happen, when working in the bank employees plead innocence if that does not work then claim it to be a mistake.	○	○	○	○	○
5. It is not the responsibility of employees to protect the bank's customer and employee data, money or IT systems.	○	○	○	○	○

Q10. To determine employees views on how their security behaviour affects the bank, customers and colleagues, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. Employees take money from the bank, it makes no dent. The bank is adequately financed, one employee stealing from it is not noticeable.	○	○	○	○	○
2. Employees may share personal data belonging to customers with third parties. This is done to steal from well off customers knowing that the bank will compensate them.	○	○	○	○	○
3. It was not a mistake that I lost the laptop. My colleagues are receiving new laptops while I am not, the insurance will pay so the bank lost nothing at all.	○	○	○	○	○
4. Many colleagues comply with information security policy, am not hurting anyone when I do not. I am only one out of thousands who comply, therefore there is no negative impact from a single non-compliant behaviour.	○	○	○	○	○
5. I comply to some principles in the policy but do not comply to many others. My compliance on some make up for those I do not comply on. In that way, no harm done to the bank.	○	○	○	○	○
6. Provide other reason(s) if reasons above do not correctly represent your views about employee security behaviour and its impacts the bank.	○	○	○	○	○

Q11. To determine employees' view on introducing internal vulnerabilities that harm the bank, customers and colleagues through their security behaviour, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. I just extracted their personal data and got a reward for sharing it.	○	○	○	○	○
2. Employees share passwords, there are too many systems used to remember all these different passwords from the different systems.	○	○	○	○	○
3. We have always discarded papers in the bin containing customer sensitive data, no risk was ever exploited before. No need to change our working process if it is not broken.	○	○	○	○	○
4. To make it easy for myself, I write the password down but I make sure I hide it so others cannot see or use it.	○	○	○	○	○

Q12. To determine employees' view on condemning others and the bank when being reprimanded, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. Managers pretend to be better than others when they behave worse, they give their friends privileges of viewing sensitive information they should not have access to.	○	○	○	○	○
2. Most employees do not comply with information security policy, colleagues know each other's secrets of non-compliancy.	○	○	○	○	○
3. Employees are put under severe pressure of achieving targets, that is the reason they end up rewarding themselves by committing fraud. The manager is at fault!	○	○	○	○	○
4. Provide other reason(s) if reasons above do not correctly represent your views about the condemnation of others and the bank when being reprimanded.	○	○	○	○	○

Q13. To determine employees' view on the scrutiny and punishment for non-compliant security behaviour, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. It is a norm in our organisation to be non-compliant with information security policy, we do not get scrutinised for deviant behaviour.	○	○	○	○	○
2. Religious beliefs force employees to be non-compliant with information security policy.	○	○	○	○	○
3. The background of employees forces them to be non-compliant with principles in the information security policy.	○	○	○	○	○
4. I should not be punished, IT department said it is ok to fix the work device myself at home when I contacted them telephonically.	○	○	○	○	○

Q14. To determine employees' view on swiftness of punishment and its effect to their security behaviour, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. Employees comply with information security policy because some behaviours are dismissible with immediate effect.	○	○	○	○	○
2. Non-compliant behaviour with information security policy is met by immediate punishment	○	○	○	○	○
3. Provide other reason(s) if reasons above do not correctly represent your views about the swiftness of punishment in the bank.	○	○	○	○	○

Q15. To determine employees' view on certainty of punishment and its effect to their security behaviour, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. Employees are motivated to comply with information security policy because it is known from experience that any behaviour contradicting it will certainly be punished, even if not immediately punished.	○	○	○	○	○
2. Non-compliance to information security policy is encouraged by knowing certainly that the employee will not be punished for it.	○	○	○	○	○
3. Provide other reason(s) if reasons above do not correctly represent your views about the certainty of punishment in the bank.	○	○	○	○	○

Q16. To determine employees' view on the severity of punishment and its effect to their security behaviour, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. Employees comply with information security policy because it is known that if any contradicting behaviour occurs, the punishment will be harsh.	○	○	○	○	○
2. Employees are motivated to be non-compliant to information security policy because they get a slap on the hand when the deviate from the policy.	○	○	○	○	○
3. Provide other reason(s) if reasons above do not correctly represent your views about the severity of punishment in the bank.	○	○	○	○	○

Q17. To determine the employees' reaction to the information security policy, please indicate the extent to which you agree or disagree with the following statements:

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
1. Employee's reaction is defensive, non-compliant to information security policy occurs because the requirements from policy infringe on the freedom to act	○	○	○	○	○
2. Employees happy for the information security policy to be enforced and comply to it because the purpose of the policy is to protect employees, customer data and the bank.	○	○	○	○	○
3. The information security policy is a useless red-tape, it does nothing for employees and the bank.	○	○	○	○	○

We thank you for your time spent taking this survey.

Your response has been recorded.