TOWARDS A FRAMEWORK FOR ENHANCING EMPLOYEES' CYBERSECURITY POLICY AWARENESS IN FINANCIAL INSTITUTIONS

by

RENEUOE CAROLINE THAMAE

Submitted in accordance with the requirements for
the degree of

MASTER OF SCIENCE

in the subject

COMPUTING

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: DR H. ABDULLAH

CO-SUPERVISOR: PROF M. MUJINGA

JULY 2024

DECLARATION

Name: Reneuoe Caroline Thamae

Student Number: 51856387

Degree: Master of Science in Computing

Towards a framework for enhancing employees' cybersecurity policy awareness in financial institutions

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

______________________ 04/07/2024

SIGNATURE DATE

ACKNOWLEDGEMENTS

Above all, I express my gratitude to **ALMIGHTY GOD** for His unwavering assistance. He has given me strength and encouragement throughout the toughest moments of completing this dissertation. I appreciate His boundless and unconditional affection, grace, and mercy that He has showered upon me.

My deepest gratitude is directed to my supervisor, Dr Abdullah and Co-supervisor, Professor Mujinga, for their continuous support, patience, and invaluable advice throughout the completion of this dissertation. Their enormous experience and knowledge kept me going in my academic study.

My special thanks to:

- Dr Sipho Maseko for editing my dissertation.
- The Lesotho Financial Institutions for granting me permission to conduct the survey with their employees.

I extend my sincere and heartfelt gratitude to my family, without ranking their contributions, for the immense support and unwavering hope they have bestowed upon me. Their support has been instrumental in making this study a reality.

- My husband, Lepekola Lepekola for his endless support. He would stay up the nights to see that I complete the work and help in peer reviewing my work.
- My two daughters, Katleho and Reitumetse and son Karabo for their patience when mummy could not give them her undivided attention due to being busy with her studies.
- My mother, 'Mamokoteli Thamae for her great love and support. I would call her when things got difficult, and she would give me words of encouragement.
- My nephew, Tumelo Thamae, for always holding the fort for me by assisting my daughter Katleho with her schoolwork when I could not help her due to my busy schedule.
- My sisters, Dr Mampiti Matete who would always give me advice about academic life and approaches, and Mphielo Petlane who instead of saying anything would laugh at me for being miserable. That laughter made me frustrated and strong, but at the same time kept me pushing my studies.

DEDICATION

I dedicate this dissertation to my husband, **Lepekola**, and our two daughters, **Katleho** and **Reitumetse**, and our son **Karabo**, for their endless encouragement and unwavering belief in me throughout this journey.

ABSTRACT

In an era marked by technological reliance and the escalating frequency of cyberattacks, prioritising cybersecurity has become imperative for organisations, particularly in the financial sector. The safeguarding of financial data and assets requires measures beyond conventional tools such as firewalls and encryption. However, a critical vulnerability persists in the form of the human element, as many financial sector employees lack adequate training in cybersecurity best practices, leaving organisations susceptible to cyber threats. To address this vulnerability, financial institutions must proactively implement effective awareness programs centred on cybersecurity policies. These programs aim to elevate employee awareness of risks, provide knowledge on identifying and responding to threats, and instilling a pervasive culture of cybersecurity. Despite the acknowledged importance of such programs, a noticeable research gap exists regarding their effectiveness and best practices.

This study bridges this gap by proposing a comprehensive framework to enhance cybersecurity policy awareness programs within the financial sector. Informed by an extensive review of relevant literature and insights from interviews with cybersecurity experts and financial professionals, the framework offers practical guidelines to fortify cybersecurity initiatives, ultimately mitigating the potential for cyberattacks.

Furthermore, employing a quantitative monomethod, the research gathered perspectives from employees of financial institutions, encompassing both IT and non-IT staff. The results unveiled a significant disparity in the impact of cybersecurity policy awareness programs on employee behaviour, exposing gender differences with males exhibiting a higher likelihood of possessing advanced cybersecurity knowledge. Recognising the implications for women's empowerment in the cybersecurity field, the framework incorporates gender mainstreaming.

To address challenges, the study recommends proactive measures, including comprehensive training programs and reporting procedures, to enhance cybersecurity knowledge across all employees. Emphasising the urgency of addressing gender disparities to foster inclusivity and diversity, the refined framework strategically positions itself to tackle compliance issues. It aims to contribute to the cultivation of a robust cybersecurity culture, ensuring a holistic and inclusive approach to policy adherence within financial organisations.

KEY TERMS:

Cybersecurity Policy; Cybersecurity Awareness; Cybersecurity Compliance; Cybersecurity Framework; Cybersecurity Training Programs; Data Breaches; Employee Behaviour; Financial Institutions; Risk Management; Social Engineering.

PEER-REVIEWED PUBLICATION FROM THIS STUDY

The following publication emanated from this research and was published during the study.

1. Thamae, R., Abdullah, H. and Mujinga, M., 2023, February. Toward a Framework to Improve Employees' Compliance with Cybersecurity Policy in Organizations. In *International Congress on Information and Communication Technology* (pp. 359-369). Singapore: Springer Nature Singapore.
2. Thamae, R., Abdullah, H. and Mujinga, M., 2024. Enhancing Cybersecurity Policy Awareness Programs in the Financial Sector: A Comprehensive Framework and Assessment of Effectiveness. The International Conference on Business and Technology (ICBT 2024). United Kingdom: Springer Nature United Kingdom.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AIC – Akaike’s Information Criterion

ANOVA – Analysis of Variance

BIC – Bayesian Information Criterion

CAIC – Consistent Akaike’s Information Criterion

CSP – Cybersecurity Policy

CSPA – Cybersecurity Policy Awareness

CSPAP – Cybersecurity Policy Awareness Programs

HR – Human Resources

I/O – Industrial Organisation

IT – Information Technology

KNN – K-Nearest Neighbour

LDA – Linear Discriminant Analysis

MLR – Multinomial Logistic Regression

Non-IT – Non-Information Technology

SPSS – Statistical Package for Social Sciences

VIF - Variance Inflation Factor

CHAPTER 1: INTRODUCTION

1.1 Introduction

With the increasing adoption of digital technologies, organisations, particularly financial institutions, face an increasing array of cybersecurity risks, including malware, phishing attacks, data breaches, and cyber espionage (Momoh, Adelaja and Ejiwumi, 2023; Onunka *et al.*, 2023). As a crucial pillar of global economic stability and growth, financial institutions are increasingly targeted by advanced cyber-attacks. This trend underscores the need for a dynamic and robust cybersecurity framework to protect assets and sensitive data (Oyeniyi *et al*., 2024). Implementing advanced security tools, such as firewalls and antivirus software, along with robust governance strategies, is crucial for protecting financial institutions from these cyber threats (Oyeniyi *et al*., 2024). Although technological defences such as antivirus software and firewalls are important, they rarely provide sufficient protection against the range of threats financial institutions face (Momoh, Adelaja and Ejiwumi, 2023). Achieving effective cybersecurity necessitates a holistic approach that includes people, processes, and technology (Furuichi and Aibara, 2019). The financial sector should emphasize the human aspect of cybersecurity, incorporating training and awareness initiatives to effectively counter social engineering attacks. Furthermore, its cybersecurity strategy should be adaptable, utilising both cutting-edge technology and human expertise to create robust defences against cyber threats (Oyeniyi *et al*., 2024).

It is crucial, however, to recognise that while off-the-shelf cybersecurity awareness training programs and external organisations play a role, relying solely on them may present certain weaknesses. A notable weakness is the lack of customisation to the specific needs and details of an organisation. Off-the-shelf programs are designed to be general and applicable to a wide range of industries and businesses. Consequently, the one-size-fits-all approach may not adequately address the unique threats that financial institution faces. A comprehensive strategy demands a tailored approach that considers the unique needs and challenges of the financial institution. This tailored approach becomes especially pertinent as organisations often struggle with the design and implementation of effective training programs, as highlighted in studies such as that by Gasiba *et al*. (2021), which revealed significant gaps in employees' cybersecurity training experiences. Engaging employees who may not prioritise cybersecurity or fully understand the risks they face is a challenge in designing effective cybersecurity awareness training (Gasiba *et al.*, 2021).

Despite the increasing prevalence of cybersecurity risks in the digital age, organisations often struggle to develop and implement engaging and effective cybersecurity awareness training programs for employees (Gasiba *et al.*, 2021). This study aims to address this gap by developing a framework for enhancing cybersecurity policy awareness programs in the financial sector. The framework will consider the diverse needs of employees and the evolving landscape of cybersecurity risks, ultimately promoting a culture of cybersecurity safety within financial institutions.

1.2 Background

Compliance with cybersecurity policies refers to the degree to which individuals within an organisation adhere to established policies, procedures, and guidelines implemented to safeguard an organisation's information and technological resources from unauthorised entry, utilisation, exposure, interruption, alteration, or eradication (Cybersecurity, 2018). Integral to risk management in financial institutions is the imperative need for compliance with cybersecurity policies (Dupont, 2019). As technology becomes increasingly intertwined with service provision and the storage of sensitive data, adherence to these policies gains heightened significance in financial institutions (Dupont, 2019). Moreover, compliance extends beyond mere adherence to in-house regulations (Cybersecurity, 2018). It encompasses alignment with laws, regulations, and industry standards pertinent to information security in financial institutions. This comprehensive approach ensures that an organisation operates within the legal and regulatory framework while meeting industry best practices to mention a few (Cybersecurity, 2018). The criticality of compliance with these cybersecurity policies serves as a stronghold, safeguarding sensitive data, financial assets, and the overall reputation of the institution. The multifaceted nature of these policies is instrumental in preserving the integrity and security of the organisation in an ever-evolving digital landscape (Cybersecurity, 2018).

Employees' Compliance with cybersecurity policies is critical for financial institutions, given the financial institutions' role in managing and protecting financial assets and transactions (Momoh, Adelaja and Ejiwumi, 2023). Furthermore, employees' compliance with cybersecurity regulations is crucial in protecting the integrity, availability, and confidentiality of financial data in financial institutions (Donalds and Osei-Bryson, 2020; Onunka *et al.*, 2023). Direct risks to financial institutions can undermine the integrity, availability, and confidentiality of financial data. Direct risks in financial institutions' cybersecurity pertain to the immediate consequences of a cyberattack on key services or components of the financial system. The direct risks can lead to financial losses for both customers and the institutions and undermine confidence in the financial system (Onunka *et al.*, 2023). Financial institutions are increasingly targeted by cybercriminals aiming to gain unauthorized access to sensitive financial data, steal funds, or disrupt operations due to the vast amount of sensitive information they hold (Momoh, Adelaja and Ejiwumi, 2023). Unauthorised access, disruption of operations and theft can be regarded as direct risks to financial institutions.

Financial institutions have adopted diverse cybersecurity protocols, including intrusion detection systems, firewalls, and encryption (Manoliu, 2022). However, there are several breaches that financial institutions face when striving to achieve effective cybersecurity compliance. As per the findings outlined in the Verizon 2022 Data Breach Investigations Report, 79% of breaches in the financial sector involved system intrusion, web applications and miscellaneous errors, while 40% involved stolen credentials (Verizon, 2022; ABA BankingJournal, 2023). The expenses incurred by financial institutions due to cyberattacks can be significant, encompassing financial damages, harm to reputation, and regulatory fines (Cybersecurity, 2018; Dupont, 2019; Nurse, 2021; Verizon, 2020).

Financial institutions have experienced a growing trend in cybercrime and data breaches in recent years, with types of cyber threats including malware attacks, skimming, social engineering, and ransomware, resulting in huge financial losses, legal liabilities, and reputational damage (Akintoye *et al.*, 2022; Momoh, Adelaja and Ejiwumi, 2023). Legal liabilities, financial losses and reputational damage can be regarded as indirect risks (Onunka *et al.*, 2023). Indirect risks in financial institutions' cybersecurity pertains to the wider consequences and implications of a cyberattack on the financial system. While not immediate, these risks can significantly impact the stability of the financial system and the overall economy. As of December 9, 2022, a staggering 566 data breaches were reported globally, compromising over 254 million records (Flashpoint, 2022; SentinelOne, 2023). Notably, 57 percent of these breaches were attributed to general hacking, highlighting the prevalent method of unauthorised access, while 6.5 percent were linked to skimming (Flashpoint, 2022). Simultaneously, ransomware attacks on financial services significantly increased, jumping from 55% in 2022 to 64% in 2023, nearly doubling the previously reported figure of 34% in 2021 (SentinelOne, 2023). The effects of cybercrime on financial institutions has been devastating, and across the world, it is anticipated to reach $10.5 trillion per year by 2025(Sausalito and Morgan, 2020).

The IBM Cost of a Data Breach Report 2023 reveals that the financial sector is the second most targeted sector by cybercriminals, trailing behind only the healthcare industry (IBM Security, 2023). These incidents highlight the need for financial institutions to take cybersecurity compliance seriously. Human factors such as insufficient awareness, along with nonconformity with security policies, are identified as the main reasons for cybersecurity breaches and incidents in financial institutions (Ofori *et al.*, 2021). Several high-profile cybersecurity breaches have occurred in the financial sector in recent years, including the

Experian data breach in 2020, Flagstar Bank in 2022, and the Capital One breach in 2023, which exposed vulnerabilities in cybersecurity policies and practices of financial institutions and the need for stricter compliance measures (Kost, 2022; Greig, 2023).

In each country, financial institutions are required to implement comprehensive security policies and procedures (Dupont, 2019). For those that operate in Lesotho, they should implement the Lesotho's Data Protection Act of 2011 and the Data Protection Act of 2013 to protect their assets and ensure compliance with regulatory requirements (Dupont, 2019). According to Almeida *et al.* (2022), financial institutions must ensure that their cybersecurity policies and practices are up-to-date and effective to prevent or mitigate the impact of cyberattacks. Despite the implementation of various cybersecurity measures by financial institutions, there remain challenges to achieving effective compliance with cybersecurity policies.

Cybersecurity policies and practices are critical to protecting financial institutions from cyber threats. However, the implementation of effective cybersecurity policies and practices in financial institutions faces several challenges, including lack of resources, resistance to change, and lack of awareness among employees (Uchendu *et al.*, 2021). Furthermore, the COVID-19 pandemic increased the risk of cyberattacks as more employees worked remotely, highlighting the need for a more robust cybersecurity policy. Financial institutions also face a lack of cybersecurity awareness among employees (Li *et al*., 2019; Almrezeq *et al.*, 2021; Daengsi *et al.*i, 2022), inadequate cybersecurity budgets (Zwilling *et al.*, 2022), the complexity of cybersecurity regulations, and the shortage of cybersecurity talent (Hu *et al.*, 2022). Some financial institutions view cybersecurity compliance as a cost centre rather than a business enabler, leading to a lack of management support and commitment to cybersecurity initiatives (Hasani *et al.*, 2023).

The cybersecurity behaviour of employees is a significant factor in protecting against cyber threats, and this behaviour is influenced by their knowledge and understanding of cybersecurity policies and practices. The shortage of skilled cybersecurity professionals is a major challenge in implementing effective cybersecurity policies and practices (Kamsamrong *et al.*, 2022). This is also recognised by Hajny *et al.* (2021), who states that a lack of appropriate cybersecurity curricula poses a challenge in producing a skilled workforce.

1.3 Problem Statement

Financial institutions increasingly rely on technology to deliver services, manage data, and process transactions. This technological dependency has significantly expanded their attack surface, making them more vulnerable to a growing number of cyberattacks. The inherent complexity of the financial sector, the integration of legacy systems with modern technology, and the need for real-time transaction processing further exacerbate these vulnerabilities. Moreover, stringent regulatory requirements demand robust cybersecurity measures and regular reporting, adding to the operational challenges faced by these institutions.

The financial sector faces unique conditions and contexts that elevate its cybersecurity risks. These include the high value of financial assets, the sensitivity of personal and financial data, and the sector's critical role in the global economy. Cybercriminals are increasingly targeting financial institutions due to the potential for substantial monetary gains and the opportunity to disrupt economic stability.

Despite these critical needs, many financial institutions struggle with insufficient employee compliance with cybersecurity policies. This non-compliance is primarily driven by inadequate employee behaviour and a lack of awareness, significantly heightening the risk of cyberattacks. Employees often lack the necessary training and understanding of cybersecurity best practices, leading to inadvertent errors and potential insider threats. Therefore, there is a need for a specialised cybersecurity framework tailored to the financial sector's unique challenges.

1.4 Research Objectives

The main objective of this study is to develop cybersecurity compliance framework for improving cybersecurity policy awareness and employee behaviour in financial institutions.

This main objective is divided into the following sub-objectives:

RO1. To identify requirements for an employee cybersecurity compliance framework in financial institutions.

RO2. To design a cybersecurity compliance framework through effective cybersecurity policy awareness programs.

RO3. To refine cybersecurity compliance framework.

1.5 Research Questions

The main research question of this study is:

How can cybersecurity compliance be improved through cybersecurity policy awareness and employee behaviour in financial institutions.

The main research question is broken into the following sub-questions.

RQ1. What are the requirements for an employee cybersecurity compliance framework in financial institutions?

RQ2. How to design a cybersecurity compliance framework through effective cybersecurity policy awareness programs?

RQ3. How to refine cybersecurity compliance framework?

1.6 Significance of the Study

The significance of this study lies in the potential to improve the effectiveness of cybersecurity policies and practices in financial institutions. As financial institutions become more reliant on technology, the risk of cyber-attacks increases, and effective cybersecurity policies become more crucial than ever. Compliance with these policies by employees is critical to ensure the protection of sensitive data, financial assets, and the overall reputation of the institution.

The recommendations of this study will be of essence to financial institutions with valuable insights into the challenges they may face in implementing effective cybersecurity policies and practices. By improving employee behaviour towards cybersecurity policy compliance, financial institutions can better protect their customers and themselves from cyber-attacks, and ultimately strengthen their position in the market. Additionally, it is crucial for financial institutions to comply with regulatory requirements to avoid penalties resulting from security breaches due to negligence.

The contribution of this study to the existing literature on cybersecurity policy compliance, employee behaviour, and awareness programs is significant. The study will fill the gaps in current research and provide a comprehensive framework for enhancing cybersecurity policy awareness programs in financial institutions. This research will benefit academics, practitioners, and policymakers in the field of cybersecurity and financial services and will ultimately contribute to improving cybersecurity practices in financial institutions.

1.7 Research Methodology

Methodology comprises the guiding principles, theories, and practices that shape the research process, including the theoretical framework, data collection methods, data analysis techniques, and the overall logic of the research design (Dawson, 2009; Ranjit, 2011). Key elements to consider in research methodology include formulating a clear research question, determining the qualitative, quantitative or mixed methods approach, selecting appropriate data collection methods, defining sampling techniques, identifying data analysis techniques, addressing ethical considerations, ensuring reliability of findings, and developing a timeline and allocating necessary resources (Dawson, 2009).

The research design adopted for this study is presented using the research onion proposed by Saunders *et al*. (2019), as illustrated in Figure 1-1. The research onion presents the research design starting from the outer layer, which encompasses research philosophy and progresses towards the innermost layer, comprising data collection and analysis methods.

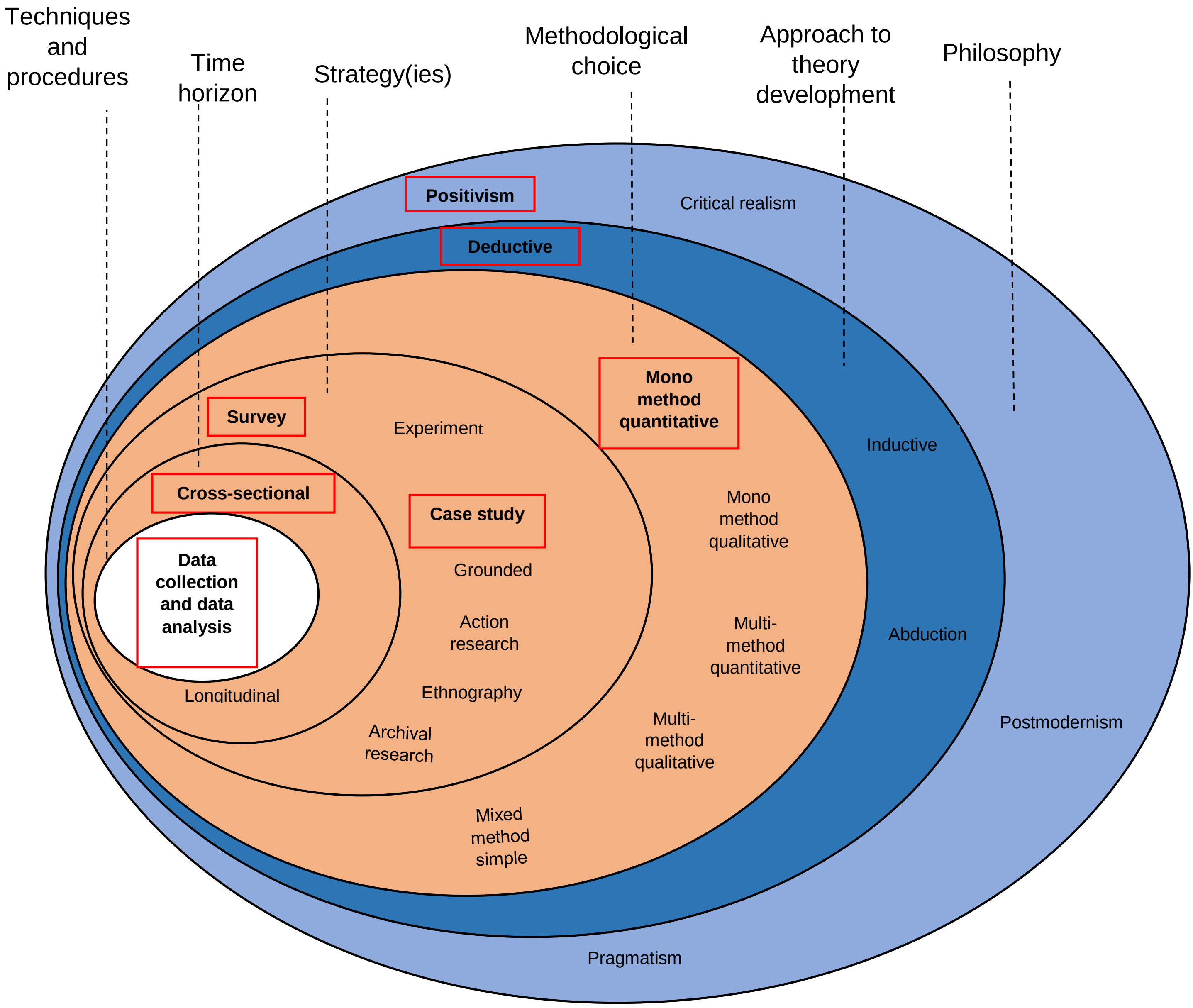


Figure 1-1: Research onion (Adapted from Saunders *et al*. (2019))

A succinct overview of the layers is provided below. A comprehensive discussion of the research methodology is provided in Chapter 3.

1.7.1 Research Philosophy

The research philosophy embodies the perspective and initial point of view of the researcher within the study, particularly with respect to how the researcher understands the essence of knowledge (Saunders *et al.*, 2019). The research philosophy is classified into five distinct philosophies as per Figure 1-1: positivism, critical realism, interpretivism, postmodernism, and pragmatism (Saunders *et al*., 2019). This researcher used the positivism philosophy for the study. The positivist philosophy was considered because positivist assumptions are more closely associated with quantitative research than with qualitative research (Saunders *et al*., 2019). Positivists aim to identify and evaluate factors that exert influence on the results (Saunders *et al*., 2019), in line with the goal of this study, which seeks to explore factors that impact employees in financial institutions to comply with cybersecurity policy.

1.7.2 Research Approach

There are three research approaches: deductive, inductive and abduction. This research adopted the deductive approach. In the deductive approach, researchers formulate a theory by initially reviewing existing literature pertinent to the ongoing study (Saunders *et al*., 2019).

1.7.3 Research Strategy

A research strategy is a plan formulated through which a researcher strives to achieve research objectives and address research inquiries (Sekaran and Bougie, 2016). The research strategy serves as a methodological link between research philosophy and methodological choices for collecting and analysing data (Saunders *et al*., 2019). Various types of research strategies are associated with methodological choices, including survey, case study, experiment, grounded theory, action research, archival research, and ethnography (Saunders *et al*., 2009). For this study, the survey is used as a research strategy. This study is quantitative, and data is collected using an online questionnaire.

1.7.4 Research Choice

Research choice helps a researcher map out the direction to follow when conducting a study, as well as to analyse and report research findings (Saunders *et al*., 2019). Research choice encompasses the following categories: monomethod, mixed methods, and multi-methods (Saunders *et al*., 2019). This study used a monomethod approach. The monomethod approach involves a researcher selecting a single data collection method and a single data analysis procedure (Saunders *et al*., 2019). In this study, the researcher collected quantitative data using an online survey questionnaire and analyse the collected data using statistical methods.

1.7.5 Time Horizon

The time horizon refers to the specific time frame during which the research takes place (Saunders *et al.*, 2019). Two different types of time horizon are cross-sectional and longitudinal (Saunders *et al*., 2019). Cross-sectional research is carried out over a short period of time while longitudinal research is carried out over a longer period (Saunders *et al*., 2019).

In this study, a cross-sectional approach was used due to time constraints; data was collected over a four-month period. This contrasts with the longitudinal approach where data can be gathered both before and after the occurrence of the phenomenon.

1.7.6 Techniques and Procedures

Techniques and procedures cover both data collection and data analysis methods (Saunders *et al*., 2009). The selection of data collection and analysis methods depends on the research question, philosophical stance, approach, and strategy used (Saunders *et al*., 2019). In this study, the researcher used nonprobability purposive sampling to select the participants and employed SPSS to analyse the collected data.

1.8 Research Location and Scope

This study focused exclusively on financial institutions due to the significant increase in cyber threats since 2020, as highlighted in Section 1.1. Specifically, the research took place in Lesotho, and its scope encompassed various types of financial institutions licenced by the Central Bank of Lesotho, including banks, insurance companies, broker insurance firms, and microfinance institutions.

To refine the proposed cybersecurity policy compliance framework, the research used an online survey questionnaire. The survey was distributed to a sample of 200 employees working within the specified financial institutions in Lesotho. This sample was intended to provide information on employee perceptions and behaviours about cybersecurity compliance.

This approach allowed for a focused examination of cybersecurity policy compliance within the unique context of Lesotho's financial institutions and offered valuable understanding into the effectiveness of the proposed framework.

1.9 Research Limitations

Although this study sought to contribute to understanding how to improve employees' compliance with cybersecurity policy in Lesotho's financial institutions, it is essential to acknowledge its inherent limitations. One limitation concerns the generalisability of the findings, as the study's scope was delimited to financial institutions, potentially limiting the applicability of the proposed framework to other industries or organisational contexts. Furthermore, the reliance on self-reported data from employees on compliance behaviour introduced the possibility of response bias, as respondents may not have always accurately portrayed their actual behaviours. Furthermore, the study's focus on short-term impacts may have omitted the consideration of longer-term effects and sustainability of the framework.

Lastly, the dynamic nature of cyber threats and the evolving landscape of technology may have posed challenges in maintaining the framework's relevance and effectiveness over time. Despite these limitations, this study offers significant information to improve the compliance of cybersecurity policies in Lesotho's financial institutions, while recognising the limitations inherent in its methodology and scope.

1.10 Ethical Considerations

To address ethical concerns within this study, the researcher obtained ethical approval. The research committee within the School of Computing at the University of South Africa (UNISA) granted the necessary ethical approval to conduct the study. This ethical approval required the researcher to guarantee anonymity and confidentiality for the participants. The researcher submitted the required documents, including a permission letter, a participant information sheet, and a consent form for study participation, for the ethical clearance application. This was done to secure permission to conduct the survey within financial institutions. The researcher obtained an ethical clearance certificate to begin data collection. The corresponding ethical clearance certificate is provided in Appendix E.

1.11 Dissertation Layout

The dissertation comprises five (5) chapters, depicted in Figure 1.2.

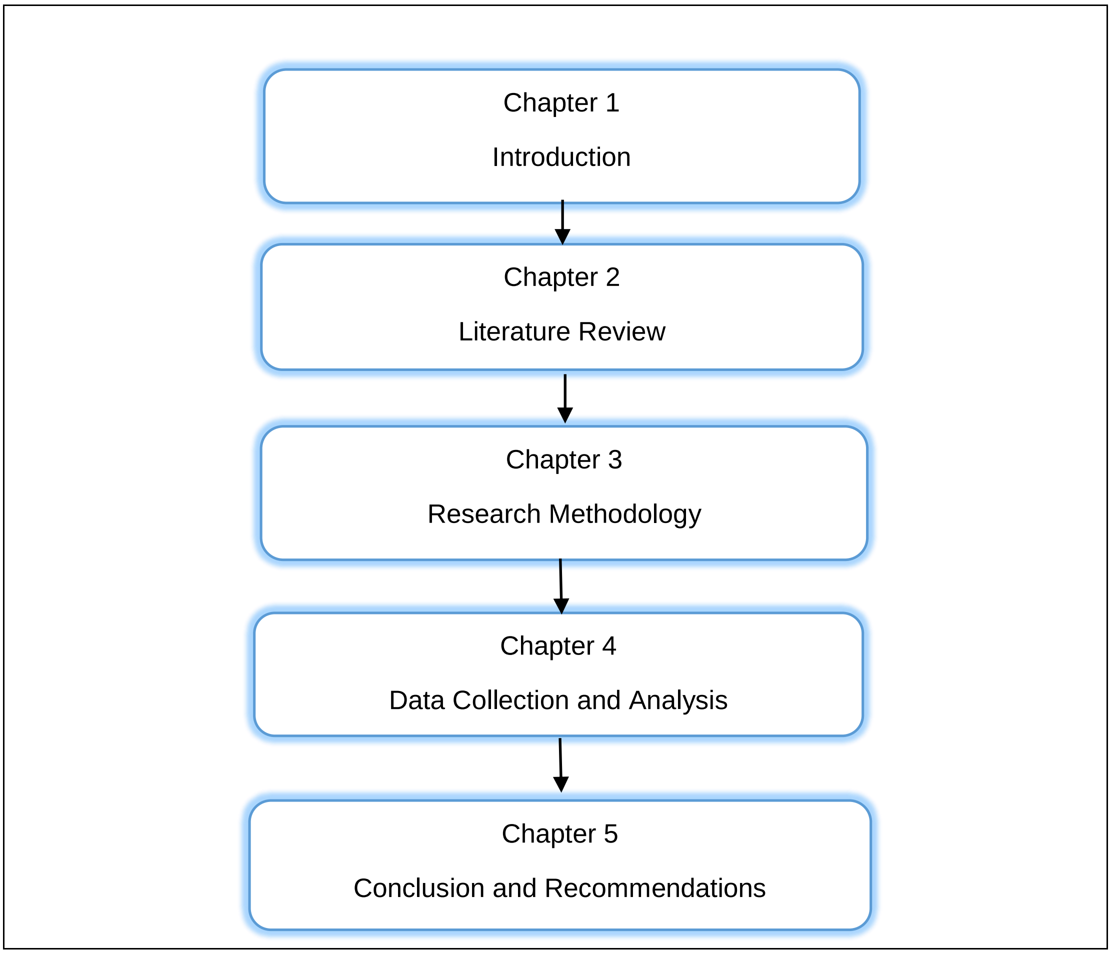


Figure 1-2: Dissertation Layout

Chapter 1 presents the background of this study. Chapter 1 introduces the purpose of the study, the problem statement, the research objectives and questions, and outlines the methodology that this study followed. Furthermore, Chapter 1 outlines the proposed contribution of the study, which is intended to bring about a solution to the gap identified in the problem statement.

Chapter 2 outlines the review of the literature. In this chapter, the background of Cybersecurity Policy Awareness Programs (CSPAP) was discussed. Arguments and debates by various researchers were presented to show the influence of effective CSPAP on employee behaviour to comply with organisational CSP.

Chapter 3 provides the research methodology followed in this study. The research methodology includes the research approach, strategy, sampling, questionnaire design, data analysis, and reliability.

Chapter 4 presents a discussion of the data collection and the results of the data analysis of the study. Interpretations of the findings are also presented in this chapter.

Chapter 5 provides the conclusions drawn from the empirical studies and the findings of this study related to the research problem. The chapter also presents future recommendations to address the gaps that have been noted in the conduct of this study. The recommendations refer not only to the improvements but also to the extension of the study to be useful in other industries, including financial institutions outside of Lesotho.

1.12 Chapter Summary

This chapter is an introduction to the research study. This chapter establishes the context and relevance of the topic, while highlighting the identified problem within the field of cybersecurity policy compliance by employees within organisations. Research objectives provide specific goals for a study and guide subsequent chapters and investigations. The research questions direct the research focus and shape the overall framework.

The significance of the study is emphasised, illustrating its potential contributions, and implications. The chosen research methodology was briefly explained, demonstrating its suitability to address the research questions and achieve the objectives of the study. Ethical considerations to emphasise the importance of integrity and participant rights were discussed. The chapter concluded with the presentation of the dissertation layout, providing an overview of the content of subsequent chapters, and aiding the reader in navigation through the study.

CHAPTER 2: LITERATURE REVIEW

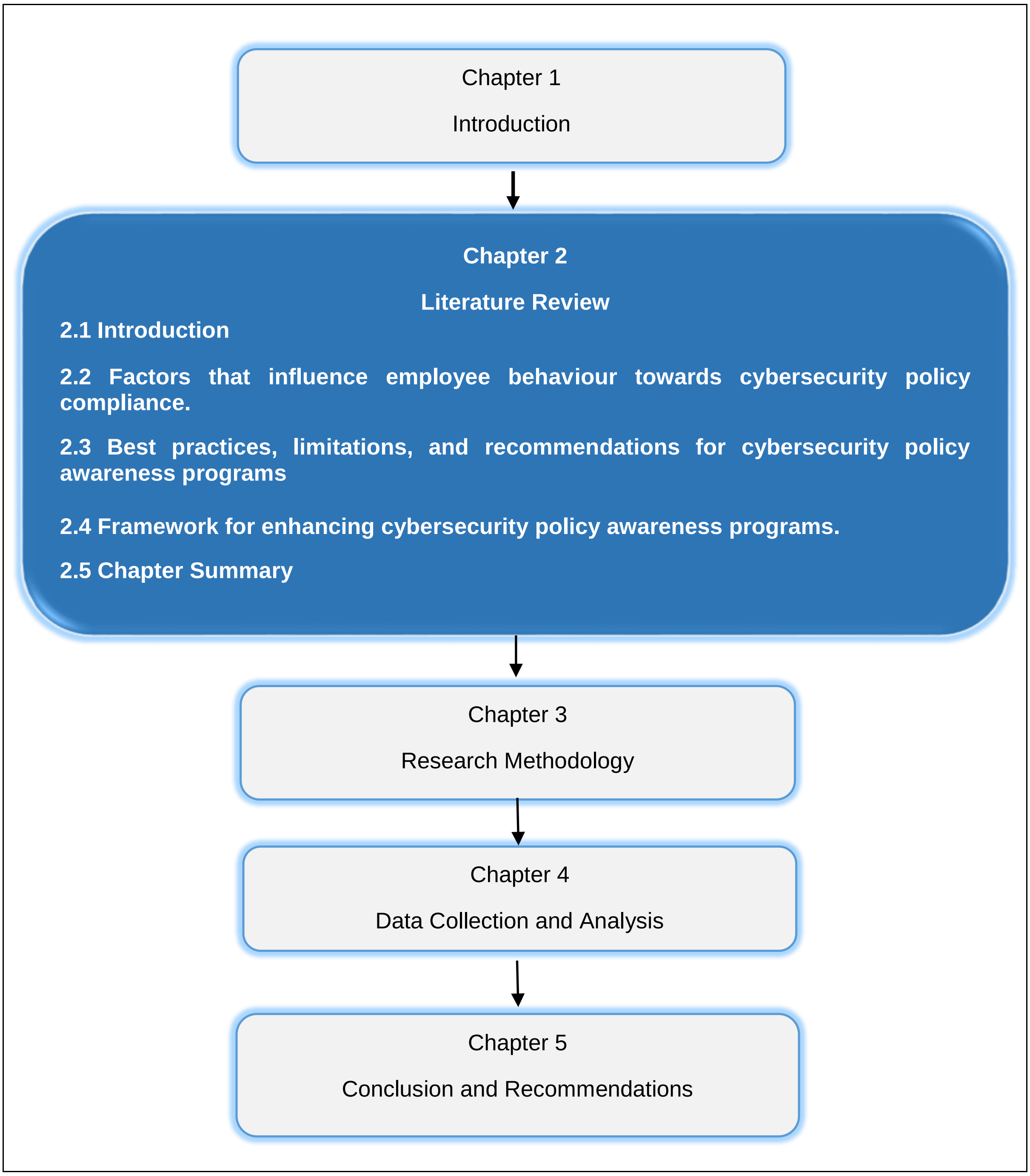

Chapter 1
Introduction
Chapter 2
Literature Review
2.1 Introduction
2.2 Factors that influence employee behaviour towards cybersecurity policy compliance.
2.3 Best practices, limitations, and recommendations for cybersecurity policy awareness programs
2.4 Framework for enhancing cybersecurity policy awareness programs.
2.5 Chapter Summary
Chapter 3
Research Methodology
Chapter 4
Data Collection and Analysis
Chapter 5
Conclusion and Recommendations

Figure 2-1: Roadmap of Chapter 2

2.1 Introduction

To emphasise the relevance and central theme of this study, this chapter provides a comprehensive overview of the literature on the effectiveness of cybersecurity policy awareness programs on employee behaviour toward cybersecurity policy compliance in financial institutions. This chapter begins by identifying key factors that influence employee behaviour toward cybersecurity policy compliance in Section 2.2. Best practices, limitations, and recommendations for cybersecurity policy awareness programs in Section 2.3. The review also outlined framework for enhancing cybersecurity policy awareness programs in Section 2.4.

2.2 Factors that Influence Employee Behaviour Toward Cybersecurity Policy Compliance

This section explores the key factors that influence employee behaviour toward compliance with cybersecurity policies in financial institutions. In addition, it provides a discussion of four factors that influence employee behaviour.

In each of the subsections, potential limitations were discussed to provide a complete understanding of the challenges and considerations related to the factors that influence the compliance of cybersecurity policies.

2.2.1 Organisational Culture and Leadership

Organisational culture and leadership are two intertwined concepts that play a crucial role in shaping employee behaviour toward cybersecurity compliance (Scholefield and Shepherd, 2019; Li *et al.*, 2019). Furthermore, organisational culture has been identified as crucial in the effectiveness of cybersecurity education and training programs in financial institutions(da Veiga *et al.*, 2020). Organisational culture is the shared values, beliefs, and norms that shape employee behaviour within an organisation, while leadership is the process of influencing others toward achieving a common goal (Li *et al.*, 2019).

The culture of an organisation has a significant impact on employee behaviour toward cybersecurity compliance in financial institutions (Huang and Pearlson, 2019).Studies have shown that a strong cybersecurity culture is positively associated with improved compliance among employees (Chang and Coppel, 2020; Corradini and Corradini, 2020).

In financial institutions, a positive cybersecurity culture is critical to promoting a shared sense of responsibility and accountability for information security (Huang and Pearlson, 2019). Employees at financial institutions are inclined to adhere to security policies when they perceive that their leaders prioritise cybersecurity and equip them with the necessary resources to guarantee compliance (Donalds and Osei-Bryson, 2020). For instance, a case study of leaders at Liberty Mutual, a financial services company, highlighted how a strong emphasis on cybersecurity from the top management led to a more vigilant and compliant workforce (Huang and Pearlson, 2019).

Leaders who prioritise cybersecurity and provide resources to support compliance initiatives can influence employees to take cybersecurity seriously (Manoliu, 2022). A strong security culture, promoted by management, can positively influence employee attitudes and promote security-conscious behaviours in financial institutions (Huang *et al*., 2019). For example, in the Liberty Mutual case study, the leaders' investment in cybersecurity actions, integrated into their in-role behaviours, encouraged employees to exhibit more vigilant behaviours, such as promptly reporting suspicious activities, minimising interactions with phishing emails, and taking steps to secure personal devices (Huang and Pearlson, 2019). Rice and Searle (2022) found that internal organisational communication plays an enabling role in insider threat activity, highlighting the importance of a culture of openness and transparency within organisations. Leaders can set the tone for this culture by emphasising the importance of cybersecurity and ensuring that policies and procedures are in place to support compliance (Rice and Searle, 2022; and Uzougbo *et al*., 2024).

One key aspect of organisational culture that can impact leadership in financial institutions is the level of trust and transparency within an organisation. Dupont (2019) argues that trust is critical for effective leadership as it allows leaders to build strong relationships with their followers and fosters open communication. Similarly, Alhashmi *et al.* (2021) suggest that transparent communication is necessary for effective leadership, as it ensures that all employees are aware of an organisation's goals and objectives.

In addition, effective leadership in financial institutions can promote ethical behaviour and prevent policy violation behaviour. Chen *et al*. (2019) argue that leaders who promote ethical behaviour can foster a culture of integrity and accountability within the financial institutions. Jeong and Zo (2021) suggest that leaders can use opportunity-reducing techniques to prevent insider threats and improve organisational security.

There are several insights into the relationship between organisational culture and leadership. Rice and Searle (2022) explored the role of internal organisational communication in insider threat activity and found that effective leadership communication can contribute to a strong organisational culture that promotes ethical behaviour and reduces the likelihood of insider threats. Tolah *et al*. (2021) developed a framework to analyse key factors in the security culture of information and found that leadership is a critical factor in shaping the security culture of an organisation. Effective leadership can set the tone for a culture of security and promote a sense of accountability among employees for protecting an organisation's information (Tolah *et al*., 2021).

In the literature, there are several examples that highlight the importance of leadership in promoting a culture of security. Zhang *et al.* (2021) proposed a cost-benefit analysis framework for cybersecurity awareness training programs and emphasised the role of leadership in supporting such initiatives. According to Ahmad *et al.* (2019), employees are more likely to engage in information security assurance behaviour when there is strong leadership support for security initiatives.

Another aspect of organisational culture that can impact leadership is the level of employee engagement within the financial institutions. Hu *et al*. (2022) suggest that leaders who prioritise employee engagement can create a positive organisational culture that fosters innovation, creativity, and productivity.

The role of leadership in the formation of organisational culture has been extensively studied. Scholefield and Shepherd (2019) argue that leaders can use gamification techniques to create a culture of cybersecurity awareness within the organisation. Acharya and Joshi (2020) suggest that leaders can implement safety mechanisms and preventive measures to protect an organisation from cyberattacks. Kweon et al. (2021) found that information security training and education can improve employees' cybersecurity incident response capabilities, but leadership support is necessary for effective implementation.

Additionally, the culture can encourage or discourage employee compliance with cybersecurity policies in financial institutions. Leaders who prioritise cybersecurity as a core value and promote a culture of security awareness can positively influence employee behaviour toward cybersecurity (Manoliu, 2022). Therefore, financial institutions should not only invest in cybersecurity technologies, but also focus on promoting a security-centric culture and providing regular cybersecurity training to their employees (Uzougbo *et al.,* 2024). By doing so, financial institutions can help prevent cyberattacks and protect sensitive information. For instance, Bank of America has implemented a comprehensive cybersecurity awareness program, which included regular training sessions and simulations, to ensure that all employees are well-versed in cybersecurity best practices (Uzougbo *et al*., 2024).

A positive organisational culture fosters compliance with employee cybersecurity policies, while effective leadership promotes a positive organisational culture (Manoliu, 2022). This discussion has highlighted the importance of organisational culture and leadership and their impact on employee behaviour in financial institutions.

However, organisational culture and leadership have limitations, which are the lack of awareness of cybersecurity policy, understanding of cybersecurity issues among the general population, as well as government and private institutions (Mosola *et al.*, 2019). Mosola *et al.*

(2019) identified a lack of collaboration and coordination between government institutions responsible for cybersecurity, resulting in a fragmented approach to cybersecurity policy implementation. Employee attitudes and perceptions towards cybersecurity policy are discussed in the next section.

2.2.2 Employee Attitudes and Perceptions Toward Cybersecurity Policy

In recent years, cybersecurity has emerged as a major worry for financial institutions globally because of the rising frequency of cyber-attacks. Employee attitudes and perceptions towards cybersecurity play a crucial role in protecting financial institutions against cyber threats. For example, in the Mutual Liberty case study, the involvement of top management underscored the significance of cybersecurity across the organisation. Employees observed a senior executive who was highly visible and personally engaged in delivering the message, which motivated them to take notice. In interviews with researchers, employees expressed that they felt empowered to safeguard the company’s data and information systems and understood the steps they could take to achieve this (Huang and Pearlson, 2019).

According to Li *et al.* (2019), employees who have a positive attitude toward cybersecurity policies, perceiving them as important and receiving adequate support from their organisation are more likely to comply with cybersecurity policies. Almrezeqa *et al*. (2021) state that employees who had experienced cybercrime were more likely to have a positive attitude towards cybersecurity policy. At Liberty Mutual, leaders leveraged major news stories on cybersecurity issues as practical examples to enhance employee awareness. This educational strategy allowed employees to develop and maintain their knowledge. For example, after the Equifax breach in the summer of 2017, the information security team clarified the breach's implications, its potential effects on employees' personal financial accounts, and the steps employees could take to safeguard themselves. This approach significantly influenced employees and underscored the importance of secure cybersecurity practices (Huang and Pearlson, 2019).

The COVID-19 pandemic caused notable changes in employee behaviour and attitudes towards cybersecurity policy, especially as remote working arrangements became prevalent (Bengaluru *et al*., 2020). These changes highlight the critical role that employee attitudes and perceptions play in ensuring robust cybersecurity practices (Bengaluru *et al*., 2020). It is important for financial institutions to understand their employees' attitudes and perceptions towards cybersecurity policy to design effective training and awareness programs that can motivate and encourage compliance (Alhashmi *et al.*, 2021; Scholefield and Shepherd, 2019; Khader *et al*., 2021; Hu *et al*., 2022). Additionally, understanding employee attitudes and perceptions toward cybersecurity can help financial institutions shape their internal communication strategies and contextual factors that can influence employee decision making regarding information security policy violation (Li *et al*., 2021; Rice and Searle, 2022).

Gamification has been suggested as a winning cybersecurity strategy to improve employee attitudes and perceptions about cybersecurity policy (Wolfenden, 2019). Financial institutions should prioritise the provision of adequate support, training programs, and awareness campaigns of cybersecurity policy to improve employee attitudes and perceptions about cybersecurity policy and promote compliance behaviour.

There exist several limitations in employee attitudes and perceptions towards cybersecurity policy. Dash and Ansari (2022) reported a lack of tailoring training programs to employees' specific roles, responsibilities, and the company's security policies. According to Dash and Ansari (2022), generic cybersecurity training programs can lead to lack of interest, relevance, and understanding among employees, which can hinder compliance. This implies that training programs should be tailored to meet the specific needs and context of each employee to improve their understanding and motivation towards cybersecurity compliance in financial institutions. Training programs should be tailored because what is effective for one individual might not be the same for another (Huang and Pearlson, 2019). Employees who receive customised training programs are more likely to comply with cybersecurity policies than those who receive generic training (Dash and Ansari, 2022).

Another limitation is the lack of evaluation and measurement of the impact of existing programs on employee behaviour toward compliance (Ghelani *et al*., 2022). A drawback is evident in the reliance on traditional training methods, such as lectures and videos, which may not be engaging or interactive enough to effectively promote behaviour change (Ghelani *et al*., 2022). Additionally, some programs may not be specific enough to the needs and roles of employees in financial institutions and may not address cultural and language differences among employees (Dash and Ansari, 2022). Cultural differences between employees in different financial institutions can also limit the effectiveness of existing cybersecurity policy training and awareness programs. According to research by Daengsi *et al*. (2022), cultural differences can affect the way employees perceive cybersecurity policies and the level of compliance they exhibit. Therefore, programs must consider cultural differences between employees in different financial institutions. Furthermore, the lack of support and participation from top management in cybersecurity awareness programs can hinder their effectiveness in changing employees' behaviour in financial institutions (Al-Alawi and Al-Bassam, 2021; Ofori *et al.*, 2021).

As the threat landscape continues to evolve, financial institutions must adopt a proactive approach to cybersecurity. Regular evaluation of cyber risks and implementation of preventive measures are essential to mitigate the consequences of noncompliance with cybersecurity policies. The consequences of noncompliance with cybersecurity policy are discussed in the next section.

2.2.3 Consequences of Noncompliance with Cybersecurity Policy

In the era of digitalisation, cybersecurity has become a critical concern for financial institutions due to the markedly large data set of sensitive data they handle.

Noncompliance with cybersecurity policy can have serious consequences for financial institutions and individuals alike, leading to various negative outcomes. These include data breaches and unauthorised access to sensitive information, resulting in financial losses, reputational damage, and legal and regulatory consequences (Almrezeqa *et al*. 2021; Hajny *et al.*, 2021; Kamsamrong *et al.*, 2022; Maennel *et al.*, 2023). As a result, financial institutions need to focus on cybersecurity compliance and risk management by putting in place strong controls and governance frameworks that show their dedication to best practices in cybersecurity (Uzougbo *et al*., 2024). This involves performing regular assessments, establishing clear responsibility for cybersecurity within the organisation, establishing clear responsibility for cybersecurity within the organisation, and ensuring transparency in reporting cybersecurity incidents to stakeholders and regulators (Uzougbo *et al*., 2024). Tackling these challenges and adopting forward-looking approaches to cybersecurity compliance will be crucial for financial institutions to effectively manage cyber risks, enhance their cybersecurity resilience, and maintain the confidence and trust of their stakeholders and customers in an increasingly interconnected and digital world (Uzougbo *et al*., 2024).

Research has identified several factors that influence employees' noncompliance with cybersecurity policies in financial institutions. These factors include a lack of awareness about cybersecurity, insufficient cybersecurity training and education, and the absence of a strong cybersecurity culture within organisations (Huang *et al*., 2019; Uddin *et al*., 2020; Alqahtani and Braun, 2021; Alzahrani, 2021; Moustafa *et al*., 2021; Georgiadou *et al.*, 2022; Murphy *et al.*, 2022; Saeed, 2023).

Moreover, individual decision-making styles, moral disengagement, opportunity-reducing techniques, cyber fatigue, and poor communication within the organisation can also drive noncompliance with cybersecurity policies (Chen *et al*., 2019; Donalds and Osei-Bryson, 2020; Reeves *et al*., 2021; Rice and Searle, 2022). The consequences of noncompliance with cybersecurity policy extend beyond individual organisations and can have broader implications for critical infrastructures, financial systems, and national security (Ahmad *et al.*, 2019; Dupont, 2019; Touhiduzzaman *et al.*, 2019; Vedral, 2021). Noncompliance with cybersecurity policies can also lead to operational disruption such as system outages, data loss, and disruption of critical services (Marcu, 2021).

Additionally, noncompliance with cybersecurity policies increases overall cybersecurity risks faced by financial institutions and individuals. Failure to follow best practices and security guidelines exposes systems and networks to increased vulnerability to cyberattacks and intrusions, compromising sensitive information, leading to theft of intellectual property as well as unauthorised access to systems and resources (Reegård *et al*., 2019; Sabillon *et al.*, 2019).

To mitigate the risks associated with noncompliance, financial institutions must prioritise improving cybersecurity awareness, implementing effective training programs, fostering a strong cybersecurity culture, and establishing security monitoring and assurance mechanisms (Ahmad *et al*., 2019; He *et al.*, 2020; Zhang *et al*., 2021; Georgiadou *et al.*, 2022).

Noncompliance with cybersecurity policy can have severe consequences for financial institutions and individuals, including data breaches, financial losses, reputational damage, and legal consequences. It is crucial for financial institutions to prioritise awareness of cybersecurity policies and a strong cybersecurity policy culture to mitigate the risks associated with noncompliance. The importance of cybersecurity policy awareness programs is discussed in Section 2.2.4.

2.2.4 The Importance of Cybersecurity Awareness Programs

In recent years, cybersecurity breaches have become a significant threat to financial institutions, with the potential to cause reputational damage, financial losses, and legal implications, as discussed in Section 2.2.3. To mitigate these risks, financial institutions should implement cybersecurity policy awareness programs for their employees.

Awareness programs are essential to educate and train employees about the risks and threats associated with cybersecurity and to promote compliance with cybersecurity policies in financial institutions (Muraguri *et al.*, 2019). Employee awareness is a crucial component of cybersecurity preparedness, given that individuals can be exploited through social engineering (Muraguri *et al.*, 2019). It is essential that everyone in financial institutions takes responsibility for adhering to cybersecurity best practices. Regular educational sessions should be conducted, and training materials must be frequently updated to reflect new threats (Muraguri *et al.*, 2019). According to various studies, awareness and training programs can significantly impact employee behaviour toward compliance with cybersecurity policies. Li *et al*. (2019), Alzahrani (2021), and Hu *et al*. (2022) found that awareness of cybersecurity policy can positively influence and improve employee cybersecurity behaviour. For instance, the case study of Liberty Mutual attests to the change in employee behaviour when cybersecurity awareness training is effective. Employees confirmed that they know what is expected of them to protect their organisation (Huang and Pearlson, 2019).

However, the importance of employee behaviour in maintaining cybersecurity cannot be overemphasized, given that more than 82% of data breaches result from credential theft, hacking, or human error (Verizon, 2022). Despite this importance, traditional training methods such as lectures and seminars can prove ineffective in improving cybersecurity awareness especially within the banking sector (Ghelani *et al*., 2022). Proctor (2016) conducted a study on the efficacy of cybersecurity training and awareness programs, revealing that while such initiatives can increase employees' knowledge of cybersecurity threats, they rarely lead to a change in their behaviour.

Several studies have emphasised the critical role of training and awareness programs in developing a culture of security in financial institutions. For example, Huang and Pearlson (2019) recognised training and awareness programs as a critical factor in influencing employee behaviour toward compliance with cybersecurity policies in financial institutions. Alhashmi *et al.* (2021) proposed a taxonomy of cybersecurity awareness delivery methods which includes training programs, simulations, and games, among others.

Training programs are crucial in developing employees' skills and knowledge toward cybersecurity policy compliance. Maennel *et al.* (2023) emphasise the importance of training programs in developing the emotional, social, and cognitive aspects of cybersecurity through multidimensional cyber defence exercises. Maennel *et al.* (2023) argue that the emotional, social, and cognitive aspects of cybersecurity should be considered in the implementation of effective cybersecurity policies and practices. This is because these aspects can affect how employees respond to cybersecurity threats and how they behave when implementing cybersecurity measures (Maennel *et al.,* 2023).

Several studies have emphasised the importance of cybersecurity policy training programs in preparing employees for potential cyber threats. For example, Hajny *et al.* (2021) proposed a framework, tools, and good practices for cybersecurity curricula, highlighting the importance of training programs in cybersecurity education. To further enhance this approach, Georgiadou *et al*. (2021) designed a cybersecurity culture assessment survey targeting critical infrastructures during the COVID-19 crisis. This cybersecurity culture assessment survey can be used to assess the level of cybersecurity awareness and culture in an organisation, identify gaps, and help address the gaps (Georgiadou *et al*., 2021). Research by Georgiadou *et al*. (2021) highlights the need for comprehensive training programs that not only address technical aspects, but also foster a robust cybersecurity culture and awareness among employees. For instance, a case study of the Capital One data breach highlights the critical need for robust cybersecurity awareness and training programs in financial institutions to prevent such incidents (Neto *et al.*, 2020). This underscores the role of employee awareness in identifying and mitigating cyber threats before they cause significant harm.

Additionally, various studies have highlighted the role of training programs in influencing employees' intentions, attitude, and behaviour toward cybersecurity policy compliance. For example, Alqahtani and Braun (2021) reviewed the influence of UTAUT2 factors on cybersecurity compliance and found that training programs significantly impacted employees' intentions and behaviour toward cybersecurity policy compliance. Moustafa *et al*. (2021) emphasised the importance of training programs in developing a security-conscious culture and improving cybersecurity management by addressing user behaviour. Additionally, the effectiveness of training programs and cybersecurity awareness campaigns can also affect employees' attitudes and perceptions toward cybersecurity.

Several studies have identified the importance of effective and tailored awareness and training programs that meet an organisation's specific needs and employees' roles and responsibilities. Stewart (2022) proposed an approach to cybersecurity training and awareness that aligns with an organisation's objectives and culture. Tolah *et al*. (2021) highlighted the importance of tailoring cybersecurity training to the needs and responsibilities of employees.

Bengaluru *et al*. (2020)) highlight the increasing need for cybersecurity awareness training to address the new and emerging threats brought about by working remotely, mainly influenced by the COVID-19 pandemic. This shift from the conventional office-based work to working remotely has introduced unique challenges such as the use of personal devices and potential vulnerabilities in home networks (Bengaluru *et al*., 2020). To mitigate these risks, financial institutions must ensure that employees are well informed about cybersecurity measures (Bengaluru *et al*.,2020). Corallo *et al.* (2022) emphasise the importance of raising awareness among employees about the security risks associated with Industrial Internet of Things (IoT) devices commonly used in remote work setups. Employees should understand the importance of complying with cybersecurity policies to safeguard organisational data and systems. The discussion on awareness and training programs highlights the importance of developing a security-conscious culture, improving employees' skills and knowledge, and preparing them for potential cyber threats.

There are several challenges in implementing effective cybersecurity policies and practices that include, among others, lack of resources, shortage of skilled cybersecurity professionals, and lack of awareness and understanding among employees (Uzougbo *et al*., 2024). Given the limitations of existing programs, it is crucial to explore improvement recommendations to enhance the effectiveness and impact of cybersecurity awareness initiatives. This is discussed in Section 2.3.2.

2.3 Best Practices, Limitations, and Recommendations for Cybersecurity Policy Awareness Programs

Effective cybersecurity policy awareness programs are essential to promote cybersecurity compliance among financial institution employees and mitigate the risks associated with cyber threats (Ofori *et al.*, 2021; Almeida *et al.*, 2022; Sulaiman *et al.*, 2022). Section 2.3.1 reviews literature on the effectiveness of cybersecurity policy awareness programs with an aim to identify best practices for such programs. Section 2.3.2 provides limitations and recommendations for improving cybersecurity policy awareness programs in financial institutions.

2.3.1 Best Practices for Cybersecurity Policy Awareness Programs

Effective cybersecurity policy awareness programs are vital to promoting compliance among employees. These practices have been identified through various studies, each addressing specific aspects and highlighting their importance in promoting cybersecurity compliance among employees. By incorporating these best practices, financial institutions can significantly improve the effectiveness of their cybersecurity policy awareness programs and empower employees with the knowledge, skills, and awareness necessary to identify and prevent cyberattacks (Ofori *et al.*, 2021; Almeida *et al.*, 2022; Sulaiman *et al.*, 2022). By allocating sufficient resources, providing regular awareness programs, emphasising continuous learning, employing interactive methods, implementing structured curricula, and fostering a cybersecurity culture, financial institutions can enhance their cybersecurity defences and empower their workforce (Ofori *et al.*, 2021; Almeida *et al.*, 2022; Sulaiman *et al.*, 2022). These best practices serve as valuable guidelines for financial institutions seeking to strengthen their cybersecurity posture and mitigate the risks associated with cyber threats. The next section discusses limitations and recommendations that financial institutions can use to improve cybersecurity policy awareness programs.

2.3.2 Cybersecurity Policy Awareness Programs Limitations and Recommendations

The evaluation of existing programs in the following section provides further information on the practical application and impact of these recommended practices, as stated in Table 2-1.

Several awareness programs have been implemented in financial institutions to improve the level of cybersecurity. However, the effectiveness of these programs in influencing employees' behaviour towards cybersecurity policy compliance remains a subject of debate (He and Zhang, 2019; Back and Guerette, 2021; Fisher, Porod and Peterson, 2021).

Previous studies have explored the effectiveness of various cybersecurity awareness programs. Back and Guerette (2021) found that cybersecurity awareness improved participants' knowledge of phishing scams and reduced their vulnerability to phishing attacks. Almrezeqa *et al*. (2021) found that despite increasing awareness of cybercrime in Saudi Arabia, most of the population lacked the knowledge and skills required to protect themselves from cyber threats. This suggests that awareness of cybersecurity policy alone may not be enough to improve employee cybersecurity behaviour.

When highlighting the importance of evaluating the effectiveness of cybersecurity training programs, He *et al.* (2020) note that evaluation helps to identify strengths, weaknesses, and areas for improvement of such programs, which can inform policy development and enhance compliance. However, most financial institutions do not evaluate their training programs, leading to the continued use of outdated or ineffective training methods, thus preventing cybersecurity compliance. Therefore, regular evaluation and feedback mechanisms should be incorporated into cybersecurity training programs to ensure their effectiveness (He *et al.*, 2020).

The effectiveness of cybersecurity awareness programs in financial institutions remains debatable. Although some programs have proven effective in improving knowledge and reducing vulnerability, traditional methods may not effectively improve awareness of cybersecurity. Increasing awareness alone is not sufficient to change behaviour. A comprehensive approach that involves training, policy implementation, monitoring, and technological measures is necessary. Regular evaluation and feedback mechanisms are essential to identify areas for improvement and improve the effectiveness of cybersecurity programs in ensuring compliance. The evaluation of existing cybersecurity policy awareness programs sheds light on their strengths and weaknesses, providing valuable information on the limitations discussed in Section 2.3.2 in these programs that are crucial for developing effective strategies and overcoming identified challenges.

Table 2-1 presents a comprehensive compilation of best practices, limitations, and corresponding recommendations to improve existing cybersecurity policy awareness programs. These best practices have been drawn from various studies that explore effective strategies to improve cybersecurity awareness and promote a security-conscious culture among employees, as discussed in Section 2.4.1. By examining these insights, financial institutions can gain valuable guidance on how to design and implement robust cybersecurity awareness initiatives. Table 2-1 shown below offers a holistic view of the challenges faced, possible solutions, and the incorporation of these practices into the context of this study. The incorporation of these recommendations will allow for a more customised, engaging, and comprehensive approach to promote employee compliance and behaviour change.

Table 2-1: Limitations of Existing Programs and Recommendations for Improvement

Best Practices	Study Title	Limitations	Recommendations	Incorporation in the study	Insights for each best practice
Customise programs to employees' needs, the organisation's context, and the risks it faces	Cybersecurity Education and Training: An Innovative Approach for Closing the Cybersecurity Skills Gap (Aldawood and Skinner, 2019)	The effectiveness of customisation may vary depending on the organisation's resources and commitment to cybersecurity. Challenges may arise in catering to individual needs in large organisations.	Develop educational programs and campaigns to raise awareness of cybersecurity risks and best practices. Engage employees at all levels of the financial institution in joint initiatives to promote cybersecurity culture and knowledge sharing. Incorporate cybersecurity training and awareness as part of educational curricula and professional development programs.	Evaluate existing cybersecurity awareness programs and identify the gaps and propose recommendations to improve their effectiveness and reach. Assess the integration of cybersecurity training in financial institutions and professional development initiatives.	• Tailor cybersecurity awareness programs to address the specific needs and roles of employees within the financial institutions. • Consider the unique context of the financial institution and the risks it faces to ensure that the training is relevant and effective
Propose an approach to achieve sustainable	A Sustainable Approach to Cybersecurity Education, Training,	The sustainability of behaviour change initiatives may require ongoing support and	Develop and implement cybersecurity awareness programs targeting the financial	Review the existing literature on cybersecurity awareness programs	• Focus on developing strategies that lead to long-term behavioural

behaviour change among employees	and Awareness (Alshaikh *et al*., 2019)	reinforcement. Long-term commitment and resources are needed to maintain sustainable behaviour changes.	institutions. Establish training initiatives to improve cybersecurity knowledge and skills among employees. Promote collaboration and knowledge-sharing platforms between employees to improve cybersecurity understanding.	and their effectiveness in enhancing awareness and understanding. Analyse the current level of cybersecurity knowledge among financial institutions and explore opportunities for improvement.	changes in employees with respect to cybersecurity practices. • Implement initiatives that encourage consistent and long-lasting cybersecurity awareness and compliance
Consider cultural, educational, technological, and regulatory factors in building cybersecurity awareness	Building Cybersecurity Awareness in Developing Countries: Insights from Cultural, Educational, Technological, and Regulatory Factors (Chang and Coppel, 2020)	Cultural and regulatory differences can present challenges in the implementation and customisation of training programs in different regions. Technological limitations in developing countries can impact the delivery and	Assess the specific roles and responsibilities of employees in financial institutions and provide relevant training. Incorporate gamification techniques to enhance employee engagement.	Conduct a needs analysis to identify the specific roles, responsibilities, and security policies of employees in financial institutions. Develop customised training programs based on identified needs and incorporate gamification elements to increase engagement.	• Recognise the impact of cultural, technological and regulatory factors on cybersecurity awareness. • Adapt training and awareness programs to align with these factors to maximise effectiveness.

		accessibility of training materials.			
Provide regular cybersecurity training and awareness programs to create awareness of cyber threats	Measurement of awareness of cybercrime in Saudi Arabia: An Exploratory Study (Almrezeqa *et al*., 2021)	Measurement of behaviour change and program effectiveness may require reliable and valid evaluation methods. Securing collaboration with cybersecurity experts and researchers can present logistic and resource challenges.	Focus on evaluating the effectiveness and impact of programs on employee behaviour. Consider the impact of education and training programs on cybersecurity behaviour.	Implement a comprehensive evaluation framework to assess the effectiveness of existing programs in influencing employee behaviour toward compliance.	• Conduct regular and ongoing training sessions to keep employees informed about current cyber threats and risks in financial institutions. • Reinforce cybersecurity awareness consistently to maintain vigilance and preparedness among employees in financial institutions.
Foster a cybersecurity culture that encourages employees to take responsibility for cybersecurity	A Survey for Assessing Cybersecurity Culture in Critical Infrastructures during the COVID-19 Crisis: Case of Greece (Georgiadou *et al*., 2021)	The adoption and acceptance of a cybersecurity culture may face resistance from employees, especially in organisations with long-established norms and practices. Encouragement of active participation	Incorporate interactive and engaging elements into training programs. Use a variety of training methods to accommodate different learning styles.	Integrate interactive and engaging elements, such as simulations and online modules, into training programs. Provide a variety of training methods to accommodate the different learning styles	• Cultivate a cybersecurity-conscious culture that emphasises individual and collective responsibility for cybersecurity. • Promote a sense of ownership among employees in protecting financial institutions' data and systems.

		can be challenging in large and diverse employee populations.		and preferences of the employees.	
Allocate sufficient resources (such as financial resources, skilled personnel, training facilities, and materials, etc.) to develop effective training and education programs	The Impact of Information Security Training and Education on Reducing Cybersecurity Incidents in Organisations (Kweon *et al*., 2021)	The allocation of sufficient resources can be hampered by budget constraints and competing organisational priorities. The availability of skilled personnel and technologies may also impact the development and implementation of training programs.	Emphasise the potential consequences of security breaches to motivate employees. Improve communication and awareness strategies.	Improve communication strategies by highlighting the potential consequences of security breaches. Develop effective awareness strategies to ensure clear and concise communication of cybersecurity policies and practices.	• Invest in the necessary resources, including financial resources, skilled personnel, and training facilities and materials. • Ensure that training and education programs are adequately supported and resourced for optimal impact.

Use interactive training methods such as phishing simulations	The Effects of Knowledge-Sharing Methods on Cybersecurity Practices: The Moderating Role of Employees' Cybersecurity Awareness (Pham *et al*., 2021)	The effectiveness of interactive training methods can vary depending on individual learning preferences and technological accessibility. Phishing simulations may need to be carefully designed to avoid causing unnecessary stress or anxiety among employees.	Develop clear, specific, and well-understood policies. Regularly assess and update programs to meet changing threats and technologies. Integrate cybersecurity policies into organisational culture.	Improve policy clarity and specificity to facilitate effective implementation and enforcement. Regularly assess and update training programs to align with evolving cyber threats and technologies. Integrate cybersecurity policies into the financial institutions culture to foster a positive security mindset.	• Employ interactive and engaging training techniques such as phishing simulations to improve employee participation and knowledge retention in financial institutions. • These methods create a more immersive learning experience and better prepare employees to recognise and respond to real-world cybersecurity threats.
Emphasise continuous cybersecurity training, as new trends and skill gaps emerge with the advancement of technology	Smart Grid Cybersecurity Education: The State of the Art Trends and Skill-Gaps (Kamsamrong *et al*., 2022)	Continuous training may require regular updates and adjustments to keep up with the latest technologies.	Assess the specific roles and responsibilities of employees and provide relevant training. Incorporate gamification techniques to enhance employee engagement.	Conduct a needs analysis to identify the specific roles, responsibilities, and security policies of employees. Develop customised training programs based on identified needs.	• Recognise that the cybersecurity landscape is continually evolving, and new threats and skill gaps may emerge. • Continuously update and adapt training programs to address emerging trends and challenges in the financial institutions.

Table 2-1 serves as a valuable resource to understand the key requirements that influence the effectiveness of cybersecurity policy awareness programs. By incorporating best-practices and recommendations identified from various studies, financial institutions can develop targeted and customised training programs that address the specific needs and challenges of their workforce. Information shown on the table; highlights the importance of continuous evaluation, tailors training programs to the specific roles and responsibilities of employees, evaluates the impact of the program, uses engaging and interactive training methods, and considers cultural differences between employees in the creation of effective cybersecurity awareness initiatives. Implementing these recommendations would enable financial institutions to create a security-conscious workforce, better equipped to defend against cybersecurity threats, and contribute to overall cyber resilience.

2.3.3 Analysis of Cybersecurity Risks in the Financial Institutions

Table 2-2: Cybersecurity Risks in Financial Institutions

Case study	**Impact of cybersecurity risk**	**Best Practices for Cybersecurity Compliance**
In 2017, Equifax, a major player in credit reporting, experience a significant data breach where cyber attackers utilised a vulnerability to access sensitive personal data belonging to around 147 million consumers (Uzougbo *et al*., 2024). The breach happened because Equifax did not patch a known vulnerability in their systems (Uzougbo *et al*., 2024).	The breach resulted in the exposure of individuals' names, birthdates, Social Security numbers, and driver's license numbers. Equifax suffered substantial reputational damage and financial loss, regulatory penalties, numerous lawsuits,, and a decline in its stock market valuation.	Provision of employee training and awareness programs on the need for timely software updates and effective vulnerability management. Regular training on recognising phishing emails and handling sensitive information could have helped mitigate the initial breach.
In 2014, JPMorgan Chase, among the largest U.S. banks, suffered a cyberattack compromising personal details of more than 76 million households and 7 million small businesses (Uzougbo *et al*., 2024). The breach was linked to hackers who infiltrated the bank's systems using compromised employee credentials (Uzougbo *et al*., 2024).	Although no financial data was compromised, the incident revealed vulnerabilities in the bank's cybersecurity defences, prompting the implementation of stronger security measures and heightened regulatory oversight.	Provision of comprehensive employee awareness on the importance of stringent access controls. Educating employees about phishing and social engineering could have prevented initial access by the attackers.

In 2018, Cyber attackers aimed a sophisticated spear phishing attack at Banco de Chile, a major bank in the country (Uzougbo *et al*., 2024). Cyber attackers successfully breached the bank's internal systems and sought to transfer $10 million to accounts based in Hong Kong (Uzougbo *et al*., 2024).	Although the bank managed to thwart the majority of the fraudulent transactions, the incident caused operational disruptions and underscored weaknesses in cybersecurity protocols across financial institutions in Latin America.	Educating employees about spear phishing tactics and implementing simulated phishing exercises could have increased awareness and prevented the initial breach.

Financial institutions exist in a landscape of ever-changing cyber threats, with attackers becoming progressively more advanced and relentless in their efforts (Uzougbo *et al*., 2024). The adoption of new technologies like artificial intelligence and the Internet of Things adds complexity to the cybersecurity landscape, introducing new avenues for attacks and vulnerabilities. To keep pace with cyber threats, financial institutions need to promote a culture of ongoing enhancement, regularly reassessing their cybersecurity strategies, practices, and technologies to address evolving risks (Uzougbo *et al*., 2024). This involves investing in the capacity to conduct routine security assessments, and adopt best practices (Lyimo and Shaaban, 2021; Uzougbo *et al*., 2024).

Cybersecurity demands constant vigilance, evaluation, and enhancement. Financial institutions must continuously review and update their cybersecurity frameworks in response to evolving threats, industry standards, and regulatory mandates to effectively mitigate cyber risks (Lyimo and Shaaban, 2021; Uzougbo *et al*., 2024). Prominent cybersecurity breaches highlight the critical need for proactive security practices like routine security evaluations, and employee awareness. Financial institutions must prioritise investments in cybersecurity and allocate adequate resources to defend against emerging risks (Lyimo and Shaaban, 2021; Uzougbo *et al*., 2024)

Cybersecurity is both a technical and cultural issue. Financial institutions need to foster a culture of cybersecurity awareness across their organisations, emphasising the importance of accountability and awareness among all employees (Lyimo and Shaaban, 2021; Uzougbo *et al*., 2024). Regular awareness and training programs are important to enable employees to identify and effectively respond to cybersecurity incidents, thereby minimising the risk of human errors and insider threats (Lyimo and Shaaban, 2021; Uzougbo *et al*., 2024)

Based on recommendations to improve cybersecurity policy awareness programs in financial institutions, and analysis of cybersecurity risks in financial institutions, Section 2.4 presents a framework for improving cybersecurity policy awareness programs to improve employee behaviour toward cybersecurity compliance.

2.4 Framework for Enhancing Cybersecurity Policy Awareness Programs

This framework provides a guide on how cybersecurity policy awareness can be improved partly through programs that aim to improve employee behaviour toward cybersecurity compliance. Cybersecurity policy awareness programs are essential to ensure that employees have the knowledge and skills necessary to protect their organisations from cyber threats.

This framework provide guidance on how financial institutions can improve their cybersecurity policy awareness programs to promote a culture of cybersecurity awareness and compliance among employees.

2.4.1 Components of the Proposed Framework

The components of the proposed framework for enhancing cybersecurity policy awareness programs are derived from the best practices discussed in Section 2.3. One of the components of the proposed framework for enhancing cybersecurity policy awareness programs is making cybersecurity policy awareness a culture for all employees, including on boarding programs for new employees and regular refresher training for existing employees, and to developing targeted and customised awareness programs for employees based on their roles and responsibilities within the financial institutions. Research has shown that a one-size-fits-all approach to cybersecurity awareness is not effective, as different job functions have different cybersecurity risks and responsibilities (Vasileiou and Furnell, 2019; Hu *et al*., 2021). Therefore, tailoring awareness programs to specific job functions can improve the effectiveness of training and increase employee engagement in the training process (Tolah *et al*., 2021). This can be achieved through the use of targeted training materials such as interactive online courses and simulations (Scholefield and Shepherd, 2019). An important component is the use of continuous and ongoing training programs (He and Zhang, 2019; Kamsamrong *et al.*, 2022). Cybersecurity threats and risks are constantly evolving, which means that training programs must also be updated and refreshed on a regular basis (He and Zhang, 2019; Kamsamrong *et al.*, 2022). This can be achieved through ongoing training programs that provide employees with regular updates on new threats and vulnerabilities, as well as opportunities to practice their skills and knowledge in simulated scenarios (He and Zhang, 2019; Kamsamrong *et al.*, 2022). In addition to targeted and ongoing training programs, the proposed framework should also include measures to reinforce positive behaviours and outcomes (Alshaikh *et al.*, 2019). This can be achieved through the use of incentives, recognition programs, and other forms of positive reinforcement, as suggested by Reeves *et al*. (2021). By reinforcing positive behaviours and outcomes, financial institutions can create a culture of cybersecurity awareness and compliance that is embraced by all employees (Reeves *et al*., 2021).

Additionally, the framework can include the implementation of simulated phishing exercises to increase employee awareness and readiness to detect and report phishing attacks (Back and Guerette, 2021). This approach involves sending simulated phishing emails to employees and tracking their responses to identify areas for improvement and provide targeted training. Lyimo and Shaaban (2021), in their study on assessing cybersecurity awareness among employees in the banking sector, attested to the use of simulated phishing emails. They noted that top financial institutions worldwide are investigating ways to measure staff cybersecurity awareness. For instance, they send 'suspicious' links to bank employees and monitor the click rates before and after cybersecurity training.

Finally, the proposed framework includes measures to assess the effectiveness of training and awareness programs. According to Moustafa *et al*. (2021), organisations should conduct regular assessments of employee knowledge, skills, and attitudes toward cybersecurity, to identify areas where additional training and support may be needed. This can be achieved by using surveys, quizzes, and other forms of assessment that provide information on employee behaviour and attitudes toward cybersecurity.

The components proposed form the basis of the framework, aiming to improve the effectiveness of cybersecurity policy awareness programs and improve employee behaviour toward cybersecurity policy compliance, as outlined in Table 2-3. The framework comprises five main elements derived from the best practices discussed in Section 2.3, which work together to foster a security-conscious culture within the financial institutions.

Table 2-3: Cybersecurity Policy Compliance Components Descriptions

Components	**Descriptions**	**Author**
Make cybersecurity policy awareness a norm	Provision of cybersecurity policy awareness for all employees, including on boarding programs and regular refresher training.	(Vasileiou and Furnell, 2019; Hu, Hsu and Zhou, 2021b; Tolah, Furnell and Papadaki, 2021)
Targeted and customised training programs	Targeted and customised training programs based on job roles and responsibilities.	(Vasileiou and Furnell, 2019; Hu, Hsu and Zhou, 2021b; Tolah, Furnell and Papadaki, 2021)
Continuous and ongoing awareness programs	Regularly updating and refreshing awareness programs to address evolving cybersecurity threats and risks.	(He and Zhang, 2019; Kamsamrong *et al.*, 2022)
Implementation of simulated phishing exercises	Conduct simulated phishing exercises to improve employee awareness and readiness to detect and report phishing attacks.	(Back and Guerette, 2021)
Evaluation of the effectiveness of the awareness program	Regular evaluations of employee knowledge, skills, and attitudes toward cybersecurity to identify areas for improvement.	(Moustafa *et al.*, 2021)

Figure 2-2 indicates the diagrammatic presentation of the components, showing their dependencies and relationships.

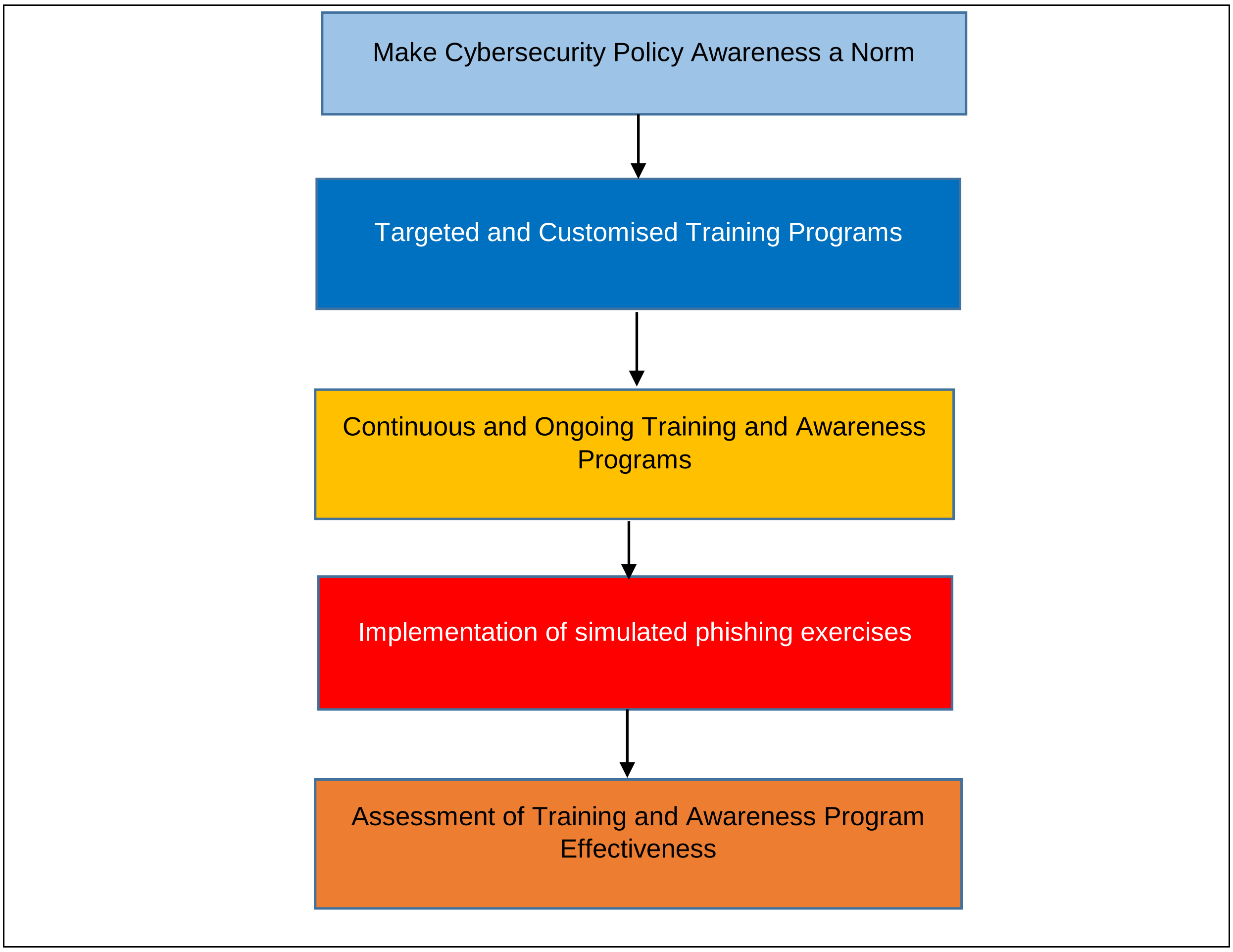

Make Cybersecurity Policy Awareness a Norm
Targeted and Customised Training Programs
Continuous and Ongoing Training and Awareness Programs
Implementation of simulated phishing exercises
Assessment of Training and Awareness Program Effectiveness

Figure 2-2: Cybersecurity Policy Compliance (CSPC)

The components have been organised to showcase the result of their implementation, which is the "Cybersecurity Policy Compliance” Framework. The framework represents the desired result of implementing the components in the financial institutions’ cybersecurity practices. The components contribute to the overall framework as follows:

- Making Cybersecurity Policy Awareness Programs a Norm sets the foundation for the framework.
- Targeted and Customised Training Programs and Gamification in Cybersecurity Training enhance the effectiveness and engagement of training efforts.
- Continuous and Ongoing Awareness Campaigns reinforce positive behaviours and maintain a culture of cybersecurity awareness.
- Implementation of Simulated Phishing Exercises increases employee awareness and readiness to detect and report phishing attacks.

- Evaluation of Training and Awareness Program Effectiveness allows for continuous improvement and identifies areas for additional training and support.

Together, these components contribute to the establishment of a robust "Cybersecurity Policy Compliance" Framework, ensuring that financial institutions have effective policies, well-trained employees, and a culture of compliance to address cybersecurity risks and threats.

2.4.2 Implementation of the Proposed Framework

Implementation of the proposed framework aimed at improving cybersecurity policy awareness programs would be guided by the conceptual framework. This abstract and theoretical structure provide a systematic and coherent approach to organising the various elements, concepts, and relationships involved in the cybersecurity policy awareness initiative. It can help shape the implementation strategy, design the training program, and ensure the alignment of technical and non-technical aspects. The conceptual framework can serve as a valuable guide throughout the implementation process, facilitating a holistic and effective approach to improving awareness of cybersecurity policies and employee behaviour. Therefore, the framework can be implemented through:

1. Making Cybersecurity policy awareness programs a norm:

   - The first step is to make cybersecurity policy awareness programs a norm for all employees. This ensures that everyone in the financial institution understands the importance of cybersecurity policy and their role in maintaining it.

   - Training should cover basic cybersecurity principles, policies, and procedures relevant to the financial institutions' specific needs and industry.

   - Compliance with this component ensures that all employees have a basic understanding of the cybersecurity policy, setting the stage for more advanced training.

2. Targeted and customised training programs and gamification in cybersecurity awareness:

   - After establishing the foundation, the financial institution should implement targeted and customised training programs. Different departments or job roles may require specific cybersecurity training tailored to their responsibilities.

   - This component improves the effectiveness of training efforts, ensuring that employees receive relevant and engaging content based on their roles, thus improving their cybersecurity knowledge and skills.

3. Continuous and ongoing awareness campaigns:

    - Beyond initial training, continuous and ongoing awareness campaigns are crucial to reinforce positive cybersecurity behaviours and maintain a culture of vigilance throughout the financial institution.
    - These campaigns can include regular reminders, newsletters, posters, and other communication methods to keep cybersecurity at the forefront of employees' minds.
    - This component helps maintain a strong cybersecurity culture, reducing the likelihood of negligence or complacency over time.

4. Implementation of simulated phishing exercises:

    - Simulated phishing exercises involve sending mock phishing emails to employees to test their ability to identify and report phishing attempts.
    - This hands-on approach helps employees develop their skills to detect suspicious emails and raises awareness about phishing risks.
    - The regular implementation of simulated phishing exercises improves overall security posture by making employees the first line of defence against real phishing attacks.

5. Evaluation of training and awareness program effectiveness:

    - To ensure the effectiveness of training and awareness initiatives, regular evaluation and evaluation are necessary.
    - Metrics such as the number of reported incidents, employee feedback, and the improvement in security incidents should be analysed.
    - The insights gained from assessments allow the financial institutions to make data-driven decisions, identifying areas of improvement and addressing any Gaps in The Training and Awareness Efforts.

2.4.3 Distinction of the Proposed Framework from Other Frameworks

In published literature, several frameworks related to cybersecurity policy training and awareness programs are reported. However, the proposed framework in this research stands out in terms of its specific focus on financial institutions and its objectives to enhance employee compliance with cybersecurity policies.

To highlight the differentiating factors of the proposed framework, a table has been provided, comparing it with other frameworks cited in the review of the literature. Table 2-4 highlights the specific focus, objectives, and key distinctions of each framework, emphasising the novel contributions of the proposed framework.

Table 2-4: Distinction of the Proposed Framework from Other Frameworks

Framework	Focus	Objectives	Key Distinctions from proposed framework
Proposed Framework (This research)	Financial institutions	Enhance employee compliance with cybersecurity policies	Specific focus on financial institutions
(Li *et al.*, 2019)	Awareness of cybersecurity policy	Investigate impact on employee behaviour	No framework to improve compliance
(Hajny *et al.*, 2021)	Cybersecurity curricula	Propose a framework for cybersecurity curricula	No focus on financial institutions
(Murphy *et al.*, 2022)	SMMEs in South Africa	Study factors affecting compliance with national cybersecurity policy	No framework to improve compliance

The framework proposed in this research distinguishes itself from other frameworks as follows:

1. Focus: The proposed framework specifically targets financial institutions, recognising their unique cybersecurity challenges and compliance requirements. By contrast, none of the current frameworks address specific cybersecurity needs in financial institutions.

2. Objectives: The proposed framework aims to develop cybersecurity compliance framework for improving cybersecurity policy awareness and employee behaviour in financial institutions, providing a practical framework for improving adherence to security protocols.

3. Key Distinctions:

    - Li *et al.* (2019) investigated the impact of awareness of cybersecurity policy but did not develop a framework to improve compliance.

    - Hajny *et al.* (2021) proposed a framework for cybersecurity curricula but did not focus on financial institutions.

    - Murphy *et al.* (2022) studied compliance factors for SMMEs in South Africa but did not provide a framework for improving compliance.

4. Comprehensive approach: The proposed framework covers various aspects, including identifying key factors that influence employee behaviour, evaluating the effectiveness of existing programs, and developing a framework to improve awareness.

5. Unique target audience: Unlike Murphy et al. (2022) who focused on compliance factors for SMMEs in South Africa, the proposed framework specifically targets financial institutions, acknowledging their distinct cybersecurity requirements.

In general, the proposed framework stands out due to its specific focus on financial institutions, comprehensive approach, and objectives to improve compliance with cybersecurity policies through awareness programs.

2.4.4 Potential Impact of the Proposed Framework on Employee Behaviour Toward Cybersecurity Compliance

It is essential to understand the potential impact of a proposed framework aimed at enhancing cybersecurity policy awareness programs on employee behaviour toward cybersecurity compliance. Several studies have examined the effectiveness of such programs in changing employee behaviour toward cybersecurity compliance. For example, Back and Guerette (2021) found that cybersecurity awareness training improved participants' knowledge of phishing scams and reduced their vulnerability to phishing attacks. Similarly, a study by Ofori *et al.* (2021); Almeida *et al.* (2022); and Sulaiman *et al.* (2022) found that cybersecurity awareness training increased employee knowledge and attitudes towards cybersecurity best practices. Furthermore, a study by He and Zhang (2019); and Kamsamrong *et al.* (2022) highlighted the importance of continuous training and awareness programs to maintain and improve employee behaviour toward cybersecurity compliance. A study by Dash and Ansari (2022) found that employees who received training on cybersecurity policies and practices were more likely to report suspicious activities and follow cybersecurity best practices compared to those who did not receive training. Similarly, another study by Li *et al.* (2019) showed that providing cybersecurity training to employees increased their knowledge and understanding of cybersecurity risks and best practices, leading to better compliance with cybersecurity policies.

In addition to training, awareness programs can also be effective in improving employee behaviour toward cybersecurity compliance. A study by Alotaibi *et al.* (2016); and He *et al.* (2020) found that cybersecurity awareness programs that emphasised the importance of cybersecurity and provided examples of cybersecurity incidents were effective in increasing employee awareness and behaviour toward cybersecurity. Furthermore, the use of technology such as simulations and games in cybersecurity training has demonstrated its efficacy in enhancing employee behaviour toward cybersecurity compliance (Alhashmi *et al.*, 2021). These technologies provide a more engaging and interactive learning experience, which can increase knowledge retention and improve behaviour towards cybersecurity policies and practices.

In general, the proposed framework has the potential to significantly improve employee behaviour toward cybersecurity compliance by providing comprehensive training and education programs, awareness campaigns, and the use of technology-based learning. The combination of these strategies can increase the knowledge and understanding of employees about cybersecurity risks and best practices, leading to better compliance with cybersecurity policies and practices. Furthermore, the literature suggests that the implementation of a framework to improve cybersecurity policy training, education, and awareness programs can have a positive impact on employee behaviour towards cybersecurity compliance. However, it is important to ensure that these programs are designed, implemented and continuously updated to address the evolving cybersecurity threat landscape (He *et al.*, 2020).

2.5 Chapter Summary

In recent years, cybersecurity breaches and incidents have become a major concern for financial institutions worldwide. The increasing complexity and sophistication of cyber threats have made it difficult for financial institutions to protect their data and systems. This chapter has provided a comprehensive overview of the current state of cybersecurity compliance in financial institutions, as well as an analysis of cybersecurity breaches and incidents in this sector. The chapter also discussed challenges associated with implementing effective cybersecurity policies and practices, and proposed a framework for enhancing cybersecurity policy education, training, and awareness programs to improve employee behaviour toward cybersecurity compliance.

Clearly, financial institutions are increasingly investing in cybersecurity measures to protect their data and systems. However, despite these efforts, cybersecurity breaches and incidents continue to occur, highlighting the need for further improvements in cybersecurity compliance. Analysis of published information reveal that cybersecurity breaches and incidents are indicators that financial institutions are particularly vulnerable to attacks due to the large amount of sensitive data they handle and the sophisticated nature of the attacks. Through reviewing literature, in this chapter, the research identified various challenges to implementing effective cybersecurity policies and practices, including a lack of resources, lack of employee awareness and training, and difficulties in keeping up with the rapidly evolving cyber threat landscape. The proposed framework aims to address these challenges by providing a comprehensive approach to improving cybersecurity policy education, training, and awareness programs. The framework includes components such as continuous and ongoing training programs, reinforcement of positive behaviours and outcomes, implementation of simulated phishing exercises, and performing regular monitoring and assessments to evaluate the effectiveness of training and awareness programs. The implementation of this framework has the potential to improve employee behaviour towards cybersecurity compliance and reduce the likelihood of cyberattacks.

In general, the literature reviewed in this chapter highlights the need for financial institutions to prioritise cybersecurity and implement effective policies and practices to protect themselves and their customers. Continued training and education are essential components of cybersecurity programs, and the proposed framework provides a comprehensive approach to improving these programs.

The research methodology of the study is discussed in the next chapter.

CHAPTER 3: RESEARCH METHODOLOGY

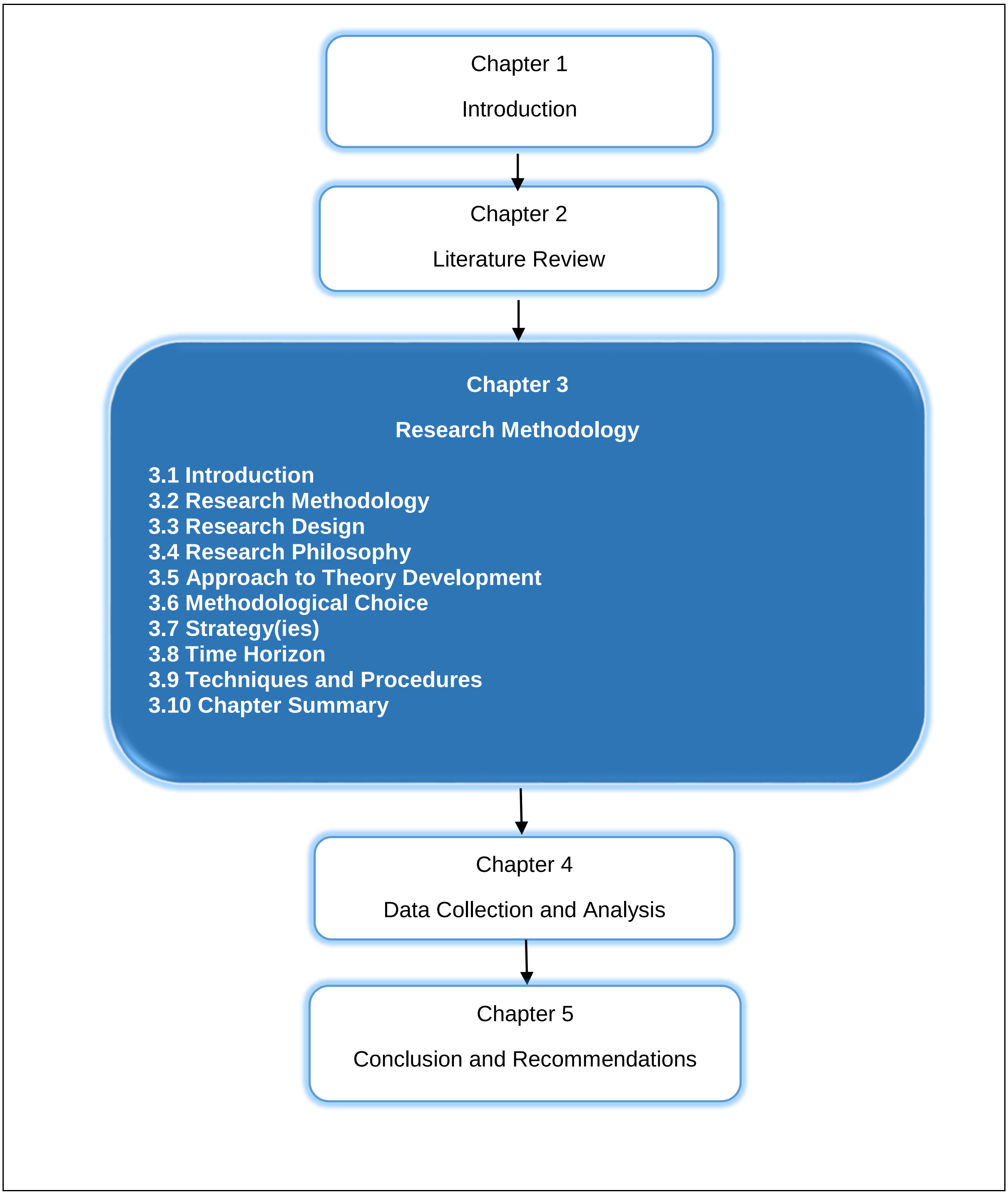


Figure 3-1: Roadmap of Chapter 3

3.1 Introduction

The objective of this research is to develop cybersecurity compliance framework for improving cybersecurity policy awareness and employee behaviour in financial institutions. The proposed framework integrates diverse best practices, guidelines, and principles into a cohesive structure aimed at fostering a security-conscious culture within organisations. By addressing key elements that influence cybersecurity awareness and behaviour, the framework is intended to help financial institutions create more effective and engaging policy awareness programs, thereby promoting better adherence to cybersecurity policies. To achieve the goal of designing and developing this cybersecurity framework, the research adopted a survey-based methodology. The survey approach is chosen due to its suitability in gathering extensive data from a broad range of participants, providing insights into current practices, perceptions, and challenges related to cybersecurity policy awareness and compliance within organisations. Surveys are particularly effective for collecting quantitative data, which can be analysed to identify trends, patterns, and areas for improvement.

3.2 Research Methodology

This chapter discusses the research methodology of the study, detailing the decisions at each phase of the research process, guided by the 'research onion' model. The 'research onion' model is chosen for its structured approach to research design, which ensures comprehensive coverage of all necessary aspects, from philosophical stances to data collection techniques. The layers of the research onion to be discussed in this chapter include research philosophy, methodological choice, approach, strategy, and time horizon. The data collection and analysis layer is briefly introduced here, with an in-depth discussion provided in Chapter 4. By systematically addressing each layer of the research onion, the study ensures a rigorous and thorough approach to developing the framework.

Research methodology refers to the general approach that outlines how a study should be conducted (Saunders *et al*., 2019). Research methodology encompasses a system of beliefs and philosophical assumptions that shape the understanding of research questions and form the basis for selecting research methods (Saunders *et al*., 2019). Research methodology addresses aspects such as research philosophy that influence the choice of the research approach, research methods, and research strategy (Saunders *et al*., 2019). The philosophical decisions driving the selection of research methodologies, data collection methods, and analysis, which pave the way for the subsequent discussion focused on the design of the research.

The approach and the steps taken in this investigation were carefully chosen to ensure that they align with the intended outcomes and the importance of the results. Saunders *et al.* (2019) provide a visualisation of the research design through an onion diagram, which was adopted in this study. The research onion, as depicted in Figure 3.2, serves as a structure for outlining the design of this study.

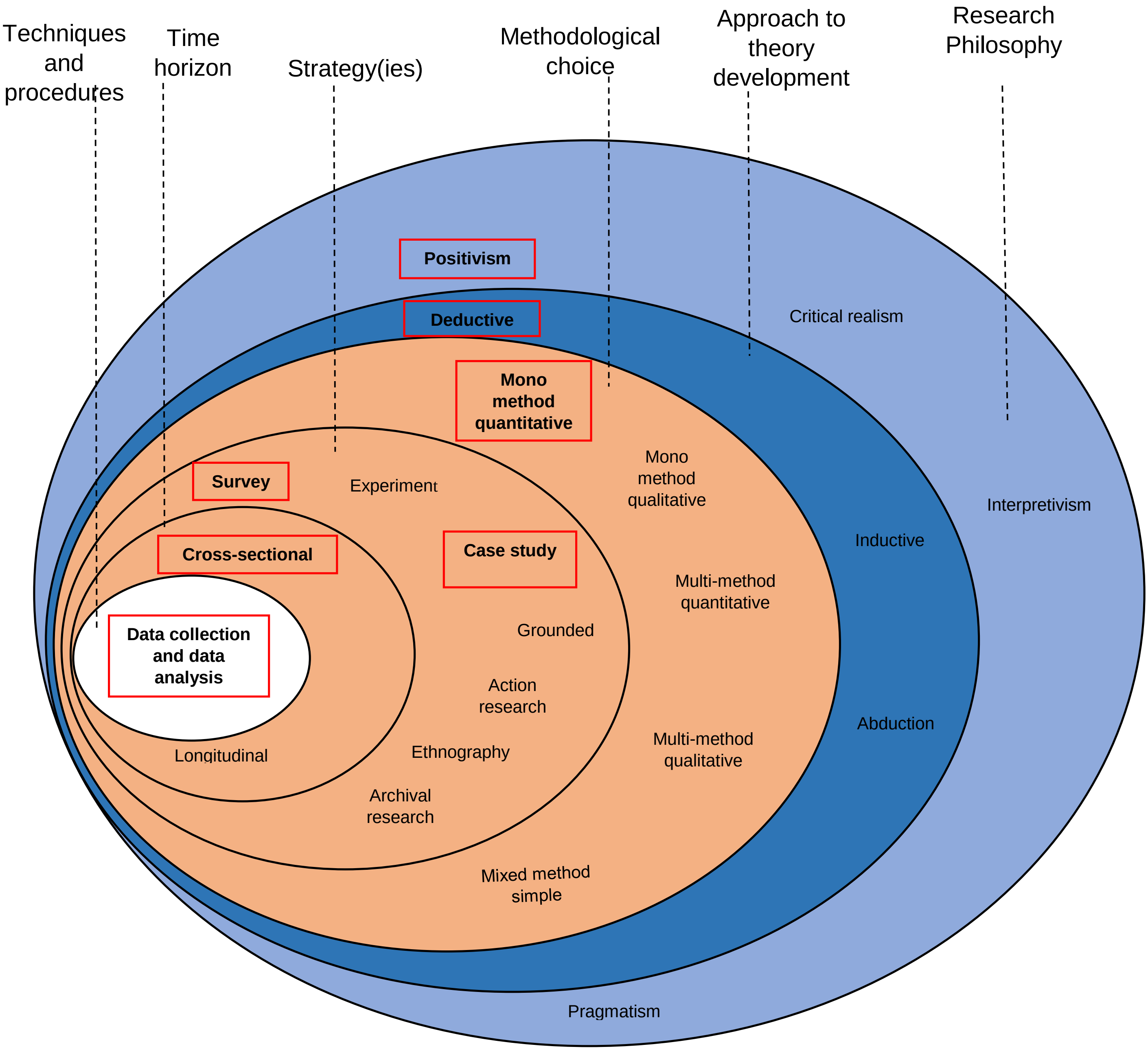


Figure 3-2: Research Onion (Adapted from Saunders et al. (2019))

Figure 3-2 emphasises the chosen options at each research onion's layer marked by a red rectangular shape.

3.2.1 Research Philosophy

Philosophy, the understanding of valid knowledge, comprises five elements: positivism, critical realism, interpretivism, postmodernism, and pragmatism. Of particular interest are positivism, a scientific approach focused on factual knowledge, and interpretivism, oriented toward exploring meanings in social interactions (Saunders *et al*., 2019). On the one hand, interpretivism emphasises understanding humans as social beings, distinguishing research among people from objects (Saunders *et a*l., 2019). Ontologically, it asserts that social phenomena are co-constructed by researchers and subjects, recognising the uniqueness of individuals and the existence of multiple realities (Saunders *et al*., 2019). Epistemologically, interpretivists contend that research findings result from the interactive process between researchers and subjects (Guba and Lincoln, 2011). Accessing reality involves social constructions like consciousness, language, tools, and shared meanings (Thanh and Thanh, 2015). Axiologically, interpretivists are value-bound, employing inductive, qualitative methods with small samples in their research to deeply understand the subjective experiences and meanings constructed by individuals (Saunders *et al*., 2019).

On the other hand, positivism, rooted in natural sciences, emphasises observable and measurable reality (Saunders *et al*., 2019). Ontologically, it adopts realism, positing an objective reality independent of human perception (Saunders *et al*., 2019). Positivists seek objective truth through measurable metrics, supporting universal generalisations (Saunders *et al*., 2019). Measurement is conducted with properties autonomous of researchers and tools (Saunders *et al*., 2019). Axiologically, positivists aim to minimise research values to prevent bias.

Positivist inquiry tends to be deductive, structured, and quantitative, using large samples and quantitative data analysis (Saunders *et al*., 2019). It is associated with theory-testing through the collection of quantitative data to enhance predictive understanding (Saunders *et al*., 2019). Positivists align with an empirical realist ontology, prioritising empirical evidence for a scientific-oriented approach (Saunders *et al*., 2019). In this study, the survey strategy adhered to the positivist paradigm, objectively examining respondents' views on cybersecurity policy awareness programs offered by financial institutions in Lesotho.

3.2.2 Approach to Theory Development

Three distinct approaches to the development of theory have been identified as abduction, deduction, and induction (Saunders *et al*., 2019). Deduction involves examining a theoretical statement employing a research approach that moves from broader to more detailed understanding via logical reasoning (Saunders *et al*., 2019). In addition, Creswell (2014) suggests that the deductive approach involves researchers confirming theories, evaluating hypotheses, and research questions, putting into operation the constructs obtained from surveys, and evaluating these constructs using research tools to obtain scores. In contrast, abduction involves collecting information to study a phenomenon, recognise fundamental themes and patterns, and potentially create a new theory or adjust an existing one for future examination (Saunders *et al*., 2019). Induction is based on the creation of a theory based on the observation of empirical data (Saunders *et al*., 2019).

In this study, the deductive approach was employed to the quantitative research since the study involved collecting numeric categorical data only from respondents which lends itself readily to quantitative analysis and interpretation. The quantitative data were gathered from both non-IT and IT employees within selected financial institutions in Lesotho. In quantitative research, sufficient information about the study's design is furnished to allow replication, verification, and confidence in the findings, as emphasised by Ranjit (2011). In addition, this study uses the deductive approach. The researcher used empirical data to design the questionnaire, which assisted in identifying requirements for enhancing cybersecurity policy awareness programs to influence employee behaviour toward cybersecurity compliance in financial institutions. The questionnaire was distributed to respondents in the financial institutions in Lesotho. The identified requirements from the collected data assisted in designing a framework for the development of effective cybersecurity policy awareness programs. The findings were then considered to refine the proposed framework.

As a result, this study adheres to a deductive approach as it endeavours to address the research objectives. The discussion on theory development approaches, particularly the emphasis on the deductive approach aligning with the study's quantitative nature, bridges the connection to the subsequent section on methodological choice.

3.2.3 Methodological Choice

Methodological choices are used for the collection, analysis, and interpretation of data, and options include mono, multi, or mixed methods research (Saunders *et al*., 2019). In a monomethod, a researcher utilises a singular approach for both data collection and analysis (Saunders *et al*., 2019). As an example, a researcher decides to gather quantitative data through a survey and employs statistical techniques for analysis or opts for qualitative data acquisition via interviews and utilises thematic analysis for data interpretation.

A multi-method approach occurs when a researcher selects multiple collection methods along with their corresponding analysis techniques (Saunders *et al*., 2019). An illustrative example involves a researcher gathering quantitative data through questionnaires and structured observation, and then analysing the information collected using statistical methods. When using mixed methods, a researcher chooses to collect data quantitatively and qualitatively with relevant collection techniques and the corresponding analysis procedures at the same time (Saunders *et al*., 2019).

This study adopted a monomethod quantitative approach due to its utilisation of quantitative data collection from sampled financial institutions in Lesotho. The collected quantitative data were analysed using the statistical software SPSS. The proposed framework was refined using the findings from the data collected from respondents in financial institutions, which identified difference between males and females regarding cybersecurity knowledge and compliance with cybersecurity policy. This identified difference was used to refine the framework and became an initial consideration component. According to Singh (2007), quantitative methods are characterised by techniques aimed at hypothesis testing, fact determination, identification of variable associations, and outcome prediction. This research approach draws strategies from the natural sciences, emphasising objectivity, generalisability, and reliability (Sârghie, 2021). Using statistical techniques, the study aims to achieve predetermined objectives related to relationships between specific variables. Therefore, quantitative methods are well suited for this investigation. The exploration of methodological choices, specifically the adoption of a combined survey and case study within the study's monomethod quantitative approach, sets the groundwork for the subsequent section on strategy(ies).

3.2.4 Strategy(ies)

In the context of research methodology, the research strategy outlines the overall plan that guides how a researcher addresses the research questions (Saunders *et al*., 2019). This plan allows the researcher to effectively address research objectives or fundamental inquiries, thus shaping the progression and structure of the study (Saunders *et al*., 2019). The selection of a specific strategy is determined by the study objectives, as emphasised by Saunders *et al*. (2019).

Among the primary research strategies available are survey, case study, ethnography, experiment, action research, grounded theory, postmodernism, and archival research. These research strategies can be applied to explanatory, exploratory, and descriptive research, with each method adaptable to all three types of research (Yin, 2013).

This study employed a survey strategy of which was data collected from a case study of financial institutions. Given the dynamic nature of cybersecurity policy compliance, which includes various dimensions such as organisational practices, employee awareness, and policy implementation, the study adopted a survey within a case study framework.

A survey strategy involves presenting a series of inquiries, typically in the form of a questionnaire, to individuals in order to collect data (Saunders *et al.*, 2019; Johnson and Christensen, 2020). While questionnaires are commonly used, other valid instruments such as observations or interviews can also be utilised in survey research (Saunders *et al.*, 2019). This approach enables researchers to gather quantitative data, which is then analysed using descriptive and inferential statistical measures. By analysing the data, researchers can propose explanations for observed variable relationships and construct models representing these relationships (Saunders *et al.*, 2019).

The survey strategy is closely associated with the deductive approach and explanatory research, allowing researchers to explore multiple variables simultaneously by collecting real-world data from respondents (Saunders *et al.*, 2019). In this study, a survey strategy was employed to identify the requirements for enhancing cybersecurity policy awareness programs to influence employee behaviour toward cybersecurity compliance in financial institutions. Data was collected from respondents in financial institutions in Lesotho. Given the numerous factors influencing non-compliance, it was essential to consider these requirements when investigating employee behaviour regarding adherence to cybersecurity policies. The utilisation of the survey strategy to identify these requirements aided in the design of a framework for developing effective cybersecurity policy awareness programs and smoothly transitions into the subsequent section on time horizons.

3.2.5 Time Horizons

Once a research strategy is adopted, a researcher ought to determine the duration for conducting the research project. Time horizons refer to the period during which research is conducted and can be categorised as either longitudinal or cross-sectional approaches (Saunders *et al*., 2009). A cross-sectional time horizon examines a specific phenomenon at a particular point in time (Saunders *et al.,* 2009). It involves collecting data from a selected sample representing a large population at one specific point in time (Saunders *et al*., 2009). On the other hand, a longitudinal time horizon involves conducting a long-term study (Saunders *et al*., 2009). Researchers can also collect data at two distinct points in time through repeated trials, with the aim of answering a research question over an extended period (Sekaran and Bougie, 2016).

For this study, a cross-sectional time horizon was used. According to Sekaran and Bougie (2016), the cross-sectional time horizon is suitable for academic research projects where data is collected once over a period of months or less to address the research questions. In this study, data was collected over four months from identified financial institutions in Lesotho. The selected cross-sectional time horizon informs the forthcoming exploration of data analysis techniques and procedural methodologies in-depth.

3.2.6 Techniques and Procedures

In research, techniques and procedures are crucial components that cover the whole process of collecting and analysing data. This involves leveraging both primary and secondary data sources, selecting sample populations, creating survey questions or interview questions, and getting ready for surveys, among other important activities. This section outlines the methodologies used for data collection and analysis within this study and their discussions based on the selected survey strategy. In addition, the reliability of the research instrument is discussed.

3.2.6.1 Population

Population represents the entirety of individuals within a particular group that is being studied or considered (Saunders *et al.,* 2019). Also, the concept represents the total quantity or a large group comprising numerous cases, constituting the entire universe of individuals being investigated, and from which results are generalised or applied (Johnson and Christensen, 2020). A population ought to share one or more characteristics that can be publicly verified (Johnson and Christensen, 2020). The elements chosen for the investigation sample are drawn from this population (Johnson and Christensen, 2020).

In quantitative research, it is crucial that the population effectively mirrors the entire range of cases involving the individuals of interest in the study (Johnson and Christensen, 2020). These individuals are classified according to demographic traits such as gender (quantified in females or males) and other constructs (Johnson and Christensen, 2020).

In this study, the entire population encompassed every employee in all financial institutions in Lesotho. Employees were classified according to traits or features considered as elements of the demographic particulars within the research, encompassing gender, age, educational background, job classifications, and years of professional experience.

3.2.6.2 Target Population

The target population refers to the specific group of interest in the research, characterised by quantifiable traits (Johnson and Christensen, 2020). According to Johnson and Christensen (2020), the target population is a comprehensive and precisely defined collection of multiple instances that serve as the focal point of the study. From an identified target population, a researcher should select a sample to gather essential information to meet the research objective, and the results or discoveries of the study are broadly applicable (Saunders *et al*., 2019; Johnson and Christensen, 2020).

In this research, the target population consisted of non-IT and IT employees from financial institutions in Lesotho, particularly in Maseru. The target population excluded general workers such as cleaners, drivers, and messengers, among others. Non-IT employees were individuals with diverse roles that extended beyond the information technology domain, highlighting the variety of professions in different departments. This includes roles such as finance, HR, marketing, and more (Alp Consulting, 2024). IT employees possessed technical expertise and were proficient in adapting to the constantly changing realm of technology. This includes roles such as software developers, cybersecurity specialists, data analysts, cloud architects, and more (Alp Consulting, 2024). These employees were identified as respondents from whom crucial information was collected to address the research objective, which was to develop cybersecurity compliance framework for improving cybersecurity policy awareness and employee behaviour in financial institutions. Non-IT employees were chosen due to their regular use of computers within their organisations' networks and systems for daily tasks. IT employees were selected based on their expertise in assessing the most effective cybersecurity policy awareness programs to provide to employees.

The target population serves as the primary source from which the study seeks to derive information and draw conclusions (Saunders *et al.*, 2019). The employees' insights were instrumental in identifying weaknesses in cybersecurity policy awareness programs and components of the cybersecurity policy compliance framework. This contribution played a crucial role in shaping the development of a comprehensive framework for the compliance of cybersecurity policies. This framework serves as the foundation for creating effective cybersecurity policy awareness programs designed to train employees and influence their compliance with cybersecurity policies within financial institutions.

3.2.6.3 Sampling

Sampling is a critical procedure in research that involves selecting a small group of participants to accurately represent a larger population, thus determining a sample size (Sekaran and Bougie, 2016). Decisions made about sampling in a research study play an essential role in the reliability of the results (Sekaran and Bougie, 2016). These decisions involve the sampling method, ensuring that the sample size is sufficient, and ensuring that the sample is a true reflection of the population (Sekaran and Bougie, 2016).

Sampling in research encompasses two fundamental types: probability and nonprobability sampling (Sekaran and Bougie, 2016; Saunders *et al.*, 2019). Probability sampling involves random selection, ensuring equal and known chances of inclusion for each individual in the target population (Saunders *et al*., 2019). This method is ideal when the goal is to achieve representativeness and generalisability.

On the contrary, nonprobability sampling is a method in which the researcher selects samples based on subjective judgment, and it does not ensure equal chances of being chosen (Sekaran and Bougie, 2016). Nonprobability sampling includes convenience and purposive methods (Sekaran and Bougie, 2016) and the two nonprobability sampling subtypes and their applications are briefly discussed below:

Convenience sampling involves gathering information from individuals who are readily available (Alkassim and Tran, 2016; Sekaran and Bougie, 2016). Although convenient, this sampling method is commonly used in the exploratory phase of research for quick and efficient access to basic information (Alkassim and Tran, 2016; Sekaran and Bougie, 2016).

Purposive sampling involves deliberately selecting individuals or elements from specific target groups to gather information (Sekaran and Bougie, 2016). Instead of choosing participants based on convenience, researchers concentrate on individuals who can provide the required information. This could be due to their exclusive possession of that information or because they meet specific criteria established by the researcher (Sekaran and Bougie, 2016). Purposive sampling includes two main types: judgment sampling and quota sampling.

- Judgment sampling involves selecting individuals who are in the most advantageous position to provide the required information (Sekaran and Bougie, 2016).
- Quota sampling involves selecting participants based on specific characteristics predetermined to match the distribution of characteristics within the larger population (Sekaran and Bougie, 2016).

Nonprobability sampling methods prove advantageous in social science research, particularly when targeting very specific populations that are not readily accessible (Kitchenham and Pfleeger, 2002). Furthermore, nonprobability sampling becomes acceptable when population characteristics are uniformly spread, ensuring that any sample size becomes sufficiently large to represent and generalise findings to the broader population. In this study, nonprobabilistic sampling methods primarily involved sending invitations to employers through an email. To ensure a representative sample of various financial institutions in Lesotho, efforts were made to distribute the survey among employers, who were responsible for distributing it to potential respondents. Considering the characteristics of IT and non-IT users in this investigation, the researcher asserts that the sampling method discussed below facilitated an accurate and representative sample of the population.

In this study, judgement sampling, a form of purposive and nonprobability sampling technique, was used. The researcher used judgement sampling to select non-IT employees actively involved in cybersecurity measures, aiming to comprehend their awareness and compliance. Simultaneously, individuals with experience in designing cybersecurity policy awareness programs or possessing cybersecurity policy knowledge within the IT department were included in the sample. The gatekeepers, including Human Resources and marketing officers designated by the employers, were responsible for distributing the questionnaires to the relevant respondents within financial institutions. The researcher ensured clear communication of the roles of the employees to whom the questionnaires were assigned to the gatekeepers.

Although this method may limit generalisability, it ensures the inclusion of key personnel who possess first-hand insights into cybersecurity policy adherence and program design, aligning with the specific objective of this study, which centred on developing cybersecurity compliance framework for improving cybersecurity policy awareness and employee behaviour in financial institutions. Judgment sampling requires special efforts to locate individuals with the required information, which makes it crucial to address certain research questions (Sekaran and Bougie, 2016).

3.2.6.4 Sample Size

The sample size indicates the number of individuals in the target group who provide information for the study (Saunders *et al*., 2019; Johnson and Christensen, 2020). While Creswell and Creswell (2018) advocate for larger sample sizes to reduce errors and improve accuracy, Sekaran and Bougie (2016) contend that managing a sizable population could present limitations in terms of time and expenses. Creswell and Creswell (2018) emphasise that sample size influences the precision of findings in representing the population. Saunders *et al.* (2019) suggest that a larger sample improves the likelihood of accurate generalisation.

In determining the necessary sample size, the initial step involves setting the minimum level of precision required for sample estimates, along with establishing the desired confidence level and considering the population size (Cochran, 1977). The estimated number of employed individuals in the 'financial and insurance industries' from the 2019 Lesotho Labour Force Survey was N = 4516, and this figure was utilised as the population size in this study (Lesotho Bureau of Statistics, 2021). It is therefore crucial, given the population’s finite size to employ Cochran’s finite population correction factor to the sample estimate (Cochran, 1977). In this research study, the level of precision (called the margin of error) was set at $e = 7.00\%$ and the confidence level at $1 - \alpha = 95\%$, leading to a significance level of $\alpha = 5\%$. This essentially imply willingness to take a small risk, $\alpha = 5\%$, that the estimates could be off by $e = 7.00\%$.

Another parameter needed in estimating a sample is the estimated proportion, p, of respondents who possess the desired characteristic, which could be any of the many proportions that can be computed from the sample data, e.g., like proportion of males or females. To give maximum variability, an assumption was made that $p = 50\%$. The normal distribution value that corresponds to the 95% two-sided confidence interval is approximately $Z_{5\%/2} = 1.96$. With all this information, Cochran's sample size is computed as:

$$n_0 = \frac{Z_{0.025}^2 \times p \times (1-p)}{e^2} = \frac{1.96^2 * 0.5 * 0.5}{0.07^2} = 196$$

Therefore, the large-population sample size is therefore 196. Now, the finite population correction factor (fpc) is

$$fpc = 1 + \frac{n_0 - 1}{N} = 1 + \frac{196 - 1}{4516}$$

Now, the final sample size, corrected for small populations and rounded up to the nearest whole number is

$$n = \frac{n_0}{fpc} = \frac{196}{1 + \frac{196-1}{4516}} = 187.887 \cong 189$$

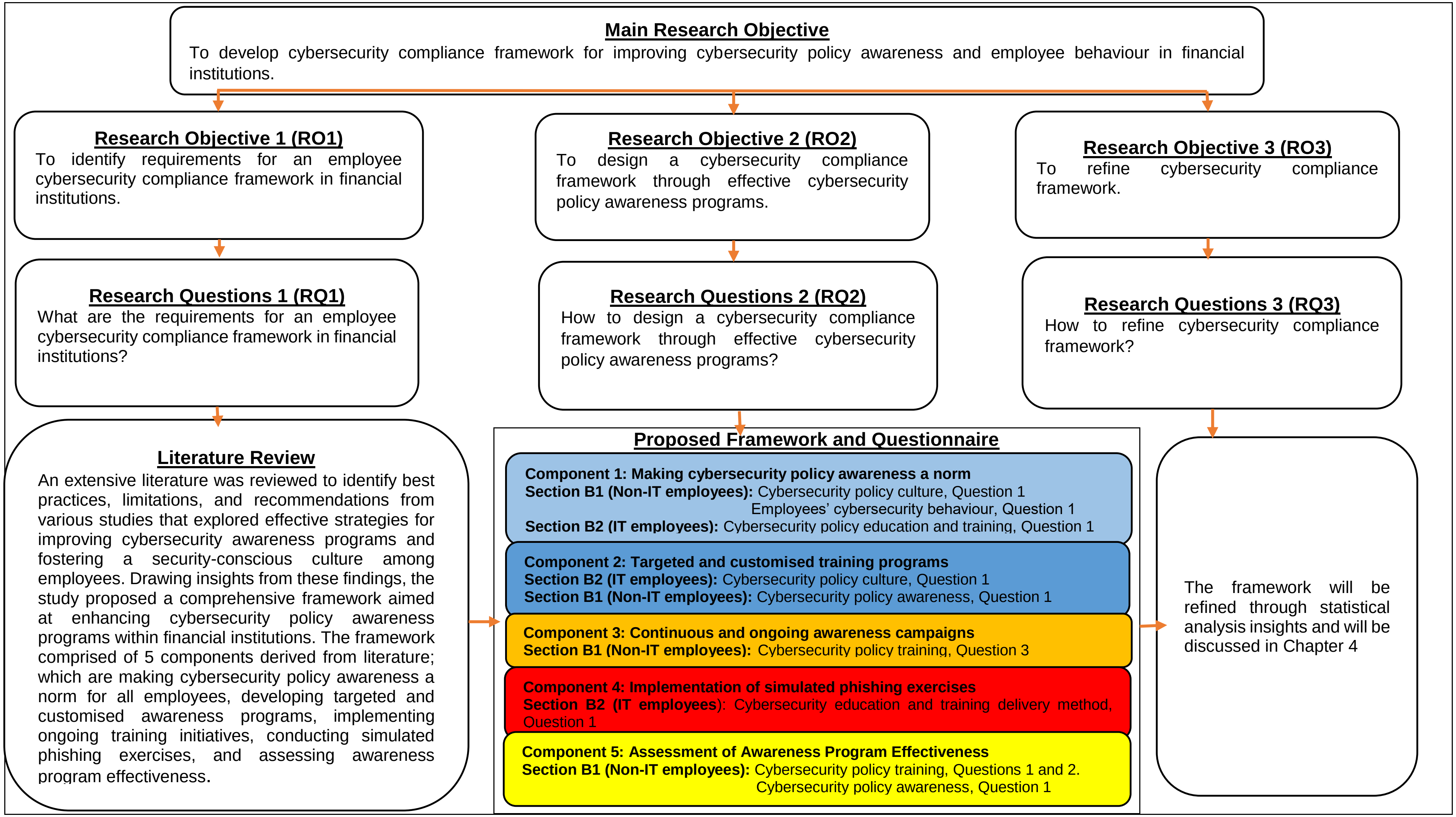
In this study, the targeted sample size was 189 employees. The survey links were sent to employer contact persons for distribution among relevant representatives or respondents.

3.2.6.5 Questionnaire Development

A questionnaire is a compilation of inquiries used to acquire information from respondent regarding their opinions, attitudes, or experiences (Bhandari, 2021). A questionnaire serves as a data collection method that formulates questions aligned with research objectives (Johnson and Christensen, 2020). A questionnaire is an effective tool for gathering deductive data for statistical analysis (Ranjit, 2011; Cohen, Manion and Morrison, 2017). Among survey instruments, the closed-ended questionnaire is the preferred choice, presenting respondents with predefined answers in the form of matrices or rating scales, encouraging written responses or marked selections (Bell *et al.*, 2022). In the context of this study, the researcher crafted questions based on the research objectives and insights from the literature review. The questionnaire (Appendix F) was designed to align with the main research objective of this study, which is to develop cybersecurity compliance framework for improving cybersecurity policy awareness and employee behaviour in financial institutions. The main research objective was addressed through three (3) specific research objectives.

The first research objective was met through the literature review, where components of the proposed framework were derived. For the second research objective, the questionnaire was designed to align with the derived components of the framework. The purpose of the questionnaire was to determine the relevance of the framework in providing effective cybersecurity policy awareness programs. Each section of the questionnaire was linked to the components of the proposed framework.

Figure 3-3 illustrates the mapping of the questionnaire to the research objectives and research questions.



Main Research Objective

To develop cybersecurity compliance framework for improving cybersecurity policy awareness and employee behaviour in financial institutions.

Research Objective 1 (RO1)

To identify requirements for an employee cybersecurity compliance framework in financial institutions.

Research Objective 2 (RO2)

To design a cybersecurity compliance framework through effective cybersecurity policy awareness programs.

Research Objective 3 (RO3)

To refine cybersecurity compliance framework.

Research Questions 1 (RQ1)

What are the requirements for an employee cybersecurity compliance framework in financial institutions?

Research Questions 2 (RQ2)

How to design a cybersecurity compliance framework through effective cybersecurity policy awareness programs?

Research Questions 3 (RQ3)

How to refine cybersecurity compliance framework?

Literature Review

An extensive literature was reviewed to identify best practices, limitations, and recommendations from various studies that explored effective strategies for improving cybersecurity awareness programs and fostering a security-conscious culture among employees. Drawing insights from these findings, the study proposed a comprehensive framework aimed at enhancing cybersecurity policy awareness programs within financial institutions. The framework comprised of 5 components derived from literature; which are making cybersecurity policy awareness a norm for all employees, developing targeted and customised awareness programs, implementing ongoing training initiatives, conducting simulated phishing exercises, and assessing awareness program effectiveness.

Proposed Framework and Questionnaire

Component 1: Making cybersecurity policy awareness a norm
Section B1 (Non-IT employees): Cybersecurity policy culture, Question 1
Employees' cybersecurity behaviour, Question 1
Section B2 (IT employees): Cybersecurity policy education and training, Question 1

Component 2: Targeted and customised training programs
Section B2 (IT employees): Cybersecurity policy culture, Question 1
Section B1 (Non-IT employees): Cybersecurity policy awareness, Question 1

Component 3: Continuous and ongoing awareness campaigns
Section B1 (Non-IT employees): Cybersecurity policy training, Question 3

Component 4: Implementation of simulated phishing exercises
Section B2 (IT employees): Cybersecurity education and training delivery method, Question 1

Component 5: Assessment of Awareness Program Effectiveness
Section B1 (Non-IT employees): Cybersecurity policy training, Questions 1 and 2.
Cybersecurity policy awareness, Question 1

The framework will be refined through statistical analysis insights and will be discussed in Chapter 4

Figure 3-3: Mapping the Research Objective to the Questionnaire

It is noteworthy that the questionnaire was tailored to two distinct groups: IT employees and non-IT employees. This deliberate separation was motivated by the unique roles these groups play in the context of the cybersecurity program. IT employees, possessing specialised expertise, contribute significantly to the design of the training program. As such, their questionnaire focused on intricate details and advanced aspects related to cybersecurity. On the other hand, non-IT employees are the recipients of this training, and their questionnaire concentrated on assessing their understanding, needs, and experiences as individuals undergoing training. This targeted approach ensures that the questions cater to the specific roles and contributions of each group, enhancing the relevance and effectiveness of the collected data. The questionnaire was structured into three sections, as outlined in Table 3-1, each section designed to address the unique perspectives and requirements of the two groups. The detailed breakdown accompanying the table provides insights into the interpretation of each section and the number of questions allocated to ensure a comprehensive and tailored data collection process. The complete questionnaire can be found in Appendix F.

Table 3-1: Questionnaire Description

Section	Description	Items
A: Biographical data	Respondents biographical data e.g. gender.	7
B1: Non-IT employees cybersecurity policy understanding	General cybersecurity policy knowledge questions that cover cybersecurity policy culture and employees' cybersecurity behaviour.	23
B2: IT employees cybersecurity policy understanding	General cybersecurity policy knowledge questions or guide for IT employees regarding the cybersecurity awareness delivery to employees e.g., cybersecurity policy culture, cybersecurity policy awareness delivery methods.	21

The subsequent sections offer comprehensive insights into the process of creating the questions.

Section A: Biographical Data

To facilitate analysis across various moderating factors, the study necessitated the gathering of respondent data. Section A focused on compiling essential personal details from participants through seven (7) mandatory questions. These inquiries sought information on key moderating factors, including gender, age, highest level of education, employment status, financial sector, and duration of work.

Section B1: Non-IT Employees' Cybersecurity Policy Understanding

This section strategically delved into the formulation of research questions aimed at non-IT employees, a group integral to the daily operations of organisations as regular users of computers within their networks. The process of creating these research questions involved a meticulous approach to align them with the overarching research objectives, ensuring they contributed meaningfully to the study.

The research questions directed at non-IT employees were designed to evaluate their knowledge and comprehension of their organisations' cybersecurity policies, shedding light on crucial aspects such as the existence of cybersecurity policy awareness, training initiatives, and the prevailing cybersecurity policy culture. The inclusion of these questions was a deliberate choice, aiming to gather insights that directly connect with the research objective of developing a framework to enhance cybersecurity policy awareness programs influencing employee behaviour in financial institutions.

The section explored specific dimensions, such as cybersecurity policy culture, cybersecurity policy training, cybersecurity policy awareness, and employees' cybersecurity behaviour. Each dimension was carefully addressed through a set of tailored questions. For instance, cybersecurity policy culture was assessed using five (5) items to gauge non-IT employees' awareness of the existing cybersecurity policy landscape within their organisations.

The focus on cybersecurity policy awareness included six (6) items to gauge respondents' perceptions of key cybersecurity policy concepts within their organisational context. Additionally, the section examined employees' cybersecurity behaviour through twelve (12) items, measuring their actions concerning cybersecurity policy aspects, such as password sharing.

It is crucial to highlight that these questions were not arbitrary; rather, they were strategically crafted to address specific facets outlined in the research objectives. The alignment of these questions with the research objectives was further expounded upon during the comprehensive analysis presented in Chapter 4. This ensures that the questions not only contribute to the depth of data collection but also directly support the study's overarching objective of developing a framework for cybersecurity policy awareness programs that influence employee behaviour in financial institutions.

Section B2: IT Employees’ Cybersecurity Policy Understanding

The research questions in this section were crafted considering the unique expertise of IT employees and their role in designing effective cybersecurity policy awareness programs for other employees. It is important to note that these questions were developed by the researcher, emphasising their originality and alignment with the research objectives.

The set of questions for IT employees was designed to explore three key areas: cybersecurity policy culture, cybersecurity policy awareness, and the delivery methods of cybersecurity policy awareness. Cybersecurity policy culture questions delved into the factors influencing the determination of cybersecurity policy awareness for employees, consisting of ten (10) items. The cybersecurity policy awareness section, comprising seven (7) items, aimed to understand the policies or practices organisations employ to educate their employees. Additionally, the questions related to cybersecurity policy awareness delivery methods, consisting of four (4) items, sought to identify the approaches organisations use to educate their employees.

The intention behind these questions was twofold: first, to identify the requirements for a framework that enhances cybersecurity policy awareness programs influencing employee behaviour in financial institutions, and second, to pinpoint components for designing effective cybersecurity policy awareness programs. The originality of these questions underscores their relevance to the research objectives. The analysis of how these questions contribute to achieving the research objectives is detailed in Chapter 4.

3.2.6.6 Questionnaire Distribution

To ensure a representative sample aligned with the population, survey links were shared with designated representatives through intermediaries such as human resources and marketing offices. These representatives were entrusted with disseminating the links to potential respondents. Efforts were made to seek the cooperation of these representatives during the permission request to conduct research in their respective employee groups. Employers chose to take on this role to maintain the anonymity of the study, avoiding the sharing of email addresses of their employees. The survey links were distributed via the email accounts of these representatives, accompanied by guidance on the expected number of responses from each category (non-IT and IT employees). It was communicated that selected respondents would be directed to the questions presented through Google Forms. Appendix F contains the data collection tool utilised in this study.

The initial page of the survey tool featured a concise research summary along with a consent agreement. Respondents expressed their willingness to participate in the research by selecting a mandatory checkbox.

3.2.6.7 Data Analysis

Analysing quantitative data encompasses the handling of outcomes obtained from collecting quantitative data, often presenting them in tabular form, figures, and graphs, and interprets the results using a statistical test (Creswell, 2014). In this study, quantitative data was analysed using descriptive and advanced statistical analysis techniques that are discussed in subsequent sections. The analysis was conducted using SPSS. Descriptive statistics are utilised to display analysed data through various graphical representations such as bar charts, histograms, and pie charts, illustrating the count of respondents based on similar and dissimilar responses (Queirós et al., 2017). The advanced statistical analysis techniques include reliability test, multicollinearity, multinomial logistic regression and classification, which are discussed in the subsequent subsections.

3.2.6.7.1 Reliability of the Measuring Instrument

The reliability test was conducted on the data collection instrument using Cronbach’s alpha and the test was computed using an SPSS. Reliability refers to the extent to which the same measuring instrument can consistently yield the same results on repeated trials of the study quantitatively (Heale and Twycross, 2015; Sürücü and Maslakci, 2020). The Cronbach's alpha is employed for the purpose of evaluating the internal consistency of the scale items by a value ranging from 0 to 1 (Creswell and Creswell, 2018).

3.2.6.7.2 Multicollinearity

Multicollinearity is a statistical phenomenon that occurs when there are strong intercorrelations among two or more independent variables within a multiple regression model (Daoud, 2018). Multicollinearity tests are necessary to ensure the reliability of the statistical model parameters as high inter-correlations among independent variables can distort or mislead the results and lead to instability of said parameters (Daoud, 2018).

When the testing multicollinearity between the variables, the use of the variance inflation factor (VIF) is employed and values greater than 10 imply that there is Multicollinearity (Shrestha, 2020). The VIF is utilised as a tool to assess and quantify the inflation of variance (Daoud, 2018). Shrestha (2020) showed that when the VIF is less than 10, the model used is free from high correlations between the independent variables. To evaluate multicollinearity, the study examined collinearity using two statistics, tolerance and variance inflation factor (VIF) and most details of the measure will be discussed in chapter 4. The VIF was used in this study as necessary initial analysis of multicollinearity as any subsequent regression analysis would produce unreliable regression coefficients if the problem of multicollinearity is not first addressed. Since the VIF is the reciprocal of tolerance, the acceptable threshold for the VIF is tied to the acceptable threshold for tolerance. Therefore, since any VIF>10 is considered problematic, it follows that tolerance below 0.1 indicates multicollinearity (Hair, 2019).

3.2.6.7.3 Multinomial Logistic Regression

Multinomial logistic regression is an expansion of binary logistic regression, specifically designed to accommodate situations where the dependent or outcome variable has more than two categories (Johnson and Christensen, 2020). A multinomial logistic regression model is a method used to analyse categorical data (Bayaga, 2010). This model focuses on a single nominal or ordinal response variable with more than two categories, encompassing both nominal and ordinal variables. In this study, based on the multi-categorical nature of the data, the multinomial logistic regression model is used to assess the level of familiarity of employees in financial institutions in Lesotho with cybersecurity policies and to estimate and predict the probability of cybersecurity knowledge among both non-IT and IT employees.

3.2.6.7.4 Classification

This study uses classification methods to carry out detailed cluster analysis using both the dependent and independent variables. Discriminant or classification techniques aim to categorise samples into groups based on predictor characteristics, but the approach to achieving this varies for each technique. Some techniques, like linear discriminant analysis (LDA), follow a mathematical path, while others, like k-nearest neighbours (KNN), take an algorithmic approach (Kuhn and Johnson, 2013).

To evaluate the differences among the clusters, analysis of variance (ANOVA) was used. The ANOVA procedure is designed to analyse the variation in a set of responses and allocate portions of this variation to each independent variable. Since it is unlikely that all variables affecting the response are included in an experiment, random variation in the responses is observed, even when all considered independent variables are held constant (Wackerly *et al.*, 2008). The main objective of ANOVA is to identify significant independent variables and understand their impact on the response (Wackerly *et al.*, 2008). In this study, the ANOVA results compared the mean z-scores of various predictor variables namely, age, gender, educational attainment, employment status, sector, experience in the sector, cybersecurity induction, existence of reporting procedure and previous cybersecurity training across four numbered clusters.

The study also discusses the application of Discriminant Analysis and Box's M Test (BOX, 1949; Box, 1954) in the context of cybersecurity knowledge classification. Discriminant Analysis was used to examine the differences in mean values of various factors related to cybersecurity knowledge. The aim was to explore the impact of predictor variables on cybersecurity knowledge. Box's Test of Equivalence of Covariance Matrices was conducted to assess whether there were significant differences in the covariance matrices across different levels of cybersecurity knowledge. The test involves analysing the natural logarithms of determinants and ranks of the covariance matrices to understand their structure and singularity.

3.3 Chapter Summary

This chapter presented a thorough review of the entire research methodology. The research procedure was explained through the analogy of the onion metaphor. Additionally, careful examination and explanation were offered for research philosophy, research strategy, and the selection of research methodology. In the chapter, a description of how the data was analysed, is presented. These considerations collectively aid in assessing the appropriateness of the data for subsequent analysis within the study.

CHAPTER 4: DATA ANALYSIS AND RESULTS

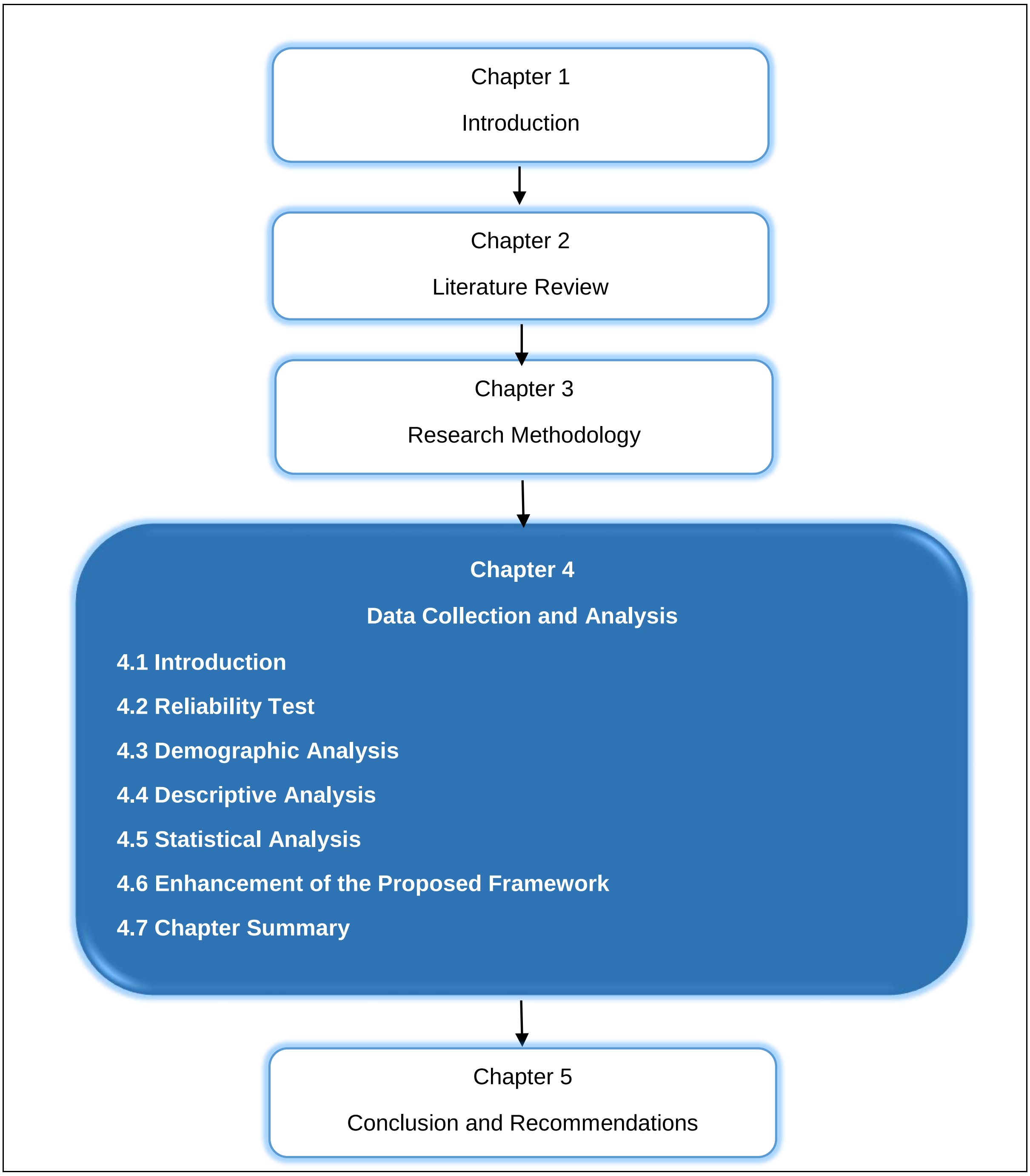


Figure 4-1: Roadmap of Chapter 4

4.1 Introduction

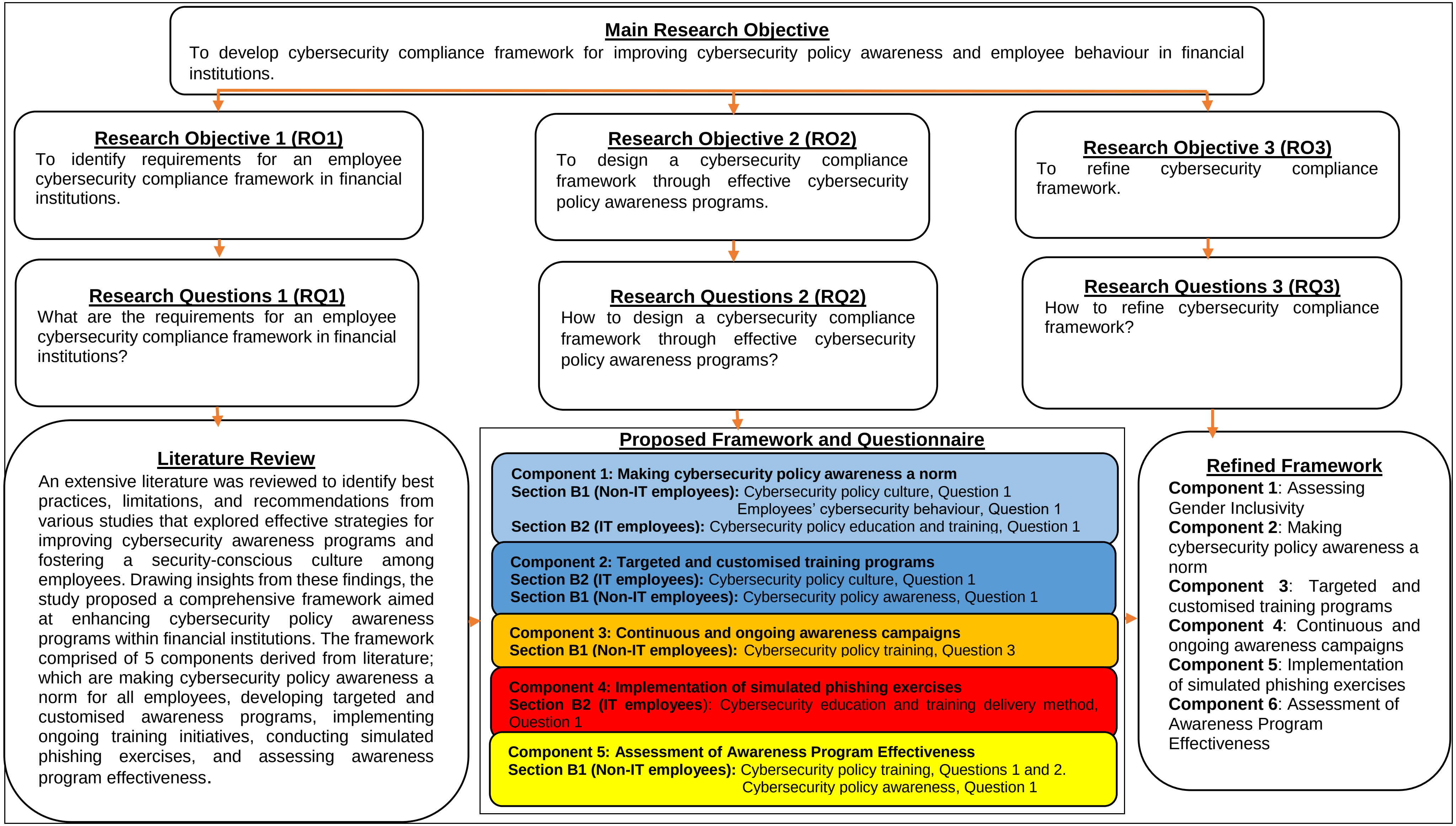
This chapter presents and analyses the survey findings to assess respondents' agreement with the proposed framework.

Data analysis is the systematic process involving the examination of information collected during research (Saunders et al., 2019).The examination encompasses the interpretation and analysis of the data in alignment with the research questions and objectives to generate outcomes that represent the results of measurement (Saunders et al., 2019). This chapter presents how the quantitative data gathered in this academic research was analysed. The primary objective of data analysis is to explore the connections between different constructs (Saunders et al., 2019).It involves applying reasoning to gain insights from the collected data, employing suitable statistical methods to identify consistent patterns, and summarising pertinent information revealed during the research (Saunders et al., 2019).

As shown in Chapter 3, the questionnaire was linked to the research objectives and questions. This linkage ensured that the questions were pertinent, aiding in drawing conclusions about the proposed framework's relevance for developing effective cybersecurity policy awareness programs.

To ensure that the proposed framework aligns with the research objectives and the questionnaire, the framework components were mapped accordingly. Each section of the questionnaire was linked to these components. Figure 4.2 illustrates the mapping of the research objectives, the questionnaire, and the framework. It is evident from Figure 4.2 that the five components of the framework—making cybersecurity policy awareness a norm, targeted and customised training programs, continuous and ongoing awareness campaigns, implementation of simulated phishing exercises, and assessment of awareness program effectiveness are aligned with both the questionnaire and the research objectives of this study.

Regarding the proposed framework, data analysis allows for the refinement of its components based on the collected data. The third research question (RQ3) aimed to refine the cybersecurity compliance framework. Collected data was analysed using the Statistical Package for the Social Sciences (SPSS). Statistical analysis involved identifying factors influencing cybersecurity knowledge, focusing on demographics such as age, education, employment status, and experience. Contrary to initial assumptions, these factors were found to be insignificant. However, a significant gender disparity emerged, with males more likely to possess advanced cybersecurity knowledge. This finding led to a crucial reconsideration of the framework, introducing gender mainstreaming into the initiation phase (becoming the first component of the framework) and integrating gender perspectives throughout the cybersecurity awareness program. The refined framework now comprises six components.



Main Research Objective

To develop cybersecurity compliance framework for improving cybersecurity policy awareness and employee behaviour in financial institutions.

Research Objective 1 (RO1)

To identify requirements for an employee cybersecurity compliance framework in financial institutions.

Research Objective 2 (RO2)

To design a cybersecurity compliance framework through effective cybersecurity policy awareness programs.

Research Objective 3 (RO3)

To refine cybersecurity compliance framework.

Research Questions 1 (RQ1)

What are the requirements for an employee cybersecurity compliance framework in financial institutions?

Research Questions 2 (RQ2)

How to design a cybersecurity compliance framework through effective cybersecurity policy awareness programs?

Research Questions 3 (RQ3)

How to refine cybersecurity compliance framework?

Literature Review

An extensive literature was reviewed to identify best practices, limitations, and recommendations from various studies that explored effective strategies for improving cybersecurity awareness programs and fostering a security-conscious culture among employees. Drawing insights from these findings, the study proposed a comprehensive framework aimed at enhancing cybersecurity policy awareness programs within financial institutions. The framework comprised of 5 components derived from literature; which are making cybersecurity policy awareness a norm for all employees, developing targeted and customised awareness programs, implementing ongoing training initiatives, conducting simulated phishing exercises, and assessing awareness program effectiveness.

Proposed Framework and Questionnaire

Component 1: Making cybersecurity policy awareness a norm
Section B1 (Non-IT employees): Cybersecurity policy culture, Question 1
Employees' cybersecurity behaviour, Question 1
Section B2 (IT employees): Cybersecurity policy education and training, Question 1

Component 2: Targeted and customised training programs
Section B2 (IT employees): Cybersecurity policy culture, Question 1
Section B1 (Non-IT employees): Cybersecurity policy awareness, Question 1

Component 3: Continuous and ongoing awareness campaigns
Section B1 (Non-IT employees): Cybersecurity policy training, Question 3

Component 4: Implementation of simulated phishing exercises
Section B2 (IT employees): Cybersecurity education and training delivery method, Question 1

Component 5: Assessment of Awareness Program Effectiveness
Section B1 (Non-IT employees): Cybersecurity policy training, Questions 1 and 2.
Cybersecurity policy awareness, Question 1

Refined Framework

Component 1: Assessing Gender Inclusivity
Component 2: Making cybersecurity policy awareness a norm
Component 3: Targeted and customised training programs
Component 4: Continuous and ongoing awareness campaigns
Component 5: Implementation of simulated phishing exercises
Component 6: Assessment of Awareness Program Effectiveness

Figure 4-2: Alignment of Research Objectives with the Refined Framework

4.2 Reliability Test

The concept of reliability test assesses the reliability of data collected for research purposes, before further analysis. For this research, the researcher used Cronbach's alpha where Cronbach α scores greater than, 0.7 are considered acceptable reliability (Sürücü and Maslakci, 2020).

Table 4-1: Reliability Results

Number of items in the scale	51
Scale reliability coefficient	0.8944

The reliability results are reported in Table 4-1. The value of the Cronbach's alpha is 0.89, meaning, the available data was reliable enough for further analysis.

4.3 Demographic Analysis

The data shown in Table 4-2 reveals the distribution of respondents by age and gender. Its analysis reveal that the sample used in this research involved 209 respondents made up of 105 females and the rest were males. The sample population is nearly evenly split between males (50.2%) and females (49.8%). The largest age group among this study's respondents was 31 to 40 years, accounting for 56.9% of the total sample. The 18 to 30 years' age group represents the second-largest segment at 23.0%, followed by the 41 to 50 years' age group at 15.8%. The 51 to 65 years and over 65 years' age groups made up smaller proportions at 3.8% and 0.5%, respectively. Gender disparities within age groups showed slight variations, with males slightly outnumbering females in the younger age groups, while females surpassed males in the 41 to 50 years' age group. Notably, the over 65 years' age group had a negligible male representation, with females comprising the entire 0.5% of respondents.

Table 4-2: Distribution of Respondents by Age and Gender

Age Group		**Male**	**Female**	**Total**
18 to 30	Count	26	22	**48**
	% of Total	12.4%	10.5%	**23.0%**
31 to 40	Count	62	57	**119**
	% of Total	29.7%	27.3%	**56.9%**
41 to 50	Count	13	20	**33**
	% of Total	6.2%	9.6%	**15.8%**
51 to 65	Count	4	4	**8**
	% of Total	1.9%	1.9%	**3.8%**
Over 65	Count	0	1	**1**
	% of Total	0.0%	0.5%	**0.5%**
	Total Count	**105**	**104**	**209**
	% of Total	**50.2%**	**49.8%**	**100.0%**

The data in Table 4-3 reveals distribution of respondents by department, gender, and highest level of education. The majority of respondents (86.6%) belonged to non-IT departments, while those from IT departments represented a smaller proportion (13.4%). Gender disparities within departments show that male respondents slightly exceeded female respondents in non-IT Departments (41.6% vs. 45.0%), while in IT departments, the males outnumbered their female (8.6% vs. 4.8%) counterparts. The most prevalent highest level of education was a bachelor's degree, followed by an associate degree, across all departments. Other qualifications such as master's degrees, honour's degrees, diplomas, and no formal education, also had varying representation.

Table 4-3: Distribution of Respondents by Department & Gender and Highest Level of Education

		Gender					
		Male		Female		Total	
		Count	Table N %	Count	Table N %	Count	Table N %
IT	No Formal Education	2	1.0%	0	0.0%	2	1.0%
	Certificate	0	0.0%	0	0.0%	0	0.0%
	Diploma	1	0.5%	0	0.0%	1	0.5%
	Associate Degree	0	0.0%	2	1.0%	2	1.0%
	Bachelor's Degree	5	2.4%	5	2.4%	10	4.8%
	Professional Qualification	0	0.0%	0	0.0%	0	0.0%
	Honours Degree	5	2.4%	0	0.0%	5	2.4%
	Master's Degree	5	2.4%	3	1.4%	8	3.8%
	IT Total	18	8.6%	10	4.8%	28	13.4%
Non-IT	No Formal Education	0	0.0%	3	1.4%	3	1.4%
	Certificate	1	0.5%	1	0.5%	2	1.0%
	Diploma	5	2.4%	12	5.7%	17	8.1%
	Associate Degree	10	4.8%	15	7.2%	25	12.0%
	Bachelor's Degree	47	22.5%	45	21.5%	92	44.0%
	Professional Qualification	7	3.3%	3	1.4%	10	4.8%
	Honours Degree	10	4.8%	10	4.8%	20	9.6%
	Master's Degree	7	3.3%	5	2.4%	12	5.7%
	Non-IT Total	87	41.6%	94	45.0%	181	86.6%
	Grand Total	**105**	**50.2%**	**104**	**49.8%**	**209**	**100%**

Table 4-4 reveal distribution of respondents by years of experience and gender. When taking into account the duration of experience within the industry, the data shows that the female participants had a higher representation (31.6%) than males (21.1%) among respondents with more than 5 years of experience. This finding suggests that females had a notable presence in senior positions within the industry. However, further research is needed to explore the factors contributing to this gender distribution across different experience levels.

Table 4-4: Distribution of Respondents by Years in Industry and Gender

Experience	Gender					
	Male		Female		Total	
	Count	Table N %	Count	Table N %	Count	Table N %
Less than a year	9	4.3%	3	1.4%	12	5.7%
1 to 3 years	28	13.4%	20	9.6%	48	23.0%
4 to 5 years	24	11.5%	15	7.2%	39	18.7%
More than 5 years	44	21.1%	66	31.6%	110	52.6%
Total	**105**	**50.2%**	**104**	**49.8%**	**209**	**100.0%**

Table 4-5 provides insights into the distribution of respondents by industry and gender. Among the various industries represented, insurance companies had the highest overall participation, accounting for 53.6% of the total sample, with females (27.8%) slightly outnumbering males (25.9%). Commercial banks and forex agencies also showed a significant representation, comprising 23.4% of the respondents, with a slightly higher proportion of females (11.5%) compared to males (12.0%). Other industries exhibited relatively lower participation rates. These findings highlight the gender distribution within different sectors and can contribute to a better understanding of gender representation in specific industries. Further research is necessary to explore the factors influencing these patterns and their implications for gender equality in the workplace.

Table 4-5: Distribution of Respondents by Industry and Gender

Industry	Gender					
	Male		Female		Total	
	Count	Table N %	Count	Table N %	Count	Table N %
Central Banking	6	2.9%	1	0.5%	7	3.3%
Commercial Banks and Forex Agencies	25	12.0%	24	11.5%	49	23.4%
Insurance Brokers	5	2.4%	11	5.3%	16	7.7%
Insurance Companies	54	25.9%	58	27.8%	112	53.6%
Mobile Money	0	0.0%	1	0.5%	1	0.5%
Asset Managers	8	3.8%	2	1.0%	10	4.8%
Financial Institutions & Insurance Regulator	0	0.0%	1	0.5%	1	0.5%
Investment	0	0.0%	1	0.5%	1	0.5%
Pensions Regulator	1	0.5%	1	0.5%	2	1.0%
FinTech	1	0.5%	0	0.0%	1	0.5%
Insurance Broker	1	0.5%	0	0.0%	1	0.5%
Micro Finance Institutions	1	0.5%	0	0.0%	1	0.5%
Assurance Services	1	0.5%	0	0.0%	1	0.5%
Finance	0	0.0%	1	0.5%	1	0.5%
Min of Finance	0	0.0%	1	0.5%	1	0.5%
Money Transfer Institution	2	1.0%	2	1.0%	4	1.9%
Total	**105**	**50.2%**	**104**	**49.8%**	**209**	**100.0%**

4.4 Descriptive Analysis

The study’s objective was to develop a framework for improving cybersecurity policy awareness programs to enhance employee behaviour toward cybersecurity compliance in financial institutions. Both IT and non-IT employees were selected because they were considered as users of systems and networks in their daily job activities, making them relevant to evaluate the effectiveness of CSPAP. The large representation of non-IT users was due to their prevalence across various departments, while IT employees were chosen for their cybersecurity expertise. The years of service were also considered as a differentiating factor in evaluating CSPAP effectiveness.

4.4.1 Perceptions

This section presents perceptions of non-IT employees about the cybersecurity posture of their organisations as well as presentation of underlying dynamics and interactions of these behaviours as informed by the data. Table 4-6 provides an analysis of the distribution of non-IT respondents based on their perceptions of their organisations regarding cybersecurity. The table presents data in terms of counts and percentages for each perception category.

In terms of working with confidential information, the results indicate that a significant majority of the respondents (64.3%) strongly agreed that they worked with confidential information. This suggests that a large portion of the participants recognised the sensitivity and importance of the information they handled. Additionally, 20.9% of respondents agreed, indicating a general acknowledgment of the presence of confidential information within their organisations. On the other hand, a smaller proportion of respondents (8.8%) strongly disagreed, while 4.9% remained neutral, and only 1.1% disagreed. These findings highlight the overall awareness and understanding of the confidential nature of the data handled within the organisations surveyed.

Regarding the perception of technical controls within their organisations, approximately half of the respondents (50.0%) agreed that their organisations had technical controls in place to enhance cybersecurity. This indicates that a considerable number of participants perceived the presence of measures and systems implemented to safeguard against cyber threats. Meanwhile, 32.4% of respondents agreed, 6.0% remained neutral, 1.6% disagreed, and 9.9% strongly disagreed. These results suggest that while most of the respondents perceived the existence of technical controls, a notable percentage either had doubts or were unaware of such measures.

Table 4-6: Distribution of Respondents by Different Perceptions of their Organisations Regarding Cybersecurity

Perceptions		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Working with confidential information	Count	16	2	9	38	117	182
	Percent	8.8%	1.1%	4.9%	20.9%	64.3%	100%
Organisation has technical controls	Count	18	3	11	59	91	182
	Percent	9.9%	1.6%	6.0%	32.4%	50.0%	100%
Everyone in org. knows how to protect confidential	Count	16	21	48	73	24	182
	Percent	8.8%	11.5%	26.4%	40.1%	13.2%	100%
Everyone in org. wants to protect confidential info	Count	15	14	23	75	55	182
	Percent	8.2%	7.7%	12.6%	41.2%	30.2%	100%
Everyone in org. thinks cybersecurity is important.	Count	14	12	34	72	50	182
	Percent	7.7%	6.6%	18.7%	39.6%	27.5%	100%
Everyone in org. complies with cybersecurity policies	Count	14	25	49	65	29	182
	Percent	7.7%	13.7%	26.9%	35.7%	15.9%	100%

The perception of whether everyone in the financial institution knew how to protect confidential information revealed a varied response. Only 8.8% of respondents strongly disagreed, indicating that a small minority believed that everyone in their financial institution lacked the necessary knowledge to protect confidential information. In contrast, a larger proportion of respondents (40.1%) agreed, suggesting that a significant portion of participants believed that their colleagues possessed the required knowledge. However, a substantial percentage (26.4%) remained neutral, indicating uncertainty or lack of awareness among respondents. Additionally, 11.5% disagreed, and 13.2% strongly agreed, reflecting differing perceptions within the surveyed financial institutions.

When considering the perception of whether everyone in the financial institution wanted to protect confidential information, the results show a similar pattern. Approximately 30.2% of respondents strongly agreed that everyone in their financial institution had the desire to protect confidential information, while 41.2% agreed. On the contrary, 8.2% strongly disagreed and 7.7% disagreed, indicating a smaller proportion of respondents who believed that not everyone shared this desire. Furthermore, 12.6% of respondents remained neutral, signifying uncertainty or lack of knowledge about their colleagues' intentions.

The perception of whether everyone in the financial institutions thought cybersecurity was important also exhibited varying viewpoints. Among the respondents, 39.6% agreed that everyone in their financial institution acknowledged the importance of cybersecurity. Moreover, 27.5% strongly agreed, suggesting a substantial number of participants who perceived a shared understanding of the significance of cybersecurity. Conversely, 18.7% remained neutral, indicating a lack of consensus or awareness within the financial institutions. Additionally, 7.7% disagreed and 6.6% strongly disagreed, indicating the presence of dissenting opinions regarding the perceived importance of cybersecurity.

Finally, the perception of whether everyone in the financial institutions complied with cybersecurity policies reflected mixed responses. Approximately 35.7% of respondents agreed that everyone in their financial institutions complied with cybersecurity policies, while 26.9% remained neutral. On the other hand, 15.9% strongly disagreed, 13.7% disagreed, and 7.7% strongly agreed. These findings highlight a lack of consensus among respondents regarding the level of compliance with cybersecurity policies within their financial institutions.

Overall, the analysis of respondents' perceptions regarding their financial institutions' cybersecurity policies reveals a range of viewpoints. While a significant proportion of participants recognised the presence of confidential information and the importance of cybersecurity, there were variations in perceptions regarding technical controls, knowledge levels, intentions, and compliance within the surveyed organisations. These findings emphasise the need for financial institutions to foster a shared understanding of cybersecurity importance, provide comprehensive awareness programs, and establish clear policies to ensure consistent compliance across the board.

Furthermore, the data on correlation, as shown in the table below (Table 4-7), presents relationships between various perceptions of IT employees towards cybersecurity issues in their respective financial institutions. Several notable correlations emerged from the table.

This analysis explores correlations between different perceptions of respondents regarding their financial institutions' cybersecurity practices. The data presented in Table 4-7 reveal relationships between various factors such as working with confidential information, the presence of technical controls, knowledge of protecting confidential information, willingness to protect confidential information, perception of the importance of cybersecurity, and compliance with cybersecurity policies. Understanding these correlations provides valuable insights into the financial institutions’ dynamics surrounding cybersecurity.

Table 4-7: Correlation of Different Perceptions of Respondents about their Organisations Regarding Cybersecurity

	Working with confidential information	**Org. has technical controls**	**Everyone in org. knows how to protect confidential info**	**Everyone in org. wants to protect confidential info**	**Everyone in org. thinks cybersecurity is important.**	**Everyone in org. complies with cybersecurity policies**	**1.00**
Working with confidential information	1.00						
Org. has technical controls	0.86**	1					
Everyone in org. knows how to protect confidential info	0.53**	0.63**	1				
Everyone in org. wants to protect confidential info	0.75**	0.79**	0.71**	1			
Everyone in org. thinks cybersecurity is important.	0.73**	0.78**	0.68**	0.87**	1		
Everyone in org. complies with cybersecurity policies	0.53**	0.67**	0.78**	0.74**	0.75**	1	**-1.00**

Notes: The correlation coefficients range from -1.00 to 1.00, with 1.00 indicating a perfect positive correlation, -1.00 indicating a perfect negative correlation, and 0 indicating no correlation. The gradient colours ranging from light green to deeper green the closer to +1.00 the correlations get.

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

The correlation between working with confidential information and the financial institutions having technical controls is strong and positive (r = 0.86). This finding suggests that organisations that deal with confidential information are more likely to implement technical controls to safeguard that information. The presence of these controls reflects an organisational commitment to protecting sensitive data and aligning security measures with the nature of information handled.

Furthermore, respondents who reported that everyone in their financial institutions knew how to protect confidential information also indicated a positive correlation with the organisation having technical controls (r = 0.63). This finding suggests that financial institutions that prioritise educating their employees about protecting confidential information are more likely to have implemented technical controls to reinforce security measures as well. This correlation highlights the importance of combining technical controls with a knowledgeable workforce to create a comprehensive cybersecurity environment.

The perception that everyone in the selected financial institutions wanted to protect confidential information demonstrates a positive correlation with both the presence of technical controls (r = 0.79) and the belief that cybersecurity was important (r = 0.71). This indicates that financial institutions fostering a culture where employees were motivated and committed to safeguarding confidential information were more likely to have implemented technical controls and prioritise cybersecurity. The positive correlations emphasise the significance of creating an organisational climate that promotes a shared responsibility for cybersecurity and aligning employees' attitudes and beliefs with the organisation's security goals.

The perception that everyone in the financial institutions thought cybersecurity was important also showed a positive correlation with the belief that everyone complied with cybersecurity policies (r = 0.75). This suggests that when employees recognise the importance of cybersecurity, they are more likely to adhere to established policies and procedures. The positive correlation underscores the role of cybersecurity awareness and the alignment of organisational values in promoting policy compliance and reinforcing a secure environment.

Lastly, the perception of everyone in the financial institutions complied with cybersecurity policies demonstrated a positive correlation with both the belief that everyone knew how to protect confidential information (r = 0.67) and the perception that everyone wanted to protect confidential information (r = 0.78). This indicates that financial institutions with a strong culture of policy compliance are more likely to have employees who possess the knowledge and motivation to protect sensitive information. The positive correlations emphasise the interplay between policy adherence, knowledge, and motivation in creating a cohesive cybersecurity culture within the organisation.

In conclusion, the analysis of correlations among perceptions regarding cybersecurity provides valuable insights into financial institutions’ cybersecurity posture. Factors such as working with confidential information, technical controls, knowledge, motivation, beliefs about cybersecurity importance, and policy compliance are interrelated. Financial institutions can leverage these findings to develop comprehensive cybersecurity strategies that include technical controls, employee education, and a culture of shared responsibility. By recognising and addressing these interrelationships, financial institutions can enhance their ability to protect confidential information and mitigate cyber threats effectively.

The analysis emphasises the need for targeted and customised training programs in cybersecurity. The analysis reveals that the respondent employees had diverse perceptions regarding their financial institutions’ cybersecurity practices, including knowledge, willingness, and importance of cybersecurity. This highlights the importance of tailored training programs that address these varying perceptions and provide employees with the necessary knowledge and skills based on their specific roles and responsibilities. Continuous awareness campaigns are also crucial to regularly update and refresh training programs and reinforce cybersecurity principles, enhancing employee awareness and readiness to tackle cybersecurity risks. Additionally, the analysis indirectly highlights the importance of evaluating the effectiveness of training and awareness programs by examining correlations between different perceptions.

4.4.2 Current Practices

The data in Figure 4-3 provides insights into the frequency of non-IT employees engaging in potentially dangerous web, app, and device habits and activities related to cybersecurity. It is encouraging to see that sharing PC logins and app logins are infrequent behaviours, with a majority of respondents (87.9% and 88.4% respectively) reporting that they never engaged in these activities. This indicates a general understanding of the importance of personal account security.

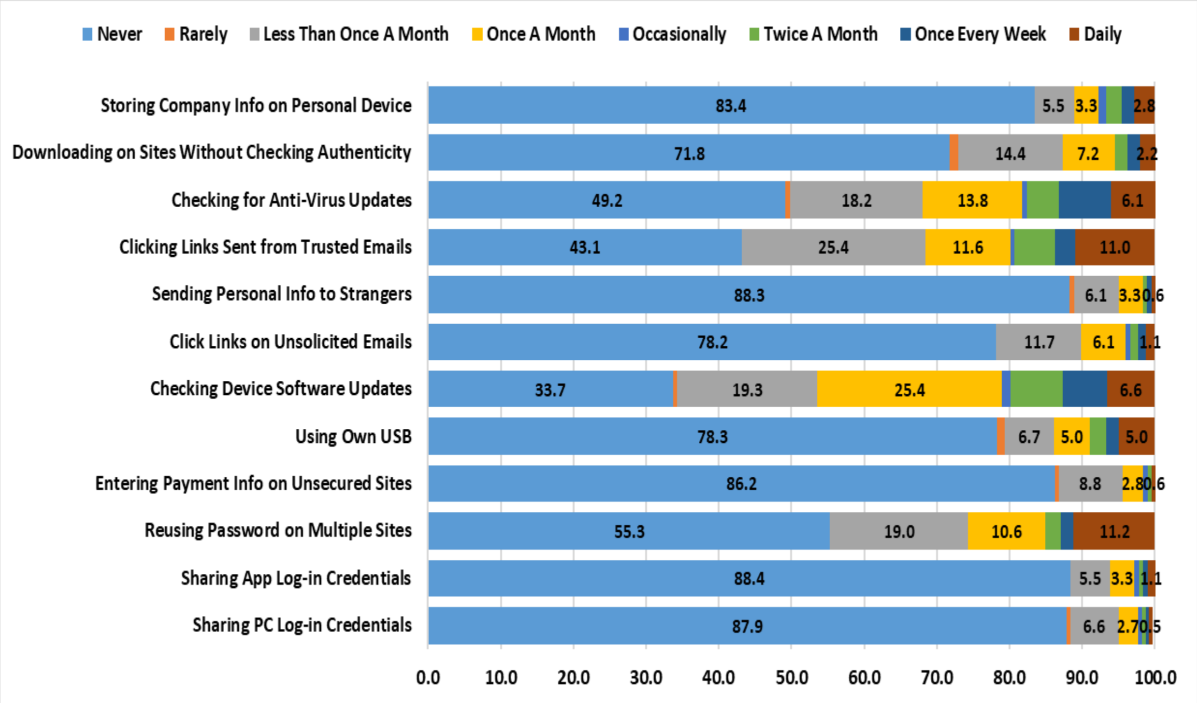


Figure 4-3: Frequency of Engaging in Potentially Dangerous Web, App and Device Habits and Activities

However, the data reveals a concerning trend in the reuse of passwords on multiple sites, with 55.3% of respondents admitting to this behaviour. This practice poses a significant cybersecurity risk, as a compromised password could potentially grant unauthorised access to multiple accounts. Financial institutions should prioritise password management education and encourage the use of unique and strong passwords for each online account.

When it comes to entering payment information on unsecured sites, the majority of respondents (86.2%) reported that they never engaged in this behaviour. This is a positive finding, as entering sensitive payment information on unsecured websites can expose individuals to the risk of financial fraud or identity theft. However, the small percentage of respondents (8.8%) who reported occasional occurrences highlights the need for ongoing awareness and education on secure online transactions.

Another concern was behaviour involving the practice of bringing personal USB devices to transfer data, which was reported by 21.7% of respondents. This behaviour poses a potential security risk, as these devices can introduce malware or unauthorised data transfers into an organisation's network. Financial institutions should implement policies and provide secure alternatives for data transfer to mitigate this risk.

On a positive note, a considerable proportion of respondents (33.7%) reported checking for software updates on their devices. Regular software updates are crucial for addressing security vulnerabilities and protecting against emerging threats. However, the percentage of respondents (25.4%) who reported checking for updates only once a month suggests that there is room for improvement in promoting more frequent software updates.

Phishing attacks remain a persistent threat, and the data shows that the majority of respondents (78.2%) reported that they never clicked on links from unsolicited emails. This is a positive finding, indicating a level of awareness and caution regarding email security. Nevertheless, the small percentage (11.7%) of respondents who reported occasional occurrences emphasises the need for ongoing education to reinforce safe email practices and help individuals identify phishing attempts.

While the majority of respondents (88.3%) reported that they never sent personal information to strangers, a small percentage (6.1%) admitted to doing so occasionally. This highlights the importance of promoting privacy awareness and educating individuals about the risks associated with sharing personal information with unknown parties. Financial institutions should emphasise the need to verify the identity and trustworthiness of recipients before sharing any sensitive information.

In conclusion, the analysis reveals both positive and concerning trends in non-IT employees' cybersecurity behaviours. While certain risky behaviours such as sharing logins or entering payment information on unsecured sites were relatively infrequent, other behaviours such as password reuse or bringing personal USB devices, were more prevalent. This underscores the need for ongoing education and awareness campaigns to reinforce secure practices and mitigate potential risks. Additionally, financial institutions should establish clear policies and provide secure alternatives to minimise the occurrence of risky behaviours and promote a culture of cybersecurity policy awareness.

The correlation data shown in table 4-8 below reveals some inter-relationships among the listed specific cybersecurity aspects. Notably, a moderate positive correlation of 0.60 is found between sharing computer log-in passwords with friends and/or colleagues and sharing application/system passwords with them. This suggests that individuals who engage in the behaviour of sharing computer log-in credentials are also more likely to share application/system passwords. This finding highlights a potential correlation between these two risky practices, indicating a pattern of insecure password sharing among individuals.

Table 4-8: Correlations of Different Unsafe Practices and Habits

	Share Comp Pass	Share App Pass	Same Pass Web	Enter Unsec Web	Bring USB	Check Soft Update	Click Unsol Email	Send Pers Info	Click Trusted Email	Check AV Update	Download Unauth Data	Store Comp Info
Share Comp Pass	1											
Share App Pass	0.6	1										
Same Pass Web	0.11	0.03	1									
Enter Unsec Web	0.1	0.13	0.28	1								
Bring USB	0.08	0	0.08	0.05	1							
Check Soft Update	0.02	0.03	0.08	-0.05	0.22	1						
Click Unsol Email	0.15	0.06	0.06	0.07	0.14	0.11	1					
Send Pers Info	0.09	0.1	0.27	0.45	0.26	0.08	0.21	1				
Click Trusted Email	0.13	0.02	0.27	0.02	-0.01	0.19	0.2	0.18	1			
Check AV Update	0.16	0.12	0.1	-0.06	0.28	0.46	0.18	0.19	0.18	1		
Download Unauth Data	0.18	0.03	0.44	0.3	0.24	0.02	0.27	0.42	0.31	0.11	1	
Store Comp Info	0.09	0.07	0.25	0.2	0.32	0.09	0.2	0.38	0.14	0.07	0.44	1

1.00

-1.00

Notes: The correlation coefficients range from -1.00 to 1.00, with 1.00 indicating a perfect positive correlation, -1.00 indicating a perfect negative correlation, and 0 indicating no correlation.

The color gradient on the right side of the table illustrates the range of the correlation coefficient from -1 to 1. Strong correlations are represented by vibrant shades of red or green, while moderate correlations are depicted in various shades of amber.

Additionally, there was a weak positive correlation of 0.28 observed between using the same password for multiple websites and entering payment information on unsecured websites. This suggests that individuals who engage in the unsafe practice of reusing passwords across multiple websites may also exhibit some tendency to enter their payment information on websites that do not provide adequate security measures. This correlation underscores the importance of promoting password hygiene and emphasising the risks associated with using the same password across multiple online platforms.

Furthermore, results of this study showed a weak positive correlation of 0.44 between downloading data and material from websites on a work computer without checking its authenticity and using the same password for multiple websites. This suggests that individuals who engage in the risky behaviour of downloading data without verifying its authenticity may be also inclined to reuse passwords across multiple websites. This correlation highlights the potential overlap between these unsafe practices and emphasises the need for caution when handling downloaded content and reinforcing the importance of using unique passwords for different online accounts.

Another noteworthy correlation is the weak positive association of 0.38 between storing company information on a personal electronic device (e.g., smartphone/tablet/laptop) and checking for updates to antivirus software. This correlation suggests that individuals who store company information on their personal devices may also exhibit a moderate level of awareness and diligence in keeping their antivirus software up to date. It indicates a potential link between responsible data handling practices and proactive cybersecurity measures.

The analysis suggests that certain unsafe practices tend to co-occur, highlighting the need for comprehensive approaches to address multiple aspects of cybersecurity. By understanding these relationships, organisations and individuals can develop more effective strategies and interventions to promote safer online practices and mitigate the risks associated with these correlated behaviours. Most of the correlations are moderate to low and not statistically significant, however, this does not mean that unsafe practices should be ignored even if occurring in relatively small amounts.

The analysis focuses on current practices related to cybersecurity policies awareness. The analysis highlights the need for targeted awareness programs in areas such as password management and secure online transactions. Furthermore, the analysis suggests tailoring training programs to educate individuals about the risks of insecure password practices and promoting the use of unique and strong passwords. Continuous awareness programs are also necessary to reinforce safe online transaction practices. Lastly, the analysis emphasises the importance of assessing employee knowledge and behaviours to identify areas for improvement and make informed decisions on awareness program effectiveness.

4.4.3 Design of Training Programs

Effective cybersecurity policy training programs are vital for organisations to enhance their employees' knowledge and skills in safeguarding against evolving cyber threats. Designing such programs requires careful consideration of various factors. Table 4-9 explores the perspectives of IT employees on critical factors to consider in the design of cybersecurity policy training programs.

Table 4-9: Views of IT Employees on Factors to Consider in the Design of Cybersecurity Training Programs for Employees

Factors to Consider in Designing Training Programs		**Don't Know**	**No**	**Yes**
Make staff training a strategic priority	Count	0	1	26
	Percent	0.0%	3.7%	96.3%
Collaborate with HR & I-O Specialists	Count	5	3	19
	Percent	18.5%	11.1%	70.4%
Use interdisciplinary team to develop training programs	Count	2	2	23
	Percent	7.4%	7.4%	85.2%
Survey bellwether best practices in designing training programs	Count	7	3	17
	Percent	25.9%	11.1%	63.0%
Establish level-specific job & cybersecurity tasks for employees	Count	2	6	19
	Percent	7.4%	22.2%	70.4%
Determine whether employees are currently performing required cybersecurity tasks.	Count	0	4	23
	Percent	0.0%	14.8%	85.2%
Training Objectives: Align knowledge, skills and attitudes with task demands	Count	0	2	25
	Percent	0.0%	7.4%	92.6%
Choose appropriate venues & methods for learning objectives and conduct training.	Count	1	8	18
	Percent	3.7%	29.6%	66.7%
Assess education and training results to gauge whether objectives are met.	Count	2	2	23
	Percent	7.4%	7.4%	85.2%
Adapt education and training initiatives or shift to non-training solutions	Count	3	2	22
	Percent	11.1%	7.4%	81.5%

Notes: IT employees are specifically targeted by this part of the study for their level of expertise in the subject area.

A notable finding from the data is the overwhelming agreement among IT employees (96.3%) that employees' cybersecurity policy training should be a strategic priority. This recognition indicates a deep understanding of the need to integrate cybersecurity policy training initiatives into the broader organisational strategy. By prioritising employees training, organisations can ensure that cybersecurity awareness and skills development receive the necessary attention and resources.

Approximately 70.4% of IT employees acknowledged the value of collaborating with Human Resources specialists (HR) and Industrial Organisation (I-O) specialists in the design of training programs. This perspective highlights an understanding of the expertise these professionals bring to the table, particularly in areas such as instructional design, performance analysis, and employee engagement. Such collaboration can ensure that cybersecurity policy training programs are tailored to meet the specific needs of employees and effectively address financial institutions goals.

The data reveals that 85.2% of IT employees believed in the importance of using interdisciplinary teams in developing training programs. This perspective aligns with best practices in instructional design, as it allows for a holistic approach that draws on diverse perspectives and expertise. Involving professionals from different disciplines, such as IT, HR, and Industrial Organisation, can contribute to the development of comprehensive and effective cybersecurity training programs.

Moreover, approximately 63.0% of IT employees considered surveying bellwether best practices in designing training programs as an essential factor. This viewpoint demonstrates a recognition of the value of learning from established practices and industry benchmarks. By surveying and incorporating best practices into the design of cybersecurity policy training programs, financial institutions can benefit from the collective wisdom and experience of the field, ensuring that their training initiatives are up to date and effective.

A significant majority (70.4%) of IT employees emphasise the importance of establishing level-specific job roles and cybersecurity tasks for employees. This perspective underscores the need for tailored training programs that align with the specific roles and responsibilities of employees. By tailoring training content to address the unique cybersecurity challenges faced by different job roles, organisations can provide targeted and relevant training that enhances employee skills and preparedness.

The data also reveals the perspectives of IT employees on the assessment and adaptation of training programs. Approximately 85.2% of respondents considered it important to assess education and training results to gauge whether objectives were met. This viewpoint highlights the significance of evaluating the effectiveness of training initiatives and making informed decisions based on the assessment outcomes. Additionally, 81.5% of IT employees believe in the importance of adapting training initiatives or shifting to non-training solutions when necessary. This perspective demonstrates a willingness to evolve and explore alternative approaches if training programs are not yielding the desired outcomes.

In conclusion, the analysis of IT employees' views on factors for designing cybersecurity policy training programs highlights key insights. The data indicates consensus on strategic employees’ training, collaboration with HR and I-O specialists, interdisciplinary teams, best practice incorporation, and level-specific roles and tasks. Assessment of training results and adaptability also enhance program effectiveness. Considering these perspectives, organisations can develop tailored training initiatives that address employee needs and bolster cybersecurity.

Table 4-10 provides some insights into the correlations between different factors considered in the design of cybersecurity training programs for employees, based on the perspectives of IT employees. By examining these correlations, researchers gain a deeper understanding of the interrelationships among key factors and their implications for effective cybersecurity training initiatives.

One of the most significant positive correlations identified was that between the prioritisation of cybersecurity training as a strategic organisational priority and the alignment of training objectives with the specific knowledge, skills, and attitudes required for effective cybersecurity practices (0.69). This strong positive correlation highlights the importance of financial institutions recognising the strategic significance of cybersecurity training and ensuring that training objectives are closely aligned with the practical demands of the job. When financial institutions view cybersecurity training as a strategic priority, they are more likely to invest in developing training programs that are directly relevant and effective in addressing the unique challenges of their workforce.

Table 4-10: Correlation of Factors in Designing Cybersecurity Training Programs for Employees: IT Employees Views

	Strategic Priority	HR Collaboration	Inter-disciplinary Teamwork	Best Practices Integration	Task Alignment	Performance Evaluation	Objective Alignment	Learning Approaches	Results Assessment	Adaptation Strategies	1.00
Strategic Priority	1										
HR Collaboration	0.38	1									
Inter-disciplinary Teamwork	-0.08	-0.16	1								
Best Practices Integration	0.08	0.04	0.39	1							
Task Alignment	0.2	0.24	0.19	0.12	1						
Performance Evaluation	0.47	0.01	-0.16	0.18	0.26	1					
Objective Alignment	0.69	0.19	-0.11	0.12	0.29	0.68	1				
Learning Approaches	0.22	0.02	0.68	0.44	0.14	0.1	0.07	1			
Results Assessment	0.27	0.26	0.08	0.24	0.51	0.02	0.14	0.21	1		
Adaptation Strategies	0.21	0.15	0.42	0.32	0.46	0.13	0.3	0.41	0.72	1	-1.00

Notes: The correlation coefficients range from -1.00 to 1.00, with 1.00 indicating a perfect positive correlation, -1.00 indicating a perfect negative correlation, and 0 indicating no correlation.

There is also a high correlation between objective alignment and performance evaluation (0.68) in designing training programs. The high correlation between designing training objectives to align with task demands and determining whether employees are performing required cybersecurity tasks underscores the necessity of clear, task-oriented training objectives. This relationship indicates that well-defined training objectives are associated with more effective performance evaluation, ensuring that employees' cybersecurity practices meet financial institutions requirements.

Furthermore, a strong positive correlation exists between, learning approaches and interdisciplinary teamwork (0.68). The strong positive correlation between choosing appropriate venues and methods for learning objectives and assembling an interdisciplinary team indicates that diverse and innovative learning approaches are more effective when developed through collaborative efforts across different departments. This emphasises the value of interdisciplinary teamwork in enhancing the effectiveness of cybersecurity training programs.

Also, there is a strong positive correlation between results assessment and adaptation strategies (0.72). A significant positive correlation between assessing training results and adapting education and training initiatives or shifting to non-training solutions highlights the importance of a robust feedback loop. Effective assessment of training outcomes drives continuous improvement and adaptation of training programs, ensuring they remain relevant.

Collaboration with Human Resources (HR) specialists and Industrial-Organisational (I-O) psychologists also emerges as a crucial factor in promoting the recognition of cybersecurity training as a strategic priority (0.38). This positive correlation suggests that involving HR specialists and I-O psychologists in the development and implementation of cybersecurity training programs can generate and sustain organisational support for these initiatives. Leveraging their expertise in areas such as talent management, employee engagement, and organisational behaviour can contribute to enhanced and successful integration of cybersecurity training into the culture and overall effectiveness of financial institutions.

The positive correlations between surveying industry’s best practices and both aligning training objectives with task demands (0.39) and choosing suitable venues and methods for learning (0.44) indicate the value of incorporating external benchmarks and insights into the design of cybersecurity training. Organisations that actively survey and integrate bellwether cybersecurity practices into their training programs are better positioned to align their training objectives with the specific needs and requirements of their employees. Additionally, by selecting appropriate venues and methods for learning, organisations can optimise the training experience and enhance knowledge retention and skills development among employees.

Furthermore, the positive correlation between the establishment of level-specific job and cybersecurity tasks and the recognition of cybersecurity training as a strategic priority (0.20) highlights the importance of clearly defining job roles and responsibilities related to cybersecurity. When financial institutions define specific tasks and expectations for employees in this domain, they are more likely to recognise and prioritise the need for comprehensive cybersecurity training. This correlation underscores the importance of job design and task clarity in driving organisational commitment to cybersecurity training initiatives.

In addition to positive correlations, the presence of negative correlations below -0.1 suggests potential trade-offs or competing priorities. Specifically, the negative correlation between assembling an interdisciplinary team to develop comprehensive cybersecurity training and the other factors ($-0.1 < r < 0.1$) indicates that organisations emphasising interdisciplinary collaboration may not prioritise other factors as strongly. While the negative correlations are relatively weak, further investigation is required to fully understand the underlying dynamics driving this behaviour.

Overall, these correlations shed light on the complex web of factors that financial institutions need to consider when designing cybersecurity training programs for their employees. The findings emphasise the importance of strategic prioritisation (0.68), collaboration with HR specialists and I-O psychologists (0.38), integration of industry best practices (0.39, 0.44), task-specific training (0.20), and performance evaluation in developing effective training initiatives. By recognising and leveraging these interrelationships, organisations can enhance their cybersecurity training programs, cultivate a culture of security awareness, and better equip their employees to mitigate cyber threats effectively.

The analysis provides comprehensive insights into multiple facets of the proposed framework for enhancing cybersecurity policy awareness programs. It emphasises the strategic importance of making cybersecurity policy awareness a norm, underlining the need to prioritise these initiatives across an organisation. Furthermore, the analysis underscores the significance of targeted and customised training programs that cater to the specific needs and responsibilities of employees, ensuring that training aligns with job roles and addresses relevant cybersecurity challenges. The analysis also highlights the value of embarking on continuous awareness campaigns, stressing the need to regularly update and refresh training programs to stay abreast of evolving threats and industry best practices. Additionally, the analysis emphasises the importance of assessing the effectiveness of awareness programs, enabling financial institutions to gauge knowledge, skills, and attitudes towards cybersecurity and make necessary adaptations.

4.4.4 Policy or Practice Areas

This analysis examines the training practices of financial institutions in various policy and practice areas, based on data obtained from the respondent IT employees. The data, presented in Table 4-11 reveals crucial perspectives into the training priorities and time horizons for implementation within the financial institutions.

Table 4-11: Policy or Practice Areas on Which Financial Institutions Train Employees as per IT Employees

Policy/Practice Areas		**Never**	**Do Not know**	**2 Years or Less**	**One Year or Less**	**Six Months or Less**	**Currently Implemented**
Restricted sites and download training (or time horizon for	Count	0	1	2	0	2	22
	Percent	0.0%	3.7%	7.4%	0.0%	7.4%	81.5%
Acceptable-use policy training or time horizon for	Count	0	4	0	1	3	18
	Percent	0.0%	15.4%	0.0%	3.8%	11.5%	69.2%
Workforce mobility security training or time horizon for	Count	1	1	0	3	1	20
	Percent	3.8%	3.8%	0.0%	11.5%	3.8%	76.9%
Cybersecurity competency testing training or time	Count	1	1	0	4	4	14
	Percent	4.2%	4.2%	0.0%	16.7%	16.7%	58.3%
Deception detection training or time horizon for	Count	1	1	0	2	2	17
	Percent	4.3%	4.3%	0.0%	8.7%	8.7%	73.9%
Password management training or time horizon for	Count	1	0	0	0	1	22
	Percent	4.2%	0.0%	0.0%	0.0%	4.2%	91.7%
Employee departure data security procedure training or	Count	4	2	0	4	1	14
	Percent	16.0%	8.0%	0.0%	16.0%	4.0%	56.0%

Notes: IT Employees are specifically targeted by this part of the study for their level of expertise in the subject area.

Restricted sites and download training appear to have been a well-implemented policy or practice area, with 81.5% of respondents indicating its current implementation. This suggests that the financial institutions recognised the importance of educating their employees on the risks associated with accessing restricted sites and downloading potentially harmful content. The high implementation rate reflects a proactive approach to mitigating cybersecurity threats in this particular area.

Acceptable-use policy training demonstrates a moderately high implementation rate, with 69.2% of respondents reporting its current implementation. While this policy area is essential for establishing guidelines and ensuring responsible use of technology resources, the relatively lower implementation rate suggests that some financial institutions may still have room for improvement in this regard. It is worth noting that 15.4% of respondents were unsure about the time horizon for implementing acceptable-use policy training, indicating a potential lack of clarity or communication regarding training plans.

Workforce mobility security training is an area that the financial institutions recognised as crucial, with 76.9% of respondents reporting its current implementation. Given the increased use of mobile devices and the potential risks associated with remote work and mobile access to sensitive information, the high implementation rate signifies a proactive approach to addressing security challenges posed by workforce mobility. This finding reflects an awareness of the need to educate employees on secure mobile practices and the potential vulnerabilities associated with mobile devices.

Cybersecurity competency testing training has a relatively lower implementation rate, with 58.3% of respondents reporting its current implementation. This finding suggests that while the selected financial institutions were aware of the importance of assessing employees' cybersecurity competency, a significant portion had yet to fully integrate this training into their programs. Implementing competency testing can help financial institutions gauge the effectiveness of their training initiatives, identify areas for improvement, and ensure that employees possess the necessary skills to protect against cyber threats.

Deception detection training is another area where the respondent financial institutions had recognised the importance of employees training, with 73.9% of respondents reporting its current implementation. The ability to detect and respond to deceptive practices such as phishing attempts or social engineering, is critical in maintaining a strong cybersecurity posture. The relatively high implementation rate indicates that the financial institutions acknowledged the significance of equipping their employees with the skills to identify and mitigate deceptive tactics.

Password management training demonstrates a remarkably high implementation rate, with 91.7% of respondents reporting its current implementation. This finding reflects the recognition of the crucial role that strong password management plays in safeguarding sensitive information. The high implementation rate suggests that financial institutions prioritised educating their employees on password security best practices, including the importance of using unique, complex passwords and regularly updating them.

Employee departure data security procedure training had a moderate implementation rate, with 56.0% of respondents reporting its current implementation. This training area focuses on educating employees about data security measures when they leave an organisation, such as revoking access rights and safeguarding sensitive information. The moderate implementation rate suggests that the financial institutions acknowledged the importance of addressing data security during employee departures, but there is still room for improvement in fully integrating this training into their programs.

Overall, the analysis of training practices in policy and practice areas within financial institutions reveals both areas of strength and potential areas for improvement. While certain policy areas such as restricted sites and download training and password management training, demonstrate high implementation rates, others, such as cybersecurity competency testing training and acceptable-use policy training, have relatively lower rates. Financial institutions can leverage these findings to enhance their training programs, ensuring comprehensive coverage of all critical policy and practice areas and aligning their training initiatives with industry best practices.

Table 4-12 presents the correlation matrix between different policy or practice areas on which companies provide education and training to their end users in the context of cybersecurity. The table provides insights into the relationships and associations between these areas. The analysis of the correlation matrix reveals the following key findings.

Restricted Sites and Downloads: There is a moderate positive correlation (0.40 to 0.78) between providing education and training in restricted sites and downloads and the other policy or practice areas. This indicates that companies that train their employees regarding restricted sites and downloads are also likely to provide education in other areas.

Acceptable-use Policy: The results showed a weak positive correlation (0.11 to 0.46) between providing education and training in acceptable-use policy and the other policy or practice areas. This suggests that companies that educate their employees about acceptable-use policy are somewhat more likely to provide education in other areas as well.

Workforce Mobility Security: There was a moderate positive correlation (0.26 to 0.58) between providing education and training in workforce mobility security and the other policy or practice areas. This implies that companies that focus on educating their employees about workforce mobility security also tend to provide education in other areas of cybersecurity.

Table 4-12: Correlation of Cybersecurity Education and Training Policy or Practice Areas

	Restricted Sites and Downloads	Acceptable-Use Policy	Workforce Mobility Security	Cybersecurity Competency Testing	Deception Detection Training	Password Management	Employee Departure Data Security Procedure	1.00
Restricted Sites and Downloads	1							
Acceptable-Use Policy	0.4	1						
Workforce Mobility Security	0.5	0.26	1					
Cybersecurity Competency Testing	0.53	0.11	0.39	1				
Deception Detection Training	0.47	0.24	0.54	0.29	1			
Password Management	0.78	0.46	0.51	0.61	0.53	1		
Employee Departure Data Security Procedure	0.24	0.21	0.58	0.22	0.23	0.34	1	-1.00

Notes: The correlation coefficients range from -1.00 to 1.00, with 1.00 indicating a perfect positive correlation, -1.00 indicating a perfect negative correlation, and 0 indicating no correlation.

Cybersecurity Competency Testing: The results revealed a weak to moderate positive correlation (0.11 to 0.61) between providing education and training in cybersecurity competency testing and the other policy or practice areas. This suggests that companies that conduct cybersecurity competency testing also tend to provide education in other areas.

Deception Detection Training: There was a weak to moderate positive correlation (0.23 to 0.54) between providing education and training in deception detection training and the other policy or practice areas. This could indicate that companies that educate their employees about deception detection in various contexts tend to provide education in other cybersecurity areas.

Password Management: A moderate to strong positive correlation (0.47 to 0.78) between providing education and training in password management and the other policy or practice areas was shown by the results. This suggests that companies that emphasise password management education for their employees are also likely to provide education in other cybersecurity areas.

Employee Departure Data Security Procedure: There is a weak positive correlation (0.21 to 0.58) between providing education and training in employee departure data security procedure and the other policy or practice areas. This implies that companies that educate their employees about data security procedures during employee departures also tend to provide education in other cybersecurity areas.

Overall, the correlation matrix indicates that there were varying degrees of positive correlations between different policy or practice areas on which companies provided education and training to their end users. These findings highlight potential associations and interdependencies between different areas of cybersecurity education within companies.

The foregoing analysis examines the training practices of financial institutions in various policy and practice areas related to cybersecurity. The analysis reveals that certain areas such as restricted sites and downloads, password management, and deception detection, were well-implemented and prioritised by the institutions. However, other areas like cybersecurity competency testing and acceptable-use policy training had lower implementation rates, indicating room for improvement. The analysis also explored correlations between different training areas, highlighting potential associations and interdependencies. These findings align with components of the Framework for Enhancing Cybersecurity Policy Awareness Programs, including making cybersecurity policy awareness a norm, targeted programs, continuous awareness campaigns, implementing simulated phishing exercises, and assessing program effectiveness. Financial institutions can use these insights to strengthen their training programs and align them with industry best practices.

The analysis focuses on the policy and practice areas addressed in cybersecurity training programs. It highlights the importance of targeted and customised training programs that align with specific policy areas in financial institutions. The analysis identifies various areas such as restricted sites and downloads, acceptable-use policy, workforce mobility security, and deception detection training. It emphasises the need for continuous awareness campaigns through methods like employee newsletters, posters, online training, and phishing simulations. The analysis indirectly indicates the importance of assessing the effectiveness of training programs by examining implementation rates and correlations between different policy areas.

4.4.5 Training Methods

This section provides an analysis of the cybersecurity policy education and training methods employed by financial institutions, focusing on IT employees given their level of expertise in the subject area and likelihood of being privy to this information. Table 4-13 presents the distribution of training methods used by these institutions.

Table 4-13: Cybersecurity Education and Training Methods Employed by Financial Institutions

Training Method	Restricted Sites and Download		Deception Detection		Password Management		Employee Departure Security Procedure	
	N	%	N	%	N	%	N	%
Not Applicable	4	14.8%	1	3.7%	1	3.7%	7	25.9%
Conventional (employee newsletters, posters), Instructor led	2	7.4%	3	11.1%	2	7.4%	1	3.7%
Phishing simulations	4	14.8%	4	14.8%	3	11.1%	1	3.7%
Online	4	14.8%	7	25.9%	8	29.6%	4	14.8%
Conventional (employee newsletters, posters), Instructor led, Online, Phishing simulations	3	11.1%	1	3.7%	1	3.7%	2	7.4%
Instructor led	2	7.4%	1	3.7%	2	7.4%	2	7.4%
Instructor led, Phishing simulations	1	3.7%	2	7.4%	2	7.4%	1	3.7%
Instructor led, Online, Phishing simulations	2	7.4%	3	11.1%	2	7.4%	2	7.4%
Conventional (employee newsletters, posters), Online, Phishing simulations	3	11.1%	2	7.4%	1	3.7%	0	0.0%
Instructor led, Online, Phishing simulations, Not Applicable	1	3.7%	0	0.0%	0	0.0%	0	0.0%
Conventional (employee newsletters, posters)	1	3.7%	0	0.0%	3	11.1%	6	22.2%
Online, Phishing simulations	0	0.0%	2	7.4%	0	0.0%	0	0.0%
Conventional (employee newsletters, posters), Online	0	0.0%	1	3.7%	2	7.4%	0	0.0%
Conventional (employee newsletters, posters), Instructor led, online	0	0.0%	0	0.0%	0	0.0%	1	3.7%
Total	**27**	**100%**		**100%**	**27**	**100%**	**27**	**100%**

Notes: IT Employees are specifically targeted by this part of the study for their level of expertise in the subject area.

A significant number of the financial institutions' IT employees indicated that the comprehensive list of training methods provided were “Not Applicable," accounting for 14.8% of responses. This indicates that a subset of institutions did not provide any specific cybersecurity policy training to their IT employees. It is crucial to address this gap in training to ensure that IT employees are equipped with the necessary knowledge and skills to mitigate cybersecurity risks effectively.

Conventional employee training methods such as newsletters and posters as well as instructor-led sessions are employed by fewer financial institutions. This approach is reported by 7.4% of institutions for restricted sites and downloads, 11.1% for deception detection, 7.4% for password management, and 3.7% for employee departure security procedures. Although these methods had been used on a regular basis, their limited adoption suggests a need for more comprehensive and interactive training approaches.

Phishing simulations, which involve creating simulated phishing attacks to test employees' ability to detect and respond to such threats, were employed by 14.8% of the financial institutions for restricted sites and downloads, 14.8% for deception detection, 11.1% for password management, and 3.7% for employee departure security procedures. The use of phishing simulations indicates an acknowledgment of the importance of practical training and the need to enhance employees' ability to identify and respond to phishing attempts.

Online training methods are utilised to a considerable extent by financial institutions. Data in this study revealed that this was reported by 14.8% of institutions for restricted sites and downloads, 25.9% for deception detection, 29.6% for password management, and 14.8% for employee departure security procedures. The popularity of online training can be attributed to its flexibility, scalability, and cost-effectiveness, making it an increasingly preferred choice for training IT employees in cybersecurity.

Financial institutions also employ a combination of training methods. For example, 11.1% of the institutions used a combination of conventional methods, instructor-led sessions, online training as well as phishing simulations for restricted sites and downloads. Similar combinations are reported for other training areas as well, reflecting a recognition that a multi-faceted approach can provide a more comprehensive training experience.

It is worth noting that a small percentage of financial institutions employ instructor-led sessions exclusively for certain training areas. For instance, 7.4% of institutions relied solely on instructor-led sessions for restricted sites and downloads, deception detection, password management, and employee departure security procedures. While instructor-led sessions offer the advantage of direct interaction and immediate clarification of doubts, their exclusive use may limit the scalability and accessibility of training programs.

In summary, the participant financial institutions in this study employed various cybersecurity policy training methods for their IT employees. While some did not provide specific training, others utilised conventional methods, phishing simulations, online training, or a combination of these approaches. The popularity of online training and the use of phishing simulations reflect a shift towards more practical and interactive training methods. However, there is room for improvement in terms of the adoption of comprehensive and multi-faceted training approaches. Financial institutions should consider integrating different training methods to enhance the effectiveness of their cybersecurity policy education programs for IT employees.

Moving on, Table 4-14 presents the correlation matrix indicating the degree of correlation between different cybersecurity education and training methods employed by financial institutions. The table provides insights into the relationships and associations between these methods followed by detailed analysis.

Table 4-14: Correlation of Cybersecurity Policy Education and Training Methods Employed by Financial Institutions

	Restricted sites and download	**Deception detection training**	**Password management**	**Employee departure data security procedure**	**1.00**
Restricted sites and download	1				
Deception detection training	0.74	1			
Password management	0.63	0.7	1		
Employee departure data security procedure	0.55	0.63	0.58	1	**-1.00**

Notes: The correlation coefficients range from -1.00 to 1.00, with 1.00 indicating a perfect positive correlation, -1.00 indicating a perfect negative correlation, and 0 indicating no correlation.

Deception Detection Training: There was a strong positive correlation of 0.74 between deception detection training and restricted sites and downloads. This suggests that financial institutions that provide education and training on deception detection are also likely to provide training on restricted sites and downloads.

Password Management: The results showed a moderate positive correlation of 0.63 between password management and restricted sites and downloads. This indicates that financial institutions that focus on educating and training end-users about password management are somewhat more likely to provide training on restricted sites and downloads as well.

Employee Departure Data Security Procedure: A moderate positive correlation of 0.55 between employee departure data security procedure and restricted sites and downloads, was revealed. This suggests that financial institutions that emphasise education and training on employee departure data security procedures are somewhat more likely to provide training on restricted sites and downloads.

Deception Detection Training and Password Management: A moderate positive correlation of 0.70 was shown between deception detection training and password management. This could indicate that financial institutions that provide education and training on deception detection are also likely to provide education and training on password management.

Deception Detection Training and Employee Departure Data Security Procedure: There was a moderate positive correlation of 0.63 between deception detection training and employee departure data security procedure. The positive relationship between the parameters could imply that financial institutions that provide training on deception detection are somewhat more likely to provide training on employee departure data security procedures.

Password Management and Employee Departure Data Security Procedure: There was a moderate positive correlation of 0.58 between password management and employee departure data security procedure. This indicates that financial institutions that focus on educating and training end-users about password management are somewhat more likely to provide training on employee departure data security procedures.

Overall, the correlation matrix indicated varying degrees of positive correlations between different cybersecurity education and training methods employed by financial institutions. These findings suggest potential associations and interdependencies between the methods, highlighting the interconnectedness of different aspects of cybersecurity policy education and training within financial institutions.

The analysis discusses training methods employed by financial institutions in cybersecurity training. Also, it emphasises the importance of targeted and customised training programs by highlighting specific training methods used for different areas, such as restricted sites and downloads, deception detection, password management, and employee departure security procedures. Furthermore, the analysis stresses the implementation of continuous and ongoing awareness campaigns through various training methods like employee newsletters, posters, online training, and phishing simulations. While not explicitly mentioned, the analysis indirectly emphasises the importance of assessing training program effectiveness by examining the distribution of training methods and correlations between different training areas.

4.5 Statistical Analysis

4.5.1 Classification

Classification, as defined by Khanna *et al*. (2021), is the systematic arrangement of data into distinct categories based on specific attributes or features. This process is crucial for systematically analysing vast categories of data and organising them into suitable classes (Khanna *et al*., 2021). Various classification methods such as k-nearest neighbours (KNN) and discriminant analysis, are employed widely across different fields to effectively categorise or classify data. KNN is a non-parametric method that assigns a class label to a new data point based on the majority vote of its k nearest neighbours (Khanna *et al*., 2021). On the other hand, discriminant analysis is a parametric method that models the differences between classes to determine the class membership of new observations (Sarker, 2021). The rest of this section is devoted to examining the results of KNN and discriminant analysis of the respondents as relates to the four levels of cybersecurity knowledge (namely, “no knowledge”, “little knowledge”, “good knowledge”, “excellent knowledge”).

4.5.1.1 K-Nearest Neighbours

The K-nearest neighbours (KNN) algorithm is a popular unsupervised machine learning technique used for cluster analysis (Kuhn and Johnson, 2013). In this study, we applied the KNN algorithm to a dataset consisting of various features related to gender, age group, educational attainment, employment status, sector, experience in the sector, cybersecurity induction, reporting procedure existence, and past cybersecurity training.

Clusters are groups of similar data points partitioned such that each point belongs to the cluster with the nearest mean, known as the centroid. The algorithm starts by initialising K centroids, then iteratively assigns each data point to the nearest centroid and recalculates the centroids as the mean of the assigned points. This process repeats until the centroids stabilise, effectively grouping the data into K distinct clusters. This process repeats until the centroids stabilize, effectively grouping the data into K distinct clusters that minimise intra-cluster variance while maximising inter-cluster variance. The clusters are formed using independent variables not the dependent variable (cybersecurity knowledge) and therefore do not directly refer to cybersecurity knowledge – this link is done directly in Discriminant Analysis and regression. The number of clusters is a hyper parameter that should be chosen carefully, as having not too many or too few clusters can improve the richness of the analysis. It is purely coincidental that they happen to match the number of levels in variable Cybersecurity Knowledge.

Furthermore, the clusters are meant to reveal the different group characteristics which may shed light on the different dynamics involved in implementing targeted interventions: e.g., the first cluster consists of mainly older males, with less stable employment, higher education among other characterisations. The way interventions to this group may be designed will differ to other groups because of the particularities of these other groups. Based on their z-scores, employees could then be assigned to each of these clusters. Given the diversity of characteristics within each cluster, they are usually identified by a numbered list rather than one or two-word phrases.

Therefore, the objective was to group individuals into clusters based on these features and gain insights into the characteristics of each cluster. In this section, a detailed analysis of the final cluster centres obtained from the KNN algorithm, is presented. The results of the KNN algorithm revealed the final cluster centres for four identified clusters. Each cluster is represented by z-scores for different variables, indicating the relative positions of the cluster centres in the multidimensional feature space. The reason z-scores were used because of the algorithm's limited ability to handle categorical variables.

The z-scores are basically the difference of the observed values (x) and their mean ($\bar{x}$), divided by their standard deviation (σ_x), thereby normalising them into z-scores, $z = (x - \bar{x})/\sigma_x$, which are assumed to be normally distributed with mean 0 and standard deviation 1. Each non-zero realisation of these scores essentially quantifies the number of standard deviations above (+) or below (-) the mean for that variable.

Analysing the first cluster centre from Table 4-15 and Figure 4-4 below, it is characterised by slightly higher z-scores for gender (0.12948) and employment status (0.25119). This suggests that individuals in this cluster were more likely to be male and employed. However, the z-scores for age group (0.25489) and educational attainment (-0.19706) indicated a mixed distribution, with slightly higher age and lower educational attainment compared to other clusters. The z-scores for sector (-0.21208) and experience in the sector (0.19746) were close to the average, suggesting a relatively balanced representation of sectors and experience levels in this cluster. The z-scores for cybersecurity induction (0.39520), reporting procedure exists (0.41893), and ever received cybersecurity training (0.45047) were positive, indicating a higher prevalence of these factors in this cluster.

Table 4-15: K-Nearest Neighbour Clusters to Understand Possible Groupings

Z-scores	**Cluster**			
	1	**2**	**3**	**4**
Gender	0.12948	-0.07197	-0.13774	0.00477
Age Group	0.25489	-0.52736	-0.45149	0.79134
Educational Attainment	-0.19706	-0.04689	0.21082	0.23092
Employment Status	0.25119	-3.50333	0.22161	0.30766
Sector	-0.21208	0.98919	-0.12517	3.81036
Experience in Sector	0.19746	-1.12935	-0.08154	0.19746
Cybersecurity Induction	0.39520	0.20494	-0.96634	0.25229
Reporting Procedure Exists	0.41893	-0.53339	-0.69341	-0.75119
Ever received cybersecurity training	0.45047	-0.33610	-0.99585	0.33921

Moving to the second cluster centre, negative z-scores for gender (-0.07197) and employment status (-3.50333) were observed, suggesting a relatively higher representation of females and a specific employment status that deviates significantly from the average.

The z-scores for age group (-0.52736) and experience in the sector (-1.12935) were also negative, indicating a lower age and less experience in the sector compared to other clusters. The z-scores for educational attainment (-0.04689) and sector (0.98919) were closer to the average, suggesting a relatively balanced distribution. The z-scores for cybersecurity induction (0.20494), reporting procedure exists (-0.53339), and ever received cybersecurity training (-0.33610) were also negative, indicating a lower prevalence of these factors in this cluster.

Moving to the third cluster centre, negative z-scores for age group (-0.45149) and employment status (0.22161) were shown, suggesting a relatively lower age and a specific employment status that deviates slightly from the average. The z-scores for gender (-0.13774) and educational attainment (0.21082) were closer to the average, indicating a relatively balanced distribution. The z-scores for sector (-0.12517) and experience in the sector (-0.08154) were also close to the average. The z-scores for cybersecurity induction (-0.96634), reporting procedure exists (-0.69341), and ever received cybersecurity training (-0.99585) were negative, indicating a lower prevalence of these factors in this cluster.

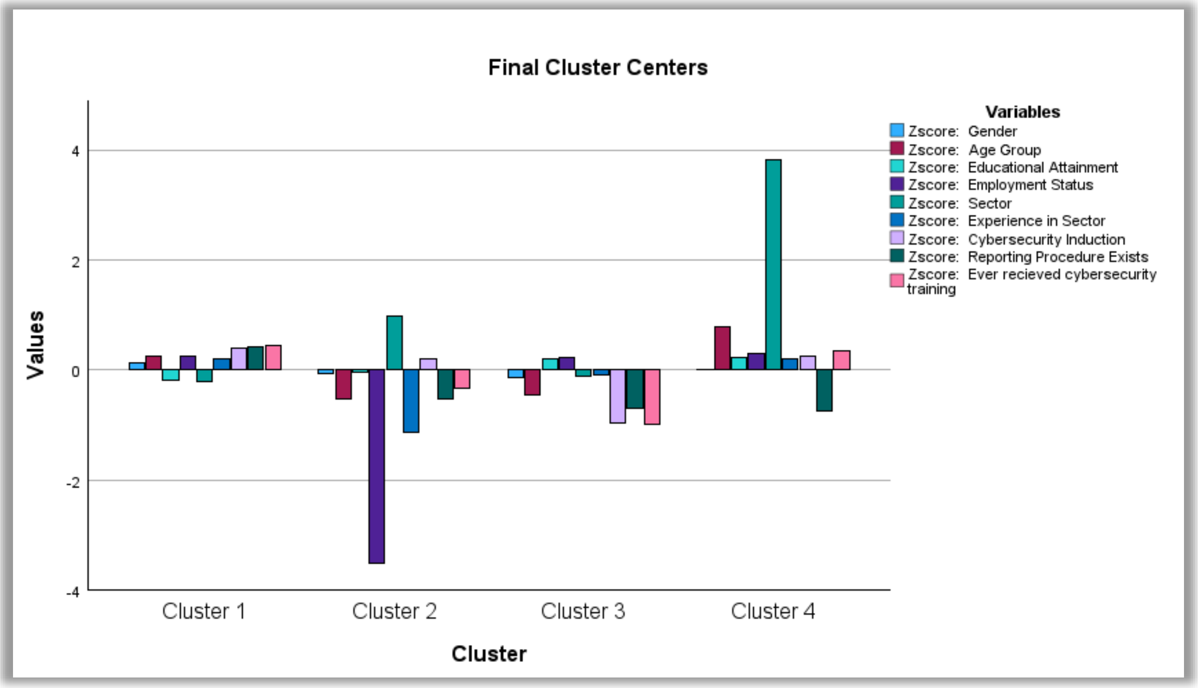


Figure 4-4: K Nearest Neighbour Clusters to Understand Possible Groupings

Finally, examining the fourth cluster centre, positive z-scores for gender (0.00477), age group (0.79134), educational attainment (0.23092), employment status (0.30766), and sector (3.81036) were observed. These positive z-scores suggest a relatively balanced distribution across these variables, with a slight emphasis on the higher end of the scale. The z-score for experience in the sector (0.19746) was close to the average. The z-scores for cybersecurity induction (0.25229) and ever received cybersecurity training (0.33921) were also positive, indicating a higher prevalence of these factors in this cluster.

In summary, the analysis of the final cluster centres reveals distinctive patterns across various variables. Each cluster exhibited different distributions and characteristics, highlighting the heterogeneity within the studied population. These findings provide valuable insights into the relationships between different factors and their impact on the clustering results. Understanding these patterns can inform the development of targeted strategies and interventions to address specific characteristics and needs within each cluster. It is conceivable that different groups would probably have different requirements for cybersecurity training, giving their gender, education, experience, among others.

4.5.1.1.1 Analysis of Variance

ANOVA (Analysis of Variance) is a statistical technique used to determine the differences between group means by analysing the variance within and between groups. In this study, a one-way ANOVA was used to evaluate the differences among clusters generated by a KNN algorithm. The clusters were formed based on various features, including gender, age group, educational attainment, employment status, sector, experience in the sector, cybersecurity induction, reporting procedure existence, and past cybersecurity training. This section presents a succinct analysis of the ANOVA results and discusses their implications.

The ANOVA results provide insights into the differences among the clusters based on the z-scores for various variables. However, it is important to note that the F tests should only be used descriptively in this context, as the clusters were specifically chosen to maximize differences among cases. Consequently, the observed significance levels cannot be interpreted as tests of the hypothesis that the cluster means are equal. The ensuing discussion is based on results presented in Table 4-16.

Examining the variables, the ANOVA for Age Group reveals a significant difference among the clusters (F (3, 178) = 9.654, $p < 0.001$). This suggests that the mean z-scores for age group varied significantly across the clusters. Similarly, the ANOVA for Employment Status indicates a significant difference among clusters (F (3, 178) = 491.691, $p < 0.001$), indicating variations in the mean z-scores for employment status across clusters.

The ANOVA for Sector also shows a significant difference among clusters (F (3, 178) = 125.143, $p < 0.001$). This suggests that the mean z-scores for sector varied significantly across the clusters. Furthermore, the ANOVA for Experience in Sector demonstrates a significant difference among clusters (F (3, 178) = 7.933, $p < 0.001$), indicating variations in the mean z-scores for experience in the sector across clusters.

The ANOVA for Cybersecurity Induction reveals a significant difference among clusters (F (3, 178) = 33.126, $p < 0.001$), suggesting variations in the mean z-scores for cybersecurity induction across clusters. Similarly, the ANOVA for Existence of Reporting Procedure for cybersecurity incidents indicates a significant difference among clusters (F (3, 178) = 23.551, $p < 0.001$), implying variations in the mean z-scores for the existence of a reporting procedure across clusters.

Table 4-16: ANOVA Results for Cluster Differences in Various Features

Z-scores	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
Gender	0.872	3	1.002	178	0.871	0.457
Age Group	8.566	3	0.887	178	9.654	<0.001
Educational Attainment	2.125	3	0.837	178	2.539	0.058
Employment Status	56.564	3	0.115	178	491.691	<0.001
Sector	44.560	3	0.356	178	125.143	<0.001
Experience in Sector	7.149	3	0.901	178	7.933	<0.001
Cybersecurity Induction	21.430	3	0.647	178	33.126	<0.001
Reporting Procedure Exists	17.143	3	0.728	178	23.551	<0.001
Ever received cybersecurity training	24.570	3	0.603	178	40.763	<0.001

The utilisation of F tests is limited to descriptive aims as the clusters are specifically selected to accentuate variations among cases within distinct clusters. The significance levels observed are unadjusted for this factor, hence incapable of serving as tests to validate the hypothesis asserting equality among cluster means

df = degrees of freedom; Sig. = statistical significance level

Lastly, the ANOVA for previous cybersecurity training shows a significant difference among clusters (F (3, 178) = 40.763, p < 0.001), suggesting variations in the mean z-scores for the receipt of cybersecurity training across clusters. Strikingly, gender and educational attainment are not statistically significant in explaining the differences (or variation between clusters, suggesting that they likely have little role in explaining the differences in the dependent variable, namely (the level of) cybersecurity knowledge. Other statistical tests will be used in the remainder of the chapter to further examine this *a priori* finding. It would be interesting to find that variables that theory would likely reason as important ex, turn out differently empirically.

In summary, the ANOVA results highlight significant differences among the clusters for several variables, including age group, employment status, sector, experience in sector, cybersecurity induction, existence of reporting procedure, and previous cybersecurity training. These findings support the notion that the clusters exhibited distinct characteristics and distributions across these variables.

4.5.1.2 Discriminant Analysis

Understanding the factors that contribute to disparities in cybersecurity knowledge is essential for developing effective strategies to enhance knowledge levels and promote a secure digital environment. Discriminant analysis was employed in this study to examine group mean differences in various factors related to cybersecurity knowledge. This section presents a comprehensive analysis of the results, shedding light on the variables that significantly influence cybersecurity knowledge levels.

The analysis aimed to explore the impact of gender, age group, educational attainment, employment status, sector, experience in the sector, cybersecurity induction, reporting procedure existence, previous cybersecurity training, and intention to attend future training sessions on cybersecurity knowledge. The findings, encapsulated by Table 4-17 below, revealed intriguing perspectives into the factors influencing cybersecurity knowledge levels. The analysis described in the next sections focus on each factor and its implications.

Table 4-17: Tests of Equality of Group Means

Variables	Wilks' Lambda	F	df1	df2	Sig.
Gender	0.978	1.313	3	178	0.272
Age Group	0.992	0.479	3	178	0.697
Educational Attainment	0.985	0.919	3	178	0.433
Employment Status	0.964	2.222	3	178	0.087
Sector	0.975	1.542	3	178	0.205
Experience in Sector	0.975	1.531	3	178	0.208
Cybersecurity Induction	0.920	5.142	3	178	0.002
Reporting Procedure Exists	0.884	7.773	3	178	<0.001
Ever received cybersecurity	0.696	25.887	3	178	<0.001
Intention to Attend	0.998	0.098	3	178	0.961
df = degrees of freedom; Sig. = statistical significance level					

The analysis of factors influencing cybersecurity knowledge levels revealed interesting insights. Gender (p = 0.272) and age group (p = 0.697) did not demonstrate a significant difference in mean cybersecurity knowledge scores, suggesting that for this study, they may not have been strong predictors of cybersecurity knowledge. Similarly, educational attainment (p = 0.433) did not significantly influence cybersecurity knowledge levels. However, it is important to continue exploring potential gender-related nuances, age-specific factors as well as the role of education in cybersecurity education and awareness programs.

On the other hand, employment status (p = 0.087) and the sector of employment (p = 0.205) did not exhibit significant differences in mean cybersecurity knowledge scores. Thus, they may not be primary determinants of cybersecurity knowledge. However, considering individuals' professional contexts and sector-specific challenges when designing cybersecurity education initiatives is crucial.

Experience in the sector (p = 0.208) also did not strongly influence cybersecurity knowledge levels. Nevertheless, understanding the role of experience in shaping individuals' understanding of cybersecurity risks and practices is important.

In contrast, factors such as cybersecurity induction, reporting procedure existence, ever received cybersecurity training, and intention to attend future training sessions demonstrated significant differences in mean cybersecurity knowledge scores ($p < 0.001$). These findings emphasise the pivotal role of training and awareness programs in enhancing cybersecurity knowledge. Implementing cybersecurity inductions, establishing reporting procedures, and providing regular training are essential for maintaining up-to-date knowledge among employees.

While the intention to attend future cybersecurity training sessions ($p = 0.961$) did not show significant differences in mean scores, individuals with higher levels of cybersecurity knowledge expressed a stronger intention to participate. This highlights the importance of fostering a culture of continuous learning and professional development to improve cybersecurity knowledge.

In conclusion, the Discriminant Analysis results shed light on the factors influencing cybersecurity knowledge levels. While gender, age group, educational attainment, employment status, sector, and experience in the sector showed no significant differences, cybersecurity induction, reporting procedure existence, previous cybersecurity training, and intention to attend future training sessions emerged as critical contributors to cybersecurity knowledge. These findings underscore the need for targeted interventions and comprehensive training programs that address the specific needs of individuals and organisations.

4.5.1.2.1 Box’s M Test

As previously explained, discriminant analysis is a statistical technique used to classify observations into different groups based on a set of predictor variables. One important assumption of discriminant analysis is that the covariance matrices of the predictor variables were equal across all groups being compared. Box's M test help in the evaluation of this assumption (Tabachnick and Fidell, 2018). Therefore, if the test statistic exceeds the critical value, it suggests that the assumption of equal covariance matrices is violated, indicating that the groups have significantly different covariance matrices.

As shown in Table 4-18, Box's Test of Equivalence of Covariance Matrices was conducted to assess whether there were significant differences in the covariance matrices across the different levels of cybersecurity knowledge. The natural logarithms of determinants and ranks of the group covariance matrices were examined to understand the structure and singularity of the matrices.

Table 4-18: Box's Test of Equivalence of Covariance Matrices

Log Determinants		
Cybersecurity Knowledge	**Rank**	**Log Determinant**
No Knowledge	.[a]	.[b]
Less Knowledge	10	-1.054
Good Knowledge	10	-2.705
Excellent Knowledge	9	.[c]
Pooled within-groups	10	-1.915
The ranks and natural logarithms of determinants printed are those of the group covariance matrices.		
a. Rank < 6		
b. Too few cases to be non-singular		
c. Singular		

Test Results[a]		
Box's M		128.063
F	**Approx.**	2.137
	df1	55
	df2	34393.338
	Sig.	<0.001
Tests null hypothesis of equal population covariance matrices.		
a. Some covariance matrices are singular and the usual procedure will not work. The non-singular groups will be tested against their own pooled within-groups covariance matrix. The log of its determinant is -1.319. df = degrees of freedom; Sig. = statistical significance level		

For the "No Knowledge" group, the rank of the covariance matrix was less than 6, indicating that the matrix had fewer dimensions than variables. As a result, the determinant of the matrix could not be computed as there were too few cases for a non-singular matrix. This suggests that the covariance matrix for the "No Knowledge" group was not suitable for further analysis.

Similarly, for the "Excellent Knowledge" group, the covariance matrix was singular, meaning that it was not invertible. Consequently, the determinant of the matrix could not be computed. This indicates that the covariance matrix for the "Excellent Knowledge" group was not suitable for further analysis.

On the other hand, the "Less Knowledge" and "Good Knowledge" groups had non-singular covariance matrices. The natural logarithm of the determinant for the "Less Knowledge" group was -1.054, while for the "Good Knowledge" group, it was -2.705. These determinants provide insights into the volume and spread of the data within each group.

To test the null hypothesis of equal population covariance matrices, Box's M test was performed. The test yielded a test statistic of 128.063 and an approximate F-statistic of 2.137. The degrees of freedom were reported as df1 = 55 and df2 = 34393.338. The p-value associated with the test statistic was less than 0.001, indicating significant differences in the covariance matrices across the groups.

Considering the singularity of some covariance matrices, an alternative approach was employed. The non-singular groups, namely the "Less Knowledge" and "Good Knowledge" groups, were tested against their own pooled within-groups covariance matrix. The log of the determinant of the pooled within-groups covariance matrix was -1.319.

In summary, the results of the Box's Test of Equality of Covariance Matrices suggest that there were significant differences in the covariance matrices across the different levels of cybersecurity knowledge. The "No Knowledge" group and the "Excellent Knowledge" group exhibited singularity in their covariance matrices, indicating that these matrices were not suitable for further analysis. On the other hand, the "Less Knowledge" and "Good Knowledge" groups had non-singular covariance matrices, allowing for meaningful analysis. The significant test results indicate that the covariance matrices differed significantly across the knowledge groups.

4.5.1.3 Canonical Discriminant Functions

The discriminant analysis in Table 4-19 yielded three canonical discriminant functions, which were used to analyse the discriminating power among the different levels of cybersecurity knowledge. The eigenvalues associated with each function provide insights into the amount of variance explained by each function and their overall contribution to the discrimination.

The first canonical discriminant function had an eigenvalue of 0.567, accounting for 80.2% of the total variance. This indicates that the first function captured the majority of the variation among the knowledge groups. The second canonical discriminant function had an eigenvalue of 0.084, explaining an additional 11.9% of the variance. The third function accounted for 7.9% of the variance with an eigenvalue of 0.056. Collectively, these three functions accounted for 92.1% of the total variance.

Table 4-19: Box's Test of Equality of Covariance Matrices

Function	Eigenvalue	% of Variance	Cumulative %	Canonical Correlation
1	0.567[a]	80.2	80.2	0.602
2	0.084[a]	11.9	92.1	0.279
3	0.056[a]	7.9	100.0	0.230
a. First 3 canonical discriminant functions were used in the analysis.				

The cumulative percentages of variance demonstrate the increasing amount of variance explained as each additional function is considered. The first function alone accounted for 80.2% of the variance, while the first two functions together explained 92.1%. Including all three functions resulted in 100% of the variance being accounted for.

Canonical correlations measure the strength and direction of the linear relationship between the discriminant functions and the original variables. The canonical correlation associated with the first function was 0.602, indicating a moderate correlation between the discriminant function and the knowledge groups. The second function had a canonical correlation of 0.279, representing a weaker relationship. The third function had the lowest canonical correlation of 0.230.

Overall, the discriminant analysis revealed three canonical discriminant functions that effectively differentiated between the levels of cybersecurity knowledge. The first function accounted for a significant portion of the variance, followed by the second and third functions. These functions demonstrated moderate to weak correlations with the original variables, indicating their ability to discriminate between the knowledge groups.

Wilks' Lambda was employed to assess the overall significance of the discriminant functions (see Table 4-20) in differentiating between the levels of cybersecurity knowledge. The test of function(s) examined the combined effects of multiple functions on the discrimination.

The results indicated that the first three functions collectively yielded a Wilks' Lambda value of .557. The associated chi-square statistic was 101.684, with 30 degrees of freedom, and the p-value was less than 0.001. These findings suggest that the discriminant functions significantly differentiated between the knowledge groups.

Table 4-20: Wilk's Lambda for the Discriminant Functions

Test of Function(s)	Wilks' Lambda	Chi-square	df	Sig.
1 through 3	0.557	101.684	30	<0.001
2 through 3	0.874	23.521	18	0.171
3	0.947	9.467	8	0.304
df = degrees of freedom; Sig. = statistical significance level				

Furthermore, the test considering the second and third functions produced a Wilks' Lambda value of 0.874. The chi-square statistic was 23.521, with 18 degrees of freedom, and the p-value was 0.171. These results indicate that the combined effects of the second and third functions were not statistically significant in discriminating between the knowledge groups.

Lastly, the third function alone yielded a Wilks' Lambda value of .947. The associated chi-square statistic was 9.467, with 8 degrees of freedom, and the p-value was .304. These findings suggest that the third function did not provide a significant contribution to the discrimination between the knowledge groups.

In summary, the results of Wilks' Lambda tests demonstrate that the first three discriminant functions collectively had a significant discriminatory power, while the combined effects of the second and third functions were not statistically significant. The third function alone did not contribute significantly to the discrimination. These findings support the utility of the first three functions in distinguishing between the levels of cybersecurity knowledge.

4.5.1.3.1 Discriminant Function Coefficients

Table 4-21 shows the Canonical Discriminant Function Coefficients. These provide valuable insights into the variables that contribute most significantly to the discrimination between the levels of cybersecurity knowledge. These coefficients represent the relationships between the discriminant functions and the predictor variables.

Analysing the coefficients for the first discriminant function, it can be said that gender (-0.401), age group (0.193), educational attainment (-0.051), employment status (0.200), sector (-0.031), experience in sector (-0.286), cybersecurity induction (-0.065), reporting procedure existence (0.573), ever received cybersecurity training (1.180), and intention to attend cybersecurity training (0.075) all had non-zero coefficients. These coefficients indicate the direction and strength of their relationships with the first discriminant function.

Table 4-21: Canonical Discriminant Function Coefficients

Variables	**Function**		
	1	**2**	**3**
Gender	-0.401	0.698	0.359
Age Group	0.193	0.147	-0.321
Educational Attainment	-0.051	0.347	-0.105
Employment Status	0.200	-0.416	0.038
Sector	-0.031	0.125	0.093
Experience in Sector	-0.286	-0.078	0.775
Cybersecurity Induction	-0.065	-0.188	-0.747
Reporting Procedure Exists	0.573	10.185	-0.041
Ever received cybersecurity training	1.180	-0.110	0.518
Intention to Attend Cybersecurity	0.075	0.010	0.187
(Constant)	-4.015	-4.020	-2.640
Unstandardized coefficients			

Similarly, for the second discriminant function, variables such as gender (0.698), age group (0.147), educational attainment (0.347), employment status (-0.416), sector (0.125), experience in sector (-0.078), cybersecurity induction (-0.188), reporting procedure existence (1.185), ever received cybersecurity training (-0.110), and intention to attend cybersecurity training (0.010) had non-zero coefficients. These coefficients provide insights into the relationships between the variables and the second discriminant function.

Lastly, the third discriminant function was associated with coefficients for gender (0.359), age group (-0.321), educational attainment (-0.105), employment status (0.038), sector (0.093), experience in sector (0.775), cybersecurity induction (-0.747), reporting procedure existence (-0.041), ever received cybersecurity training (0.518), and intention to attend cybersecurity training (0.187). These coefficients indicate existence of relationships between the variables and the third discriminant function.

In summary, the Canonical Discriminant Function Coefficients highlight the importance of various variables in discriminating between the levels of cybersecurity knowledge. Gender, age group, educational attainment, employment status, sector, experience in sector, cybersecurity induction, reporting procedure existence, previous cybersecurity training, and intention to attend cybersecurity training all play significant roles in the discrimination process. These findings provide valuable insights into the factors that contribute to differences in cybersecurity knowledge among individuals.

The classification results shown in Table 4-22 provide insights into the accuracy of the discriminant analysis in predicting the group membership of individuals based on their cybersecurity knowledge levels. The table presents the original group membership counts and the corresponding predicted group membership counts.

Table 4-22: Classification Results

		Cybersecurity Knowledge	Predicted Group Membership				Total
			No Knowledge	Less Knowledge	Good Knowledge	Excellent Knowledge	
Original	Count	No Knowledge	3	2	1	0	**6**
		Less Knowledge	1	30	20	0	**51**
		Good Knowledge	1	13	88	1	**103**
		Excellent	0	0	21	1	**22**
	%	No Knowledge	50.0	33.3	16.7	.0	**100.0**
		Less Knowledge	2.0	58.8	39.2	.0	**100.0**
		Good Knowledge	1.0	12.6	85.4	1.0	**100.0**
		Excellent	.0	.0	95.5	4.5	**100.0**

a. 67.0% of original grouped cases correctly classified.

Upon examining the results, it is evident that the discriminant analysis achieved a relatively high classification accuracy. Out of the total original cases, 67.0% were correctly classified into their respective knowledge groups.

In terms of specific group memberships, 50.0% of the individuals originally classified as having no knowledge were accurately predicted to belong to the no knowledge group. Similarly, 58.8% of the individuals originally classified as having less knowledge were correctly assigned to the less knowledge group. For the good knowledge group, 85.4% of the individuals were accurately classified, and for the excellent knowledge group, 4.5% were correctly assigned.

Overall, the classification results indicate the effectiveness of the Discriminant Analysis in distinguishing between the different levels of cybersecurity knowledge. The high percentage of correctly classified cases suggests that the discriminant functions derived from the analysis can reliably predict the group membership of new individuals based on their cybersecurity knowledge.

In summary, the Discriminant Analysis achieved a classification accuracy of 67.0%, with a significant number of individuals being correctly assigned to their respective knowledge groups. These findings highlight the utility of the analysis in accurately categorising individuals based on their cybersecurity knowledge levels.

4.5.2 Multicollinearity

Multicollinearity tests are necessary to ensure the reliability of the statistical model parameters as high inter-correlations among independent variables can distort or mislead the results and lead to instability of said parameters. Table 4-23 below shows collinearity diagnostics report for the ten independent variables that were intended to regress against cybersecurity knowledge to uncover the underlying relationship between them and cybersecurity knowledge improvement. To evaluate multicollinearity, the study examined collinearity using two statistics, tolerance and variance inflation factor (VIF), Table 4-23 provides the details.

Tolerance signifies the proportion of variability in an independent variable that is not predictable from other independent variables (Johnson and Wichern, 2002). A tolerance value nearing 1 signifies limited multicollinearity whereas values closer to 0 indicate heightened multicollinearity (Shrestha, 2020).

Conversely, VIF, being the reciprocal of tolerance, measures the degree of multicollinearity (Shrestha, 2020). VIF values surpassing 1 denote the existence of multicollinearity, with values exceeding 10 commonly raising concerns (Shrestha, 2020).

In this analysis, the collinearity statistics suggest that multicollinearity is not a significant issue among the independent variables. The tolerance values range from 0.689 to 0.899, indicating that there was no excessive redundancy or high inter-correlation among the variables. Similarly, the VIF values range from 1.071 to 1.451, all below the threshold of 10 (Shrestha, 2020). These findings suggest that the independent variables in the model did not suffer from severe multicollinearity, and their relationships with the dependent variable could be assessed without major concerns about distorted results or unreliable coefficient estimates.

Table 4-23: Collinearity Diagnostics for Independent Variables

Independent Variables	**Collinearity Statistics**	
	Tolerance	**VIF**
Gender	0.886	1.129
Age Group	0.728	1.375
Educational Attainment	0.934	1.071
Employment Status	0.865	1.157
Sector	0.899	1.112
Experience in Sector	0.689	1.451
Cybersecurity Induction	0.705	1.417
Reporting Procedure Exists	0.782	1.279
Ever received cybersecurity training	0.745	1.342
a. Dependent Variable: Cybersecurity Knowledge. N = 182 cases were used as valid cases.		

The absence of multicollinearity among the independent variables enhances the robustness and interpretability of statistical models, as it ensures that each variable contributes unique information to the prediction of cybersecurity knowledge. Researchers and analysts can have greater confidence in the individual effects and significance of the independent variables when multicollinearity is not present.

In summary, the collinearity statistics indicate that multicollinearity was not a significant concern among the independent variables in the statistical model. This suggests that the relationships between the independent variables and the dependent variable, cybersecurity knowledge, can be assessed without the risk of skewed or misleading results due to excessive inter-correlations.

4.5.3 Multinomial Logistic Regression

After confirming the absence of excessive multicollinearity among the independent variables, analyses focused on the relationship between these variables and the dependent variable, cybersecurity knowledge. Cybersecurity knowledge is a categorical variable and consists of four ordered levels (no knowledge, little knowledge, good knowledge and excellent knowledge), making it an ordinal categorical variable. Given the categorical nature of the dependent variable, the appropriate model to employ is logistic regression as it is suited for categorical variables.

The analysis employs a multinomial logistic regression (MLR) model to examine the relationship between the independent variables and the dependent variable. To model this relationship, the analysis applies the cumulative logit link function, which is suitable for ordered categorical variables. This link function is specifically designed for ordered categorical variables and allows for the estimation of cumulative probabilities (Hosmer and Lemeshow, 2000). By using the cumulative logit link function, the analysis can assess the cumulative odds of an individual belonging to a higher level of cybersecurity knowledge based on the independent variables.

The probability distribution used in this analysis is the multinomial distribution. This distribution is appropriate when dealing with a categorical dependent variable that has multiple levels. By utilising the multinomial distribution, the analysis can estimate the probabilities associated with each level of cybersecurity knowledge. This provides valuable insights into the likelihood of individuals belonging to different knowledge levels based on the independent variables.

By combining the multinomial probability distribution with the cumulative logit link function, the analysis effectively models the relationship between the independent variables and the ordered levels of cybersecurity knowledge. This approach enables the estimation of probabilities and cumulative odds associated with each knowledge level, providing a comprehensive understanding of the factors influencing individuals' cybersecurity knowledge at different levels.

From here on, results of fitting a MLR model to investigate the relationship between cybersecurity knowledge and relevant demographic variables namely, gender, age, education, employment status, experience, sector, existence of reporting procedure as well as previous cybersecurity training, are described.

The parameter estimates obtained from the analysis are presented in Table 4-24. The Wald chi-square test is a statistical hypothesis test used to assess the significance of individual coefficients in a regression model. It specifically examines whether a coefficient is significantly different from zero, providing insights into the contribution of each variable in the model's predictive power (Agresti, 2015). By evaluating the significance of these coefficients, the Wald chi-square test helps us understand the relative importance of variables in explaining the variation in the dependent variable and making accurate predictions. Regression coefficients with positive values indicate a direct relationship with the log-odds of the dependent variable, meaning that as the independent variable increases, the dependent variable also tends to increase. Conversely, negative coefficients suggest an inverse relationship, where the log-odds of the dependent variable tend to decrease as the independent variable increases.

Starting with the threshold estimates for the three levels of cybersecurity knowledge, it was observed that the estimated threshold for the "No Knowledge" category was -8.044 (SE = 3.0403)[1]. This indicates a negative relationship with the reference category. The 95% Wald

[1] SE = Standard Error

confidence interval for this threshold ranged from -14.003 to -2.085. The Wald chi-square test (χ^2 = 7.001, df = 1, p = 0.008) indicated that the threshold was statistically significant, suggesting a clear distinction between individuals with no cybersecurity knowledge and those with some level of knowledge.

For the "Less Knowledge" category, the estimated threshold was -4.291 (SE = 2.9766). However, the Wald chi-square test (χ^2 = 2.078, df = 1, p = 0.149) did not provide enough evidence to establish a statistically significant relationship. In contrast, the estimated threshold for the "Good Knowledge" category was negligible (SE = 2.9478), with a wide confidence interval ranging from -5.767 to 5.788. The Wald chi-square test (χ^2 = 0, df = 1, p = 0.997) indicated that this threshold was not statistically different from zero, suggesting that individuals with good cybersecurity knowledge did not significantly differ from the reference category.

Table 4-24: Parameter Estimates for the Ordinal MLR of Cybersecurity Knowledge Against Demographic Variables

Parameter		B	Std. Error	95% Wald Confidence Interval		Hypothesis Test		
				Lower	Upper	Wald Chi-Square	df	Sig.
Threshold	[Cybersecurity Knowledge= No Knowledge]	-8.044	3.0403	-14.003	-2.085	7.001	1	0.008
	[Cybersecurity Knowledge= Less Knowledge]	-4.291	2.9766	-10.125	1.543	2.078	1	0.149
	[Cybersecurity Knowledge= Good Knowledge]	0.011	2.9478	-5.767	5.788	0.000	1	0.997
[Gender=Male]		0.654	0.3803	-0.092	1.399	2.955	1	0.086
[Gender=Female]		0[a]	.	.	.	.	.	.
[Age Group=18 to 30]		-2.833	2.6718	-8.070	2.403	1.125	1	0.289
[Age Group=31 to 40]		-1.914	2.6179	-7.045	3.217	0.535	1	0.465
[Age Group=41 to 50]		-1.735	2.5896	-6.810	3.341	.449	1	0.503
[Age Group=51 to 65]		-2.834	2.6824	-8.091	2.424	1.116	1	0.291
[Age Group= Over 65]		0[a]	.	.	.	.	.	.
[Educational Attainment= No Formal Education]		-0.875	1.4587	-3.734	1.984	0.360	1	0.549
[Educational Attainment= Certificate]		0.324	1.7405	-3.087	3.736	0.035	1	0.852
[Educational Attainment=Diploma]		0.858	0.9258	-0.957	2.672	0.858	1	0.354
[Educational Attainment= Associate Degree]		-0.840	0.8913	-2.587	0.907	0.889	1	0.346
[Educational Attainment= Bachelor's Degree]		0.364	0.7645	-1.134	1.863	0.227	1	0.634
[Educational Attainment= Professional Qualification]		-1.098	1.1729	-3.397	1.201	0.877	1	0.349

[Educational Attainment= Honour's Degree]	-0.544	0.9211	-2.349	1.261	0.349	1	0.555
[Educational Attainment= Master's Degree]	0^{a}	.	.	.	.	.	.
[Employment Status= Part-time Employed]	-0.270	0.8736	-1.982	1.442	0.095	1	0.757
[Employment Status= Apprentice]	23.276	31069.6883	-60872.194	60918.746	0.000	1	0.999
[Employment Status= Contract]	1.105	1.4753	-1.786	3.997	0.561	1	0.454
[Employment Status= Self-Employed/Consultant]	0.627	1.0663	-1.463	2.717	0.346	1	0.556
[Employment Status= Full-time Employed]	0^{a}	.	.	.	.	.	.
[Sector= Central Banking]	1.580	1.7495	-1.849	5.009	0.816	1	0.366
[Sector= Commercial Banks and Forex Agencies]	-0.647	1.4604	-3.509	2.215	0.196	1	0.658
[Sector= Insurance Brokers]	-1.927	1.5273	-4.921	1.066	1.592	1	0.207
[Sector= Insurance Companies]	-0.167	1.4204	-2.951	2.617	0.014	1	0.907
[Sector= Asset Managers]	-0.348	1.5526	-3.391	2.695	0.050	1	0.823
[Sector= Financial Institutions & Insurance Regulator]	21.152	31069.6883	-60874.318	60916.622	0.000	1	0.999
[Sector= Insurance Company]	-2.438	2.5811	-7.496	2.621	0.892	1	0.345
[Sector= Investment]	-5.444	2.6082	-10.556	-0.332	4.357	1	0.037
[Sector= Pensions Regulator]	-1.421	2.7688	-6.848	4.006	0.263	1	0.608
[Sector= Regulator]	-0.062	2.7760	-5.503	5.378	0.001	1	0.982
[Sector= Telecommunications]	-1.560	2.7775	-7.003	3.884	0.315	1	0.574
[Sector= FinTech]	-4.871	2.5824	-9.932	0.190	3.558	1	0.059
[Sector= Insurance Broker]	0.619	2.7763	-4.823	6.060	0.050	1	0.824

[Sector= Micro Finance Institutions]	-2.174	2.8831	-7.825	3.477	0.568	1	0.451
[Sector= Assurance Services]	0.329	2.9297	-5.413	6.071	0.013	1	0.911
[Sector= Finance]	1.580	1.7495	-1.849	5.009	0.816	1	0.366
[Sector= Min of Finance]	-0.647	1.4604	-3.509	2.215	0.196	1	0.658
[Sector= Money Transfer Institution]	-1.927	1.5273	-4.921	1.066	1.592	1	0.207
[Experience in Sector= Less than a year]	0.344	0.9066	-1.433	2.120	0.144	1	0.705
[Experience in Sector= 1 to 3 years]	1.096	0.5270	0.063	2.129	4.326	1	0.038
[Experience in Sector= 4 to 5 years]	0.315	0.5228	-0.709	1.340	0.364	1	0.546
[Experience in Sector= More than 5 years]	0[a]	.	.	.	.	.	.
[Reporting Procedure Exists= Yes]	-1.877	0.6556	-3.161	-0.592	8.194	1	0.004
[Reporting Procedure Exists= No]	-0.716	0.6978	-2.084	0.651	1.053	1	0.305
[Reporting Procedure Exists= Don't Know]	0[a]	.	.	.	.	.	.
[Ever received cybersecurity training= Yes]	-3.214	0.5051	-4.204	-2.224	40.495	1	<0.001
[Ever received cybersecurity training= No]	-2.681	1.1734	-4.981	-0.0381	5.221	1	0.022
[Ever received cybersecurity training= Not Sure]	0[a]	.	.	.	.	.	.
(Scale)	1[b]						

Dependent Variable: Cybersecurity Knowledge

Model: (Threshold), Gender, Age Group, Educational Attainment, Employment Status, Sector, Experience in Sector, Reporting Procedure Exists, Ever received cybersecurity training

df – degrees of freedom; Sig – significance level

a. Set to zero because this parameter is redundant.

b. Fixed at the displayed value.

Moving on to the demographic variables, the parameter estimate for Gender showed that being male (B = 0.654, SE = 0.3803) was associated with higher cybersecurity knowledge compared to the reference category (female). However, the Wald chi-square test (χ^2 = 2.955, df = 1, p = 0.086) did not reach statistical significance at the conventional threshold (α = 0.05).

Regarding age groups, individuals in the categories "18 to 30," "31 to 40," "41 to 50," and "51 to 65" exhibited lower cybersecurity knowledge compared to the reference category "Over 65." However, none of these age groups showed statistically significant differences in cybersecurity knowledge based on the Wald chi-square tests ($p > 0.05$). On educational attainment, the parameter estimates for different levels of education indicated that no specific level showed a significant association with cybersecurity knowledge. None of the Wald chi-square tests for the educational attainment categories reached statistical significance ($p > 0.05$). In terms of employment status, none of the categories displayed a statistically significant relationship with cybersecurity knowledge, as indicated by the non-significant Wald chi-square tests ($p > 0.05$).

Analysing sector-related variables, the parameter estimates suggested that being in the "Investment" sector was associated with significantly lower cybersecurity knowledge (B = -5.444, SE = 2.6082, χ^2 = 4.357, df = 1, p = 0.037). However, the remaining sectors did not show statistically significant associations with cybersecurity knowledge. Regarding experience in the sector, individuals with 1 to 3 years of experience (B = 1.096, SE = 0.527, χ^2 = 4.326, df = 1, p = 0.038) exhibited higher cybersecurity knowledge compared to those with less than a year of experience. No other experience categories showed significant associations.

Concerning reporting procedures and cybersecurity training, individuals who reported the existence of reporting procedures (B = -1.877, SE = 0.6556, χ^2 = 8.194, df = 1, p = 0.004) and those who had received cybersecurity training (B = -3.214, SE = 0.5051, χ^2 = 40.495, df = 1, $p < 0.001$) demonstrated significantly higher cybersecurity knowledge compared to their respective reference categories. Conversely, the parameter estimates for previous cybersecurity training, suggested lower cybersecurity knowledge for individuals who have not received such training (B = -2.681, SE = 1.1734, χ^2 = 5.221, df = 1, p = 0.022).

In summary, the multinomial logistic regression analysis revealed that the thresholds for different levels of cybersecurity knowledge were significantly associated with the demographic variable of gender, as well as the presence of reporting procedures and the receipt of cybersecurity training. However, age groups, educational attainment, and employment status did not exhibit statistically significant relationships with cybersecurity knowledge. Additionally, specific sectors and experience levels showed limited associations with cybersecurity knowledge. Overall, this information helps us understand the factors influencing cybersecurity knowledge and informs the development of interventions and training programs on the basis of variables that would have the most effect on the cybersecurity knowledge of employees.

4.5.3.1 Goodness of Fit MLR

After fitting the multinomial logistic regression model, its goodness of fit and different measures, were examined. Table 4-25 presents the goodness of fit measures for the analysed model, which includes the dependent variable "Cybersecurity Knowledge" and several independent variables. These measures assess how well the model fits the observed data and provide insights into the model's overall performance.

The deviance value, which measures the difference between the observed and predicted values, is 213.553. The deviance value-to-degrees-of-freedom ratio is a measure used to assess the goodness of fit of a statistical model. It represents the average amount of deviance per degree of freedom in the model. A lower ratio generally indicates a better fit, implying that the model explains a larger proportion of the observed data's variability relative to the number of parameters estimated (Agresti, 2015). Therefore, with 396 degrees of freedom, the value-to-degrees-of-freedom ratio is 0.539. This ratio indicates that the deviance is slightly larger than expected, suggesting that the model may have a slight lack of fit. However, further analysis is needed to determine the significance and practical implications of this deviation.

Similarly, the scaled deviance value is also 213.553, indicating the same level of discrepancy between the observed and predicted values. The lack of fit observed in the deviance and scaled deviance values suggests that there may be unexplained variability in the model, which could be attributed to factors not included in the current set of independent variables.

The log likelihood function, displayed as -118.801, represents the maximum likelihood estimation of the model based on the observed data. This function is used to calculate various information criteria that assess the model's goodness of fit.

Table 4-25: Goodness of fit Statistics for the Ordinal Multinomial Logistic Regression of Cybersecurity Knowledge Against Demographic Variables

Goodness of Fit Measures[a]	**Value**	**df**	**Value/df**
Deviance	213.553	396	0.539
Scaled Deviance	213.553	396	
Pearson Chi-Square	720.285	396	1.819
Scaled Pearson Chi-Square	720.285	396	
Log Likelihood[b]	-118.801		
Akaike's Information Criterion (AIC)	321.603		
Finite Sample Corrected AIC (AICC)	347.588		
Bayesian Information Criterion (BIC)	456.171		
Consistent AIC (CAIC)	498.171		
Dependent Variable: Cybersecurity Knowledge			
a. Information criteria are in smaller-is-better form.			
b. The full log likelihood function is displayed and used in computing information criteria.			

The Pearson chi-square value, which assesses the discrepancy between the observed and expected frequencies, was 718.285. This value is associated with 396 degrees of freedom, resulting in a value-to-degrees-of-freedom ratio of 1.819. The ratio greater than 1 suggests that there was a significant discrepancy between the observed and expected frequencies, indicating a lack of fit. Similar to the Pearson chi-square value, the scaled Pearson chi-square value was also 718.285. This value further confirms the lack of fit observed in the model.

The Akaike's Information Criterion (AIC) is 321.603, while the Finite Sample Corrected AIC (AICC) is 347.588. Both criteria indicate the model's fit, with smaller values indicating better fit. The Bayesian Information Criterion (BIC) is 456.171, and the Consistent AIC (CAIC) is 498.171. These criteria provide additional measures of the model's fit, with lower values indicating better fit.

In summary, an assessment of fit across all measures was consistent. The goodness of fit measures suggests that the analysed model may have a slight lack of fit, as indicated by the deviance, scaled deviance, and Pearson chi-square values. These findings imply that there might be unexplained variability or factors not captured by the current set of independent variables. The information criteria, including AIC, AICC, BIC, and CAIC, provide further insights into the model's fit, with lower values indicating better fit.

Overall, these measures highlight the need for further examination and potential refinement of the model to improve its fit to the observed data. In this study therefore, an omnibus test was run in order to gain understanding of the overall fit of the model. If the results of the omnibus test were to be positive, there would have been a need to fit a reduced model taking moderate-to-highly significant variables and also examine its goodness of fit.

4.5.3.2 Omnibus Test

All prior analysis of regression outputs and statistical goodness of fit tests show that some of the fitted independent variables are not highly statistically significant in explaining individuals' level of cybersecurity knowledge, essentially delivering a scathing verdict on their predictive strength. The omnibus test essentially moderates this view by comparing the fitted model with the thresholds-only model. An omnibus test is a type of statistical test that assesses the significance of multiple parameters within a model simultaneously (Bobbitt, 2021).

Table 4-26: Omnibus Test of Goodness of Fit for the Ordinal Multinomial Logistic Regression of Cybersecurity Knowledge Against Ten Demographic Variables

Likelihood Ratio Chi-Square[a]	**df**	**Sig.**
113.224	42	<0.001
Dependent Variable: Cybersecurity Knowledge Model: (Threshold), Gender, Age Group, Educational Attainment, Employment Status, Sector, Experience in Sector, Reporting Procedure Exists, Ever received cybersecurity training		
a. Compares the fitted model against the thresholds-only model.		

Table 4-26 presents the results of the omnibus test, which assesses the overall significance and fit of the analysed model for the dependent variable and multiple independent variables. This test compares the fitted model against a thresholds-only (basically intercept-only) model, aiming to determine if the inclusion of the independent variables significantly improves the model's fit.

The likelihood ratio chi-square value for the omnibus test is 113.224, with 42 degrees of freedom. The significance level, indicated as "<0.001," suggests that the chi-square value is statistically significant, providing evidence against the null hypothesis that the thresholds-only model fits the data equally as well as the fitted model.

The significant chi-square value implies that the inclusion of the independent variables in the model significantly improves the fit compared to the thresholds-only model. This finding suggests that the independent variables considered in the analysis contribute valuable information for explaining and predicting individuals' cybersecurity knowledge levels.

In summary, the results of the omnibus test indicate that the fitted model, which includes various independent variables, demonstrates a significantly better fit compared to the thresholds-only model. This implies that the independent variables considered in the analysis contribute significantly to explaining the variations in individuals' cybersecurity knowledge levels. These findings support the inclusion of the independent variables in the model and highlight their relevance in understanding and predicting cybersecurity knowledge. Therefore, the next step involved having to fit a reduced model, as shown in the next section.

4.5.4 Reduced MLR Model

Given that the Omnibus test has indicated that using predictor variables results in a better fit than an intercept-only model, next, a reduced model was fit, taking only those variables that had shown moderate to high statistical significance in the larger model.

The regression output is shown in Table 4-27. The table presents the parameter estimates for a reduced ordinal MLR model that analyses the relationship between cybersecurity knowledge and demographic variables (gender, reporting procedure exists, previous cybersecurity training). The regression coefficients provide insights into the effects of different independent variables on the odds of higher cybersecurity knowledge.

Regarding the thresholds for different knowledge categories, the coefficients indicate their influence on the odds of being in higher knowledge categories. For the "No Knowledge" category, the coefficient is -5.069 (SE = 0.5651), indicating a significant negative effect on the odds of transitioning into higher cybersecurity knowledge categories (Wald chi-square = 80.462, df = 1, p < 0.001). Similarly, the "Less Knowledge" category has a coefficient of -1.677 (SE = 0.2865), also negatively and significantly impacting the odds of transitioning into higher cybersecurity knowledge categories (Wald chi-square = 34.272, df = 1, p < 0.001). The "Good Knowledge" category, on the other hand, has a coefficient of 1.844 (SE = 0.2947), suggesting a positive and significant effect on the odds of transitioning into a higher cybersecurity knowledge category (Wald chi-square = 39.165, df = 1, p < 0.001).

Table 4-27: Parameter Estimates for the Reduced Ordinal MLR of Cybersecurity Knowledge Against Demographic Variables

Parameter		**B**	**Std. Error**	**95% Wald Confidence Interval**		**Hypothesis Test**		
				Lower	**Upper**	**Wald Chi-Square**	**df**	**Sig.**
Threshold	[Cybersecurity Knowledge= No Knowledge]	-5.069	0.5651	-6.177	-3.961	80.462	1	<0.001
	[Cybersecurity Knowledge= Less Knowledge]	-1.677	.2865	-2.239	-1.116	34.272	1	<0.001
	[Cybersecurity Knowledge= Good Knowledge]	1.844	0.2947	1.267	2.422	39.165	1	<0.001
[Gender=Male]			0.3245	0.017	1.289	4.047	1	0.044
[Gender=Female]			.	.	.	.	.	.
[Reporting Procedure Exists= Yes]			0.5923	-2.813	-0.492	7.784	1	0.005
[Reporting Procedure Exists= No]			0.5115	-1.946	0.059	3.401	1	0.065
[Reporting Procedure Exists= Don't Know]			.	.	.	.	.	.
[Ever received cybersecurity training= Yes]			0.4026	-3.317	-1.739	39.438	1	<0.001
[Ever received cybersecurity training= No]			0.9958	-4.389	-0.486	5.991	1	0.014
[Ever received cybersecurity training= Not Sure]			.	.	.	.	.	.
(Scale)		1^b						
Dependent Variable: Cybersecurity Knowledge Model: (Threshold), Gender, Reporting Procedure Exists, Ever received cybersecurity training								
a. Set to zero because this parameter is redundant.								
b. Fixed at the displayed value.								

In terms of gender, the coefficient for males is 0.3245 (SE = 0.017), indicating a statistically significant and positive effect on the odds of possessing higher cybersecurity knowledge (Wald chi-square = 1, df = 1, p = 0.044).

Regarding the presence of a reporting procedure, having such a procedure is associated with a coefficient of 0.5923 (SE = 2.813), indicating a significant and positive effect on the odds of possessing higher cybersecurity knowledge (Wald chi-square = 1, df = 1, p = 0.005). On the other hand, not having a reporting procedure shows a coefficient of 0.5115 (SE = 1.946), suggesting a potential but marginally significant and positive effect on the odds of higher cybersecurity knowledge (Wald chi-square = 1, df = 1, p = 0.065).

Lastly, the coefficients for having previously received cybersecurity training reveal its impact on the odds of higher cybersecurity knowledge. The coefficient for individuals who had received training was 0.4026 (SE = 3.317), indicating a significant and positive effect on the odds of higher cybersecurity knowledge (Wald chi-square = 1, df = 1, p < 0.001). Conversely, not having received cybersecurity training was associated with a coefficient of 0.9958 (SE = 4.389), implying a significant effect on the odds of higher cybersecurity knowledge (Wald chi-square = 1, df = 1, p = 0.014).

In summary, the parameter estimates from the reduced ordinal MLR model highlight the effects of different variables on the odds of higher cybersecurity knowledge. The thresholds for different knowledge categories (No Knowledge, Less Knowledge, Good Knowledge) significantly influence the odds of being in higher knowledge categories. Gender (specifically males) and the presence of a reporting procedure also showed statistically significant effects on higher cybersecurity knowledge. Similarly, having received or not received cybersecurity training significantly impacted the odds of higher cybersecurity knowledge.

4.5.4.1 Goodness of Fit Reduced MLR

After fitting the reduced multinomial logistic regression model, its goodness of fit and different measures was examined. The goodness-of-fit statistics for the reduced MLR model examining the relationship between cybersecurity knowledge and the variables of gender, reporting procedure existence, and receipt of cybersecurity training are presented in Table 4-28.

The deviance, a measure of the difference between the observed data and the model's fitted values, is 25.554 with 37 degrees of freedom (df). The scaled deviance is a key metric used to assess the goodness of fit in generalised linear models (GLMs). It quantifies the ratio of the deviance to the dispersion parameter and is employed to test the adequacy of the GLM model (Dobson and Barnett, 2008). The scaled deviance estimated from fitting the model is also 25.554. Both deviance values suggest a relatively good fit to the data.

Table 4-28: Goodness of fit Statistics for the Ordinal MLR of Cybersecurity Knowledge Against Demographic Variables

Goodness of Fit Measures[a]	**Value**	**df**	**Value/df**
Deviance	25.554	37	0.691
Scaled Deviance	25.554	37	
Pearson Chi-Square	21.341	37	0.577
Scaled Pearson Chi-Square	21.341	37	
Log Likelihood[b]	-33.013		
Akaike's Information Criterion (AIC)	82.026		
Finite Sample Corrected AIC (AICC)	82.858		
Bayesian Information Criterion (BIC)	107.658		
Consistent AIC (CAIC)	115.658		
Dependent Variable: Cybersecurity Knowledge Model: (Threshold), Gender, Reporting Procedure Exists, Ever received cybersecurity training			
a. Information criteria are in smaller-is-better form.			
b. The full log likelihood function is displayed and used in computing information criteria.			

The Pearson chi-square statistic, which assesses the discrepancy between observed and expected frequencies, was 21.341 with 37 df. The scaled Pearson chi-square, calculated by dividing the Pearson chi-square by the scale parameter, was also 21.341. These values indicate a reasonable fit of the model to the data.

The log likelihood, a measure of how well the model fits the observed data, was -33.013. A higher log likelihood value would suggest a better fit, but the negative value here indicates that the model may not fit the data optimally.

Several information criteria are provided to evaluate the model's goodness of fit. The Akaike's Information Criterion (AIC) is 82.026, the Finite Sample Corrected AIC (AICC) is 82.858, the Bayesian Information Criterion (BIC) is 107.658, and the Consistent AIC (CAIC) is 115.658. These criteria allow for model comparison, with lower values indicating a better fit. Based on these criteria, the model appears to provide a reasonable fit to the data.

In summary, the multinomial logistic regression model, including the variables of gender, reporting procedure existence, and receipt of cybersecurity training, shows a relatively good fit to the data. The deviance, Pearson chi-square, and their scaled counterparts indicate that the model adequately captures the relationship between the predictors and the cybersecurity knowledge. However, the negative log likelihood suggests that the model may not be the best fit for the data. The information criteria further support the notion that the model provides a reasonable fit, although further model refinement may be necessary to improve the fit.

4.6 Enhancement of the Proposed Framework: Incorporating Insights from Survey Analysis

The research objectives, RO1 and RO2, are effectively tackled through the development of the framework outlined in Section 2.4, titled "Framework for Enhancing Cybersecurity Policy Awareness Programs". This comprehensive framework serves as a key tool in addressing the objectives. The various components of this framework are summarised in Table 4-29, highlighting their relevance, and demonstrating how they contribute to the overall significance of the framework. The table offers a comprehensive representation of both the breadth and depth of these components, emphasising their importance within the framework.

Moving on to the third research question, labelled as RQ3, its objective was to refine the cybersecurity compliance framework. The framework was refined by identifying the factors that influenced cybersecurity knowledge. The data analysis specifically focused on evaluating the impact of demographic factors such as Age, Education, Employment Status, and Experience. Contrary to initial assumptions, the findings challenged the significance of these factors in influencing an individual's cybersecurity knowledge. Notably, the analysis revealed a striking gender disparity, indicating a higher likelihood for males to possess advanced cybersecurity knowledge.

This revelation prompts a pivotal reconsideration of the existing cybersecurity awareness framework. In recognition of the identified gender disparity, a ground-breaking element; gender mainstreaming is introduced into the initiation phase of the framework. Gender mainstreaming involves the integration of gender considerations and perspectives into all stages of the cybersecurity awareness program.

Table 4-29: Evaluation for Cybersecurity Policy Compliance Components Relevance from Data Analysis Results

Components	**Descriptions**	**Insights from Analysis**
Making cybersecurity policy awareness a norm	Provision of cybersecurity policy awareness for all employees, including on boarding programs and regular refresher training;	The relevance of embedding cybersecurity policy awareness as a norm in the compliance framework is evident through a thorough analysis of organisational practices. Questions on new employee induction and on boarding processes identify areas for improvement, such as lower adoption rates in acceptable use training, indicating opportunities to strengthen on boarding programs. Evaluation of policy/procedure training coverage and timelines aligns with the framework's refresher training component. Correlations between different training methods and policy areas highlight interconnectivity, emphasising the need to consider this in refresher design. Establishing cybersecurity as a strategic priority, collaborating with cross-functional teams, and aligning with best practices reflect the framework's goal of making awareness a norm. Performance evaluation and adaptive initiatives based on assessments further support this aspect. By understanding strengths and gaps revealed through questions and analyses, financial institutions can modify induction and refresher processes, fully institutionalising cybersecurity awareness. The findings offer guidance for continually reinforcing policies throughout employee lifecycles, fostering a culture where cybersecurity awareness becomes integral to organisational practices.
Targeted and customised training programs	Targeted and customised training programs based on job roles and responsibilities	The need for targeted and customised training within the cybersecurity policy compliance framework is evident, as survey responses unveil diverse understandings among employees in various roles regarding confidential information, technical controls, knowledge levels, and compliance. Roles not directly handling sensitive data may lack comprehension of compliance policies, emphasising the necessity for tailored training. Simultaneously, role-specific variations in cybersecurity awareness indicate potential gaps, prompting the integration of customised training to reinforce the link between tasks and risks. Correlations between perceived cybersecurity importance and compliance behaviours

		guide role-specific training efforts, ensuring a focused understanding of technical controls in specific work contexts. The targeted training component is crucial, as specific cybersecurity behaviour analysis reveals the importance of emphasising behaviours like password sharing, acknowledged by 50% of respondents. A positive correlation between information sensitivity recognition and technical controls suggests the need for simulated phishing exercises. Feedback on the dangers of password reuse could be supplemented with modules for reinforcement. Combining both targeted and customised training within the framework maximises impact, effectively addressing specific issues and cultural shifts identified through analyses, optimising awareness across the financial institution by resonating directly with diverse work functions.
Continuous and ongoing awareness campaigns	Regularly updating and refreshing training and awareness programs to address evolving cybersecurity threats and risks	The relevance of the continuous and ongoing training component in the cybersecurity policy compliance framework is supported by survey responses. The analysis, focusing on intentions for future training, revealed that an overwhelming 83.6% of respondents expressed positive intentions toward attending cybersecurity training programs. A substantial percentage, 42.9%, agreed, while an even higher 40.7% strongly agreed, demonstrating robust interest. Few respondents expressed uncertainty or negativity, with only 8.2% holding negative views and another 8.2% being neutral. These detailed response breakdowns indicate widespread positive reception among employees for continuous, ongoing cybersecurity awareness efforts, aligning well with the framework's proposed approach. The significant percentage expressing strong interest suggests a keen willingness to participate in additional training. Incorporating these insights into planning future training programs, structured as envisioned, financial institutions can anticipate high levels of participation and engagement from their workforces. The findings affirm that regularly updated and interactive training courses resonate with employees' preferences and interests, ensuring the effectiveness of ongoing cybersecurity education efforts.

Implementation of simulated phishing exercises	Conduct simulated phishing exercises to improve employee awareness and readiness to detect and report phishing attacks	In this study, financial institutions employ diverse cybersecurity policy training methods for IT employees, ranging from no specific training to conventional methods, phishing simulations, and online training, or a mix. The increasing popularity of online training and the integration of phishing simulations signal a shift towards practical and interactive approaches. This reflects a recognition of the dynamic nature of cyber threats, emphasising experiential learning. Implementing simulated phishing exercises within the cybersecurity policy compliance framework is crucial for enhancing training effectiveness. This approach not only aligns with evolving preferences but also fosters a proactive, hands-on approach, preparing IT employees to navigate real-world cyber threats more adeptly.
Assessment of Awareness Program Effectiveness	Regular assessments of employee knowledge, skills, and attitudes towards cybersecurity to identify areas for improvement	The assessment of awareness program effectiveness is crucial within the cybersecurity training framework, as revealed by the questionnaire and analyses. These components evaluate participants' education levels, training attendance, and self-rated knowledge, exposing gaps in awareness and uncertainties about training status. The analyses underscore the importance of comprehensive assessments to identify knowledge gaps and uncertainties, emphasising the need for alignment with desired cybersecurity practices. The correlation analysis among IT employees' perceptions reveals the interconnectedness of factors like working with sensitive information, technical controls, knowledge, attitudes, and policy compliance. These findings stress the significance of ongoing assessments, targeted training initiatives, and a comprehensive approach to enhance employees' cybersecurity knowledge, skills, and attitudes.

4.6.1 Refined Framework: Cybersecurity Policy Compliance

This section presents a refined and inclusive framework for a cybersecurity policy awareness program, enriched by the recognition of gender disparities and the subsequent integration of gender mainstreaming as an essential and transformative component. This evolution aims not only to fortify organisational cybersecurity culture but also to create an environment that is equally empowering for all individuals, irrespective of gender, in their journey toward cybersecurity proficiency.

1. Assessing Gender Inclusivity

- **Objective:** Evaluate the current state of gender inclusivity within cybersecurity policies and practices.
- **Actions:**
    - Secure leadership support for addressing gender disparities.
    - Define objectives prioritising gender inclusivity.
    - Form a diverse cross-functional team considering gender perspectives.
    - Tailor the communication plan to be inclusive, avoiding gender stereotypes.
    - Conduct a comprehensive analysis of gender-specific cybersecurity knowledge and skills gaps.

2. Make Cybersecurity Policy Awareness a Norm:

- **Objective:** Provide cybersecurity policy awareness for all employees.
- **Actions:**
    - Incorporate gender-inclusive language and scenarios in policy awareness programs.
    - Integrate gender considerations in on boarding programs and regular refresher training.

3. Targeted and Customised Training Programs:

- **Objective:** Provide targeted training based on job roles and responsibilities.
- **Actions:**
    - Identify gender-specific training needs based on the analysis conducted during the initiation phase.

    - Customise training programs to address gender-specific cybersecurity challenges.

4. Continuous and Ongoing Awareness Programs:

- **Objective:** Regularly update and refresh awareness programs.
- **Actions:**
    - Integrate gender mainstreaming principles into ongoing awareness efforts.
    - Ensure that updates address gender-specific trends and concerns.

5. Implementation of Simulated Phishing Exercises:

- **Objective:** Improve employee awareness and readiness to detect phishing attacks.
- **Actions:**
    - Include gender-inclusive scenarios in simulated phishing exercises.
    - Evaluate responses considering gender-related nuances.

6. Evaluation of the Effectiveness of the Awareness Program:

- **Objective:** Regularly evaluate employee knowledge, skills, and attitudes.
- **Actions:**
    - Incorporate gender-specific metrics in evaluations.
    - Use feedback mechanisms to gather insights into the effectiveness of gender-inclusive strategies.

By incorporating the initiation phase (**Assessing Gender Inclusivity)** and emphasising gender inclusivity throughout the framework, the cybersecurity awareness program becomes not only more robust in addressing cybersecurity policy compliance challenges but also more inclusive and supportive of individuals of all genders in their pursuit of proficiency in cybersecurity.

In conclusion, this study has successfully addressed the research objectives through the development of a comprehensive framework for enhancing cybersecurity policy awareness programs. The framework, outlined in Section 4.6.1, served as a valuable tool in achieving the objectives. The components of the framework, summarised in Table 4-29, showcase its breadth and depth in addressing cybersecurity challenges. The research also enhances the framework by exploring the factors that influence cybersecurity policy knowledge.

Understanding these determinants can contribute to the development of targeted awareness programs, ensuring a more tailored approach to enhancing employee behaviour and compliance. The findings highlight the importance of making cybersecurity policy awareness a norm, targeted and customised awareness programs, continuous and ongoing awareness programs, implementation of simulated phishing exercises, and the assessment of awareness programs effectiveness. By implementing these components, financial institutions can enhance employee cybersecurity knowledge, reduce vulnerabilities, and foster a culture of security awareness. The study's insights contribute to the growing body of knowledge on cybersecurity education and provide practical recommendations for organisations seeking to improve their cybersecurity policies and compliance.

4.7 Chapter Summary

Chapter 4 presents empirical outcomes derived from the methodologies outlined in Chapter 3. Reliability analysis was employed to gauge data dependability and alignment with proposed analysis methods, using Cronbach's alpha to evaluate internal consistency. Demographic and descriptive analyses shed light on cybersecurity data attributes. Advanced statistical techniques such as regression analysis, diagnostic testing, and machine learning were used effectively, accompanied by detailed analytical essays. This chapter further presents the refined proposed framework. Chapter 5 concludes with an overview of findings and suggestions for future research.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

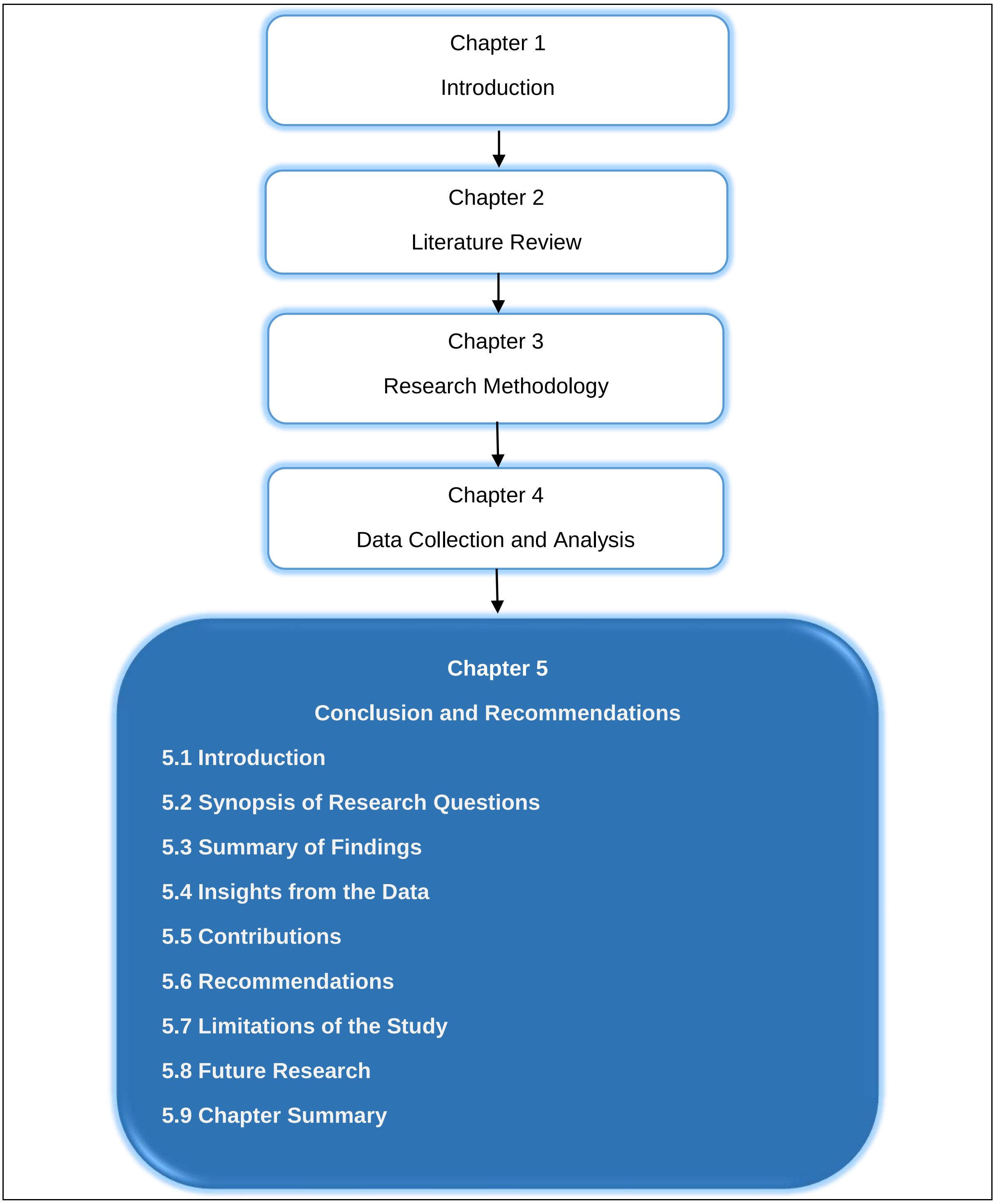


Figure 5-1: Roadmap of Chapter 5

5.1 Introduction

This concluding chapter synthesised the research journey undertaken to enhance the effectiveness of cybersecurity policy awareness programs in financial institutions. At the core of this investigation were the research questions and objectives outlined in Chapter 1. The primary research question focused on how can cybersecurity compliance be improved through cybersecurity policy awareness and employee behaviour in financial institutions. The chapter commenced with a synopsis of the research questions, evaluating the extent to which the study has fulfilled its objectives. This discussion was followed by a summary of findings, insights drawn from data analysis, the study's contributions, and recommendations tailored for pertinent stakeholders. Additionally, the chapter addressed the study's limitations, introduced an enhanced and refined framework, and concluded with a chapter summary.

5.2 Synopsis of Research Questions

The researcher stated research questions and research objectives to be answered and achieved for the successful completion of the study. This section outlines how these research objectives were addressed to attain the overall objective of the study which was to develop a framework for improving cybersecurity policy awareness programs to enhance employee behaviour toward cybersecurity compliance in financial institutions.

The problem addressed in this research is **that the cybersecurity policy awareness programs do not influence employees to comply with their organisational cybersecurity policies**. The research proposed a cybersecurity compliance framework to improve cybersecurity policy awareness and employees' behaviour in financial institutions. This led to the primary research question, formulated as follows**:**
How can cybersecurity compliance be improved through cybersecurity policy awareness and employee behaviour in financial institutions? This question led to the study's primary objective: **To develop cybersecurity compliance framework for improving cybersecurity policy awareness and employee behaviour in financial institutions.**
This section offers an overview of how each sub-question was addressed to answer the research question and achieve the research objective.

5.2.1 Research Question 1

What are the requirements for an employee cybersecurity compliance framework in financial institutions?

To address Research Question 1, extensive literature was reviewed to identify best practices, limitations, and recommendations from various studies that explored effective strategies for improving cybersecurity awareness programs and fostering a security-conscious culture among employees, as detailed in Section 2.3. Drawing insights from these findings, the study proposed a comprehensive framework in Section 2.4 aimed at enhancing cybersecurity policy awareness programs within financial institutions.

The proposed framework is built upon components derived from identified best practices. These components include making cybersecurity policy awareness a norm for all employees, developing targeted and customised awareness programs, implementing ongoing training initiatives, conducting simulated phishing exercises, and assessing awareness program effectiveness. The framework is designed to address the specific needs and challenges of employees' roles within financial institutions, emphasising the importance of tailored, continuous, and interactive approaches.

5.2.2 Research Question 2

How to design a cybersecurity compliance framework through effective cybersecurity policy awareness programs?

To answer Research Question 2, the study presents a detailed preliminary framework in Section 2.4 for enhancing cybersecurity policy awareness programs. This framework is meticulously designed to improve employee behaviour towards cybersecurity compliance within financial institutions. The components of the proposed framework, as outlined in Section 5.2.1 were systematically organised to illustrating their interdependencies and contribution to the overarching "Cybersecurity Policy Compliance” Framework. The study further outlined the systematic implementation of this framework, guided by a conceptual framework. The step-by-step process involves making cybersecurity policy awareness a norm, implementing targeted and customised training programs, conducting continuous awareness campaigns, executing simulated phishing exercises, and evaluating program effectiveness. This implementation strategy ensures a comprehensive and effective approach to designing and deploying cybersecurity policy awareness programs that foster a culture of compliance and address evolving cybersecurity risks.

Furthermore, to answer Research Question 2, the researcher developed a questionnaire to determine the relevance of the components of the proposed framework. The collected data was analysed, and the findings presented in Section 4.6, Table 4-29 confirmed the relevance of the components. The study did not only confirm the relevance of the components of the proposed framework through data analysis but also identified additional component such as gender inclusivity assessment, which could be integrated into the framework for a more comprehensive approach, which is addressed in Section 5.2.3.

5.2.3 Research Question 3

How to refine cybersecurity compliance framework?

In this study, a statistical analysis was conducted using the multinomial logistic regression (MLR) model to examine the relationship between a four-level ordinal categorical variable of

Cybersecurity Knowledge ("No Knowledge," "Less Knowledge," "Good Knowledge," and "Excellent Knowledge") and a set of predictors. We chose the MLR model due to its appropriateness and effectiveness in modelling such relationships. The predictor variables included in the initial model were Gender, Age Group, Educational Attainment, Employment Status, Sector, Experience in Sector, Existence of Reporting Procedure, and Previous Cybersecurity Training.

After conducting comprehensive Goodness of Fit tests, including deviance, Pearson chi-square, and various Information Criteria, there existed many of the variables that were not statistically significant at the α = 5% significance level. Consequently, these variables were removed from the final reduced model. The variables that remained statistically significant in the final model were Gender, Existence of Reporting Procedure, and Previous Cybersecurity Training.

These findings were enlightening as they challenged our previously held and untested assumption that Age, Education, Employment Status, and Experience would significantly influence an individual's level of cybersecurity knowledge, hence their inclusion in the initial model. The results indicate that institutions cannot solely rely on factors such as hiring highly educated and experienced individuals or individuals from specific age groups to improve their cybersecurity culture. Instead, organisations need to take concrete steps, such as providing training and establishing reporting procedures for cybersecurity incidents, in order to enhance employees' cybersecurity knowledge and the institutions cybersecurity culture.

Furthermore, this study’s analysis revealed an important finding regarding gender differences. Males were found to be more likely to have higher cybersecurity knowledge, which raises implications regarding empowerment issues concerning women in the field of cybersecurity. This gender disparity was also considered as a new component to be incorporated into the proposed refined framework presented in Section 4.6.1, with a focus on gender mainstreaming.

Overall, this study highlights the importance of proactive measures such as training programs and the establishment of reporting procedures, in improving cybersecurity knowledge among employees. It also emphasises the need to address gender disparities in cybersecurity to promote inclusivity and diversity. Through this analysis, the requirements of the third research objective quite comprehensively, were met.

5.3 Summary of Findings

1. In the classification analysis, the K-nearest neighbours (KNN) algorithm was applied to group individuals into clusters based on various features. Four clusters were identified, each exhibiting distinct characteristics. Cluster 1 showed a higher representation of males and employed individuals. While the age in this cluster was slightly higher, the educational attainment was lower compared to other clusters. Cluster 2 had a higher representation of females, a specific employment status that deviated significantly from the average, lower age, and less experience in the sector. Cluster 3 had a relatively lower age, a specific employment status that slightly deviated from the average, and lower prevalence of certain cybersecurity factors. Cluster 4 showed a relatively balanced distribution across variables, with a slight emphasis on higher scores and higher prevalence of certain cybersecurity factors.
2. ANOVA was used to examine differences among the clusters generated by the KNN algorithm. Significant variations were found in several variables across clusters. These variables included age group, employment status, sector, experience in the sector, cybersecurity induction, existence of a reporting procedure, and previous cybersecurity training. The ANOVA results indicated that these variables significantly contributed to the differences observed among the clusters.
3. The discriminant analysis results provide insights into the factors influencing cybersecurity knowledge levels. While some factors such as gender, age group, educational attainment, employment status, sector, and experience in the sector showed no significant differences, factors related to training, induction, and intention to participate in future training emerged as critical contributors to cybersecurity knowledge. These findings emphasise the need for targeted interventions and comprehensive training programs that address the specific needs of individuals and organisations.
4. It was highlighted in the methodology chapter that high inter-correlations among independent variables can distort statistical model parameters and lead to unreliable results. The data analysis chapter assessed multicollinearity using tolerance and variance inflation factor (VIF). The findings indicated that the independent variables in the model did not suffer from severe multicollinearity. Tolerance values ranged from 0.689 to 0.952, suggesting low multicollinearity, while VIF values ranged from 1.051 to 1.451, all below the threshold of 10. This implies that the relationships between the independent variables and cybersecurity knowledge could be assessed without significant concerns about distorted results.
5. The analysis employs multinomial logistic regression to examine the relationship between the independent variables and the dependent variable, which represents different levels

of cybersecurity knowledge. The cumulative logit link function and multinomial distribution are used to estimate probabilities associated with each knowledge level. The results show that individuals with no cybersecurity knowledge are significantly less likely to have higher knowledge levels compared to those with some level of knowledge. Additionally, males tend to have a slightly higher likelihood of possessing greater cybersecurity knowledge than females.

6. Regarding the demographic variables, age groups, educational attainment, employment status, and most sectors do not exhibit significant associations with cybersecurity knowledge. However, individuals with 1 to 3 years of experience in the sector have a significantly higher likelihood of possessing greater cybersecurity knowledge. Conversely, the presence of a reporting procedure for cybersecurity incidents is associated with a significantly lower likelihood of higher knowledge levels. Similarly, not receiving cybersecurity training is linked to a significantly lower likelihood of greater cybersecurity knowledge.
7. A reduced-form multinomial logistic regression was finally fitted to the model as the many-variable model showed significant lack of fit to the data. Consequently, this model performed much better and showed significant fit almost across the board. Gender, existence reporting procedure, previous cybersecurity training was found to have significantly better fit to the data, although gender was not significant at the 5% level.

5.4 Insights from the Data

In this study, the chapter showing the analyses is crucial for understanding prevailing cybersecurity perceptions and attitudes among individuals and organisations. It provides insights into current practices regarding password management, data privacy protection, and other relevant issues. Notably, the regression modelling reveals that many variables that could theoretically positively influence individuals' cybersecurity knowledge do not have a statistically significant effect. This highlights an important dimension: institutions cannot assume that having a highly educated and experienced workforce guarantees a healthy cybersecurity culture or environment. Only the presence of a reporting procedure and previous cybersecurity training was found to be statistically significant, underscoring the fact that higher education and experience in the financial sector do not automatically impart strong cybersecurity traits. Although model fit is often a concern in various applications, in this case, it is a welcome development, as it elucidates a crucial dynamic.

Moreover, the classification analysis (KNN and Discriminant Analysis) indicates that distinct groups of people may exist, requiring different types of training based on their varying levels of cybersecurity knowledge, influenced by inherent traits such as age, gender, education, and experience. Younger, less experienced, and less educated employees may have different attitudes, practices, and behaviours related to cybersecurity compared to their older, more educated, and experienced counterparts. Utilising classification methods can ensure that the appropriate training and awareness campaigns are directed at the specific groups that require them.

This information should then be vital in designing cybersecurity policy, as it is imperative that such policy be completely indifferent to intrinsic social and demographic characteristics of individuals. It is only actual interventions by institutions that are likely to yield the desired effects.

5.5 Contributions

This study, which addressed cybersecurity policy compliance in financial institutions, has produced significant contributions, both in theoretical and practical terms. This section aims to highlight and discuss these valuable contributions in relation to the objectives of the study.

5.5.1 Theoretical Contribution

The theoretical contribution of this study lies in the comprehensive framework developed (Cybersecurity Policy Compliance (CSPC)) for enhancing cybersecurity policy awareness programs within financial institutions. The research objectives (RO1-RO2) were systematically addressed through the formulated framework, emphasising essential components necessary for effective cybersecurity policies. The framework entails making cybersecurity policy awareness a norm, targeted and customised awareness programs, continuous awareness programs, simulated phishing exercises, and ongoing assessment of program effectiveness. This framework not only educates employees about cybersecurity, but also tailors training to their specific roles and incorporates engaging elements such as gamification.

5.5.2 Practical Contribution

The contribution of a study can be significant in several ways, such as

Improved Cybersecurity: The framework can help organisations improve their overall cybersecurity posture by improving the knowledge, skills, and awareness of employees about cybersecurity threats and best practices.

Reduced Cyber Risk: By implementing the framework, organisations can reduce the risk of cyber-attacks and data breaches, which can result in significant financial and reputational damage.

Better Compliance: The framework can help organisations comply with relevant cybersecurity regulations and standards, which can help them avoid penalties and legal consequences.

Improved Employee Engagement: The use of targeted and customised training programs, gamification, and incentives can help engage employees in the cybersecurity program, leading to higher levels of awareness, motivation, and participation.

Improved Organisational Culture: By fostering a cybersecurity culture, the framework can help embed cybersecurity as a core value and priority within the organisation, leading to greater collaboration, communication, and shared responsibility for cybersecurity.

In general, the theoretical contribution lies in the development of the CSPC framework, while the practical contribution includes improved cybersecurity, reduced cyber risk, better compliance, improved employee engagement, and an enhanced organisational cybersecurity culture.

5.6 Recommendations

Based on the findings and insights gained from this study, the following recommendations are proposed to enhance cybersecurity policy awareness programs and foster inclusivity within organisational cybersecurity cultures:

Regularly Update and Refine Awareness Programs: Given the dynamic nature of cybersecurity threats and the evolving understanding of demographic influences, financial institutions should ensure that awareness programs are regularly updated and refined. Incorporate new insights and adapt strategies to address emerging challenges unique to the financial sector.

Establish Reporting Mechanisms for Discrepancies: Financial institutions should implement clear reporting mechanisms for individuals who may perceive or experience gender-based discrepancies in knowledge and skills development. Encourage open communication and take prompt action to address any identified issues, recognising the specific challenges within the financial sector.

Leadership Support and Advocacy: Financial institutions should secure support from organisational leadership to drive gender-inclusive initiatives. Advocate for the importance of diversity and inclusion in cybersecurity within the financial sector to create a culture that values the contributions of individuals irrespective of gender.

Measure and Evaluate Inclusivity Impact: Financial institutions should implement metrics and evaluation mechanisms specifically focused on inclusivity and diversity within cybersecurity awareness programs. Regularly assess the impact of gender mainstreaming initiatives within the financial context and adjust strategies based on feedback and outcomes tailored to the unique challenges of the financial industry.

5.7 Limitations of the Study

The study had limitations that are discussed below:

The scope of the study was limited to financial institutions in Lesotho, and the developed framework may not be applicable to other industries or organisations. The study was also limited to a quantitative analysis of the current state of cybersecurity policy training in financial institutions and did not involve a qualitative analysis of the effectiveness of the proposed framework. Therefore, future research is needed to assess the effectiveness of the framework developed in this study.

Another limitation of this study is that it was cross-sectional, and data was collected at one time. The studies reviewed were limited to a specific time frame (2016-2023) and those published in the English language, which may lead to the exclusion of relevant articles published in other languages. Additionally, due to the rapidly changing nature of cybersecurity threats, some of the articles included in the review of the literature may not reflect the latest developments in the field of cybersecurity. Therefore, the effect of the survey could not be measured after the intervention was administered. Longitudinal studies may be needed to assess the sustainability of the intervention and changes in the attitudes and behaviours of employees over time.

Lastly, due to Covid-19 regulations, the researcher was not allowed to physically meet the participants and the study was carried out using an online survey questionnaire. The survey provided participants with predefined answers, as the questions were closed-ended. The researcher assumed that asking participants to provide answers on their own in a qualitative form would take time. In addition, participants might not provide the correct answers as they might need clarity, which would be a challenge as the researcher would not be present at the time they fill the questionnaire. As a result, the researcher may not easily obtain the reasons for some of the questions, which may be answered by participants who may disagree with the statements. The limitations in data collection may have affected the reliability of the study, and future studies may need to explore different data collection methods to obtain a more nuanced understanding of the attitudes and behaviours of employees toward cybersecurity compliance.

5.8 Future Research

To enhance the reliability and applicability of the developed framework, future research should adopt a dual-pronged strategy. Firstly, there is a pressing need to validate the framework using diverse datasets, incorporating a range of demographic backgrounds and institutional settings. This comprehensive validation is crucial to thoroughly assess the generalisability and ensure its robustness in predicting cybersecurity knowledge across varied populations and contexts. The scope of future research should extend beyond the confines of the current study, with the aim of applying and refine the developed framework in other industries or organisations. Conducting similar studies in diverse sectors could contribute to a more holistic understanding of cybersecurity awareness needs and facilitate adjustments to the framework to accommodate different organisational contexts.

Moreover, collaboration with cybersecurity experts during the validation process is paramount. Leveraging the insights of experts would provide an external perspective, aligning the framework with industry best practices, current threat landscapes, and emerging trends in cybersecurity. This collaborative effort would significantly contribute to refining the framework's effectiveness and relevance in real-world cybersecurity scenarios. Future research should incorporate qualitative methodologies, such as interviews or focus groups, to deepen the subjective experiences and perceptions of individuals who undergo cybersecurity policy training. This will provide a more holistic understanding of the impact and identify areas for improvement.

Furthermore, future research should advocate for longitudinal studies to establish causal relationships between demographic variables and changes in cybersecurity knowledge over time. Understanding how these variables influence knowledge development longitudinally can provide valuable insights for targeted educational interventions. This approach allows for a deeper understanding of the dynamics between demographic factors and cybersecurity awareness, enabling the development of more effective and tailored awareness programs.

5.9 Chapter Summary

This chapter addressed the research objectives and summarised the study findings. The research objectives of this study focused on improving cybersecurity policy awareness programs and their impact on employee behaviour toward cybersecurity compliance in financial institutions. The first objective was to identify the requirements for a framework that would effectively enhance cybersecurity policy awareness programs and influence employee behaviour. The second objective involved designing and analysing a framework that would facilitate the development of effective cybersecurity policy awareness programs tailored to the specific needs of financial institutions. Finally, the third objective was to refine the proposed framework by incorporating insights from the statistical analysis. Together, these objectives aimed to contribute to understanding how to improve awareness of cybersecurity policies and promote compliance among financial sector employees.

Based on these conclusions, recommendations were proposed to prioritise cybersecurity, implement best practices, and foster a culture of cybersecurity. These recommendations are directed at organisations, employees, customers, government agencies, and cybersecurity professionals, with the aim of improving overall cybersecurity, reducing risk, promoting compliance, and improving employee engagement.

The study made theoretical contributions by developing the Cybersecurity Policy Compliance Framework (CSPC), which serves as a valuable tool for organisations to strengthen their cybersecurity posture and mitigate risks. However, limitations such as the non-random sampling method, limited generalisability, and lack of qualitative analysis and longitudinal data should be considered. Future research should explore the effectiveness of the framework in different contexts and industries and incorporate qualitative and longitudinal approaches.

In summary, this study provides valuable information on employee behaviour towards cybersecurity compliance in financial institutions and proposes a framework to enhance cybersecurity education programs. The findings and recommendations have practical implications for strengthening cybersecurity policy measures and mitigating risks in the digital landscape. By implementing the framework and recommended practices, organisations can improve their posture toward cybersecurity policies and protect against potential cyber threats.

REFERENCES

ABA BankingJournal (2023) ‘Verizon report : cyber incidents , breaches driven by external actors’.

Acharya, S. and Joshi, S. (2020) *Impact Of cyber-attacks on Banking Institutions in India: A Study Of Safety Mechanisms and Preventive Measures*, *PJAEE*.

Agresti, A. (2015) *Foundations Linear Generalized Linear Models*, *John Wiley & Sons, Inc.*

Ahmad, Z. *et al.* (2019) ‘Security monitoring and information security assurance behaviour among employees: An empirical analysis’, *Information and Computer Security*, 27(2), pp. 165–188. Available at: https://doi.org/10.1108/ICS-10-2017-0073.

Akintoye, R. *et al.* (2022) ‘Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria’, *Universal Journal of Accounting and Finance*, 10(3), pp. 643–652. Available at: https://doi.org/10.13189/ujaf.2022.100302.

Al-Alawi, A.I. and Al-Bassam, S.A. (2021) ‘Assessing the factors of cybersecurity awareness in the banking sector’, *Arab Gulf Journal of Scientific Research*, 37(4), pp. 17–32. Available at: https://doi.org/10.51758/agjsr-04-2019-0014.

Alhashmi, A A *et al.* (2021) *Taxonomy of Cybersecurity Awareness Delivery Methods: A Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats Countermeasure for Phishing Threats Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure*, *IJACSA) International Journal of Advanced Computer Science and Applications*. Available at: www.ijacsa.thesai.org.

Alkassim, R.S. and Tran, X. (2016) ‘Comparison of Convenience Sampling and Purposive Sampling Related papers’. Available at: https://doi.org/10.11648/j.ajtas.20160501.11.

Almeida, M.C. *et al.* (2022) ‘Do Leadership Styles Influence Employee Information Systems Security Intention? A Study of the Banking Industry’, *Global Journal of Flexible Systems Management*, 23(4), pp. 535–550. Available at: https://doi.org/10.1007/s40171-022-00320-1.

Almrezeq, N., Alserhani, F. and Humayun, M. (2021) ‘Exploratory Study to Measure Awareness of Cybercrime in Saudi Arabia’, *Turkish Journal of Computer and Mathematics Education*, 12(10), pp. 2992–2999.

Alotaibi, F. *et al.* (2016) ‘A Review of Using Gaming Technology for Cyber-Security

Awareness', *International Journal for Information Security Research (IJISR)* [Preprint]. Available at: www.gamespot.com;

Alp Consulting (2024) 'Difference Between IT Recruitment & non-IT Recruitment'.

Alqahtani, M. and Braun, R. (2021) 'Reviewing influence of UTAUT2 factors on cyber security compliance: A literature review', *IBIMA Business Review*. IBIMA Publishing. Available at: https://doi.org/10.5171/2021.666987.

Alshaikh, M. *et al.* (2019) 'Toward sustainable behaviour change: An approach for cyber security education training and awareness', *27th European Conference on Information Systems - Information Systems for a Sharing Society, ECIS 2019* [Preprint], (November).

Alzahrani, L. (2021) 'Factors Impacting Users' Compliance with Information Security Policies: An Empirical Study', *International Journal of Advanced Computer Science and Applications*, 12(10), pp. 437–447. Available at: https://doi.org/10.14569/IJACSA.2021.0121049.

Back, S. and Guerette, R.T. (2021) 'Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks', *Journal of Contemporary Criminal Justice*, 37(3), pp. 427–451. Available at: https://doi.org/10.1177/10439862211001628.

Bayaga, A. (2010) 'Quantitative Methods Inquires MULTINOMIAL LOGISTIC REGRESSION : USAGE AND APPLICATION IN RISK ANALYSIS', pp. 288–297.

Bell, E., Bryman, A. and Harley, B. (2022) *Business research methods*. Oxford university press.

Bengaluru, K., Singh, M.K. and Kumar, V. (2020) 'Impact of Covid-19 Pandemic on Working Culture: An Exploratory Research Among Information Technology (IT) Professionals in Impact of Covid-19 Pandemic on Working Culture: An Exploratory Research Among Information Technology (IT) Professionals in Bengaluru, Karnataka (India)'. Available at: https://www.researchgate.net/publication/342657957.

Bhandari, P. (2021) 'Questionnaire Design | Methods, Question Types & Examples', *Scribbr* [Preprint]. Available at: https://www.scribbr.com/methodology/questionnaire/.

Bobbitt, Z. (2021) 'What is an Omnibus Test? (Definition & Examples)', *Stratology* [Preprint]. Available at: https://www.statology.org/omnibus-test/.

BOX, G.E. (1949) ‘A general distribution theory for a class of likelihood criteria.’, *Biometrika*, 36(3–4), pp. 317–346. Available at: https://doi.org/10.1093/biomet/36.3-4.317.

Box, G.E.P. (1954) ‘Some Theorems on Quadratic Forms Applied in the Study of Analysis of Variance Problems , II . Effects of Inequality of Variance and of Correlation Between Errors in the Two-Way Classification Author (s): G . E . P . Box Published by : Institute of Mathe’, 25(3). Available at: https://about.jstor.org/terms.

Catherine Dawson (2009) ‘Introduction to Research Methods A Practical Guide for Anyone Undertaking a Research Project by Catherine Dawson (z-lib.org)’.

Chang, L.Y.C. and Coppel, N. (2020) ‘Building cyber security awareness in a developing country: Lessons from Myanmar’, *Computers and Security*, 97, p. 101959. Available at: https://doi.org/10.1016/j.cose.2020.101959.

Chen, H., Chau, P.Y.K. and Li, W. (2019) ‘The effects of moral disengagement and organizational ethical climate on insiders’ information security policy violation behavior’, *Information Technology and People*, 32(4), pp. 973–992. Available at: https://doi.org/10.1108/ITP-12-2017-0421.

Cochran, W.G. (1977) ‘Cochran_1977_Sampling Techniques.pdf’, pp. 1–428.

Cohen, L., Manion, L. and Morrison, K. (2017) *Research Methods in Education*.

Corallo, A. *et al.* (2022) ‘Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review’, *Computers in Industry*, 137. Available at: https://doi.org/10.1016/j.compind.2022.103614.

Corradini, I. and Corradini, I. (2020) ‘Building a Cybersecurity Culture’, in *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology*. Springer Nature Switzerland AG 2020, pp. 63–86. Available at: https://doi.org/10.1007/978-3-030-43999-6.

Creswell, J.W. (2014) *Research Design: qualitative, quantitative, and mixed methods approaches*. Fourth Edi. SAGE Publications, Inc.

Creswell, J.W. and Creswell, D.J. (2018) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Fifth Edit. Edited by H. Salmon et al. Los Angeles: SAGE Publications, Inc. Available at: https://lccn.loc.gov/2017044644 (Accessed: 29 April 2022).

Cybersecurity, C.I. (2018) ‘Framework for Improving Critical Infrastructure Cybersecurity’, *National Institute of Standards and Technology* [Preprint], (Version 1.1).

Daengsi, T., Pornpongtechavanich, P. and Wuttidittachotti, P. (2022) ‘Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks’, *Education and Information Technologies*, 27(4), pp. 4729–4752. Available at: https://doi.org/10.1007/s10639-021-10806-7.

Daoud, J.I. (2018) ‘Multicollinearity and Regression Analysis’, *Journal of Physics: Conference Series*, 949(1). Available at: https://doi.org/10.1088/1742-6596/949/1/012009.

Dobson, A.J. and Barnett, A.. (2008) *An Introduction to Generalized Linear Models*, *Technometrics*. Available at: https://doi.org/10.2307/1269239.

Donalds, C. and Osei-Bryson, K.M. (2020) ‘Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents’, *International Journal of Information Management*, 51, p. 102056. Available at: https://doi.org/10.1016/J.IJINFOMGT.2019.102056.

Dupont, B. (2019) ‘The cyber-resilience of financial institutions: Significance and applicability’, *Journal of Cybersecurity*. Oxford University Press. Available at: https://doi.org/10.1093/cybsec/tyz013.

Farheen Ansari, M. (2022) *An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy*. Available at: www.irjet.net.

Fisher, R., Porod, C. and Peterson, S. (2021) ‘Motivating Employees and Organisations to Adopt a Cybersecurity-Focused Culture’, *Journal of Organizational Psychology* [Preprint].

Flashpoint (2022) ‘Flashpoint Year In Review_ 2022 Financial Threat Landscape _ Flashpoint’. Available at: https://flashpoint.io/blog/risk-intelligence-year-in-review-financial/.

Furuichi, M. and Aibara, M. (2019) ‘A Challenge of Developing Serious Games to Raise the Awareness of Cybersecurity Issues’, in *Proceedings of DiGRA 2019*.

Gasiba, T.E. *et al.* (2021) ‘Cybersecurity Awareness Platform with Virtual Coach and Automated Challenge Assessment’, *In Computer Security: ESORICS 2020 International Workshops* [Preprint]. Available at: http://arxiv.org/abs/2102.10430.

Georgiadou, A. *et al.* (2022) ‘A Cyber-Security Culture Framework for Assessing Organization Readiness’, *Journal of Computer Information Systems*, 62(3), pp. 452–462. Available at: https://doi.org/10.1080/08874417.2020.1845583.

Georgiadou, A., Mouzakitis, S. and Askounis, D. (2021) ‘Designing a Cyber-security Culture Assessment Survey Targeting Critical Infrastructures During Covid-19 Crisis’, *International Journal of Network Security & Its Applications*, 13(1), pp. 33–50. Available at: https://doi.org/10.5121/ijnsa.2021.13103.

Ghelani, D. *et al.* (2022) ‘Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking’, *American Journal of Computer Science and Technology*, x, No. x, pp. x–x. Available at: https://doi.org/10.22541/au.166385206.63311335/v1.

Greig, J. (2023) ‘Capital One becomes latest bank affected by cyberattack on debt-buying giant’.

Guba, E.G. and Lincoln, Y.S. (2011) ‘“Paradigmatic Controversies, Contradictions and Emerging Confluences, revised” The Sage handbook of qualitative research’, *The Landscape of Qualitative Research*, 4, pp. 97–128.

Hajny, J. *et al.* (2021) ‘Framework, Tools and Good Practices for Cybersecurity Curricula’, *IEEE Access*, 9, pp. 94723–94747. Available at: https://doi.org/10.1109/ACCESS.2021.3093952.

Hasani, T. *et al.* (2023) *Evaluating the adoption of cybersecurity and its influence on organizational performance*, *SN Business & Economics*. Springer International Publishing. Available at: https://doi.org/10.1007/s43546-023-00477-6.

He, W. *et al.* (2020) ‘Improving employees’ intellectual capacity for cybersecurity through evidence-based malware training’, *Journal of Intellectual Capital*, 21(2), pp. 203–213. Available at: https://doi.org/10.1108/JIC-05-2019-0112.

He, W. and Zhang, Z. (2019) ‘Enterprise cybersecurity training and awareness programs: Recommendations for success’, *Journal of Organizational Computing and Electronic Commerce*, 29(4), pp. 249–257. Available at: https://doi.org/10.1080/10919392.2019.1611528.

Heale, R. and Twycross, A. (2015) ‘Validity and reliability in quantitative studies’, 18(3), pp. 66–67.

Hosmer, D. and Lemeshow, S. (2000) ‘Applied_Logistic_Regression.pdf’.

Hu, S., Hsu, C. and Zhou, Z. (2021a) ‘Security Education, Training, and Awareness Programs: Literature Review’, *Journal of Computer Information Systems* [Preprint]. Available at: https://doi.org/10.1080/08874417.2021.1913671.

Hu, S., Hsu, C. and Zhou, Z. (2021b) 'Security Education, Training, and Awareness Programs: Literature Review', *Journal of Computer Information Systems* [Preprint]. Available at: https://doi.org/10.1080/08874417.2021.1913671.

Hu, S., Hsu, C. and Zhou, Z. (2022) 'Security Education, Training, and Awareness Programs: Literature Review', *Journal of Computer Information Systems*. Taylor and Francis Ltd., pp. 752–764. Available at: https://doi.org/10.1080/08874417.2021.1913671.

Huang Cybersecurity, K., Sloan, M. and Cybersecurity, K.P. (2019) 'For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture', in *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Available at: https://hdl.handle.net/10125/60074.

Huang, K. and Pearlson, K. (2019) 'Building a Model of Organizational Cybersecurity Culture', *Mit Cams*, pp. 1–25.

IBM Security (2023) 'IBM: Cost of a Data Breach Report', *Computer Fraud & Security*, 2021(8), pp. 4–4. Available at: https://doi.org/10.1016/s1361-3723(21)00082-8.

Jeong, M. and Zo, H. (2021) 'Preventing insider threats to enhance organizational security : The role of opportunity-reducing techniques', *Telematics and Informatics*, 63(January), p. 101670. Available at: https://doi.org/10.1016/j.tele.2021.101670.

Johnson, R.A. and Wichern, D.W. (2002) *Applied Multivariate Statistical Analysis*. Fifth Edit. Printice Hall.

Johnson, R.B. and Christensen, L. (2020) *Educational Research:Quantitative, Qualitative, and Mixed Approahes*. Seventh Ed. Edited by S. Scoble et al. SAGE Publications Inc. Available at: https://lccn.loc.gov/2019020136%0D.

Kamsamrong, J. *et al.* (2022) 'State of the Art, Trends and Skill-gaps in Cybersecurity in Smart Grids Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)', *Erasmus+ Strategic Partnership Project.* [Preprint].

Khader, M., Karam, M. and Fares, H. (2021) 'Cybersecurity awareness framework for academia', *Information (Switzerland)*, 12(10). Available at: https://doi.org/10.3390/info12100417.

Khanna, A., Dey, N. and Gupta, D. (2021) *Applications of Big Data in Healthcare: Theory* *and Practice*, *Applications of Big Data in Healthcare: Theory and Practice*. Available at: https://doi.org/10.1016/B978-0-12-820203-6.00020-5.

Kost, E. (2022) '10 Biggest Data Breaches in Finance [Updated August 2022] | UpGuard', *Upguard.Com*, (August 2022), pp. 1–21. Available at: https://www.upguard.com/blog/biggest-data-breaches-financial-services.

Kuhn, M. and Johnson, K. (2013) *Applied Predictive Modeling with Applications in R*, *Springer*. Available at: http://appliedpredictivemodeling.com/s/Applied_Predictive_Modeling_in_R.pdf.

Kweon, E. *et al.* (2021) 'The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence', *Information Systems Frontiers*, 23(2), pp. 361–373. Available at: https://doi.org/10.1007/s10796-019-09977-z.

Lawrence Damilare Oyeniyi, Chinonye Esther Ugochukwu and Noluthando Zamanjomane Mhlongo (2024) 'Developing Cybersecurity Frameworks for Financial Institutions: a Comprehensive Review and Best Practices', *Computer Science & IT Research Journal*, 5(4), pp. 903–925. Available at: https://doi.org/10.51594/csitrj.v5i4.1049.

Lesotho Bureau of Statistics (2021) '2019 Labour Force Survey (LFS) Report', (5), pp. 1–256. Available at: www.bos.gov.ls.

Li, H., Luo, X. and Chen, Y. (2021) 'Understanding information security policy violation from a situational action perspective', *Journal of the Association for Information Systems*, 22(3), pp. 739–772. Available at: https://doi.org/10.17705/1jais.00678.

Li, L. *et al.* (2019) 'Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior', *International Journal of Information Management*, 45, pp. 13–24. Available at: https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Lyimo, B.J. and Shaaban, S.Y. (2021) 'Cybersecurity Awareness Among Employees in Banking Industry in Tanzania : A Case of National Microfinance Bank - Magomeni Branch', 3(1), pp. 1–4.

Maennel, K. *et al.* (2023) 'A Multidimensional Cyber Defense Exercise: Emphasis on Emotional, Social, and Cognitive Aspects', *SAGE Open*, 13(1), p. 215824402311563. Available at: https://doi.org/10.1177/21582440231156367.

Manoliu, A. (2022) 'Cyber security and awareness, investing in a culture of safety', *In*

Proceedings of the International Conference on Business Excellence [Preprint].

Marcu, M. (2021) ‘The Impact of the COVID-19 Pandemic on the Banking Sector’, *Dynamics in the Knowledge Economy,* 9(2), pp. 205–223. Available at: https://doi.org/10.2478/mdke-2021-0013.

Momoh, I., Adelaja, G. and Ejiwumi, G. (2023) ‘Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution’, (December). Available at: https://doi.org/10.13140/RG.2.2.35640.52489.

Mosola, N.. *et al.* (2019) ‘cybersecurity-protection-structures-the-case-of-lesotho’, *International Journal of Computer and Information Engineering* [Preprint].

Moustafa, A.A., Bello, A. and Maurushat, A. (2021) ‘The Role of User Behaviour in Improving Cyber Security Management’, *Frontiers in Psychology*. Frontiers Media S.A. Available at: https://doi.org/10.3389/fpsyg.2021.561011.

Muraguri, N.N., Mwalili, T. and Mose, T. (2019) ‘Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi country’, *International Academic Journal of Information Systems and Technology*, 2(1), pp. 157–182. Available at: http://www.iajournals.org/articles/iajist_v2_i1_157_182.pdf.

Murphy, C. *et al.* (2022) ‘Factors Affecting Compliance with the National Cybersecurity Policy by SMMEs in South Africa’, in *Kennesaw State University Kennesaw State University DigitalCommons@Kennesaw State University DigitalCommons@Kennesaw State University African Conference on Information Systems and Technology THE 8TH ANNUAL ACIST PROCEEDINGS (2022)* , pp. 45–57. Available at: https://doi.org/https://digitalcommons.kennesaw.edu/acist.

Neto, N.N. *et al.* (2020) ‘A Case Study of the Capital One Data Breach’, *SSRN Electronic Journal*, (January), pp. 0–24. Available at: https://doi.org/10.2139/ssrn.3542567.

Nurse, J.R.C. (2021) *Cybersecurity Awareness*, *Encyclopedia of Cryptography, Security and Privacy*. Springer Berlin Heidelberg. Available at: https://doi.org/10.1007/978-3-642-27739-9.

Ofori, K.S. *et al.* (2021) ‘Factors Influencing Information Security Policy Compliance Behavior’, in *Research Anthology on Business Aspects of Cybersecurity*. IGI Global, pp. 213–232. Available at: https://doi.org/10.4018/978-1-6684-3698-1.ch010.

Onunka, O. *et al.* (2023) ‘Cybersecurity in U.S. and Nigeria Banking and Financial

Institutions: Review and Assessing Risks and Economic Impacts', *Acta Informatica Malaysia*, 7(1), pp. 54–62. Available at: https://doi.org/10.26480/aim.01.2023.54.62.

Queirós, A., Faria, D. and Almeida, F. (2017) 'Srengths and Limitations of Qualitative and Quantitative Research Methods', *European Journal of Education Studies*, 3(9), pp. 1–19. Available at: https://doi.org/10.5281/zenodo.887089.

Ranjit, K. (2011) *Research Methodology: A step-by-step guide for beginners*. Third Edit. SAGE Publications.

Reegård, K., Blackett, C. and Katta, V. (2019) 'The Concept of Cybersecurity Culture', *Proceedings of the 29th European Safety and Reliability Conference.*, pp. 4036–4043. Available at: https://doi.org/10.3850/978-981-11-2724-3.

Reeves, A., Delfabbro, P. and Calic, D. (2021) 'Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue', *SAGE Open*, 11(1). Available at: https://doi.org/10.1177/21582440211000049.

Rice, C. and Searle, R.H. (2022) '"The Enabling Role of Internal Organizational Communication in Insider Threat Activity – Evidence From a High Security Organization"', *Management Communication Quarterly*, 36(3), pp. 467–495. Available at: https://doi.org/10.1177/08933189211062250.

Sabillon, R. *et al.* (2019) 'An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness Training Model (CATRAM). A case study in Canada', *Journal of Cases on Information Technology*, 21(3), pp. 26–39. Available at: https://doi.org/10.4018/JCIT.2019070102.

Saeed, S. (2023) 'Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia', *Sustainability*, 15(7), p. 6019. Available at: https://doi.org/10.3390/su15076019.

Sârghie, M.M.P. (2021) 'Using Social Marketing to Tackle Compulsive Buying', *Social Marketing Quarterly*, 27(1), pp. 3–12. Available at: https://doi.org/10.1177/1524500420988263.

Sarker, I.H. (2021) 'Machine Learning: Algorithms, Real-World Applications and Research Directions', *SN Computer Science*, 2(3), pp. 1–21. Available at: https://doi.org/10.1007/s42979-021-00592-x.

Saunders, M., Lewis, P. and Thornhill, A. (2009) *Research methods for business students*. Available at: www.pearsoned.co.uk.

Saunders, M., Lewis, P. and Thornhill, A. (2016) *Research Methods for Business Students*. Seventh Edition. Available at: www.pearson.com/uk.

Saunders, M.N.., Lewis, P. and Thornhill, A. (2019) *Research Methods for Business Students*. Eighth Edi. New York. Available at: www.pearson.com/uk.

Sausalito, C. and Morgan, S. (2020) ‘Cybercrime To Cost The World $10’. Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Scholefield, S. and Shepherd, L.A. (no date) *Gamification Techniques for Raising Cyber Security Awareness*.

Sekaran, U. and Bougie, R. (2016) *Research Methods for Business*. Seventh Ed. United Kingdom: John Wiley & Sons Ltd. Available at: www.wileypluslearningspace.com.

SentinelOne (2023) ‘Cyber-Attacks-on-Financial-Institutions-Why-Banks-Are-Caught-in-the-Crosshairs’, p. 2023.

Shrestha, N. (2020) ‘Detecting Multicollinearity in Regression Analysis’, *American Journal of Applied Mathematics and Statistics*, 8(2), pp. 39–42. Available at: https://doi.org/10.12691/ajams-8-2-1.

Singh, K. (2007) ‘Quantitative Social Research Methods’, *Quantitative Social Research Methods* [Preprint]. Available at: https://doi.org/10.4135/9789351507741.

Stewart, H. (2022) ‘A systematic framework to explore the determinants of information security policy development and outcomes’. Available at: https://doi.org/10.1108/ICS-06-2021-0076.

Straver, P. and Ravesteyn, P. (no date) *End-users Compliance to the Information Security Policy: A Comparison of Motivational Factors*, *Communications of the IIMA*. Available at: https://scholarworks.lib.csusb.edu/ciimaAvailableat:https://scholarworks.lib.csusb.edu/ciima/vol16/iss4/1.

Sulaiman, N.S. *et al.* (2022) ‘Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks’, *Information (Switzerland)*, 13(9). Available at: https://doi.org/10.3390/info13090413.

Sürücü, L. and Maslakci, A. (2020) 'Validity and Reliability in Quantitative Research', *Business & Management Studies: An International Journal*, 8(3), pp. 2694–2726. Available at: https://doi.org/10.15295/bmij.v8i3.1540.

Tabachnick, B.G. and Fidell, L.S. (2018) 'Using Multivariate Statistics', *Research Methods in Public Administration and Nonprofit Management*, pp. 233–250. Available at: https://doi.org/10.4324/9781315181158-21.

Thanh, N.C., Thi, T. and Thanh, L. (2015) 'The Interconnection Between Interpretivist Paradigm and Qualitative Methods in Education', 1(2), pp. 24–27.

Tolah, A., Furnell, S.M. and Papadaki, M. (2021) 'An empirical analysis of the information security culture key factors framework', *Computers and Security*, 108, p. 102354. Available at: https://doi.org/10.1016/j.cose.2021.102354.

Touhiduzzaman, M. *et al.* (2019) 'A Review of Cybersecurity Risk and Consequences for Critical Infrastructure', *Proceedings - 2019 Resilience Week, RWS 2019*, pp. 7–13. Available at: https://doi.org/10.1109/RWS47064.2019.8971975.

Uchendu, B. *et al.* (2021) *Developing a cyber security culture: Current practices and future needs*, *Computers & Security Journal*.

Uddin, M.H., Ali, M.H. and Hassan, M.K. (2020) 'Cybersecurity hazards and financial system vulnerability: a synthesis of literature', *Risk Management*, 22(4), pp. 239–309. Available at: https://doi.org/10.1057/s41283-020-00063-2.

Uzougbo, N.S., Ikegwu, C.G. and Adewusi, A.O. (2024) 'Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations', *International Journal of Science and Research Archive*, 12(1), pp. 533–548. Available at: https://doi.org/10.30574/ijsra.2024.12.1.0802.

Vasileiou, I. and Furnell, S. (2019) *Cybersecurity Education for Awareness and Compliance*, *Cybersecurity Education for Awareness and Compliance*.

Vedral, B. (2021) 'The Vulnerability of the Financial System to a Systemic Cyberattack', *International Conference on Cyber Conflict, CYCON*, 2021-May(March), pp. 95–110. Available at: https://doi.org/10.23919/CyCon51939.2021.9468291.

da Veiga, A. *et al.* (2020) 'Defining organisational information security culture—Perspectives from academia and industry', *Computers and Security*, 92. Available at:

https://doi.org/10.1016/j.cose.2020.101713.

Verizon (2020) *Data Breach Investigations Report*. Available at: https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf (Accessed: 17 April 2023).

Verizon (2022) ‘2022 Data Breach Investigations Report (DBIR)’, *Verizon.Com*, (May), pp. 5–108. Available at: https://doi.org/10.13140/RG.2.2.28833.89447.

Wackerly, D.D., Mendenhall, W. and Scheaffer, R.L. (2008) *Mathematical statistics with applications*, *Mathematical Statistics With Applications*. Available at: https://doi.org/10.1201/9781315275864.

Wolfenden, B. (2019) ‘Gamification as a winning cyber security strategy’, *Computer Fraud and Security*, 2019(5), pp. 9–12. Available at: https://doi.org/10.1016/S1361-3723(19)30052-1.

Yin, R.K. (2013) ‘Validity and generalization in future case study evaluations’, *Evaluation*, 19(3), pp. 321–332. Available at: https://doi.org/10.1177/1356389013497081.

Zhang, Z. (Justin) *et al.* (2021) ‘Cybersecurity awareness training programs: a cost–benefit analysis framework’, *Industrial Management and Data Systems*, 121(3), pp. 613–636. Available at: https://doi.org/10.1108/IMDS-08-2020-0462.

Zwilling, M. *et al.* (2022) ‘Cyber Security Awareness, Knowledge and Behavior: A Comparative Study’, *Journal of Computer Information Systems*, 62(1), pp. 82–97. Available at: https://doi.org/10.1080/08874417.2020.1712269.

LIST OF APPENDICES

Appendix A – Permission Letter

Request for permission to conduct research at Metropolitan Lesotho

“Investigating the effectiveness of cybersecurity policy education, training and awareness programs on employee behaviour towards cybersecurity compliance in financial sectors.”

06/06/2021

Mr Phafa Khoboko

Metropolitan Lesotho Building, Kingsway Road

Human Resources Department

+266 2222 2300, pkhoboko@metropolitan.co.ls

Dear Mr. Phafa Khoboko, the Learning and Development Manager

I, <Reneuoe Thamae> am doing research with Dr Hanifa Abdullah, a Senior Lecturer in the Department of School of Computing towards a Master of Science in Computing at the University of South Africa. We are inviting you to participate in a study entitled < Investigating the effectiveness of cybersecurity policy education, training and awareness programs on employee behaviour towards cybersecurity compliance in financial sectors >.

The aim of the study is to collect information that could help financial institutions propose a framework that will influence all employees comply with cybersecurity policy.

WHY AM I BEING INVITED TO PARTICIPATE?

Your company has been selected because it is a financial institution and it involves the use of digital devices and internet in the performing of administration issues, which are deemed vulnerable to cyberattacks. Therefore, it is considered relevant to the topic of the study. By acknowledging to take part in this survey, you agree that the information that will be provided by the respondents may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves a semi-closed ended survey questionnaire, with the fixed list of answer options to select from and a space to provide an additional response if need be. If you choose to participate in this survey, it will take up no more than 20 minutes of respondents' time.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

It is envisioned that the findings of this study will benefit financial sectors in proposing a framework that will influence all employees comply with cybersecurity policy. The framework will further assist financial institutions who have not yet adopted and practiced the SETA (security, education, training and awareness) programs to start introducing them and ensuring that employees comply with cybersecurity policy.

WHAT ARE THE POTENTIAL RISKS OF TAKING PART IN THIS STUDY?

Your organisation will not experience any negative consequences by allowing the respondents complete the survey as sharing of confidential information (personal information and/or information relating to the company) will not be required. However, should there be any discomfort experienced as part of the research, communicate it with the researcher immediately. The researcher(s) undertake to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

HOW WILL THE FINDINGS/RESULTS OF THE RESEARCH BE COMMUNICATED?

If you would like to be informed of the final research findings, please contact <Reneuoe Thamae> on <+266 58 068 722, 51856387@mylife.ac.za>. The findings are accessible for five years for audit purposes where after it will be permanently destroyed <electronic versions will be permanently deleted from the hard drive of the computer and cell phone>. Should you require any further information or want to contact the researcher about any aspect of this study, please contact <+266 58 068 722, 51856387@mylife.unisa.ac.za>.

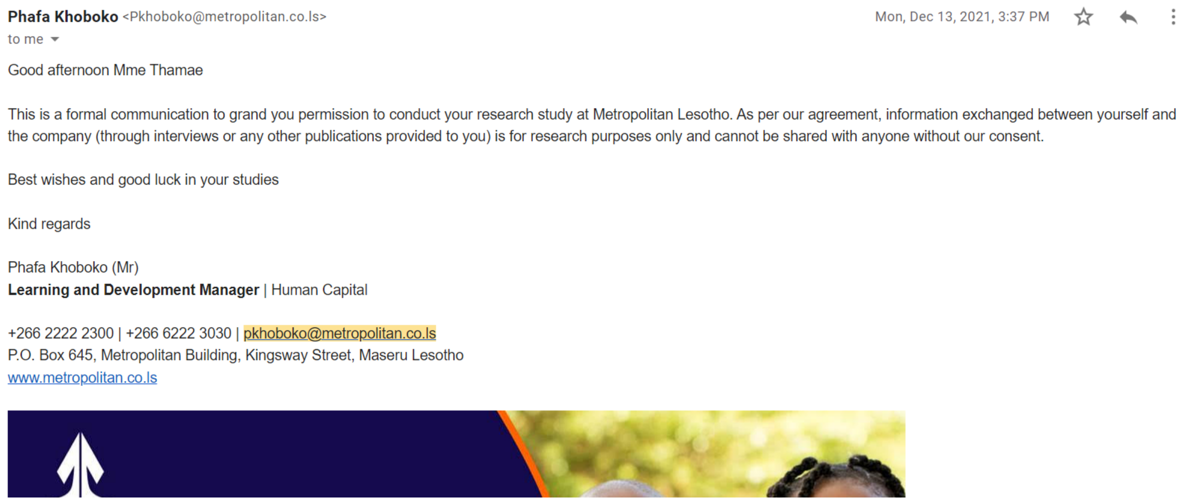
Should you have concerns about the way in which the research has been conducted, you may contact < Dr H. Abdullah> during office hours on <+27 011 670 9100, abdulh@unisa.ac.za>. Contact the research ethics chairperson of the School of Computing Ethics Review Committee, Dr. Danie Bischoff, <011 471 2130, Dbischof@unisa.ac.za or SocEthics@unisa.ac.za> if you have any ethical concerns.

Yours sincerely

Reneuoe Thamae

A master of science in computing student at the University of South Africa.

Appendix B – Permission Granted from Metropolitan Lesotho – Insurance Company



Phafa Khoboko <Pkhoboko@metropolitan.co.ls>

to me

Mon, Dec 13, 2021, 3:37 PM

Good afternoon Mme Thamae

This is a formal communication to grand you permission to conduct your research study at Metropolitan Lesotho. As per our agreement, information exchanged between yourself and the company (through interviews or any other publications provided to you) is for research purposes only and cannot be shared with anyone without our consent.

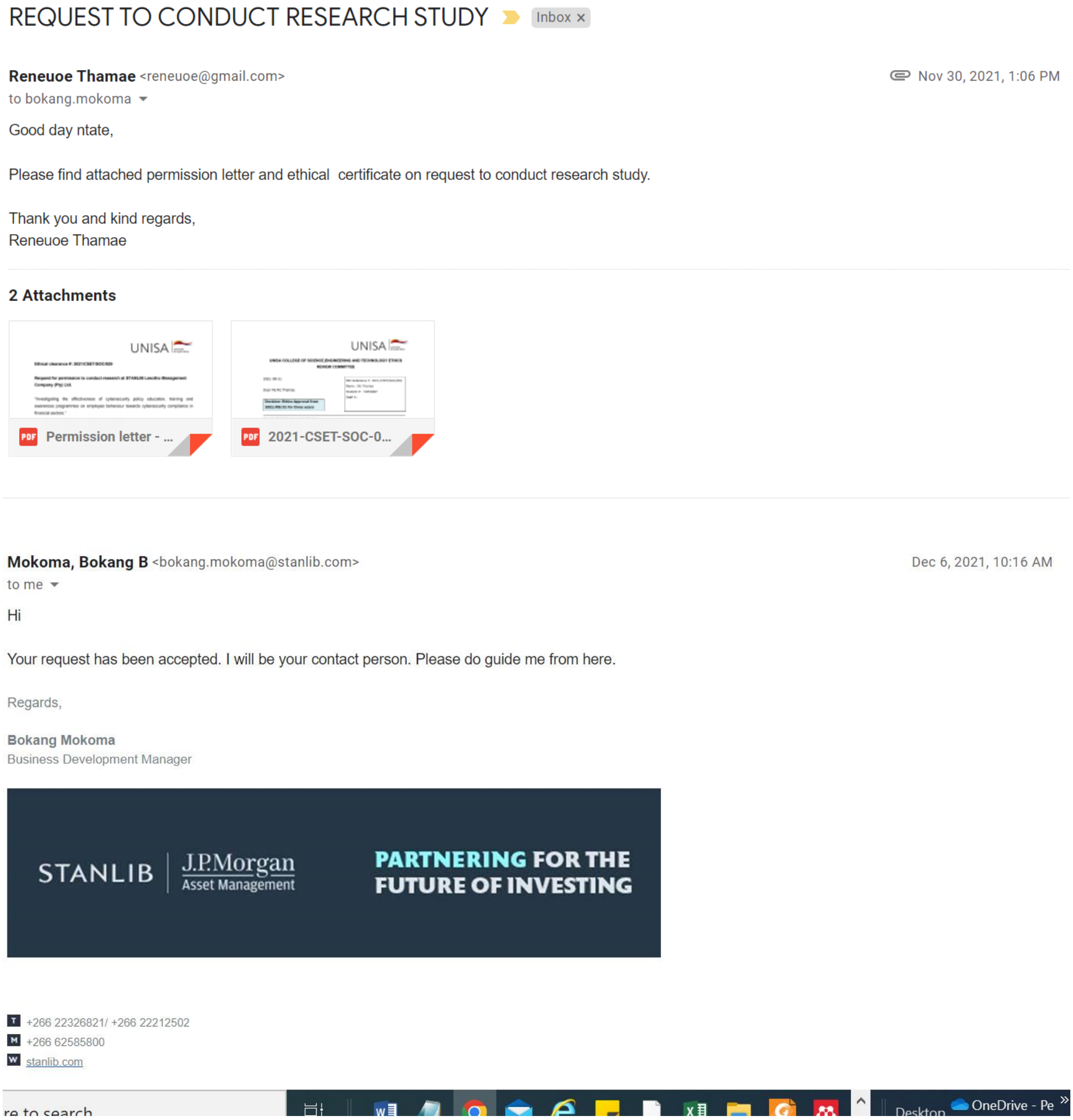
Best wishes and good luck in your studies

Kind regards

Phafa Khoboko (Mr)
Learning and Development Manager | Human Capital

+266 2222 2300 | +266 6222 3030 | pkhoboko@metropolitan.co.ls
P.O. Box 645, Metropolitan Building, Kingsway Street, Maseru Lesotho
www.metropolitan.co.ls

Email request to Stanlib – Asset Managers with permission letter and ethical certificate attached. Screen shot when Stanlib contact person was giving a permission is attached as well.



REQUEST TO CONDUCT RESEARCH STUDY

Reneuoe Thamae <reneuoe@gmail.com>
to bokang.mokoma

Nov 30, 2021, 1:06 PM

Good day ntate,

Please find attached permission letter and ethical certificate on request to conduct research study.

Thank you and kind regards,
Reneuoe Thamae

2 Attachments

Mokoma, Bokang B <bokang.mokoma@stanlib.com>
to me

Dec 6, 2021, 10:16 AM

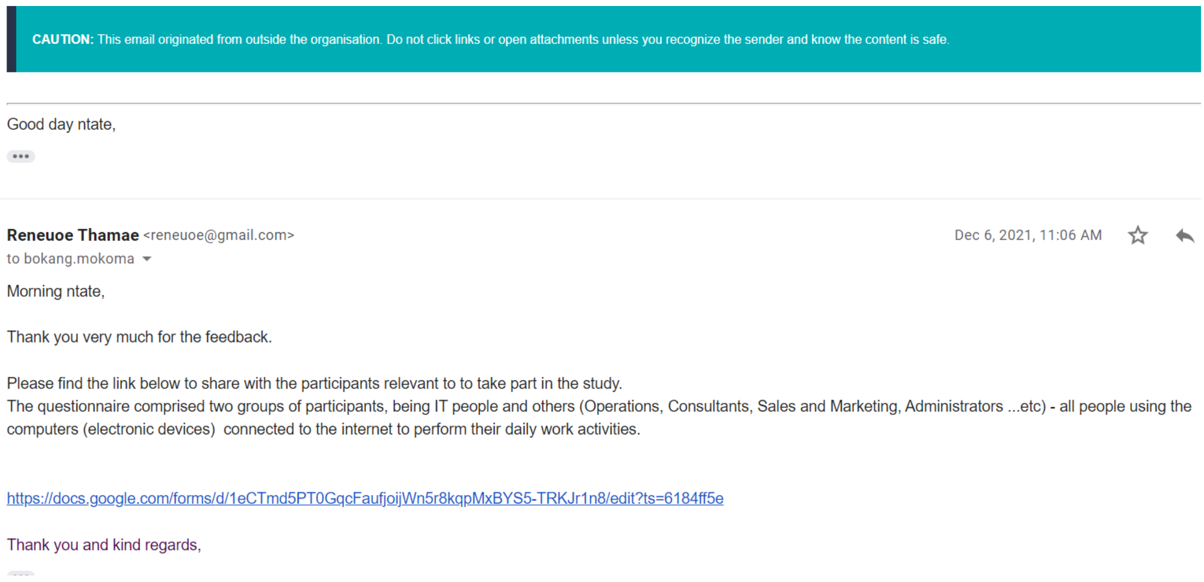
Hi

Your request has been accepted. I will be your contact person. Please do guide me from here.

Regards,

Bokang Mokoma
Business Development Manager

T +266 22326821/ +266 22212502
M +266 62585800
W stanlib.com



CAUTION: This email originated from outside the organisation. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Good day ntate,

Reneuoe Thamae <reneuoe@gmail.com>
to bokang.mokoma
Dec 6, 2021, 11:06 AM

Morning ntate,

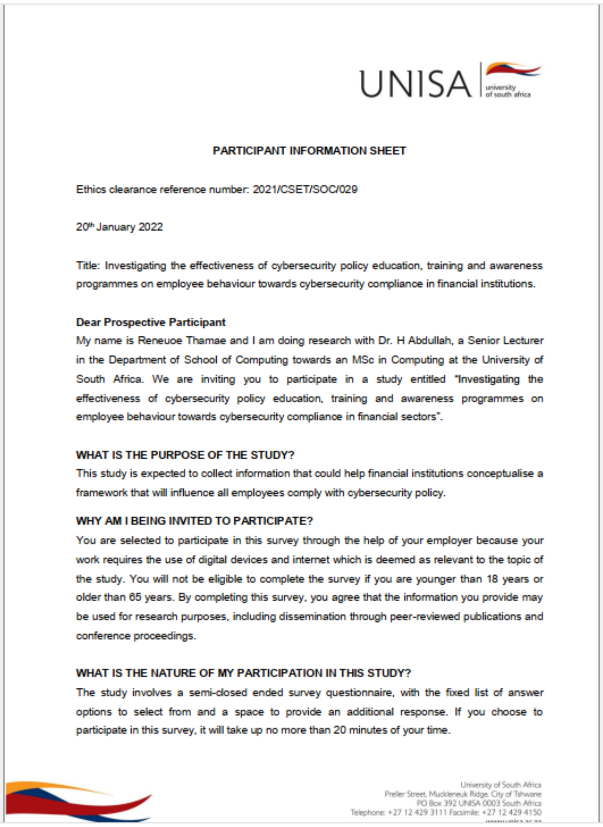
Thank you very much for the feedback.

Please find the link below to share with the participants relevant to to take part in the study.
The questionnaire comprised two groups of participants, being IT people and others (Operations, Consultants, Sales and Marketing, Administrators ...etc) - all people using the computers (electronic devices) connected to the internet to perform their daily work activities.

https://docs.google.com/forms/d/1eCTmd5PT0GqcFaufjoijWn5r8kqpMxBYS5-TRKJr1n8/edit?ts=6184ff5e

Thank you and kind regards,

Appendix C – Participant Information Sheet



UNISA university of south africa

PARTICIPANT INFORMATION SHEET

Ethics clearance reference number: 2021/CSET/SOC/029

20th January 2022

Title: Investigating the effectiveness of cybersecurity policy education, training and awareness programmes on employee behaviour towards cybersecurity compliance in financial institutions.

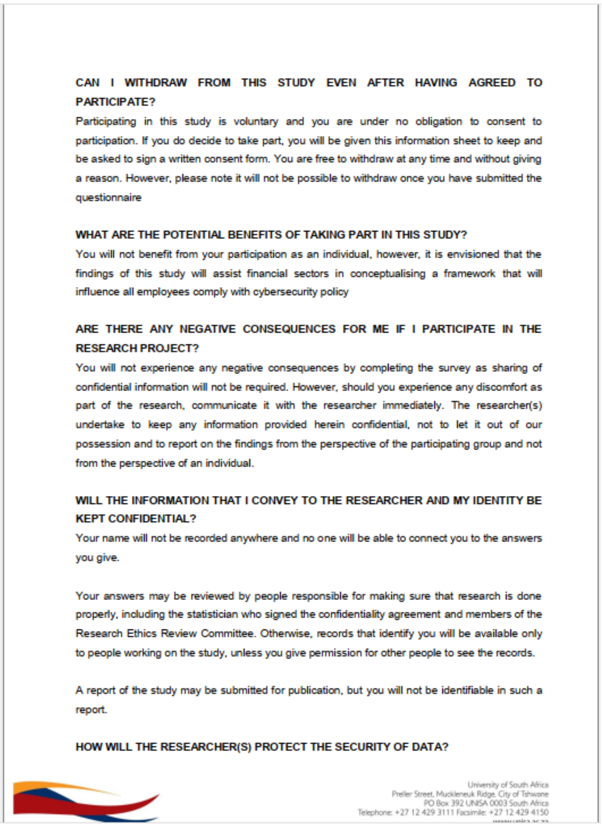
Dear Prospective Participant
My name is Reneuoe Thamae and I am doing research with Dr. H Abdullah, a Senior Lecturer in the Department of School of Computing towards an MSc in Computing at the University of South Africa. We are inviting you to participate in a study entitled "Investigating the effectiveness of cybersecurity policy education, training and awareness programmes on employee behaviour towards cybersecurity compliance in financial sectors".

WHAT IS THE PURPOSE OF THE STUDY?
This study is expected to collect information that could help financial institutions conceptualise a framework that will influence all employees comply with cybersecurity policy.

WHY AM I BEING INVITED TO PARTICIPATE?
You are selected to participate in this survey through the help of your employer because your work requires the use of digital devices and internet which is deemed as relevant to the topic of the study. You will not be eligible to complete the survey if you are younger than 18 years or older than 65 years. By completing this survey, you agree that the information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?
The study involves a semi-closed ended survey questionnaire, with the fixed list of answer options to select from and a space to provide an additional response. If you choose to participate in this survey, it will take up no more than 20 minutes of your time.

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



CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?
Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. However, please note it will not be possible to withdraw once you have submitted the questionnaire

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?
You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will assist financial sectors in conceptualising a framework that will influence all employees comply with cybersecurity policy

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?
You will not experience any negative consequences by completing the survey as sharing of confidential information will not be required. However, should you experience any discomfort as part of the research, communicate it with the researcher immediately. The researcher(s) undertake to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

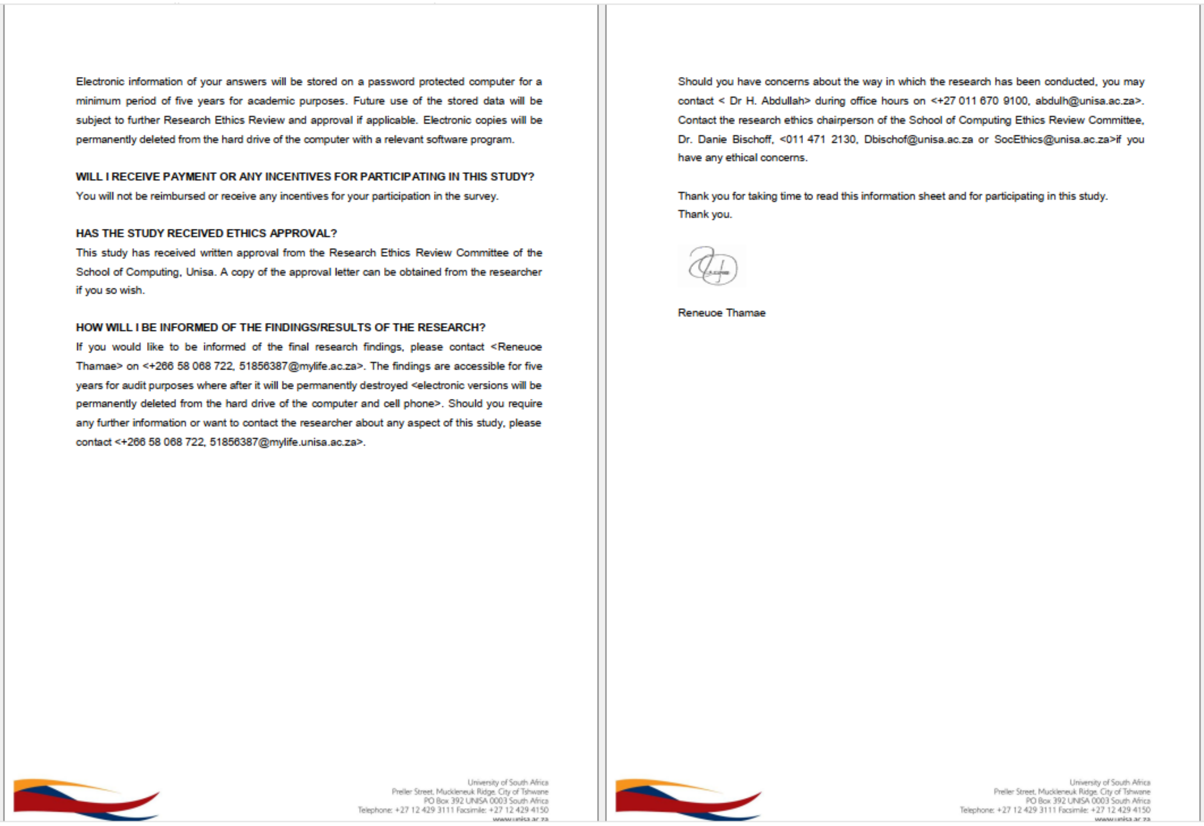
WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?
Your name will not be recorded anywhere and no one will be able to connect you to the answers you give.

Your answers may be reviewed by people responsible for making sure that research is done properly, including the statistician who signed the confidentiality agreement and members of the Research Ethics Review Committee. Otherwise, records that identify you will be available only to people working on the study, unless you give permission for other people to see the records.

A report of the study may be submitted for publication, but you will not be identifiable in such a report.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

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



Electronic information of your answers will be stored on a password protected computer for a minimum period of five years for academic purposes. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Electronic copies will be permanently deleted from the hard drive of the computer with a relevant software program.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?
You will not be reimbursed or receive any incentives for your participation in the survey.

HAS THE STUDY RECEIVED ETHICS APPROVAL?
This study has received written approval from the Research Ethics Review Committee of the School of Computing, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?
If you would like to be informed of the final research findings, please contact <Reneuoe Thamae> on <+266 58 068 722, 51856387@mylife.ac.za>. The findings are accessible for five years for audit purposes where after it will be permanently destroyed <electronic versions will be permanently deleted from the hard drive of the computer and cell phone>. Should you require any further information or want to contact the researcher about any aspect of this study, please contact <+266 58 068 722, 51856387@mylife.unisa.ac.za>.

Should you have concerns about the way in which the research has been conducted, you may contact < Dr H. Abdullah> during office hours on <+27 011 670 9100, abdulh@unisa.ac.za>. Contact the research ethics chairperson of the School of Computing Ethics Review Committee, Dr. Danie Bischoff, <011 471 2130, Dbischof@unisa.ac.za or SocEthics@unisa.ac.za>if you have any ethical concerns.

Thank you for taking time to read this information sheet and for participating in this study.
Thank you.

Reneuoe Thamae

Appendix D – Consent Form

CONSENT TO PARTICIPATE IN THIS STUDY

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

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

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

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

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

I agree to take part in the study.

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

Participant Name and Surname……………………………………… (please print)

Participant Signature…………………………………………. .Date…………………

Researcher's Name and Surname: Reneuoe Thamae

Researcher's signature _________ Date 06/06/2021

Consent form was however not send back by clients as they consented on the survey first page. Screen shot is attached:

Towards a Framework for enhancing employees' cybersecurity policy awareness in Financial Institutions

Welcome!

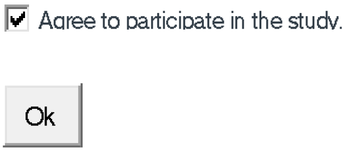
The survey intends to investigate how employees understand the role they play in complying with cybersecurity policy in order to combat cybersecurity breaches that are likely to occur most in the use of computer networks and systems in their organisations. You have been chosen to participate in this study because you are an employee in the financial industry, deal with customers and handle sensitive data using computer networks and systems.

Participating in this study is voluntary and you are free to withdraw from the study at any time and without giving a reason before submitting your responses.

If you choose to participate in this survey, it will not take longer than 20 minutes of your time. You will be required to be as honest as possible.

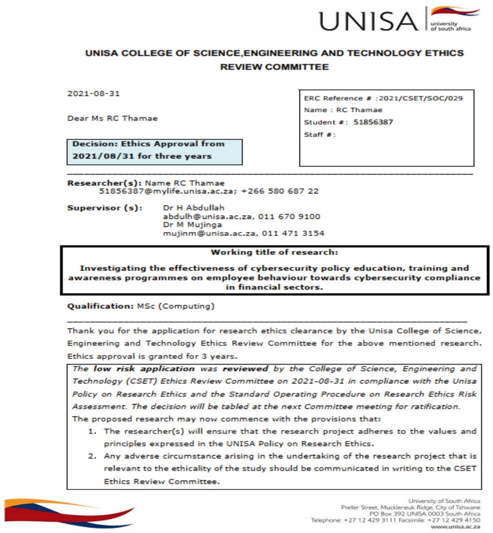
For any questions or concerns, kindly feel free to contact
The Researcher
Reneuoe Thamae

51856387@mylife.unisa.ac.za



☑ Agree to participate in the study.

Appendix E – Ethical Clearance Certificate



UNISA university of south africa

UNISA COLLEGE OF SCIENCE,ENGINEERING AND TECHNOLOGY ETHICS REVIEW COMMITTEE

2021-08-31

Dear Ms RC Thamae

Decision: Ethics Approval from 2021/08/31 for three years

ERC Reference # :2021/CSET/SOC/029
Name : RC Thamae
Student #: 51856387
Staff #:

Researcher(s): Name RC Thamae
51856387@mylife.unisa.ac.za; +266 580 687 22

Supervisor (s): Dr H Abdullah
abdulh@unisa.ac.za, 011 670 9100
Dr M Mujinga
mujinm@unisa.ac.za, 011 471 3154

Working title of research:

Investigating the effectiveness of cybersecurity policy education, training and awareness programmes on employee behaviour towards cybersecurity compliance in financial sectors.

Qualification: MSc (Computing)

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

*The **low risk application** was **reviewed** by the College of Science, Engineering and Technology (CSET) Ethics Review Committee on 2021-08-31 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision will be tabled at the next Committee meeting for ratification.*

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CSET Ethics Review Committee.

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

Appendix F – Questionnaire

Appendix F - Questionnaire.pdf

Towards a Framework for enhancing employees' cybersecurity policy awareness in Financial Institutions

Welcome!

The survey intends to investigate how employees understand the role they play in complying with cybersecurity policy in order to combat cybersecurity breaches that are likely to occur most in the use of computer networks and systems in their organisations. You have been chosen to participate in this study because you are an employee in the financial industry, deal with customers and handle sensitive data using computer networks and systems.

Participating in this study is voluntary and you are free to withdraw from the study at any time and without giving a reason before submitting your responses.

If you choose to participate in this survey, it will not take longer than 20 minutes of your time. You will be required to be as honest as possible.

For any questions or concerns, kindly feel free to contact
The Researcher
Reneuoe Thamae

51856387@mylife.unisa.ac.za

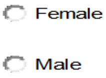
□ Agree to participate in the study.

The survey comprises of two sections which are SECTION A: PARTICIPANT BIOGRAPHICAL DATA and SECTION B - CYBERSECURITY UNDERSTANDING

You are invited to provide responses to questions for the survey. Please note that some questions require a single response whilst others will allow you to enter multiple responses.

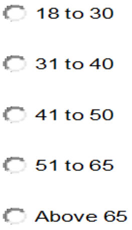
SECTION A: PARTICIPANT BIOGRAPHICAL DATA

1. Gender


○ Female

○ Male

2. Age


○ 18 to 30

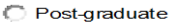
○ 31 to 40

○ 41 to 50

○ 51 to 65

○ Above 65

3. Highest level of education


○ Post-graduate

○ Under-graduate

○ Diploma

○ High School

○ Other (Specify) ______

4. Employment status

○ Full-time employed

○ Part-time employed

○ Self employed

○ Other (Specify) ______

5. Select your financial sector

○ Banking

○ Insurance companies

○ Insurance brokers

○ Stockbrokers

○ Other (Specify) ______

6. How long have you been involved in the industry specified?

○ Less than 1 year

○ 1 to 3 years

○ 4 to 5 years

○ Over 5 years

7. What is your role within the organisation?

○ Other departments

○ Information Technology and Information Security department

SECTION B1 – EMPLOYEES CYBERSECURITY POLICY UNDERSTANDING

Cybersecurity policy culture

1. What is your organisation state as per the listed cybersecurity policy aspects?

Organisational Cybersecurity status	Yes	No	Do not know
My organisation has information security policy in place	○	○	○
My organisation has a cybersecurity training and awareness campaign for employees.	○	○	○
New employees in my organisation attend induction training where information security and cybersecurity is discussed.	○	○	○
My organisation has reporting procedure that employees follow to report cybersecurity breaches/incidents.	○	○	○

Cybersecurity policy training

1. Have you attended cybersecurity policy training?

1	2	3
Yes	No	not sure
○	○	○

2. With training attended, how can you rate your cybersecurity policy knowledge?

1	2	3
Not so good	Good	Very good

3. Do you intend to attend cybersecurity policy training to improve cybersecurity policy awareness?

1	2	3	4	5
Definitely not	Probably not	Probably	Probably yes	Definitely yes

○	○	○	○	○

Cybersecurity policy awareness

1. What is your perception with regard to the following cybersecurity policy concepts within your organisation?

Cybersecurity policy concepts	1	2	3	4	5
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I work with confidential or sensitive information	○	○	○	○	○
My organisation implements technical controls to protect information on the organisation's IT systems.	○	○	○	○	○
I think that everyone in my organisation knows how to protect confidential information in electronic format (e.g. on the IT systems)	○	○	○	○	○
I believe that everyone in my organisation wants to protect organisational information.	○	○	○	○	○
I think that everyone in my organisation believes that cybersecurity policy is important.	○	○	○	○	○
I believe that everyone in my organisation is complying with cybersecurity-related policies.	○	○	○	○	○

Employees' cybersecurity behaviour

1. How often did you engage in the listed specific cybersecurity policy aspects during a 6-month period?

Behavioural aspects	0	1	2	3	4	5
	Never	Very rarely	Rarely	Occasionally	Very Frequently	Daily
Sharing computer log-in password with friends and/ or colleagues	○	○	○	○	○	○
Sharing applications/ systems password with friends and/ or colleagues	○	○	○	○	○	○
Using the same password for multiple websites	○	○	○	○	○	○
Entering payment information on unsecured websites.	○	○	○	○	○	○
Bringing in your own USB to work in order to transfer data onto it.	○	○	○	○	○	○
Checking that software for your smartphone/tablet/laptop/PC is up to date.	○	○	○	○	○	○
Clicking on links contained in unsolicited emails from an unknown source.	○	○	○	○	○	○
Sending personal information to strangers over the internet.	○	○	○	○	○	○

Clicking on links contained in an email from a trusted friend or work colleague.	○	○	○	○	○	○
Checking for updates to any anti-virus software, you have installed.	○	○	○	○	○	○
Downloading data and material from websites on my work computer without checking its authenticity.	○	○	○	○	○	○
Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop).	○	○	○	○	○	○

SECTION B2 – IT AND SECURITY PRACTITIONERS/TRAINERS: CYBERSECURITY POLICY UNDERSTANDING

Cybersecurity policy culture

1. What should be considered in order to determine cybersecurity policy training for employees?

Cybersecurity policy training checklist for employees	1	2	3
	Yes	No	Do not know
Ensure that employee training on cybersecurity policy is a strategic organisational priority	○	○	○
Collaborate with Human Resources specialists and I-O psychologists to generate and sustain support	○	○	○
Assemble an interdisciplinary team to develop comprehensive cybersecurity policy training.	○	○	○

Survey bellwether cybersecurity practices for integration into education and training.	○	○	○
Establish level-specific job and cybersecurity tasks for employees in the organisation.	○	○	○
Determine whether employees are currently performing required cybersecurity tasks.	○	○	○
Design cybersecurity training objectives to align knowledge, skills and attitudes with task demands.	○	○	○
Choose appropriate venues and methods for learning objectives and conduct training.	○	○	○
Assess education and training results to gauge whether organisation objectives are met.	○	○	○
Adapt education and training initiatives or shift to non-training solutions when needed.	○	○	○

Cybersecurity policy education and training

1. Which of the following policy or practice areas does your company educate and train end users? For those areas that you do not currently provide education or training, please indicate the expected time horizon (if any) for implementation.

Policy/Practice	1	Time Horizon for Implementation				
		2	3	4	5	6
	Currently implemented	<= six months	<= one year	<= two years	Never	Do not know
Restricted sites and download	○	○	○	○	○	○
Acceptable-use policy	○	○	○	○	○	○

Workforce mobility security (e.g. secure Internet connection, VPN, safety, etiquette)	○	○	○	○	○	○
Cybersecurity competency testing	○	○		○	○	○
Deception detection training for e-mails, web, social networking, downloads (e.g., visual spoofing, phishing cues, etc.)	○	○	○	○	●	○
Password management (e.g., change frequency, construction and protection standards)	○	○	○	○	○	○
Employee departure data security procedure	○	○	○	○	○	○

Cybersecurity education and training delivery method

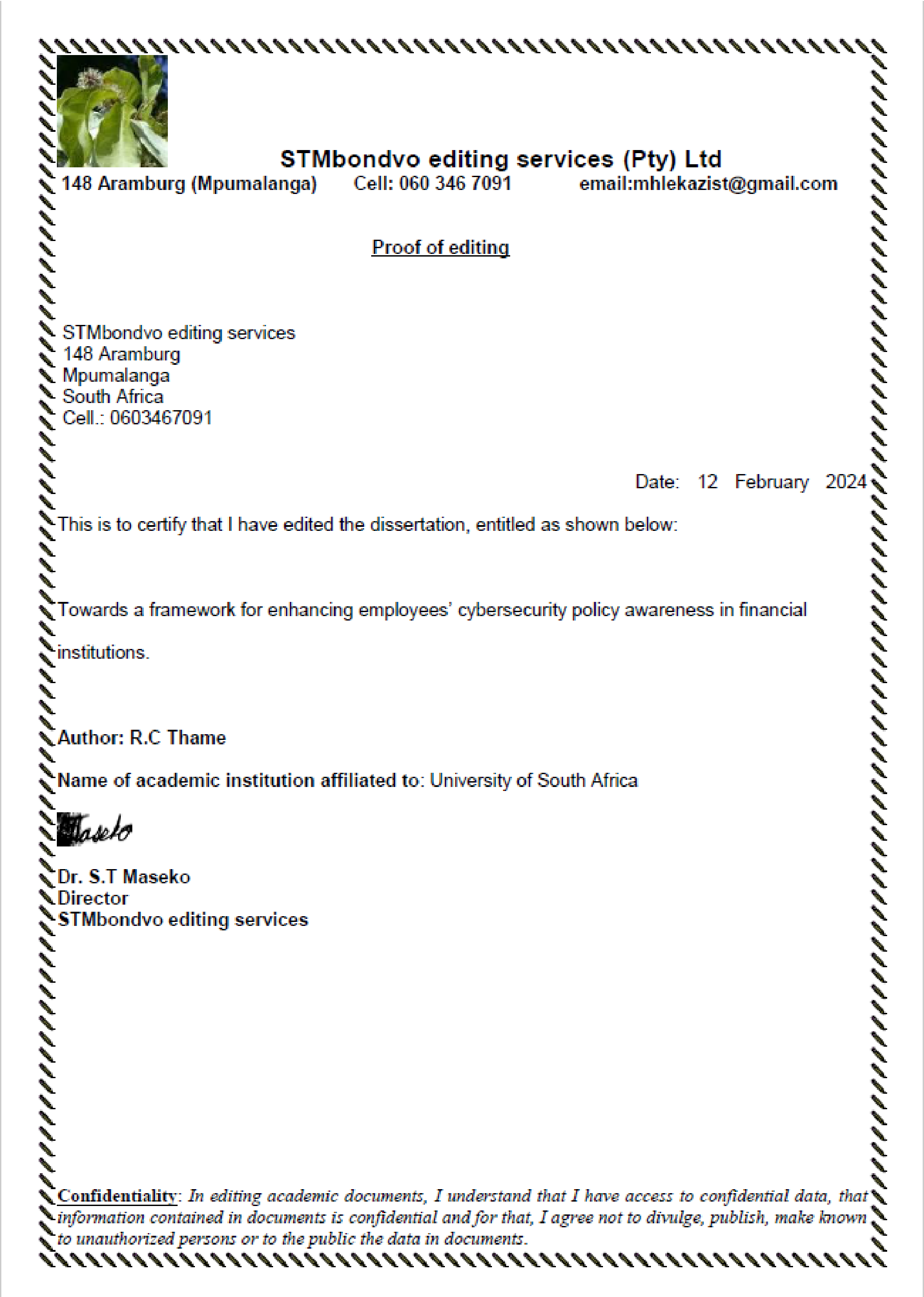
1. Which of the following methods does your company use to educate and train end-users about information security and cybersecurity policies or practices? Select all that apply.

Delivery methods

Policy/Practice	Delivery Methods				
	1	2	3	4	5
	Conventional (employee	Instructor led	Online	Phishing simulations	N/A

	newsletters, posters				
Restricted sites and download	□		□	□	□
Acceptable-use policy	□				
Workforce mobility security (e.g. secure Internet connection, VPN, safety, etiquette)	□	□	□	□	□
Cybersecurity competency testing	□	□	□	□	□
Deception detection training for e-mails, web, social networking, downloads (e.g., visual spoofing, phishing cues, etc.)	□	□	□	□	□
Password management (e.g., change frequency, construction and protection standards)	□	□	□	□	□
Employee departure data security procedure	□	□	□	□	□

Appendix G – Editor's Certificate



STMbondvo editing services (Pty) Ltd

148 Aramburg (Mpumalanga) Cell: 060 346 7091 email:mhlekazist@gmail.com

<u>Proof of editing</u>

STMbondvo editing services
148 Aramburg
Mpumalanga
South Africa
Cell.: 0603467091

Date: 12 February 2024

This is to certify that I have edited the dissertation, entitled as shown below:

Towards a framework for enhancing employees' cybersecurity policy awareness in financial institutions.

Author: R.C Thame

Name of academic institution affiliated to: University of South Africa

Maseko

Dr. S.T Maseko
Director
STMbondvo editing services

<u>Confidentiality</u>: *In editing academic documents, I understand that I have access to confidential data, that information contained in documents is confidential and for that, I agree not to divulge, publish, make known to unauthorized persons or to the public the data in documents.*