EMPLOYEES' CYBERSECURITY AWARENESS AND BEHAVIOUR IN SOUTH AFRICAN HIGHER EDUCATION INSTITUTIONS

by

Abdullahi Abiodun Yusuf
u20800917

Submitted in partial fulfilment of the requirements for the degree

MIT(IS)

in the

FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY
at the

UNIVERSITY OF PRETORIA

Study leader:

Professor R. Steyn

Date of submission:
May 2024

DECLARATION

I (full names & surname):	Abdullahi Abiodun Yusuf
Student number:	u20800917

Declare the following:

1. I understand what plagiarism entails and am aware of the University's policy in this regard.
2. I declare that this thesis is my own, original work. Where someone else's work was used (whether from a printed source, the internet or any other source) due acknowledgement was given and reference was made according to departmental requirements.
3. I did not copy and paste any information directly from an electronic source (e.g., a web page, electronic journal article or CD ROM) into this document.
4. I did not make use of another student's previous work and submitted it as my own.
5. I did not allow and will not allow anyone to copy my work with the intention of presenting it as his/her own work.
6. When using IT/ AI-supported writing tools, I have listed these tools in full in the section "Overview of tools used", with their product name, my source of supply (e.g. URL) and information on how I used it.

Yusuf AA — Signature

05/01/2024 — Date

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious, the Most Merciful (Al-Rahman, Al-Rahim). All praise and thanks are due to Allah (SWT) for granting me the strength, wisdom, and knowledge to undertake and complete this research. His guidance and support throughout this journey have been invaluable.

In a rapidly changing world, education remains an indispensable tool for progress (World Bank, 2018) and the most powerful weapon for change (Nelson Mandela, 2003). Shaped by the role of people, this study on Employees' Cybersecurity Awareness and Behaviour in South African Higher Education Institutions contributes to this vital discussion.

I would also like to express my sincere gratitude to my supervisor, Professor Riana Steyn, Department of Informatics, Informatics Faculty of Engineering, Built Environment and Information Technology (EBIT), University of Pretoria. Professor Steyn's unwavering support, belief in my abilities, and invaluable academic guidance, particularly during the development of the research proposal, ethical clearance process, and final structuring of the thesis, were instrumental in shaping this research and motivating me to persevere through challenges.

My most profound appreciation goes to Mrs Rhona Vander, Department of Informatics, EBIT UP, for her exceptional administrative support. Her efficiency and willingness to go the extra mile ensured a smooth research journey, allowing me to focus on the academic aspects of the project. I also want to thank Dr Olukorede Adeniran at the Tshwane University of Technology for his frequent telephone advice and motivation throughout this journey.

To my parents, siblings, and wife, Ms. MT Agunbiade, I offer my heartfelt thanks for your unwavering mental and emotional support and prayers. You have all been a source of strength and encouragement during this challenging academic endeavour.

Finally, I am grateful to Imam Ayoub for his spiritual guidance and prayers. Your timely advice and support provided me with the peace and focus needed to persevere throughout this journey, reminding me of the importance of faith alongside academic pursuits.

May Allah (SWT) reward everyone who has supported me in this endeavour. JazakAllahu Khairan (May Allah reward you with goodness) to all who have directly or indirectly supported me on this journey. Wa Billahi Tawfiq (And upon Allah lies all success). Allah knows best!

LIST OF ACCRONYMS AND ABBREVIATIONS

ANOVA - Analysis of Variance
ATT - Attitude
AVE - Average Variance Extracted
CA - Cybersecurity Awareness
CCB - Cybersecurity-Compliant Behaviour
CEI - Cybersecurity Experience in Institutions
CPA - Cybersecurity Policy Awareness
CRE - Coping Response Efficacy
CSE - Cybersecurity Self-Efficacy
DHET - Department of Higher Education and Training (SA)
EBIT - Faculty of Engineering, Built Environment, and IT
ENISA - European Union Agency for Cybersecurity
GDT - General Deterrence Theory
HEIs - Higher Education Institutions
HR - Human Resources
HTMT - Heterotrait-Monotrait Ratio
ICP - Institution Cybersecurity Policy
ICT - Information and Communication Technology
IEC - International Electrotechnical Commission
IS - Information Systems
ISO - International Organisation for Standardisation
IT - Information Technology
ITU - International Telecommunication Union
M - Mean
NIST - National Institute of Standards and Technology (US)
PBC - Perceived Behavioural Control
PII - Personally Identifiable Information
PLS-SEM - Partial Least Squares Structural Equation Modeling
PMT - Protection Motivation Theory
POPIA - Protection of Personal Information Act (SA)
Q^2 - Q-squared
R^2 - R-squared
SA - South African

SA-NCPF - South African National Cybersecurity Policy Framework

SD - Standard Deviation

SEM - Structural Equation Modeling

SMART-PLS - SmartPLS software

SN - Subjective Norm

SPSS - Statistical Package for the Social Sciences

TAM - Technology Acceptance Model

TPB - Theory of Planned Behaviour

Tukey's HSD - Tukey's Honestly Significant Difference

UK - United Kingdom

UP - University of Pretoria

US - United States of America

VIF - Variance Inflation Factors

β - Path Coefficient

EMPLOYEES' CYBERSECURITY AWARENESS AND BEHAVIOUR IN SOUTH AFRICAN HIGHER EDUCATION INSTITUTIONS

ABSTRACT

The widespread cyberattacks necessitate robust cybersecurity practices within South African higher education institutions (HEIs). System users, particularly employees, are often the inadvertent major entry for cyberattacks, highlighting the critical need for employees' cybersecurity behaviour to adhere to ethical guidelines and adapt to evolving cyber threats. This study investigates how South African HEIs' cybersecurity environment, encompassing factors like cybersecurity awareness, policies and prior employee experience, influences employee cybersecurity behaviour. Building on the protection motivation theory and the theory of planned behaviour, the study developed a conceptual model that integrates and explores the impact of cybersecurity awareness, policy awareness and experience within the institutional context on employee attitudes, subjective norms, perceived behavioural control, threat appraisal, and self-efficacy, ultimately leading to cybersecurity-compliant behaviour. This model was tested using data from a survey of 283 employees in South African HEIs. Structural equation modelling, ANOVA and post hoc procedures are employed to test the proposed hypotheses. The findings indicate that employees are more competent in managing cybersecurity tasks when they are aware of or know their institutions' cybersecurity policies than those unaware. The findings show that institutions' cybersecurity environment, including cybersecurity awareness, policy and experience, positively influences employees' attitudes, subjective norms and perceived behavioural control, which, in turn, positively contribute to their cybersecurity-compliant behaviour. Similarly, perceived behavioural control, threat appraisal and self-efficacy directly and significantly impact cybersecurity-compliant behaviour. These results highlight the importance of fostering a comprehensive South African HEIs cybersecurity environment, highlighting awareness training, transparent policies, practical experience, and efforts to cultivate empowerment sense amongst employees regarding cybersecurity practices. This study contributes to advancing knowledge on cybersecurity behaviour in South African HEIs by offering insights specific to the institutional cybersecurity environment and ultimately fostering a more secure cybersecurity structure within these institutions.

Keywords: Cybersecurity behaviour, Higher Education Institutions (HEIs), South African, Cybersecurity awareness, training, Institutional cybersecurity environment, Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Cybersecurity policies

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The recent cyberattack on the Tshwane University of Technology, which compromised vast amounts of data, highlights the rapidly growing vulnerability of South African (SA) higher education institutions (HEIs) to cybercrimes and related incidents (Govender, 2024). Similarly, incidents like the University of Zululand data breach in 2019 and the University of Witwatersrand ransomware attack in 2020 further underscore the severity of these breaches within these institutions (Charandura, 2022; Pieczywok, 2021; Pretorius, 2019). These vulnerabilities are increasingly emphasised by the growing reliance on technology within HEIs, which has transformed how individuals and organisations conduct their daily operations (Eltahir & Ahmed, 2023; Kumar & Nanda, 2020). The integration of technology in HEIs demonstrably enhances teaching, learning and operational efficiency (Abdel-Aziz et al., 2016; Kumar & Nanda, 2020). These technologies empower institutions and individuals to transform and streamline their work processes (Eltahir & Ahmed, 2023). However, this transformation has exposed HEIs to cybersecurity risks, making them susceptible to cybercrime due to increased interconnectedness, presenting an alarming increase in cyber threats (Eltahir & Ahmed, 2023).

Especially, Information and Communication Technology (ICT), technological platforms have become pivotal components of modern society, profoundly influencing our daily lives (Serrat, 2023; Abdel-Aziz et al., 2016). A significant impact of these is the imminent need for remote work during the global lockdowns imposed due to the COVID-19 pandemic. ICT was crucial in connecting organisations, enabling teleworking and ensuring smooth access to information (Eltahir & Ahmed, 2023). The significance of these platforms also extends to HEIs, where they have transformed the delivery, accessibility and learning experience. Thus, these platforms have become essential tools for students and educators, significantly improving education accessibility, quality and flexibility (Giovannella, 2021). Unfortunately, the growing adoption of ICT brings about an ever-increasing wave of cybercrime that impacts individuals and organisations (Martens, De Wolf & De Marez, 2019; Lowry et al., 2017; Dang-Pham & Pittayachawan, 2015).

HEIs manage a wealth of sensitive data, making them prime targets for cyberattacks, including ransomware, phishing and malware (Zwilling et al., 2022). The study of Pieterse (2021) suggests that data exposure incidents affecting higher education and other public sectors are

among the leading sources of cyberattacks. The vast amount of sensitive and valuable information within HEIs has made them appealing targets to cybercriminals (Mohammed et al., 2018). Also, the rapid adoption and reliance on technology in HEIs has led to a rise in cyber threats (Cheng & Wang, 2022). Therefore, Bada et al. (2019) advocate for the enhancement and improvement of the approach as cybersecurity measures in HEIs are often ineffective.

Many factors have contributed to organisations, including HEIs, vulnerability to data breaches and cyber-attacks. For example, a significant factor revolves around employee-related issues (Ponemon Institute, 2016) and is considered the primary target through which cybercriminals exploit organisations' networks (Vishwanath et al., 2020). These encompass deficiencies in training, employee negligence, inadvertent errors, inadequate cybersecurity awareness and deviations from established cybersecurity protocols (Sohrabi Safa et al., 2016). Notably, many cyberattacks targeting organisations, like HEIs, are attributed to employees' non-compliance with security policies (Alshammari et al., 2018). Thus, this underscores the need for organisations to consider human factors when addressing cybersecurity concerns.

In today's digital landscape, the human factor presents a considerable cybersecurity challenge as cyberattacks against organisations and individuals increase (Branley-Bell et al., 2021; Choi, Martins, & Bernik, 2018). The IBM (2021) report reveals that 95% of cybersecurity breaches revolve around human error, such as interactions with malicious links or falling victim to phishing scams. This report is consistent with Verizon Data's earlier findings (2020), which revealed that 22% of data breaches involve human error, encompassing instances such as inadvertently transmitting sensitive data to unauthorised recipients or misconfiguring databases. These statistics align with previous studies indicating that human factors account for 20% of organisations' cybersecurity losses (Richardson, 2007). Furthermore, many employees' susceptibility to cyberattacks is compounded by their limited proficiency in proactively identifying and addressing cyber threats (Khairil et al., 2016; Richardson et al., 2020). Given this background, it becomes evident that institutions' cybersecurity is inextricably linked to employee awareness and behaviour. Employees are pivotal in fortifying cybersecurity measures, serving as the primary defence against cybercrimes.

The education sector accounts for 7.2% of the total breaches, signifying a notable rise in cyber-attacks in HEIs (Risk Based Security, 2020). This statistic highlights the escalating threats HEIs face as cybercriminals increasingly exploit vulnerabilities within online learning

models. Given this critical situation, this study focuses on employees' cybersecurity awareness and behaviour within SA HEIs, emphasising the necessity of active employee engagement for effective cybersecurity measures.

Research suggests that implementing comprehensive cybersecurity awareness programs within HEIs can enhance employees' understanding of cybersecurity best practices, thereby mitigating and preventing cyberattacks (Bada et al., 2019). Despite extensive research on cybersecurity in general, a notable gap exists in specific studies focusing on cybersecurity awareness and behaviour within SA HEIs (Bada et al., 2019; Mare et al., 2018). While some studies exist, they particularly stress the need for a more comprehensive exploration of cybersecurity awareness programs in these institutions. More recently, Eltahir and Ahmed (2023) further advocate for additional research within the cybersecurity domain, signalling the need for a more detailed investigation into cybersecurity within the SA HEIs context.

Research efforts in South African HEIs remain crucial in raising cybersecurity awareness and developing best practices (Mitrovic, Thakur, & Palhad, 2023). However, funding constraints often hinder these efforts and limit the exploration and development of effective cybersecurity awareness (Oke & Fernandes, 2020). Mitrovic et al. (2023) added that investments in cybersecurity are essential to addressing the evolving threat landscape and protecting sensitive institutional information. Furthermore, Mare et al. (2018) previously emphasised the urgency of addressing SA HEIs' lack of preparedness for cyberattacks. Therefore, when especially considering the underexplored nature of cybersecurity awareness programs, it becomes crucial to identify the factors hindering SA HEIs' preparedness against cyber threats.

Cultural and social factors should be proactively considered when implementing cybersecurity awareness programs, as highlighted by Albreem and Almutairi (2018). Therefore, this study seeks to investigate the factors influencing employees' cybersecurity awareness and behaviour in SA HEIs and develop effective strategies for enhancing cybersecurity measures. The study employed surveys to gather data from employees within SA HEIs. The findings will advance the understanding of cybersecurity awareness in SA HEIs and contribute to developing more effective cybersecurity awareness programs.

1.1 BACKGROUND INFORMATION

The technological revolution has transformed how HEIs operate and fostered increased connectivity and seamless employee access to information (Hina et al., 2019). However, this pervasive access introduces novel cyber risks and threats, potentially compromising the vast amount of sensitive data HEIs manage, including student records, research information, financial details and intellectual property (Zwilling et al., 2022). The openness of HEIs, operational requirements, and the diverse IT workforce with varying IT skills further exacerbate their cyberattack vulnerability (Hina et al., 2019). While this revolution empowers HEI employees to retrieve information locally and remotely, enhancing productivity (Hina et al., 2019), it also introduces new risks like cyberattacks, leading to data breaches, reputational damage and financial losses (Chen et al., 2018; Perera et al., 2022).

HEIs are organisational structures with systems vulnerable to cyber-attacks, yet cybersecurity research overlooks or ignores these environments (Sadaf et al., 2019). Due to their openness to the public, operational requirements, and the need for employees to access distributed networks, HEIs are particularly vulnerable to cyber-attacks (Hina et al., 2019). For example, they store and manage a repository of sensitive data and intellectual property, including student records, research data and financial information, making them vulnerable to cybercrimes (Perera et al., 2022). Further, HEIs are communities of a diverse workforce, including students, faculty, admin and other staff members (Coman et al., 2020), each with unique and various needs regarding cybersecurity awareness and IT skills.

While the general literature offers abundant studies on cybersecurity awareness, HEIs need more research focusing specifically on cybersecurity awareness and risk (Ulven & Wangen, 2021). Recent contributions like Zwilling et al. (2022) stress the importance of cybersecurity awareness for HEI employees to mitigate cyber-attack risks. However, the effectiveness of cybersecurity awareness training significantly hinges on the design and implementation of these programs. Moreover, cultural and social factors impacting users' behaviours may constrain success and hinder effectiveness (Mogoane & Kabanda, 2019). Understanding and addressing these factors are pivotal in optimising the impact of cybersecurity awareness initiatives within HEIs.

The inception of the Internet has led to the introduction of technology platforms that have enabled individuals and institutions to communicate more effectively (Haleem et al., 2022).

The growth in technology in daily operations has made cybersecurity awareness a crucial aspect of organisational management. South African HEIs are not immune to cyber threats, which can lead to data breaches and other cybersecurity incidents (Bongiovanni, 2019). In 2020, the University of Witwatersrand experienced disruptions on its online learning platforms due to cyber-attacks. Therefore, investigating cybersecurity awareness among employees in SA HEIs is crucial. This study investigates the factors influencing employees' cybersecurity awareness and behaviour in SA HEIs and develops effective strategies for improving cybersecurity measures.

1.2 PROBLEM STATEMENT

The growing reliance on technology in SA HEIs has significantly increased their cyberattack vulnerability. These attacks threaten the vast amount of sensitive data HEIs manage, including student records, research information, financial details, and intellectual property (Zwilling et al., 2022). Such breaches carry profound repercussions, encompassing financial losses, reputational damage and disruptions to academic activities.

Employees are often the weakest link in the cybersecurity posture due to a lack of awareness regarding cyber threats and best practices. This lack of knowledge can lead to them falling victim to phishing scams, clicking on malicious links, or unknowingly introducing vulnerabilities through improper data handling (Chen et al., 2018; Pool et al., 2024).

While limited research exists on employee cybersecurity awareness and behaviour within SA HEIs as a critical area of focus, this study also acknowledges the broader challenges facing South Africa, such as the lack of understanding of core cybersecurity concepts and inadequate data protection policies (Shingange, 2022). According to recent statistics by Accenture (2020), the general public's lack of understanding of cybersecurity concepts significantly contributes to the nation's vulnerability to cyber threats, costing the economy over two billion rands annually. Furthermore, research by Bada et al. (2019) indicates that CSA remains underexplored across Africa, highlighting the need for more research within the SA HEI context (Chandarman & Van Niekerk, 2017). This knowledge gap hinders the development of effective cybersecurity measures in SA HEIs despite government efforts through legislation like POPIA (2013) and the Cybercrimes and Cybersecurity Bill (2017). By understanding and addressing these factors, this study aims to develop more effective and targeted cybersecurity awareness programs for

HEIs, ultimately bolstering cybersecurity readiness, mitigating cyber risks, and fostering a secure learning environment.

1.3 RESEARCH PURPOSE

The rapidly expanding digital landscape of SA HEIs has been accompanied by a worrisome rise in cyber-attacks (Risk Based Security, 2020), highlighting the pressing need for robust cybersecurity measures. This study addresses this concern by comprehensively examining and explaining the factors influencing employee cybersecurity awareness and behaviour within SA HEIs. Drawing from the established theoretical models of the Theory of Planned Behaviour (TPB) (Ajzen, 1991) and Protection Motivation Theory (PMT) (Rogers, 1975), this investigation delves into the intricate factors influencing employee cybersecurity readiness within this unique context. These concepts are explored in detail in sections 2.4 and 2.5.

1.4 RESEARCH OBJECTIVES

This study aims to investigate the factors influencing employee cybersecurity awareness and behaviour in SA HEIs and to identify effective strategies for enhancing cybersecurity measures. The study proposes the following objectives to achieve this goal and address the research question:

Main Research Objective: To investigate how cybersecurity awareness and related factors influence employee cybersecurity behaviour in SA HEIs.

The specific objectives of the study are:

1. To explore the cybersecurity awareness programs currently available in SA HEIs.
2. To investigate effective methods for measuring current employee cybersecurity awareness levels in SA HEIs.
3. To identify and analyse the factors influencing employees' cybersecurity awareness and behaviour in SA HEIs.
4. To investigate the challenges that hinder the effectiveness of cybersecurity awareness programs and practices in SA HEIs.

1.5 RESEARCH QUESTIONS

Based on the preceding discussion and research objectives, this study seeks to answer the following main research question and sub-questions to gain a deeper understanding of the main research question (RSQ denotes research sub-question):

Main Research Question: How do cybersecurity awareness and other factors influence employee cybersecurity behaviour (CCB) in SA HEIs?

RSQ1: What are the cybersecurity awareness programs currently available in SA HEIs?
RSQ2: How can current employee cybersecurity awareness levels in SA HEIs be effectively measured?
RSQ3: What factors influence employees' cybersecurity awareness and behaviour in SA HEIs?
RSQ4: What challenges impede the effectiveness of cybersecurity awareness programs and practices in SA HEIs?

1.6 SIGNIFICANCE OF THE STUDY

Security incidents such as the University of Zululand data breach in 2019, the University of Witwatersrand and the University of Johannesburg ransomware attacks in 2020 highlight the severity of cybersecurity breaches and the urgent need for effective cybersecurity measures and awareness among employees within HEIs in South Africa (Pretorius, 2019; Pieczywok, 2021; Charandura, 2022). However, despite the significant roles of HEIs, limited cybersecurity studies have focused explicitly on employees' CCB in SA HEIs (Chandarman & Van Niekerk, 2018; Cheng & Wang, 2022; Bada et al., 2019). This study aims to contribute to the theoretical knowledge of employees' CCB in SA HEIs and the development of practical solutions. By investigating the factors leading to cybersecurity-compliant behaviour, this study can inform the creation of more effective cybersecurity awareness programs within these institutions.

The findings of this study will benefit a wide range of stakeholders.

Policymakers: This research can inform the development of targeted policies that promote cybersecurity awareness and training within SA HEIs. By understanding the factors influencing

employee cybersecurity behaviour, policymakers can design interventions that address these specific areas, ultimately strengthening the overall cybersecurity posture of HEIs.

Students: Improved cybersecurity awareness among employees translates into a safer learning environment for students. By identifying the factors contributing to positive cybersecurity behaviour, this study can contribute to developing training programs that empower staff to make better cybersecurity decisions, ultimately reducing the risk of data breaches and protecting student information.

Administrative and Academic Staff: Understanding their cybersecurity behaviour patterns will be crucial for administrative and academic staff. This study provides valuable insights that can inform the development of more targeted training programs tailored to their specific needs. Employees will be better equipped to protect sensitive information and contribute to a more secure digital HEI landscape by improving cybersecurity awareness and skills.

Ultimately, this study bridges a significant gap in existing knowledge and offers valuable insights to guide practice, shape policy, and fortify SA HEIs' digital security stance.

1.7 ASSUMPTIONS

Several assumptions underlie this study. Firstly, the researcher assumes that employees in SA HEIs have varying levels of cybersecurity awareness, influenced by factors such as training, experience, organisational policy and culture. Secondly, another assumption is that effective cybersecurity awareness programs can improve employees' cybersecurity knowledge and behaviours, thereby ultimately reducing the risk of cybersecurity incidents in SA HEIs. Thirdly, given the similarities in cybersecurity risks and awareness challenges across sectors and contexts, the researcher also assumes that the study's findings and recommendations will have broader applicability beyond the SA HEIs sector. Fourthly, the data collected from respondents is accurate and reliable, and the measures used to assess cybersecurity awareness and program effectiveness are valid and reliable. The last assumption is that SA HEIs and other interested parties will implement and adopt the study's recommendations.

1.8 CONTRIBUTION

This study contributes to the information systems (IS) body of knowledge on cybersecurity awareness in SA HEIs by investigating the factors influencing cybersecurity awareness and developing an effective cybersecurity awareness program for SA HEIs. The study will also enhance employees' cybersecurity awareness levels and inform the design of effective cybersecurity awareness programs for other sectors and industries.

The findings of this study will be valuable to several stakeholders, including SA HEIs and their employees, the South African Department of Higher Education and Training (DHET) and other interested parties. By addressing the gaps in the literature on cybersecurity awareness in SA HEIs and developing effective training programs, this study seeks to improve cybersecurity preparedness in these institutions and ultimately contribute to the protection and security of digital assets.

This chapter discusses cybersecurity risks and threats SA HEIs face. It highlights their vulnerability to cyber-attacks due to the storage and management of sensitive data and intellectual property and a diverse workforce with varying cybersecurity awareness and digital skills. It emphasises the importance of effective cybersecurity awareness programs for employees, identifying factors that may limit their effectiveness, such as design, implementation, cultural and social factors, and employees' technology knowledge. It also noted that ineffective and inadequate training could result in security breaches, data loss, reputational damage and significant financial implications for HEIs. The chapter presents the research objectives and questions to address knowledge gaps, discusses its assumptions and limitations and provides an overview of SA HEIs' challenges concerning cybersecurity risks and threats.

This study's contribution is significant given the increasing cybersecurity threats and incidents in SA HEIs. The study's recommendations inform the design of effective cybersecurity awareness programs and contribute to developing a more secure digital environment in SA HEIs, which will apply to other sectors and industries.

1.9 BRIEF CHAPTER OVERVIEW

The study comprises six chapters: introduction, literature review, methodology, data interpretation and discussion of findings, discussions and conclusion, structured as follows:

Chapter One - Introduction:
This chapter introduces the study based on cybersecurity awareness in SA HEIs and highlights the importance of this issue and the factors influencing employees' cybersecurity awareness and behaviour. The researcher structures the chapter into the following sections: background, problem statement, study's significance, research questions, objectives, assumptions, limitations, contribution and conclusion.

Chapter Two - Literature review:
This chapter reviews the extant literature on cybersecurity awareness and related phenomena, including cyber threats and risks, cybersecurity awareness programs, and cybersecurity theoretical frameworks. It also discusses the gaps in the literature and presents how this study would contribute to the body of knowledge. Lastly, it gives the study's theoretical underpinning.

Chapter Three – Research Model and Hypotheses:
This chapter presents the research model and hypotheses developed to address this study's research questions and objectives. It introduces the underlying theoretical frameworks and factors informing the research model. It then outlines the research model, illustrating the relationships between the key variables. Based on the literature review and theoretical foundation, each hypothesis is presented and justified.

Chapter Four – Research Design and Methodology:
This chapter outlines the research methodology and planning, covering the research design, paradigm, strategy, data collection, and analysis. It also covers the methods and instruments used for data collection and discusses the ethical considerations of this study.

Chapter Five - Interpretation and Discussion of Findings:
This chapter analyses and presents the data collected in this study. It uses various statistical methods to test the hypotheses and answer the research questions. It also presents the study's results and briefly discusses the hypothesis test results.

Chapter Six – Conclusions and Recommendations:
This chapter discusses the impact of this study's findings, presents the limitations, and recommends possible further research. It also answers the main and sub-research questions, explains the decisions, summarises the research's main findings, discusses the implications of the results for SA HEIs, and presents recommendations.

1.10 CONCLUSION

This chapter introduces the study on cybersecurity awareness in SA HEIs. It highlights the importance of this issue and the factors influencing employees' cybersecurity awareness. The chapter is structured as follows: introduction, background, problem statement, research questions, objectives, significance, and conclusion.

The chapter provided an overview of the thesis's structure, including the remaining chapters. Chapter two focuses on the extant literature on cybersecurity frameworks, awareness, risks, threats, and programs. The research model and hypothesis present the conceptual model and hypotheses employed to validate it. The research design and methodology chapter outlines the research design and data collection, while the succeeding chapters cover data analysis, findings, discussions and conclusions. The next chapter presents the study's literature review.

2 LITERATURE REVIEW

2.1 INTRODUCTION

This chapter delves into the existing body of knowledge through a comprehensive literature review, serving as a vital foundation for the investigation, offering valuable insights and laying the groundwork for further exploration within the cybersecurity field (von Solms & von Solms, 2018). The primary objective of this chapter is to conduct an in-depth assessment of the existing literature related to cybersecurity awareness among employees in South African (SA) Higher Education Institutions (HEIs). This review encompasses a wide range of discussions, including associated activities and measures designed to strengthen the security frameworks of HEIs. The goal is to provide profound insights into the rapidly evolving landscape of cybersecurity within HEIs.

The study comprehensively explores essential themes related to cybersecurity awareness and behaviour within SA HEIs and guides readers through a detailed examination of various aspects of cybersecurity, including:

- **Cybersecurity and Cybercrime in SA HEIs:** This section introduces the concepts of cybersecurity and cybercrime, highlighting their relevance to HEIs and explaining how the two are interlinked.
- **Cybersecurity Policies and Regulations in South Africa:** This section explores the current landscape of cybersecurity policies and regulations in South Africa, particularly those relevant to HEIs.
- **Cybersecurity Awareness and Effective Strategies:** These sections explore the cybersecurity landscape, strategies, and their correlation with employees' cybersecurity behaviour.
- **Cybersecurity Risk Management:** This section delves into the role of risk management in fostering cybersecurity awareness within HEIs.
- **Cybersecurity Behaviour:** This section examines existing research factors informing acceptable or compliant cybersecurity behaviour.
- **Theoretical Foundations:** This section explores the theoretical foundations for understanding employee cybersecurity awareness and behaviour.

The chapter concludes with a summary and a synthesised perspective on the multifaceted discussions. This synthesis helps to facilitate a seamless transition into the subsequent sections, ensuring a cohesive flow of ideas and concepts. The deliberate structure of this literature review prepares readers to navigate the following content with a clear understanding of the discourse's trajectory and the foundational insights that support it. This sets the stage for introducing the study's proposed model, which builds upon this knowledge base to address the research gap identified earlier.

2.2 CYBERSECURITY AND CYBERCRIME IN SA HEIS

Cybersecurity encompasses a comprehensive set of measures to protect information systems, networks, and devices from unauthorised access, use, disclosure, disruption, modification, or destruction (Raimundo & Rosario, 2022). This suggests that cybersecurity is a multifaceted strategy crucial for protecting sensitive information assets in today's digital landscape. This multi-layered approach employs technical and administrative measures to secure digital assets (Furstenau et al., 2021). Thus, understanding these layers is essential for developing effective cybersecurity awareness and policies within HEIs. Information security is a subset of cybersecurity that focuses on safeguarding confidential information from unauthorised access, modification, or deletion (World Economic Forum, 2019). Information security is significant for HEIs as they handle massive amounts of sensitive student and staff data and intellectual property.

Conversely, cybercrime is any criminal activity targeting or exploiting computer systems and networks (Schwab, 2019), highlighting the ever-present threat malicious actors pose in the digital age. HEIs, with their vast networks and valuable data, become prime targets for cybercriminals. Cybercriminals employ various tools and methodologies, often leveraging readily available devices like smartphones and laptops to execute illicit activities (Raimundo & Rosario, 2022). This ease of access for criminal actors and attackers strengthens the importance of employees' vigilance within HEIs.

The pervasive digitisation of SA HEIs has made cybersecurity a top priority globally (Eltahir & Ahmed, 2023). This dependence on technology exposes institutions to diverse cyber threats, ranging from malware attacks to data breaches (Mogoane & Kabanda, 2019). These threats are growing in frequency and severity and are often influenced by employees' insecure

behaviour (Mou et al., 2022; Millett et al., 2019; King et al., 2018). Sutherland (2018) asserts that employees' lack of cybersecurity awareness makes them and their institutions prime targets for these threats. Mitigating these risks requires a multifaceted approach, combining robust technical safeguards with a human element (Malatji et al., 2022).

Creating awareness and educating employees about cyber threats, and fostering appropriate security behaviours, are crucial for mitigating risks and protecting sensitive data and resources within HEIs (Cheng & Wang, 2022). This chapter reviews extant cybersecurity literature and delves into the current landscape of cybersecurity policies and regulations in South Africa, focusing on employee training, risk management, and awareness programs within HEI contexts. It further explores the theoretical foundations for cybersecurity and presents relevant research models and hypotheses. Ultimately, this analysis aims to identify and understand the factors influencing employee cybersecurity awareness and behaviours, thereby informing the development of effective cybersecurity strategies for SA HEIs.

Several vital interventions can empower HEIs to build a more secure digital environment. These interventions, aligned with research by Vrhovec et al. (2023), include the following:

- **Education Initiatives:** Equipping employees with knowledge about online threats and mitigation strategies is crucial for fostering secure behaviour within HEIs.
- **Awareness-Raising Campaigns:** Regular reminders about potential threats and countermeasures help maintain vigilance and preparedness.
- **Training Programs:** Developing essential information security skills, such as secure password management and phishing identification, empowers employees to contribute actively to cybersecurity efforts.

Despite being custodians of sensitive information, many SA HEIs lack comprehensive cybersecurity measures, rendering them vulnerable to cyberattacks and data breaches (Cloete, 2017; Osuagwu et al., 2020). This alarming reality underscores the urgent need for HEIs to implement robust cybersecurity measures, including effective employee awareness programs, to mitigate risks and protect valuable institutional resources (Cheng & Wang, 2022; Osuagwu et al., 2020; Cloete, 2017).

It is paramount for SA HEIs to ensure that all employees adhere to CCB when accessing institutional network resources and the internet to strengthen national cybersecurity capability

(National Integrated ICT Policy, 2017; SA Government Gazette, 2015). Also, the South African National Cybersecurity Policy Framework (SA-NCPF) is a comprehensive strategy that underscores the importance of integrating human factors into cybersecurity measures (Department of Telecommunications and Postal Services, 2019). As the SA-NCPF emphasis on human behaviour aligns with this study's focus on employees, it can be a key legal statute for the current investigation. Also, by fostering a culture of awareness and promoting adherence to best practices through effective education and training programs, HEIs can significantly reduce cyberattack risks and protect their critical assets (SA Government Gazette, 2015). This collective effort requires the collaboration of institutional leadership, IT professionals, and all employees, ultimately safeguarding the digital landscape of SA HEIs.Therefore, the following section explores the cybersecurity regulations and policies in SA HEIs to understand how these threats can be effectively mitigated.

2.3 CYBERSECURITY REGULATIONS AND POLICIES

2.3.1 Human Behaviour: The Critical Factor in Cybersecurity Efforts

Several studies consistently highlight that employee non-compliance with established cybersecurity policies is a significant cause of cyber breaches (Khatib & Barki, 2022; Aldawood & Skinner, 2019; Sommestad et al., 2015). This underscores human behaviour's critical role in cybersecurity, consistent with the current study's emphasis on addressing the human element within SA HEIs. While cybersecurity regulations exist, Porcedda (2018) argues that they often focus on symptoms rather than root causes, potentially exacerbating vulnerabilities. Recognising and mitigating this national and institutional security limitation, South Africa has implemented a comprehensive legal framework to address these challenges (Malatji et al., 2022). This development aligns with the global need for robust cybersecurity frameworks to safeguard against evolving cyber threats (Schwab, 2019; Srinivas et al., 2019). Further, the International Telecommunication Union (ITU) highlights the importance of formulating national cybersecurity strategies with proactive measures for prevention, response and recovery from cyberattacks (ITU, 2019, 2020).

2.3.2 Cybersecurity Regulations and Policies in South Africa

The South African Government has responded to the cyberattack surge by introducing cybersecurity legislation, regulations, and frameworks (Khan et al., 2022). These legislative efforts are pivotal in fortifying digital and national cybersecurity environments. For example, South Africa's legal framework, particularly the SA National Cybersecurity Policy Framework (SA-NCPF), calls for a concerted national approach to establishing cybersecurity and provides the measures and mechanisms for policy coordination nationwide (Steenkamp-Fonseca & Van Wyk, 2021). It aims to protect information infrastructure in cyberspace and prevent cyberattacks and threats (Chigada, 2023), emphasising the human element in cybercrime (Malatji et al., 2022). Thus, consideration of human behaviour becomes fundamental within comprehensive cybersecurity strategies and overarching regulations.

The SA-NCPF, published in May 2015 (SA Government Gazette, 2015), is a comprehensive framework designed to create a secure cyber environment. This framework addresses four key cybersecurity issues: an inadequate regulatory framework, uncoordinated approaches, lack of public awareness, and insufficient skills and resources. It outlines ten core elements to tackle these challenges, including establishing a dedicated policy, protecting critical information infrastructure, promoting cybersecurity cultures, and forming public-private partnerships. The emphasis on cybersecurity culture and awareness underscores NCPF's consideration of human behaviour and its recognition of cybersecurity awareness, which aligns with the current study's focus on employee awareness and behaviour.

Despite its comprehensive structure, the NCPF faces several challenges that hinder its effectiveness. These include complex stakeholder relationships and misaligned cyber legislation, as Bote (2019) highlighted. This misalignment creates gaps that cybercriminals can exploit (Pokwana & Kyobe, 2016). Furthermore, Steenkamp-Fonseca and Van Wyk (2021) argue that the NCPF's effectiveness hinges on proper cybersecurity legislation to provide a strong foundation. Recognising this need, South Africa has implemented legislative measures.

The Protection of Personal Information Act (POPIA) (Information Regulator, 2013) enforces stringent data security standards and compels organisations to safeguard personal data. This significantly impacts SA HEIs by highlighting the need for proactive measures against cybercrime, such as employee awareness programs. Thus, exploring how POPIA compliance

translates into employee awareness and compliance behaviour within HEIs can provide valuable insights for this study. Similarly, the Cybercrimes Act (Act 19 of 2020) is another legislation that strengthens the legal framework by criminalising various malicious cyber activities and compelling organisations to report cybercrimes (South African Government, 2021). While these acts primarily deter illegal operations, they offer valuable insights for institutions to strengthen their cybersecurity postures. These insights inform the need for effective employee cybersecurity awareness and policy development within SA HEIs.

The SA-NCPF further emphasises the importance of ongoing education and awareness programs, aligning with the recognition that technical measures alone are insufficient (Department of Telecommunications and Postal Services, 2019). By equipping employees with the knowledge and skills to identify and respond to cybersecurity risks, HEIs can significantly reduce their vulnerabilities. This focus on human behaviour bridges the gap identified in the NCPF's limitations. By promoting a culture of cybersecurity awareness through training programs, this study aims to empower employees and strengthen the overall cybersecurity posture of SA HEIs.

2.3.3 Limitation of Frameworks and Need for Cybersecurity Awareness

Despite well-intentioned frameworks like the SA-NCPF, South Africa's cybersecurity landscape continues to face challenges. The NCPF lacks robust alignment with legislation, which is necessary to make it effective. (Steenkamp-Fonseca & Van Wyk, 2021). This misalignment creates loopholes that cybercriminals exploit (Pokwana & Kyobe, 2016). It also requires complex stakeholder relationships that hinder the NCPF's operational efficiency (Bote, 2019). Given this background, Chigada (2023) underscores the need to review this framework to enhance its effectiveness in addressing cybersecurity issues.

Chang and Coppel (2020) advise that the exponential growth of cyber threats demands a multi-pronged approach beyond frameworks and legislation. The NCPF's emphasis on promoting awareness and cybersecurity culture further echoes this view. Thus, as earlier highlighted, the combined approach should include addressing behaviour that remains significant in cybersecurity. Due to insecure behaviour, the human element, including employees, remains the weakest link in cybersecurity (Malatji et al., 2021). Aldawood and Skinner (2019) highlighted that employees' lack of awareness and training remains a

significant cause of their susceptibility to social engineering attacks and manipulation, ultimately compromising institutional cybersecurity. Moreover, Costa and Figueira (2016) suggest that the NCPF and other frameworks should require organisations to enhance their employee awareness programs against social engineering threats. Therefore, having explored the national frameworks and legal landscape, the following section delves into the role of employee awareness programs in SA HEIs.

2.3.4 International Comparisons and Areas for Improvement

Recent and increasing cyberattacks on institutions underscore the importance of robust cybersecurity measures, as highlighted in section 1.6. This incident highlights the critical need for institutions such as HEIs to implement and enforce effective cybersecurity measures to protect sensitive data (Bana & Bhana, 2018). South Africa's emphasis on human behaviour in its cybersecurity frameworks aligns with the growing global recognition of this factor (Malatji et al., 2022; ITU, 2020). However, some countries, such as the US and the UK, have implemented mandatory employee cybersecurity awareness and training (ITU, 2020). The ITU (2020) report indicates that many countries, including South Africa, have introduced data breach and incident reporting requirements in legislation, frameworks and policies. This highlights a positive step towards strengthening the national cybersecurity landscape.

An analysis of the 2020 Global Cybersecurity Index (ITU, 2020) reveals that while South Africa ranks 8th on the continent and 59th globally, this calls for improvement in its overall cybersecurity approach. Specifically, the "Organisational Measures" category, which examines governance and coordination mechanisms for cybersecurity, highlights areas for improvement and development. The index's leading countries, like the USA, UK, Saudi Arabia, and Estonia, have set higher standards in areas such as legal frameworks, technical infrastructure, policy-coordinating institutions, and investment in research development, education and training programs (ITU, 2020; Tvaronavičienė et al., 2020). The future of cybersecurity regulations in South Africa might involve the development of more specific data privacy regulations similar to those implemented by the leading countries that have already set higher standards. Such regulations could further enhance personal data protection within SA institutions, including HEIs, and strengthen the overall cybersecurity landscape.

2.3.5 Cybersecurity Policies in SA HEIs

The global landscape reveals inadequate cybersecurity policies, leaving many organisations susceptible to cyberattacks (Lippert & Cloutier, 2021). This vulnerability particularly affects SA HEIs, which increasingly rely on technology to store and manage sensitive student and staff data and intellectual property (DHET, 2020). A report by the Department of Higher Education and Training (DHET) highlights that many colleges lack formal cybersecurity policies and training programs, underscoring a broader challenge within the SA HEIs sector. HEIs play a crucial role in establishing and communicating clear cybersecurity policies. These policies outline legal obligations and shape organisations' overall cybersecurity posture by emphasising the importance of employee behaviour (Srinivas et al., 2019). Effective policies go beyond mere technical considerations; they encompass a comprehensive strategy that outlines individual and collective responsibilities across regulatory, legal, technical, and behavioural aspects (Srinivas et al., 2019).

Cybersecurity policies play a crucial role in shaping the overall cybersecurity posture of SA HEIs. These policies outline the acceptable rules and procedures that guide employees in utilising computer resources (Sommestad et al., 2015). They establish clear lines of cybersecurity responsibilities within the institution and, importantly, mandate employee awareness and training programs. The scope of cybersecurity policies has expanded in research. For example, Mishra et al. (2022) propose a broader definition encompassing not just rules but also tools, best practices and management techniques. This holistic definition ensures that policies address the various aspects of cybersecurity, including technical measures and human behaviour. These policies serve as a foundational framework, defining the standard behaviours employees expect to maintain a secure cyber environment.

More than establishing cybersecurity policies is required, as Almansoori et al. (2023) highlight that active enforcement and implementation are critical for their success. This involves integrating cybersecurity best practices into the HEI's overall structure. The effectiveness of these strategies thrives on a multi-pronged approach:

- **Active Policy Enforcement:** Ensuring clear consequences for non-compliance strengthens the impact of the policies.

- **Employee Awareness and Training:** It is essential to equip employees with the knowledge and skills to identify and respond to cyber threats.
- **Integration of Best Practices:** It is crucial to continuously update policies to reflect the evolving cyber threat landscape and incorporate best practices.

This comprehensive approach, addressing both technical and human vulnerabilities, is vital to a robust cybersecurity posture. The International Telecommunication Union (ITU, 2020) also emphasises the importance of awareness campaigns, training, and incentives to develop a strong cybersecurity culture within HEIs. By effectively implementing these elements, South African HEIs can leverage cybersecurity policies to empower employees and create a secure digital environment.

2.3.6 Necessitating Cybersecurity Awareness Programs

While the primary objectives of POPIA and the Cybercrimes Act are to deter illegal cyber activities, such as mandating data breach disclosures, they also offer valuable insights that guide future defensive strategies (Pieterse, 2021). These legislations directly impact SA HEIs, necessitating robust measures to safeguard personal information against data breaches. Organisations such as SA HEIs must legally uphold and protect all processed personal data's confidentiality, integrity and availability (Information Regulator, 2013). This proactive stance ensures ongoing improvement in security and reduces vulnerabilities that cybercriminals exploit.

SA HEIs must comply with these regulations and promote employee awareness through comprehensive training programs. Effective policy implementation requires concerted efforts to raise awareness, educate employees about the legal landscape, and foster a security-conscious culture (South African Government, 2021). In line with Malatji et al. (2022), research confirms the critical role of employee cybersecurity awareness and training in enhancing the effectiveness of cybersecurity policies and preventing data breaches.

Having explored the national frameworks and legal landscape, the transition to cybersecurity awareness programs within SA HEIs necessitates a deeper exploration of employee awareness. This aligns with current legal requirements and the increasing emphasis on the human factor in cybersecurity. Therefore, the subsequent sections delve into the mechanisms

and benefits of such programs, providing a comprehensive understanding of their critical role in enhancing the cybersecurity posture of SA HEIs.

2.4 CYBERSECURITY AWARENESS

Recent research suggests that over 60% of all cybersecurity incidents result from a lack of employee knowledge and understanding (McIlwraith, 2021). This highlights the critical importance of cybersecurity awareness programs in combating cyber threats. Cybersecurity safeguards cyberspace and organisational assets, ensuring information availability, integrity, and reliability (Von Solms & Van Niekerk, 2013; von Solms & von Solms, 2018). It encompasses the protective mechanisms individuals and organisations adopt to shield interconnected systems, including computer networks, hardware, software, and data, from a spectrum of online risks (Perwej et al., 2021). These definitions mirror information security, which emphasises the critical aspects of information availability, integrity, and confidentiality (Safa et al., 2016).

Cybersecurity, primarily linked to data in cyberspace, distinguishes itself from information security, which encompasses protection for all information (Khan et al., 2020). The International Telecommunications Union (2020) defines cybersecurity as a multifaceted collection of tools, policies, security concepts, risk management approaches, best practices, assurances, and technologies deployed to protect users, organisations, and the cyber environment. Similarly, Chigada and Kyobe (2018) define information security as safeguarding information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction, aiming to establish integrity, confidentiality and availability.

The terms “information security” and “cybersecurity” are often used interchangeably in academic literature, with some scholars arguing that cybersecurity encompasses and replaces information security (von Solms & von Solms, 2018). However, despite the overlap, they are frequently treated synonymously. This study uses both terms interchangeably to align with the perspective in the literature. Nevertheless, it is crucial to recognise that cybersecurity is not a simple task but a multifaceted undertaking encompassing technology, individuals with diverse roles within organisational structures, and related processes that significantly influence operations (Clark et al., 2020).

The root causes of employee errors often stem from a lack of cybersecurity awareness, ignorance, negligence, apathy, mischief and resistance (Safa et al., 2016). The lack of awareness poses a significant challenge in preventing cyberattacks (Awoleke & Adigun, 2017; Brynard, 2016). Furthermore, studies have revealed a concerning lack of cybersecurity awareness among employees in various sectors, including the Nigerian banking industry (Awoleke & Adigun, 2017) and healthcare workers in South Africa (Brynard, 2016). These findings underscore the criticality of cybersecurity awareness, warranting an investigation into the factors influencing it. This aligns with this study's primary objective of investigating factors influencing employee cybersecurity awareness and behaviour in SA HEIs (see Section 1.4).

In response to the escalating concerns regarding cyberattacks in organisational settings, substantial resources have been invested in addressing this issue (Li et al., 2019). Building cybersecurity awareness plays a pivotal role in preparing employees to understand, manage and prevent attacks in organisations (Wang et al., 2021; Berkman et al., 2018). Chandarman and Van Niekerk (2017) define *awareness* as the correlation between knowledge, self-perception of skills, actual skills and behaviour, attitudes and other elements, establishing it as a non-technical measure utilised by organisations to augment employees' cybersecurity defences (Paolini, 2021). This multi-dimensional construct involves various factors that strengthen employees' ability to defend themselves against online threats by enhancing their understanding of attack risks and preventive measures (Bhana & Bhana, 2018). Equipping individuals with knowledge about cybercrime threats and preventive measures enables organisations, such as SA HEIs, to better prepare employees to tackle cyberattacks. Compliance with organisational security policies that deter deviant behaviour further enhances cybersecurity measures (Alshaikh, 2020).

The primary goal of cybersecurity awareness is to disseminate information about cybersecurity threats, vulnerabilities, and potential mitigation strategies, ensuring alignment with security policies and best practices (Bowen et al., 2006). Promoting cybersecurity awareness enables organisations, including SA HEIs, to fortify data protection against malicious actors and cybercriminals (Richet, 2022). Highlighting the criticality of cybersecurity awareness in preventing cyberattacks and safeguarding sensitive information underscores its importance. Therefore, SA HEIs' cybersecurity measures must prioritise building employees' awareness of cyber threats and risks to establish a secure organisational environment (Jalali et al., 2019).

2.4.1 Factors Influencing Employees' Cybersecurity Awareness

Several factors influence cybersecurity awareness among HEI employees. A critical factor is the need for effective cybersecurity training. Employees must have the knowledge and skills to recognise and respond to cybersecurity threats (Harindranath, 2018). For example, Brynard (2016) found that 86% of South African organisations still require a formal cybersecurity awareness and training program.

The lack of comprehensive cybersecurity awareness and training significantly contributes to inadequate awareness in SA HEIs: this directly aligns with this study's objective, which investigates the effectiveness of the current strategies. Training should cover topics beyond the basics, including social engineering, phishing, and ransomware, as these attack mechanisms are widespread (Harindranath, 2022; Wang et al., 2021; Mansoori & Welch, 2020; da Silva, Feitosa, & Garcia, 2020). Even when employees receive training, they may not retain the information if the programs are ineffective (Awoleke & Adigun, 2020). This emphasises the need for well-designed, engaging training programs; this aligns with this study's sub-objective that explores how training effectiveness influences employee awareness.

Another crucial factor influencing cybersecurity awareness is the perception of cybersecurity risk. Employees who perceive cybersecurity risks as low are generally less inclined to take appropriate actions (Chikandiwa et al., 2021). Conversely, employees who perceive the risks as high are likelier to adopt suitable measures (Li et al., 2019). Therefore, it is imperative to raise awareness regarding the risks of cyberattacks and emphasise the significance of protection (Wong et al., 2022). Furthermore, organisational culture plays a significant role. A robust cybersecurity culture educates employees about risks and instructs them on mitigation measures (Uchendu et al., 2021; Awoleke & Adigun, 2020). This can be fostered through top-level management support, regular training programs, and transparent communication (Mogoane & Kabanda, 2019; Alshaikh, 2020).

2.5 EFFECTIVE STRATEGIES FOR CYBERSECURITY AWARENESS

Effective Strategies and Employee Training: Various strategies have successfully improved cybersecurity in different sectors. Cybersecurity awareness education and training are significant measures to prevent cybersecurity incidents like cyber threats (Back & Guerette, 2021; Mihelič et al., 2019). Training should cover threat identification and response, password

management and data protection (Bryant & Conger, 2019). Additionally, organisations can leverage technology to fortify network perimeters and enhance cybersecurity (e.g., encryption, firewalls, intrusion detection systems). Fostering a cybersecurity awareness culture through regular communication and mandatory threat recognition and response training is also crucial (Awoleke & Adigun, 2017).

Challenges and Considerations: Implementing effective cybersecurity measures in HEIs faces challenges, such as insufficient funding (Bana & Bhana, 2018). Continued investment and improvement are necessary to address the evolving threat landscape. Another challenge is the lack of understanding and awareness of the importance of cybersecurity organisation-wide, leading to a lack of management commitment (Fernandes & Alves, 2020). Therefore, organisations need to create a culture of awareness where employees are informed and trained on their role in establishing a secure environment.

Employee training is a cornerstone of effective cybersecurity, particularly in HEIs, where data breaches can severely affect institutions (Cloete, 2017). Regularly training all employees increases awareness and helps prevent cyber-attacks and potential intellectual property violations (He et al., 2020). Research suggests the effectiveness of training in enhancing awareness and reducing security incidents (Liu et al., 2019; Ozturk & Bilge, 2018). Organisations must invest in training programs that equip employees with the knowledge and skills to identify and proactively prevent cyber-attacks (Awoleke & Adigun, 2017). These programs should include:

- **Regularly Updated:** The cybersecurity threat landscape constantly evolves, so training content needs to reflect the latest threats and tactics (Fernandes & Alves, 2020).
- **Tailored to the Organization's Needs:** Training should address the specific risks and vulnerabilities relevant to the HEI's environment (Awoleke & Adigun, 2020).
- **Engaging and Interactive:** Traditional lecture-style training may be less effective than interactive simulations, role-playing or gamification methods (Bhana & Bhana, 2018).
- **Accompanied by Continuous Support:** Training should be part of an ongoing awareness program with regular communication updates and reminders about cybersecurity best practices (Awoleke & Adigun, 2017).

Thus, by implementing a comprehensive cybersecurity awareness program that incorporates effective employee training and fosters a culture of security consciousness, HEIs can significantly reduce their cyber risks and protect sensitive information. This will create a more secure learning and research environment for students, faculty, and staff. Having reviewed how cybersecurity awareness contributes to an institution's cybersecurity structures, the following section focuses on risk management.

2.6 RISK MANAGEMENT

In addition to training employees, effective risk management is paramount for addressing cybersecurity issues within HEIs (Brynard, 2016; Bhana & Bhana, 2018). Risk management, a systematic approach to identifying, assessing and mitigating potential risks (i.e., cyber threats), allows institutions to safeguard their digital assets proactively. This focus on risk management aligns with the research objective of identifying effective strategies for enhancing cybersecurity measures in SA HEIs (see Section 1.4).

Implementing a well-defined risk management process is a cornerstone of effective risk management (Brynard, 2016). This process involves several key steps:

Identification of vulnerabilities and threats: This initial stage systematically catalogues potential security weaknesses within the HEI’s IT infrastructure, data, and user behaviour (Pieterse, 2021). The research sub-question (Section 1.5) delves deeper into understanding these factors influencing employee behaviour.

Likelihood and impact assessment: Following identification, each vulnerability and threat is evaluated to determine the probability of its occurrence and the potential severity of its impact on the HEI (Brynard, 2016).

Mitigation strategy development: Based on the assessment, institutions develop and implement appropriate countermeasures to address the identified vulnerabilities and threats. These measures can be technical (e.g., firewalls, intrusion detection systems) or non-technical (e.g., security policies, training programs).

Risk management should be an ongoing and iterative process, with institutions regularly reviewing and updating their strategies to effectively address emerging and evolving threats (Brynard, 2016). This iterative approach ensures that HEIs remain adaptable in the ever-changing cybersecurity landscape. Furthermore, adherence to recommended standards and best practices, such as those outlined by the National Institute of Standards and Technology (NIST) Cybersecurity Framework or ISO/IEC 27001, can provide valuable guidance for developing a comprehensive risk management strategy (Pieterse, 2021).

One valuable HEI approach is utilising cybersecurity frameworks, such as NIST's cybersecurity framework or ISO/IEC 27001. These frameworks provide guidance and best practices for managing cybersecurity risks, covering aspects like identifying, protecting, detecting, responding to, and recovering from cyber-attacks (NIST, 2018). What makes these frameworks particularly valuable is their adaptability to an organisation's specific needs, aiding institutions in developing a comprehensive cybersecurity strategy that aligns with our primary research objective (Section 1.4). Thus, South African HEIs can adopt these valuable frameworks to improve and strengthen their cybersecurity preparedness.

Since not all employees may possess a high level of cyber-savviness and might be unaware of the potential risks associated with their online behaviour, regular training, education, and user awareness sessions are crucial for mitigating cybersecurity risks (Pieterse, 2021). This aligns with our research objective of investigating the factors influencing employee cybersecurity awareness and behaviour (Section 1.4). Consequently, institutions must implement robust risk management practices by employing technological measures to secure their network systems, including firewalls, antivirus software, intrusion detection, and prevention systems (Brynard, 2016). Furthermore, institutions should consistently update their systems and software with the latest security patches to prevent potential vulnerabilities from being exploited.

Research has underscored the importance of effective risk management in preventing cyber-attacks on HEIs (Osuagwu et al., 2020). Several studies have explored risk management strategies in different contexts. For instance, Amin et al. (2018) developed a risk management framework for the banking sector in Pakistan, while Hasan et al. (2019) proposed a framework for the healthcare sector in India. These studies, along with the investigation into the specific context of SA HEIs, emphasise the need for organisations to implement effective risk management strategies tailored to their unique needs.

2.7 CYBERSECURITY BEHAVIOUR

The significant consequences of cybersecurity incidents on organisations are well-highlighted (Ponemon Institute, 2020; Verizon, 2020). Increased attention should focus on encouraging employees to comply with information security policies that inform cybersecurity behaviour (Balozian et al., 2019; Cram et al., 2019). Cybersecurity behaviour is crucial for fortifying institutions' information security measures and encompasses actions to mitigate vulnerabilities and enhance cybersecurity among end-users in organisational settings (Adams, 2019; Rasmussen et al., 2020).

Drawn from the personal hygiene concept of public health systems' literature, cyber-hygiene denotes cleanliness measures against germs and diseases (Vishwanath et al., 2020). Given its relevance, the personal hygiene concept should be employed and incorporated into the organisations' cybersecurity environment to establish healthy online organisation conditions and cybersecurity-compliant behaviour (ENISA, 2016, p. 4). Cybersecurity behaviour signifies practices aligned with security policies to ensure information confidentiality, availability and integrity within organisational frameworks (Vishwanath et al., 2020).

2.7.1 Cybersecurity-Compliant Behaviour and Protective Behaviour

In response to cyber risks and threats, end-user employees adopt various measures to mitigate vulnerabilities, including cyber hygiene, protective behaviour, and cybersecurity-compliant behaviour (CCB). Within information security management, CCB refers to practices aligned with security policies, ensuring information confidentiality, availability, and integrity within organisations (Vishwanath et al., 2020). It captures users' actions to protect personal and organisational digital assets (Watkins et al., 2016). While some studies differentiate between CCB and protective behaviour, this study adopts the term CCB to encompass employees' adherence to security policies and best practices (Borrajo et al., 2015). This broader definition is consistent with our research objective, investigating the factors influencing employee cybersecurity behaviour in South African HEIs (see Section 1.4). Aligned with the Protection Motivation Theory (PMT), cybersecurity protective behaviour aims to mitigate human vulnerabilities by promoting secure cyber practices (Borrajo et al., 2015), often synonymous with CCB.

Guided by the organisation's cybersecurity environment, CCB encompasses actions such as adopting robust password practices, utilising multi-factor authentication, exercising caution with phishing emails and routinely backing up critical data (Cain et al., 2018).

Gaunt (2000) emphasises the significance of the human elements within organisational cybersecurity structures. They are often identified as the weakest link in the cybersecurity chain (Abraham & Chengalur-Smith, 2010; Aloul, 2012). The author highlights the need for employee awareness, further supported by recent studies demonstrating that organisations and individuals can address security vulnerabilities by adopting CCB (van Bavel Rodríguez-Priego et al., 2019; Zimmermann & Renaud, 2019; Lee, 2021). However, limited research explores the specific factors influencing CCB in the context of South African HEIs. This study addresses this gap by investigating how various factors influence employee CCB in these institutions.

2.7.2 Cybersecurity Behaviour in Organisational Contexts

In an organisation's cybersecurity context, "cybersecurity behaviour" characterises employee's actions, reactions and overall conduct, aligning with an organisation's cybersecurity awareness, policies, and prior experience (Li et al., 2019; Safa et al., 2015). Different organisations' settings significantly influence user behaviours, with varying behaviours observed in diverse environments (Liang & Xue, 2010; Kruger et al., 2011). Policies and regulations guide employee security behaviour within organisational settings, supplemented by cybersecurity awareness training shaping compliance with these policies (Blythe, 2013).

2.7.3 Standardisation and Awareness of Cybersecurity Behaviour

This study primarily focuses on classifying cybersecurity behaviour within organisational security settings, emphasising the necessity for standardised definitions and associated security behaviours (Blythe, 2013). The diverse interpretations of CCB across various studies highlight the need for standardisation in defining and implementing these behaviours. Understanding user behaviour aims to foster a culture of cybersecurity compliance while discouraging non-compliant behaviour that could be malicious. Cybersecurity behaviour is multifaceted and influenced by various factors, including organisational settings, policies, regulations, awareness training and theoretical frameworks (van Bavel Rodríguez-Priego et

al., 2019). Standardising and raising awareness of these behaviours is essential, especially amid the rapidly evolving cybercrimes. Understanding how these factors influence cybersecurity-compliant behaviour in SA HEIs aligns with the research objective, investigating the factors influencing employee cybersecurity awareness and behaviour (Section 1.4). The following section reviews theories and organisational factors that underpin CCB.

2.8 THEORETICAL UNDERPINNING

The rapidly expanding digital landscape of SA HEIs has raised significant cybersecurity concerns. This study examines and explains employee cybersecurity awareness and behaviour within this unique context. This section explores the theoretical underpinnings for understanding employee cybersecurity awareness and behaviour within organisations such as HEIs. It emphasises the critical role of employee cybersecurity awareness in fostering CCB within institutions, as evidenced by theoretical and empirical insights (Kovacevic, Putnik & Toskovic, 2020). Studies consistently demonstrate that motivated employees who prioritise the protection of organisational assets are more inclined to comply with cybersecurity policies that significantly contribute to fostering CCB. Sikora and Biros (2016) noted a positive correlation between employees' motivation to comply with cybersecurity policies and their engagement in secure behaviours, such as adopting robust passwords and promptly reporting suspicious activities. The investigations by Hoxhaj et al. (2021) substantiated this viewpoint by highlighting that employees possessing heightened cyber threat awareness tend to comply with security policies. These studies highlight the role of employee motivation in driving CCB within organisational environments, underlining that security compliance is a primary defence against multifaceted cyber threats.

Commonly Applied Behavioural Theories in Cybersecurity Research

Among the commonly applied behavioural theories in cybersecurity studies are the General Deterrence Theory (GDT), Planned Behaviour (TPB) and Protection Motivation Theory (PMT) (Nasir et al., 2018; Lebek et al., 2014; Sommestad et al., 2014). While the Technology Acceptance Model (TAM) is included in some studies, its application is relatively less frequent (Nasir et al., 2018). Notably, TPB and PMT stand out for their effectiveness and extensive use as foundational theories in cybersecurity research (Almansoori et al., 2023; Williams & Joinson, 2020). While TPB focuses on attitudes, subjective norms (i.e., beliefs about what

others expect), and perceived behavioural control, PMT emphasises the role of threat and coping appraisals.

TAM and GDT share some conceptual similarities with PMT (Nasir et al., 2018). TAM suggests that users are more likely to adopt security measures they perceive as valuable and easy to use, similar to PMT's focus on coping appraisal (perceived effectiveness of security measures) (Davis, 1989; Rogers, 1975). Likewise, GDT acknowledges the potential negative consequences of non-compliance, aligning with PMT's threat appraisal (Grasmick et al., 1993). However, TAM's primary focus on explaining initial technology adoption (Steyn et al., 2015) may not be as relevant today, where ICT is already widely used. In this environment, understanding effective security behaviours becomes more critical. Additionally, TAM does not account for existing security knowledge, which can significantly influence cybersecurity behaviours. PMT's focus on threat appraisal indirectly considers security knowledge by emphasising the perceived seriousness of cybersecurity threats. For these reasons, PMT provides a more suitable framework for investigating the factors influencing employees' cybersecurity awareness and behaviours in South African Higher Education Institutions.

TAM and GDT are also relevant as they share some conceptual similarities with PMT. TAM suggests that users are more likely to adopt security measures they perceive as valuable and easy to use, similar to PMT’s focus on coping appraisal (perceived effectiveness of security measures). Like PMT’s threat appraisal, GDT acknowledges the potential negative consequences of non-compliance (Grasmick et al., 1993). However, TAM’s primary focus on explaining initial technology adoption (Steyn, 2015) may not be as relevant today, where ICT is already widely used. Interestingly, PMT’s concept of threat appraisal aligns with GDT’s focus on sanctions. Both theories acknowledge the potential negative consequences of non-compliance (Rogers, 1975; Grasmick et al., 1993). Similarly, PMT’s coping appraisal aligns with TAM’s perceived usefulness and ease of use. Like TAM, which suggests that users are more likely to adopt easy-to-use technologies (Davis, 1989), PMT theorises that individuals are more likely to adopt protective behaviours if they believe they are effective (Rogers, 1975). This alignment makes PMT a valuable tool in cybersecurity research (Nasir et al., 2018). Thus, its connection with TPB will be explored by integrating both theories.

Studies that employed TPB and PMT identify factors that promote employee compliance with cybersecurity policies and protocols, encompassing awareness, training initiatives and

leadership support (Hina et al., 2019; Lowry & Moody, 2015; Cheng et al., 2013; Ifinedo, 2012; Vance et al., 2012). These theories provide valuable frameworks for comprehending and explaining the relationship between these factors within the cybersecurity landscape. This is evident by their successful application in studies focusing on cybersecurity behaviours, establishing them as fundamental theories in the field (Kuppusamy et al., 2020).

The traditional TPB model focuses on behavioural intention, while PMT emphasises threat appraisal and risk perception (Almansoori et al., 2023). HEIs possess unique cybersecurity environments shaped by diverse local and international standards and regulations (Hina et al., 2019; Goel et al., 2017). It is argued that with well-defined security policies and comprehensive awareness programs, HEIs' cybersecurity environment significantly influences its cybersecurity culture (Hina et al., 2019; Goel et al., 2017; Chen & Wen, 2015). Therefore, considering this distinction, this study explores a broader variety of dimensions by integrating TPB and PMT (Almansoori et al., 2023). Specifically, it utilises PMT for adaptive responses to threats and TPB to enhance employees' policy compliance in HEIs, as noted in several studies (i.e., Burns et al., 2017a; Bulgurcu et al., 2010).

The study's conceptual model draws from PMT and TPB, encompassing key variables such as attitude, subjective norms, perceived behavioural control, self-efficacy, threat appraisal, response efficacy and response cost (Han et al., 2017). Previous studies have demonstrated the potential of integrating these theories to predict security policy compliance (Ifinedo, 2012; Bulgurcu et al., 2010). Other studies investigate antecedents of cybersecurity policy compliance, including habits, perceived threats and the severity of security breaches (Vance et al., 2012; Herath & Rao, 2009a). With detailed discussion in (section 2.9), the conceptual framework comprises three primary components— cybersecurity awareness, policy and experience within the organisational (i.e., institutional herein) cybersecurity environment— which influence TPB and PMT to shape employees' CCB. Having highlighted the foundation of the study's conceptual framework, the following subsections provide a detailed discussion of the theories and constructs related to the research purpose.

2.8.1 Theory of Planned Behaviour

Among the commonly applied behavioural theories in cybersecurity studies, TPB stands out for its effectiveness and extensive use (Almansoori et al., 2023; Williams & Joinson, 2020).

Developed by Ajzen (1991), TPB builds upon the Theory of Reasoned Action by introducing the concept of perceived behavioural control as a determinant of behaviour (Ajzen, 2011). It has also been integrated with other theories, such as social cognitive theory, to develop more comprehensive models of human behaviour (Ajzen, 2011). For instance, the integrated model of cybersecurity behaviour combines TPB with social cognitive theory to predict and explain employee security-related behaviours (Sommestad & Hallberg, 2013). Figure 1 illustrates the TPB antecedent and consequence constructs.

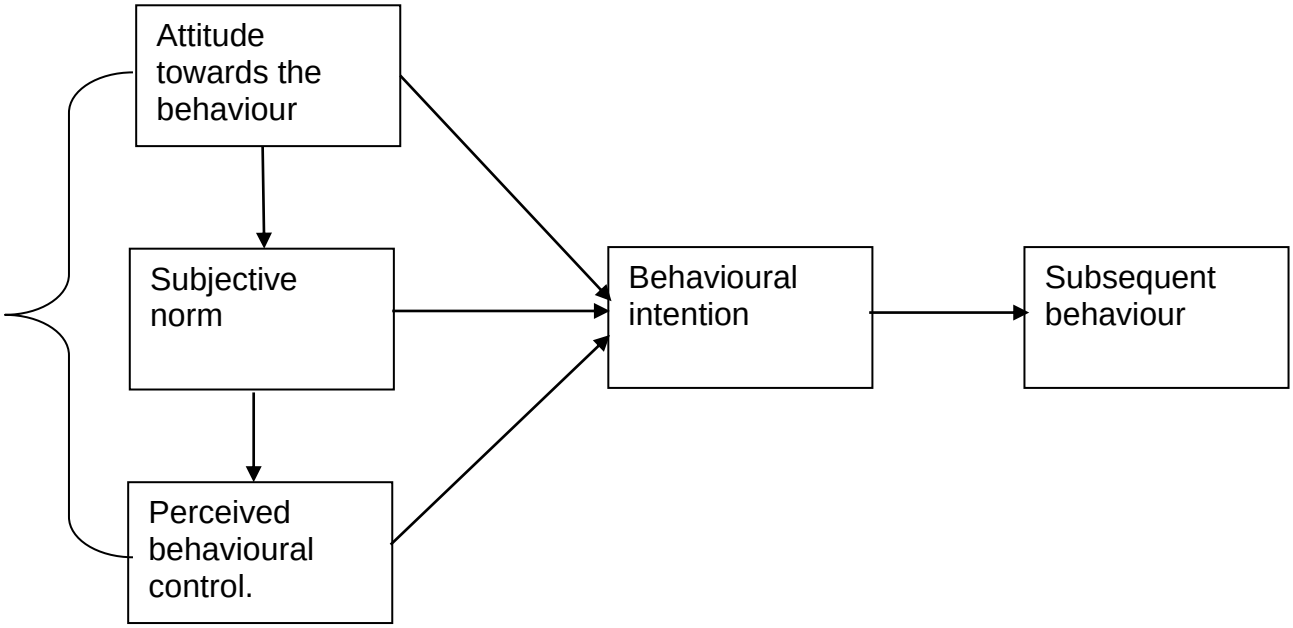

Figure 1: Theory of Planned Behaviour (Ajzen, 1991)

Model and Construct Definitions

The TPB model focuses on three key determinants to explain behavioural intention:

- **Attitude:** An employee or individual's positive or negative evaluation of performing a specific behaviour, shaped by their beliefs about the outcomes of that behaviour (Bulgurcu et al., 2010; Blythe et al., 2015).
- **Subjective Norms:** These are perceived social pressures or expectations related to behaviour, which include the beliefs of significant individuals or groups and the motivation to comply with these beliefs (Bulgurcu et al., 2010).
- **Perceived Behavioural Control (Self-Efficacy):** employee perceived ability to perform a behaviour, considering factors such as skills, resources and external constraints (Bulgurcu et al., 2010; Rhee et al., 2009).

TPB posits that these constructs collectively influence employees' intention to engage in a behaviour, predicting the actual behaviour. For example, employees with positive attitudes towards cybersecurity, who perceive that their colleagues or supervisors expect them to practice cybersecurity and who feel confident in their ability to do so, are more likely to engage in CCB.

Benefits and Shortfalls

The TPB offers several advantages, including its comprehensive outlook, predictive efficacy and clear targets for behaviour change interventions. Lebek (2014) highlighted its significance and dominance, recently supported by Nasir et al. (2018), noting that its three determinant constructs are consistently robust predictors of cybersecurity behaviour. However, like any theory, TPB has limitations. For instance, it may not fully account for the influence of intricate contextual factors on behaviour or accurately predict automatic or unconscious behaviours, especially in dynamic and rapidly changing contexts such as cybersecurity threats.

Past Applications

TPB adaptability is evident in its widespread application across diverse domains, including cybersecurity, where it has been validated to predict security policy compliance well (Nasir et al., 2018). It has also been used to study users' intentions to use social networking websites (Pelling & White, 2009), understand environmental actions like recycling (Teng et al., 2013; Lam, 1999), and explore factors influencing entrepreneurship (Miralles et al., 2015). TPB has been deployed in cybersecurity to predict and influence compliance with security practices (Bulgurcu et al., 2010; Chandarman & Van Niekerk, 2017).

Relevance to the Study

In the HEIs, the TPB's applicability to cybersecurity awareness and behaviour is noteworthy. It sheds light on how employees' beliefs about cybersecurity (attitude), social pressures from colleagues and superiors (subjective norms), and perceived ability to perform secure behaviours (perceived behavioural control) influence their intentions and actual cybersecurity behaviours. Despite the limitations mentioned earlier, TPB remains a suitable foundation for this study, particularly when complemented by other theories, such as PMT. Having explored the focus of TPB on behavioural intention, the next section now delves into the PMT model.

2.8.2 Protection Motivation Theory

PMT (Rogers, 1975) is a prominent social psychological theory that sheds light on how individuals (i.e. employees herein) react to potential threats and adopt protective behaviours (Rogers et al., 1983). Initially developed to understand health-related decision-making (Menard et al., 2018; Posey et al., 2015), PMT has gained adoption in cybersecurity research. It has been valuable in exploring employee CCB within organisations such as HEIs, as investigated in the current study.

PMT Main Constructs

PMT revolves around two fundamental constructs: threat appraisal and coping appraisal (Rogers et al., 1983). Threat appraisal focuses on an individual's perception of a cyber threat's severity (how serious the consequences could be) and susceptibility (how likely they are to be targeted). Coping appraisal examines an individual's belief in the effectiveness of available security measures (response efficacy) and their confidence in using them (self-efficacy). These combined appraisals trigger a motivational process that significantly determines an individual's or employee's intention to engage in CCB (Rogers et al., 1983). Figure 2 visually illustrates PMT's core constructs and their influence on behaviour.

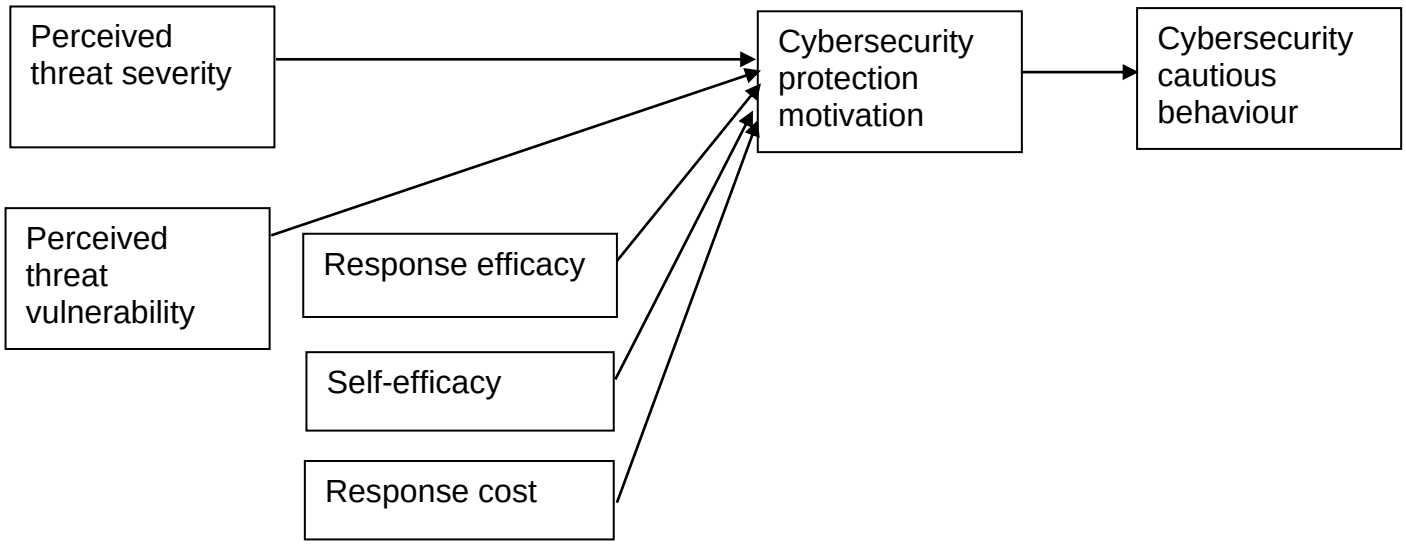

Figure 2: Protection Motivation Theory (Rogers, 1975)

PMT Strengths and Limitations

PMT offers many benefits, such as leveraging fear appeals to motivate behavioural change, and it is a valuable tool in cybersecurity awareness campaigns. It also provides a holistic

assessment of factors influencing behaviour by considering threat perception and coping mechanisms. Additionally, PMT demonstrates versatility across various domains, including cybersecurity (Dang-Pham & Pittayachawan, 2015). Studies by Johnston and Warkentin (2010) highlight how PMT's core constructs, particularly threat severity, self-efficacy and response efficacy, significantly influence employee cybersecurity behaviours when dealing with spyware threats. This aligns with research by Boss et al. (2015), which suggests that PMT is a valuable tool for understanding the motivation behind using anti-malware software.

However, similar to TPB, as highlighted above, PMT also faces limitations, as critics argue that it struggles to capture the complexities of specific cybersecurity phenomena (Karjalainen & Siponen, 2011; Moody et al., 2018; Roberts, 2021). For instance, the theory often emphasises personal threats rather than those specific to the workplace environment (Warkentin et al., 2016). Additionally, PMT assumes rational decision-making, potentially neglecting the impact of emotional or situational factors on behaviour. Furthermore, some studies have reported inconsistent results regarding its effectiveness (Mou et al.,2022), suggesting it may not fully capture all influences on behaviour.

PMT Past Applications and Relevance to this Study

PMT was initially used to explore responses to health threats, and PMT has been successfully applied in environmental conservation and cybersecurity research. Studies demonstrate its dominance in predicting factors influencing the intention to adopt cybersecurity-compliant behaviours (Dang-Pham & Pittayachawan, 2015). Research (i.e., Boss et al., 2015; Burns et al., 2017a; Ifinedo, 2012; Menard et al., 2018) demonstrate PMT's effectiveness in predicting intentions to comply with cybersecurity practices. Similarly, Herath and Rao (2009) and Vance et al. (2012) explored the influence of PMT on factors affecting compliance with cybersecurity policies, validating the theory's explanatory power in this domain.

This study focuses on employee CCB in SA HEIs, making PMT particularly relevant. The theory helps to understand how employees' assessments of cybersecurity threats - severity and likelihood and their beliefs about coping mechanisms - response efficacy and self-efficacy influence their cybersecurity practices. While limitations exist regarding emotional and situational factors (Mou et al.,2022), PMT remains valuable, especially when complemented with theories like the TPB.

2.8.3 Integrating TPB and PMT for a Comprehensive Understanding

Having individually explored the TPB and PMT, this section examines how the theories can be integrated to provide a comprehensive understanding of the reason behind employee belief and motivation for secure behaviours. These theories complement each other by focusing on different aspects. While the TPB focuses on employees' beliefs and social influences (Ajzen, 1991), PMT emphasises their perceptions of threats and coping mechanisms (Rogers et al., 1983). By integrating these significant factors, this study forms a richer picture of what informs and motivates employees to adopt CCB within their institutions. The urgent need for employee cybersecurity awareness is emphasised and well-documented (Kovacevic et al., 2020; Li et al., 2019) as it directly impacts the formation of secure behaviours. This emphasis aligns with other studies highlighting a positive correlation between employee motivation and secure behaviours (Sikora & Biros, 2016; Hoxhaj et al., 2021).

Rationale for Integrating TPB and PMT in this Study

TPB and PMT provide frameworks to explore the factors influencing employee cybersecurity awareness and behaviour (objective 4, see section 1.4). For instance, PMT's threat appraisal can be linked to employees' challenges in recognising cyber threats through employee security awareness (Vance et al., 2013). Similarly, TPB is a strong tool for predicting behavioural intentions based on attitudes, subjective norms and perceived behavioural control, while PMT excels in describing how threat appraisal and coping appraisal influence protective behaviours
By integrating these theories, this study proposes a comprehensive framework that captures the multifaceted nature of cybersecurity behaviour. This combined approach provides a holistic understanding of the cognitive, social and motivational factors influencing employees' CCB within SA HEIs.

The integrated model proposes that a combination of factors influences CCB:

- TPB Constructs: Attitudes, subjective norms, and perceived behavioural control
- PMT Constructs: Threat appraisal and coping appraisal

The study integrates these theories by utilising PMT to facilitate adaptive responses to threats among employees in South African HEIs (Burns et al., 2017a). The combined constructs from both theories (TPB's attitude, subjective norms, perceived behavioural control, and PMT's threat appraisal and coping appraisal) are hypothesised to influence employees' CCB in HEIs.

The following sections delve deeper into the research model and hypotheses, exploring how these combined theories are applied to the organisations' cybersecurity environment concepts to establish a robust and comprehensive research model. Table 1 summarises the key insights from the literature review regarding the theoretical foundations of cybersecurity research.

Table 1: ***Summary of Key Insights from Theories of Cybersecurity Behaviour***

Theory	Key Insights
Theory of Planned Behaviour	Employees' attitudes, social norms and perceived control over cybersecurity behaviours influence their behaviour.
General Deterrence Theory	Individuals are discouraged from engaging in undesirable behaviour when they witness others facing adverse consequences for similar actions.
Protection Motivation Theory	Employees' perceived vulnerability to cyber threats and the perceived effectiveness of protective behaviours influence their motivation to engage in cybersecurity behaviours.
Technology Acceptance Model	Employees' perceived usefulness and ease of use of technology or cybersecurity awareness measures may influence their acceptance and use of technology as cybersecurity measures.

2.9 EMPIRICAL SECTION

This section reviews related empirical studies on cybersecurity to better understand the factors influencing these outcomes. The studies reviewed are discussed under the three distinct categories below and further illustrated in Table 2. The study uses the TPB and PMT theories to investigate the factors influencing employees' cybersecurity awareness and behaviour in SA HEIs. Cybersecurity awareness and behaviour are essential for protecting SA HEIs and their employees from cyber threats resulting from insecure behaviour. These findings collectively underscore the pivotal role of insecure and non-compliant security behaviour.

2.9.1 Psychological Factors

Psychological factors, such as self-efficacy, attitude, threat appraisal and response efficacy, play vital roles in shaping cybersecurity awareness and CCB, as Safa et al. (2018) noted. For instance, Ifinedo (2012) conducted a study revealing that employees with high self-efficacy, positive attitudes and a strong belief in response efficacy were more inclined to comply with cybersecurity policies. Similarly, Farooq, Ndiege, and Isoaho (2019) emphasised that self-efficacy and attitude significantly predict employees' intentions to adopt cybersecurity measures. Likewise, De Kimpe et al. (2022) extended this exploration by investigating protection motivation in cybersecurity behaviour. Their findings revealed that perceived knowledge, internet trust and protection motivation influence individual cybersecurity decision-making. Furthermore, Sulaiman et al. (2022) studied government employees and identified the critical roles of severity, vulnerability, response efficacy and self-efficacy in motivating employees to comply with cybersecurity practices.

While these studies contributed substantially to understanding the impact of psychological factors on compliant behaviour, none exclusively examined the influence of an organisation's cybersecurity environment, such as cybersecurity awareness, on psychological factors (i.e., attitudes). Therefore, the current study endeavours to bridge this gap by considering the impact of an organisation's cybersecurity environment while leveraging the insights from these studies. Further, it investigates the influence of cybersecurity awareness on attitudes, which subsequently lead to cybersecurity-compliant behaviour within the SA HEIs setting.

2.9.2 Behavioural Factors

Considering the behavioural aspects, Tsai et al. (2016) examined the factors influencing online safety behaviours. Their findings highlighted the significance of coping appraisal variables and the perceived threat severity in establishing individuals' online navigation and internet use. Furthermore, Sommestad, Karlzén, and Hallberg (2015) introduced the concept of anticipated regret as a powerful motivator for adhering to cybersecurity policies, offering a novel angle on predictors of cybersecurity policy compliance. In another vein, Van Bavel et al. (2019) explored the impact of cybersecurity notifications on behaviour. They discovered that notifications incorporating coping messages were notably more effective in promoting secure and compliant behaviour. Khan et al. (2023) investigated cybersecurity awareness training and found that PMT-based training effectively enhances self-efficacy and triggers behavioural change.

These findings collectively underscore the pivotal role of behavioural factors in shaping cybersecurity compliance within individual contexts. They form the empirical foundation for this study, which explores the impact of PMT variables on cybersecurity-compliant behaviour within organisational contexts.

2.9.3 Organisational Factors

This exploration delves into the organisational factors influencing employees' cybersecurity awareness and compliance. Employee awareness and policy compliance significantly impact CCB in organisational settings (Nifakos et al., 2021). For instance, Kadir et al. (2016) found that positive acceptance and adherence to cybersecurity policies enhanced CCB in Malaysian organisations. Similarly, Brown and Johnson (2019) found that stringent policy enforcement impacted users' compliance with cybersecurity measures in HEIs. In a more recent study, Garcia et al. (2020) emphasised the roles of employees' attitudes and threat appraisals in promoting CCB within HEIs. Chen and Kim (2021) extended this knowledge by demonstrating the positive effects of cybersecurity training on awareness and behaviour among employees in HEIs. Adams (2022) also found high levels of threat appraisal among employees in HEIs, albeit accompanied by neutral attitudes and low self-efficacy.

When exploring the influence of organisational experience, Li et al. (2016) revealed that employees' cybersecurity experience significantly improves cybersecurity behaviour within organisational settings. Building upon this, a more recent study by Li et al. (2019) further expanded our understanding by delving into employee cybersecurity experience and its effects on the severity of cybersecurity threats. Using a sample of 579 business managers and professionals, their study highlighted how employees acquire competencies, especially when exposed to organisations' cybersecurity awareness programs. Li et al.'s (2016; 2019) findings shed light on the critical influence of policy awareness and the organisation's cybersecurity environment on threat appraisal and coping appraisal toward CCB. This study synthesises empirical findings to explore the factors influencing employees' CCB. This study addresses these limitations by integrating PMT and TPB to highlight the significance of organisational factors in shaping CCB. Table 2 summarises key literature on employee CCB within HEIs, categorised into three focused groups: psychology, organisation, and behavioural factors.

Table 2: ***Summary of Key Studies in Cybersecurity Research***

Author & Year	Research Title & Category	Key Variables Investigated	Key Findings
Ifinedo (2012)	Understanding information systems security policy compliance Psychological Factors	Self-efficacy, attitude toward compliance, subjective norms, response efficacy, perceived vulnerability.	Self-efficacy, attitude, subjective norms, response efficacy and perceived vulnerability influence employees' intentions to comply with security policy.
Farooq et al. (2019)	Factors Affecting Security Behavior of Kenyan Students. Psychological Factors	Self-efficacy, attitude	Self-efficacy and attitude significantly shape the intention to adopt security measures.
De Kimpe et al. (2022)	What we think we know about Cybersecurity Psychological Factors	Perceived knowledge, internet trust, protection motivation	Perceived knowledge, internet trust, and protection motivation influence cybersecurity behaviour.
Sulaiman et al. (2022)	Cybersecurity Behavior among Government Employees. Psychological Factors	Severity, vulnerability, response efficacy, self-efficacy	Highly motivated employees actively engage in cybersecurity compliance practices.
Tsai et al. (2016)	Understanding online safety behaviors: A protection motivation theory perspective Behavioural Factors	Coping appraisal variables, threat severity	Coping appraisal variables and threat severity influence online safety behaviours.
Sommestad, Karlzén &	The sufficiency of the theory of	Anticipated regret	Anticipated regret is a significant predictor of

Hallberg (2015)	planned behavior for explaining information security policy compliance. Behavioural Factors		cybersecurity policy compliance.
Van Bavel et al. (2019)	Using protection motivation theory in the design of nudges to improve online security behavior Behavioural Factors	Coping messages	Coping messages in notifications promotes secure behaviour.
Khan et al. (2023)	Evaluating protection motivation-based cybersecurity awareness training on Kirkpatrick's Model. Behavioural Factors	Self-efficacy	PMT-based cybersecurity awareness training enhances self-efficacy and behavioural change.
Smith (2018)	Cybersecurity Awareness Program in SA HEIs. Organisations Factors	Awareness program impact	A robust cybersecurity awareness program in SA HEIs enhances employees' cybersecurity awareness and compliance behaviour.
Brown & Johnson (2019)	Impact of Security Policies on HEIs Organisations Factors	Policy enforcement	Policy enforcement influences user behaviour and cybersecurity compliance.
Garcia et al. (2020)	Psychological Factors in	Attitudes, Threat Appraisals	Employees' attitudes and threat appraisals

	Cybersecurity Compliance in HEIs Organisations Factors		promote cybersecurity compliance.
Chen & Kim (2021)	Cybersecurity Training Impact on HEIs Organisations Factors	Training Effectiveness	Cybersecurity training has a positive impact on employees' cybersecurity awareness and behaviour.
Adams (2022)	Employee Perceptions of Cybersecurity Threats in HEIs Organisations Factors	Threat appraisal, awareness, self-efficacy	Employees have high levels of threat appraisal but neutral attitudes and low self-efficacy.
Li et al. (2019)	Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour Organisations Factors	Threat and coping appraisals, policy, awareness.	Policy awareness and the organisation's security environment significantly impact threat appraisal and coping appraisal towards cybersecurity-compliant behaviour.

2.9.4 Empirical Findings and Recommendations

These empirical studies offer comprehensive insights into the multifaceted aspects of cybersecurity awareness, policy, employee experience, behaviour, and the interconnected factors that shape them. They are the robust foundation upon which these study endeavours are grounded, further enriching the mission to enhance cybersecurity awareness and cultivate compliance behaviour, particularly within the SA HEIs context. Based on the insights gained from the empirical studies reviewed in this section, the following recommendations can be proposed to enhance cybersecurity awareness and promote compliant behaviour within SA HEIs:

1. Develop and implement comprehensive, tailored cybersecurity awareness programs to educate employees about threats, best practices, and the importance of compliance.
2. Implement clear and concise cybersecurity policies, ensuring effective communication with employees.
3. Provide regular cybersecurity training, covering topics like phishing awareness, password security, and social engineering.
4. Foster a cybersecurity awareness and compliance culture by encouraging employees to report suspicious activities and rewarding adherence to cybersecurity best practices.

By implementing these recommendations, SA HEIs can significantly strengthen their cybersecurity posture against the evolving landscape of cybersecurity threats and protect institutions and employees.

2.10 LINKING RESEARCH QUESTIONS TO THE LITERATURE

Exploring the landscape of cybersecurity awareness programs within SA HEIs provides a focal point for fortifying defences against evolving cyber threats. This section meticulously examines the role of Cybersecurity Awareness, delving into its pivotal contribution to safeguarding data against cybercrimes. It scrutinises the significance of diverse approaches, including educational programs, technological measures, and cultivating a cybersecurity-aware culture within organisational settings.

These discussions underline the critical importance of cybersecurity awareness and offer insights into the multifaceted strategies currently employed across various sectors in SA HEIs. This comprehensive analysis aligns with the study's sub-research question.

2.10.1 Cybersecurity Awareness and Risk Management in SA HEIs

Sections 2.4 and 2.6 extensively explore cybersecurity awareness and risk management, providing crucial insights into SA HEIs' cybersecurity landscape. In Section 2.4, the literature emphasises the pivotal role of cybersecurity awareness in fending off cyber-attacks. Notably, studies (e.g., Awoleke & Adigun, 2017; Brynard, 2016) stress the urgency of heightened employee awareness, especially within SA HEIs, underscoring the pressing need to elevate awareness levels. Moreover, Section 2.6 delves into risk management and its direct correlation with cybersecurity awareness levels within HEIs. Effective risk management becomes a

marker of prevailing awareness among employees. These insights help to answer the research question: What is the current level of employees' cybersecurity awareness in SA HEIs?

2.10.2 Key Determinants of Cybersecurity Awareness and Behaviour in SA HEIs

Multiple sections meticulously dissect multifaceted factors shaping cybersecurity awareness and behaviour among employees in SA HEIs. Section 2.5 extensively examines critical elements such as the necessity of training programs, the perception of cybersecurity risks, and the significant impact of organisational culture on cybersecurity behaviours. Furthermore, Section 2.8 introduces leading cybersecurity theories like TPB and PMT, offering profound insights into factors influencing employees' cybersecurity awareness and behaviours within SA HEIs. The comprehensive analysis addresses the research question: What factors influence employees' cybersecurity awareness and behaviour in SA HEIs?

2.10.3 Strategies for Enhancing Cybersecurity Awareness in SA HEIs

Section 2.5, Effective Strategies for Cybersecurity Awareness, delineates successful strategies across industries to improve cybersecurity. This section provides valuable insights into potential approaches applicable to SA HEIs, encompassing education, technology utilisation, and fostering a cybersecurity-aware culture. These strategies offer actionable pathways to enhance cybersecurity awareness within SA HEIs.

Integrating literature across Sections 2.2 to 2.9 seamlessly interconnects and addresses research questions cohesively. It thoroughly analyses the theories underpinning cybersecurity awareness programs, existing awareness levels, influential factors, challenges and potential improvement strategies within SA HEIs. Building upon the theoretical frameworks of TPB and PMT, this study investigates the relationship between various factors influencing employee cybersecurity behaviour in SA HEIs. To empirically examine these complex relationships and model formative constructs like cybersecurity awareness and organisational policies, this study employs partial least squares structural equation modelling (PLS-SEM). PLS-SEM offers several advantages for this study, including its ability to handle non-linear relationships, accommodate formative constructs (Petter et al., 2007), and work effectively with small sample sizes and non-normally distributed data (Gefen et al., 2011). Also, this study implemented

established procedures and statistical tests outlined by MacKenzie et al. (2011) to minimise and test for common method bias.

2.11 CONCLUSIONS

This chapter comprehensively reviewed existing literature on cybersecurity awareness, employee training, risk management in HEIs, and prominent cybersecurity theories. It emphasises the crucial role of cybersecurity awareness in safeguarding sensitive information and preventing cyber-attacks. The review highlights practical strategies for improving cybersecurity, including employee training programs and robust risk management practices.

Key Findings from the Literature Review: Importance of Cybersecurity Awareness: Existing research confirms the crucial role of cybersecurity awareness in mitigating cyber threats. Strategies for Improvement: The review identifies practical approaches for enhancing cybersecurity, such as employee training and risk management frameworks. The review also identifies critical gaps in the existing literature, including the unique cybersecurity challenges and needs of the higher education sector, the influence of cultural factors on employee cybersecurity awareness, and the effectiveness of various training delivery methods in promoting cybersecurity awareness.

3 RESEARCH MODEL AND HYPOTHESES

3.1 INTRODUCTION

This chapter presents the research model and hypotheses developed to address this study's research questions and objectives. Drawing from the literature and existing theoretical frameworks discussed in the preceding chapter, this study investigates employee cybersecurity-compliant behaviour (CCB) in South African Higher Education Institutions (SA HEIs). It integrates the Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT) within organisational cybersecurity environments. These environments are absent in traditional models focusing solely on individual psychological factors influencing cybersecurity behaviour. Some studies noted inconsistent results from PMT and TPB due to a lack of moderating constructs (Schuetz et al., 2020), while others found some TPB factors inadequate (Karlsson et al., 2018; Sommestad et al., 2019). Safa et al. (2015) and Li et al. (2019) underscore promoting a strong cybersecurity culture through security policies and employee awareness (Safa et al., 2015; Li et al., 2019). Considering this background, this study proposed the institutional cybersecurity environment as an antecedent that influences the psychological factors considered in TPB and PMT. These antecedents include:

Cybersecurity Awareness refers to employees' knowledge and understanding of cyber threats and best practices. Studies by Bada et al. (2019), Heidt et al. (2019), and Wong et al. (2022) suggest that awareness acts as an intrinsic motivator, driving employees to adopt secure practices due to a sense of internal responsibility. Employees who understand cyber threats are more likely to take proactive steps to protect themselves and the organisation.

Cybersecurity Policy: Clear and well-defined policies set expectations for secure behaviour and provide a framework for employees to follow. These policies can serve a dual purpose: acting as a guide for secure practices and as an extrinsic motivator for compliance, as evidenced by research from Li et al. (2019) and Safa et al. (2015). By outlining acceptable and unacceptable behaviour, policies encourage employees to prioritise cybersecurity.

Employee Experience: This component considers the past encounters and practical knowledge employees have gained from cybersecurity incidents. Previous experiences with

cyberattacks or data breaches can heighten awareness and influence employees' perception of the threat landscape. Li et al. (2016, 2019) and Safa et al. (2015) show that experiences can shape behaviour and act as intrinsic motivators. Employees may be more likely to adopt secure practices to avoid similar incidents in the future. Table 3 presents the proposed constructs used in the study's model to investigate employee CCB within SA HEIs. Each construct is defined to ensure clarity and understanding of its role within the model (Table 3).

Table 3: *Proposed Constructs' Meaning and Usage*

Construct	Meaning	Usage
Cybersecurity Awareness (CA)	Refers to an individual's comprehension of cybersecurity threats and the necessity for protective actions.	Assessing employees' understanding of cybersecurity threats and their importance.
Institution Cybersecurity Policy (ICP)	Refers to the organisation's security policy formulated to instruct and guide employees on the acceptable standard of cybersecurity behaviour.	Evaluating the impact of organisational security policies on employees' behaviour.
Cybersecurity Experience (CEI)	Employees' cybersecurity experience and involvement in dealing with previous cybersecurity incidents, training and related activities.	Assessing the influence of employees' prior cybersecurity experiences on their behaviour.
Attitude (ATT)	Represents an individual's overall evaluation of performing cybersecurity-compliant behaviour.	Examining the influence of employees' attitudes toward cybersecurity-compliant behaviour.
Subjective Norm (SN)	Reflects the perceived social pressure or approval/disapproval from significant others regarding cybersecurity-compliant behaviour.	Assessing the impact of subjective norms on employees' cybersecurity compliance.
Perceived Behavioral Control (PBC)	This measures the perceived ease or difficulty in performing cybersecurity-compliant behaviour.	Examining the influence of perceived behavioural control on employees' ability to comply with cybersecurity practices.
Threat Appraisal (TA)	This assesses an individual's perception of the severity and vulnerability of the threat, which, in this case, refers to cybersecurity threats.	Evaluating how employees perceive the severity and vulnerability of cybersecurity threats in the context of their compliance behaviour.
Response Efficacy (CRE)	Reflects an individual's confidence in the effectiveness of recommended measures against cybersecurity risks.	Assessing the effectiveness of recommended cybersecurity measures perceived by employees.
Self-Efficacy	Denotes an individual's belief in their	Evaluating employees'

Construct	Meaning	Usage
(CSE)	capacity to perform recommended cybersecurity actions successfully.	confidence in their ability to perform recommended cybersecurity actions.
Cybersecurity-Compliant Behaviour (CCB)	Depicts an individual's adherence to advised cybersecurity practices.	Measuring the level of compliance with recommended cybersecurity practices among individuals.

3.2 CYBERSECURITY AWARENESS

Despite significant investments in technological solutions, the human factor remains crucial in mitigating cyber threats (McCormac et al., 2017). Studies highlight the critical role of cybersecurity awareness in strengthening an organisation's digital security posture (Kruger & Kearney, 2006; Safa et al., 2015). In HEIs, cybersecurity awareness extends beyond mere knowledge to encompass threat understanding, their potential impacts, and the specific context of the institution (Öłütçü et al., 2016). This heightened awareness fosters positive attitudes towards secure behaviours, ultimately leading to Cybersecurity-compliant behaviour (CCB) (Herath & Rao, 2009a).

The TPB provides a valuable framework for understanding this relationship (Ajzen, 1985). It posits that attitudes, subjective norms and perceived behavioural control are key determinants of intention to perform a specific behaviour. In HEIs, cybersecurity awareness is crucial in shaping attitudes and PBC. Organisations leverage cybersecurity awareness programs, security policies and prior experiences to influence employees' understanding of threats, their role in cybersecurity and their confidence in performing secure actions (Bada et al., 2019; Burns et al., 2018). This, in turn, leads to positive attitudes, subjective norms and perceived behaviour towards CCB.

Effective awareness programs are dynamic, contextually relevant, and aligned with organisational culture to minimise breaches and ensure employee engagement (Li et al., 2019; Safa et al., 2015). Such programs and insights into potential attack methods significantly impact employees' attitudes and behaviours (Allam et al., 2014; Safa & Von Solms, 2016). Furthermore, prior experience, knowledge sharing, training interventions, and collaborative

efforts can further influence positive behaviour (Abawajy, 2014; Feledi et al., 2013; Tamjidyamcholo et al., 2014).

Several studies support the positive impact of cybersecurity awareness on shaping secure attitudes and behaviours (e.g., Venkatesh et al., 2003; Herath & Rao, 2009a; Bulgurcu et al., 2010; Bada et al., 2019; Heidt et al., 2019; Wong et al., 2022). This reinforces the strong connection between awareness and both attitudes. Thus, it is hypothesised that:

H1: Cybersecurity awareness positively impacts employees' attitudes that lead to CCB.

3.3 ORGANISATION'S CYBERSECURITY POLICY

Institutions advocate policies such as acceptable behaviour, social media, ethical email and computer use to establish compliant behaviour among employees (Ifiendo, 2012). These policies are pivotal in mitigating threats and strengthening institutions' cybersecurity structure. Herath and Rao's (2009) research reveals that factors such as social norms, potential penalties and peer behaviours significantly influence employees' adherence to these policies. Furthermore, when an organisation's culture aligns with its cybersecurity policies, it reinforces compliance (Jaeger, 2018). Organisations allocate substantial resources to cybersecurity technology tools in the current digital landscape. However, these tools are futile once users do not utilise security measures properly or neglect basic security policies (Martens et al., 2019). Also, abundant studies have shown that relying solely on technological solutions is insufficient to address the complexity of cybersecurity (Whitman & Mattord, 2018; Ponemon Institute, 2018; Safa et al., 2015; Chu & Chau, 2014; Herath & Rao, 2009).

Despite this understanding, organisations often prioritise technical security controls over addressing the human factor (Evans et al., 2019). For instance, Bojjagani and Sastry (2017) proposed cryptography as a technological solution to enhance data security and integrity. However, concerns persist regarding how technology users apply cryptographic techniques, necessitating further scholarly investigation (Eastin et al., 2016). Hence, Safa and Maple (2016) outline human behavioural approaches that mitigate cybersecurity concerns, including conscious care behaviour and clear, comprehensible policies and procedures (Evans et al., 2019). Therefore, technology users must acquire cybersecurity awareness concerning technology usage while adhering to policies guided by subjective norms and CCB.

Within the organisational context, non-compliance refers to actions that disregard established cybersecurity policies, often resulting in adverse consequences for employees and organisations. Cybersecurity behavioural studies conducted by Cheng et al. (2013) and Williams et al. (2019) have concentrated on employees exhibiting non-compliance and the underlying intentions driving such behaviour. This emphasis on non-compliance highlights the importance of investigating compliance, given the prevalence of explicit security policies in many organisations (Li et al., 2019). Adherence to these policies serves as a safeguard against insecure behaviours.

The evolving challenge posed by users' behaviour is serious within organisations, including HEIs, underscoring the significance of cybersecurity policies and procedures on cybersecurity behaviour (Safa et al., 2016; Crossler et al., 2013). Implementing awareness programs and rigorously enforcing security policies is an effective strategy to mitigate cybersecurity breaches (Herath & Rao, 2009). The interplay of intrinsic and extrinsic motivations significantly shapes employee compliance, with social norms, peer influence and penalties resonating within cybersecurity behaviour (Herath & Rao, 2009).

D'Arcy's (2014) empirical findings show that cybersecurity culture can influence employees' compliance with security policies in an organisation. Organisations must enhance employees' awareness in alignment with security policies to foster a security policy compliance culture. Organisational culture is crucial in promoting cybersecurity, with employees consistently exhibiting compliant behaviour when their self-efficacy beliefs align with policies (Jaeger, 2018; Stanton et al., 2005). Clear and well-communicated policies and procedures are essential to forming the basis for positive employee behaviour (Jaeger, 2018). An individual's adherence to security policies significantly influences subjective norms towards CCB (Hina, 2019). Consequently, this study proposes the following hypothesis:

H2: Organisational policies positively affect subjective norms towards performing CCB.

3.4 CYBERSECURITY EXPERIENCE

Several models propose that previous cybersecurity experience significantly influences users' decision-making in cybersecurity (Li et al., 2019; Safa et al., 2015). Recent research has revealed a positive correlation between cybersecurity experience and users' attitudes toward

compliance with cybersecurity policies (Ifinedo, 2014; Bulgurcu et al., 2010). Furthermore, the value of a prior experience lies in users' anticipation that lessons learned from cybersecurity incidents and training will cultivate a culture of compliance (Ahmad et al., 2015). However, it is noteworthy that Ahmad's case study represents a small subset of research focused on integrating employees' cybersecurity experience into the PMT domain, as most studies within the PMT domain primarily explore the causal relationship between threat and coping appraisal on intended behaviour (Anderson & Agarwal, 2010; Herath & Rao, 2009b; Johnston & Warkentin, 2010; Siponen et al., 2014).

The interplay of users' cybersecurity experience profoundly influences their beliefs regarding the feasibility of executing security-related behaviours. Users with substantial cybersecurity experience inherently comprehend risks and threats better than their less-experienced counterparts. Armed with the skills and knowledge to adhere to security policies and protocols, experienced users tend to exhibit stronger self-efficacy beliefs, leading to increased CCB (Hosseini et al., 2017). Likewise, users deeply involved in cybersecurity are more likely to recognise the criticality of security and possess a heightened motivation to protect their organisation's data and information assets (Siponen et al., 2007). This experience often translates to enhanced self-efficacy beliefs in executing cybersecurity-related behaviours, consequently contributing to increased CCB. Therefore, this study hypothesises that:

H3: Employees' experience positively affects perceived behavioural control towards performing CCB.

3.5 TPB'S ATTITUDE, SUBJECTIVE NORMS AND BEHAVIOURAL CONTROL

According to TPB, an individual's intention to engage in a specific behaviour is influenced by attitudes, subjective norms and perceived behavioural control (Ajzen, 1991). In complying with organisational cybersecurity measures, including policies, these determinants affect an individual's intention to comply (Siponen et al., 2007; Ajzen, 1991; Albrechtsen, 2007). Cybersecurity Attitudes refer to an individual's positive or negative evaluation of cybersecurity-related behaviour and reflect how people perceive and feel about complying with policies. The TPB is a successful model of the attitude-behaviour relationship, given its apparent ability to predict and explain human behaviour. Research by Ifinedo (2014) shows that individuals with a positive attitude toward cybersecurity are more inclined to comply with policies. Conversely,

those with a negative attitude are less likely to adhere to them. This highlights the need for organisations to foster environments that support positive attitudes toward CCB.

Subjective norms or normative beliefs influence an employee's behavioural intentions and actions (Bulgurcu et al., 2010). Furthermore, influence from management, supervisors and colleagues significantly impacts employees' cybersecurity behaviour (Cheng et al., 2013), suggesting that others influence individuals in their decision-making processes. Subjective norms encompass the perceived social pressure individuals experience regarding their engagement in certain behaviours. These norms pertain to how individuals perceive their peers' and supervisors' expectations and opinions regarding compliance with security policies. Abundant studies have shown that subjective norm is a significant direct predictor of behaviour (Anderson & Agarwal, 2010; Herath & Rao, 2009). Also, research like Cheng et al. (2013) shows that individuals who sense pressure from their peers and supervisors to adhere to these policies are more likely to do so. Thus, organisations can encourage CCB by fostering a positive environment and culture that supports subjective norms.

Perceived behavioural control refers to an individual's belief about how easy or difficult it is to perform a behaviour. In cybersecurity, perceived behavioural control refers to how people feel about their ability to comply with cybersecurity policies. Individuals who believe it is easy to comply with policies are likelier to do so (Albrechtsen, 2007). It is worth noting that perceived behavioural control and self-efficacy represent similar concepts when observing an individual's perceived ease or difficulty in performing a specific behavioural action.

Several studies have conclusively shown that attitudes, subjective norms and perceived behavioural controls influence individuals' behaviour (Bauer & Bernroider, 2017). For instance, Martens et al. (2019) found that subjective normative is an important predictor of an individual's intentions to protect against cybercrimes, which informs CCB. Additionally, the integration of TPB with other theories has significantly impacted compliance with cybersecurity policies (Aurigemma & Panko, 2012; Bulgurcu et al., 2010; Ifinedo, 2014; Safa et al., 2015; Siponen et al., 2014). Consistent with Herath and Rao (2009) and Anderson and Agarwal (2010), this study conceptualises that attitudes, subjective norms and perceived behavioural control positively impact employees' CCB. Thus, this study proposes that:

H4: Attitude towards cybersecurity has a positive impact on performing CCB.

H5: Subjective norms have a positive impact on performing CCB.

H6: Perceived behavioural control has a positive impact on performing CCB.

3.6 PMT'S THREAT PERCEPTION

The organisational environment influences employees' CCB, security management efforts and employees' cybersecurity experience (Ahmad et al., 2015). Aligning the organisational environment with cybersecurity awareness helps employees identify security threats and understand their severity (Moon et al., 2018). PMT offers a comprehensive framework for explaining how employees' prior computer security experience influences their perception of threat severity and vulnerability, shaping their CCB. Thus, this section explores the impact of PMT on employees' CCB, emphasising that individuals' perception of threat severity and vulnerability, combined with belief in their ability to execute recommended responses (response efficacy) and their capacity to implement these responses (self-efficacy), motivates them to protect themselves (Rogers, 1975). In this context, employees adopt CCB.

PMT outlines two key motivational routes that drive individuals to adopt cybersecurity-protective and compliant behaviours: threat appraisal and coping appraisal (Hina et al., 2019; Li et al., 2019; Safa et al., 2015; Boss et al., 2015; Topa & Karyda, 2015). Threat appraisal involves how employees assess the seriousness of threats (perceived severity) and susceptibility to these threats (perceived vulnerability). It evaluates how severe a cybersecurity incident could be regarding damage resulting from non-compliance with cybersecurity policy (Siponen et al., 2014). Furthermore, it assesses how likely employees may fall victim to a cyber threat if they fail to adhere to the organisation's cybersecurity policy and embrace CCB (Topa & Karyda, 2015).

To illustrate PMT in the context of cybersecurity, the researcher references the malware example presented by Tsai et al. (2016). When computer users encounter malware threats, threat appraisal involves assessing how likely their computer will be infected by the malware (perceived vulnerability). If they perceive a high likelihood of infection, they evaluate whether the consequences of malware infection are as severe as resulting in a system failure (perceived severity). Then, coping appraisal comes into play to assess the effectiveness of their computer antivirus software (response efficacy) and whether they possess the knowledge to take appropriate measures to install and manage the software for dealing with malware

(self-efficacy). The combination of threat and coping appraisals predicts whether the computer user will use antivirus software for protection.

In this study, threat perception is pivotal in encouraging employees to engage in cybersecurity training and adopt appropriate cybersecurity-compliant practices (Herath & Rao, 2009a). Prior research suggests that employees who understand the significant damage that may result from cybersecurity threats are more likely to participate in cybersecurity training programs and actively adopt protective and compliant behaviours (Ahmad et al., 2015). Additionally, perceived vulnerability to cyber-attacks has been found to influence employees' willingness to prevent new incidents (Ng et al., 2009). Thus, the study proposes the following hypothesis:

H7: Threat appraisal positively impacts employees' CCB.

3.7 PMT'S COPING APPRAISAL

The PMT posits that the coping appraisal process is triggered in response to the perception of a cyber threat, following the earlier threat appraisal process, to determine an appropriate coping response (Boss et al., 2015). Coping appraisal involves individuals' decisions on effectively handling a cyber threat, where adherence to an organisation's cybersecurity policy may vary among employees (Boss et al., 2015).

PMT operationalises coping appraisal through three key elements: response efficacy, self-efficacy, and response cost (Floyd et al., 2000; Mousavi et al., 2020; Vrhovec & Mihelič, 2021). Hypotheses suggest that response efficacy and self-efficacy positively influence the attitude toward CCB, whereas response cost is modelled to influence the attitude toward behaviour negatively (Martens et al., 2019). Some prior research suggests that response cost is often a barrier and is generally an insignificant predictor of CCB (Blythe & Coventry, 2018; Menard et al., 2017). Also, Sommestad et al. (2015) suggest that high response costs could indicate low self-efficacy, thereby representing inverse concepts. More recent studies, like Martens et al.'s (2019), did not operationalise response cost due to its difficulty and ambiguity, leading to its exclusion from the current study.

The recent adoption of PMT indicates that self-efficacy and response efficacy significantly correlate with individuals' behavioural intentions to comply with cybersecurity (Miraja et al.,

2019). Additionally, several studies highlight a positive relationship between response efficacy and protective behaviour, indicating that individuals who strongly believe in the effectiveness of a protective measure are motivated to adopt corresponding behaviours (Martens et al., 2019; Tsai et al., 2016). Likewise, self-efficacy significantly influences protective behaviour, with individuals confident in their ability to execute certain behaviours and being more motivated to undertake protective measures (Martens et al., 2019; Dang-Pham & Pittayachawan, 2015).

In the organisations' cybersecurity context, research indicates that both response efficacy and self-efficacy are pivotal in fostering CCB (Mou et al., 2022; Tsai et al., 2016; Siponen et al., 2007), underscoring their importance in influencing individuals' intentions and actions related to cybersecurity compliance. In this study, response efficacy reflects employees' confidence that adhering to institutionally recommended cybersecurity policies and procedures will effectively mitigate a cyber threat. Simultaneously, self-efficacy relates to employees' belief in their ability to execute cybersecurity procedures (Boss et al., 2015).

The recent integration of PMT and TPB suggests that employees who believe in the effectiveness of their actions (i.e., response efficacy) are more likely to exhibit CCB (Boobalan & Nachimuthu, 2020; Grimes & Marquardson, 2019; Herath & Rao, 2009; Masser et al., 2020; Pang et al., 2021; Youn et al., 2021; Zhang et al., 2019). Conversely, employees who believe in their capacity to perform a specific behaviour (self-efficacy) are also more likely to exhibit positive behaviour or CCB (Herath & Rao, 2009). Existing literature suggests that response efficacy and self-efficacy can significantly impact CCB (Pang et al., 2021; Zhang et al., 2019; Herath & Rao, 2009). Therefore, it is proposed that:

H8a: Cybersecurity response efficacy has a positive impact on CCB.
H8b: Cybersecurity self-efficacy has a positive impact on CCB.

Table 4 summarises the theories and main constructs adopted for this study, along with information such as the theoretical application fields, definition and authors (see Table 4). Figure 3 (Based on Literature) depicts the proposed model investigating the factors influencing employee CCB within SA HEIs' cybersecurity environment. The model integrates the influence of cybersecurity awareness, policy and experience on employee attitudes, subjective norms, perceived behavioural control, threat appraisal and self-efficacy, ultimately leading to CCB. Arrows represent the hypothesised relationships between the constructs.

Table 4: ***Theories and Main Constructs***

Theory	Source	Field	Definition	Main Constructs
TPB	Ajzen (1991)	Psychology	Powerful theory explanatory theory for predicting behavioural intention, such as employees' CCB	Attitudes; Subjective Norms; Perceived Behavioural Control.
PMT	Rogers (1975). Maddux & Rogers(1983)	Psychology	Highly effective theory for predicting intention to engage in protective actions such as employees' CCB. It explains behaviours elicited as a response to fear appeal.	Threat Appraisal; Response Efficacy; Self-Efficacy.

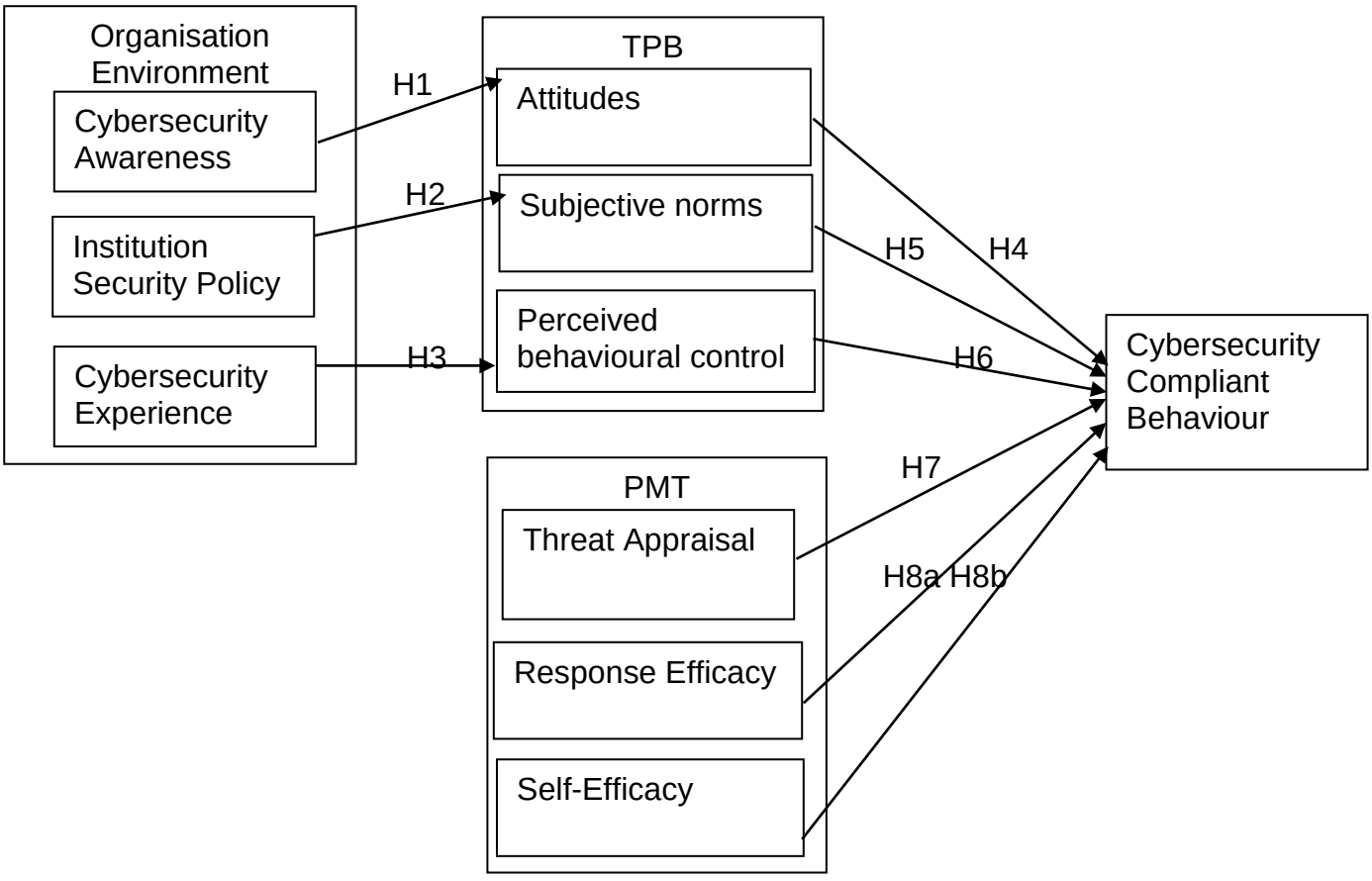

Figure 3: Conceptual Model

3.8 CYBERSECURITY POLICY AWARENESS AND COMPLIANCE

Human error is a major contributor to organisational cybersecurity failures and is often considered a leading cause of successful cyberattacks (Connolly et al., 2019). Studies reveal that less than 1% of such attacks exploit system vulnerabilities (ProofPoint, 2019; IBM, 2019). To combat this evolving threat, cybersecurity professionals and researchers continuously identify factors that mitigate cyber risks in organisations like Higher Education Institutions (HEIs) (Connolly et al., 2019; Crossler et al., 2019). While technology-based countermeasures offer risk reduction (Connolly et al., 2019), research highlights the need for human-centric approaches, as technology alone is insufficient (Connolly et al., 2019; Li et al., 2019; Rocha Flores & Ekstedt, 2016; Safa et al., 2015).

This emphasis on human factors and organisational disruptions has prompted institutions to re-evaluate their cybersecurity policies to guide employees and stay ahead of evolving threats (Li et al., 2019). However, evidence suggests that employees do not always comply with policies designed to protect institutional digital assets and prevent information system misuse, abuse, and destruction (Li et al., 2019; Ifinedo, 2014). Therefore, this study expands its investigation of employee cybersecurity behaviour to examine its correlation with their awareness of the institution's cybersecurity policy. Building upon prior research by Li et al. (2019) and Ifinedo (2012), this study identifies three categories of employee attitudes towards institutional cybersecurity policies:

(1) Aware: Those who are aware of the institution's cybersecurity policies.

(2) No Policy: Those whose institutions lack a cybersecurity policy.

(3) Unaware: Those who are unaware of their institution's cybersecurity policy.

Based on these categories, the study proposes the following hypothesis:

H9: Cybersecurity policy awareness will positively impact employees' cybersecurity-compliant behaviour.

Based on the Literature, Table 5 presents the hypotheses (H1-H9) derived from the literature review. Each hypothesis outlines the predicted relationship between the independent and dependent variables within the model described in Figure 3. These hypotheses will be tested using data collected from employees within SA HEIs. Further, hypothesis (9), illustrated in Figure 4, will be tested on a large data sample of employees within SA HEIs using Analysis of variance (ANOVA) and post hoc procedure (see Figure 4).

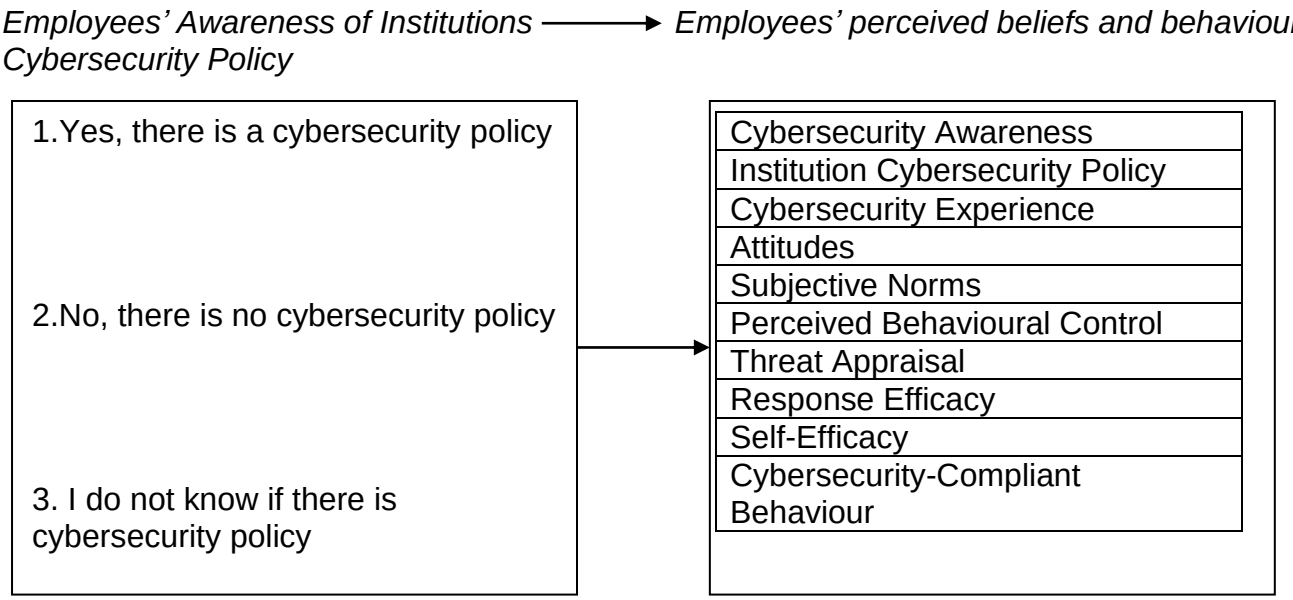

Figure 4: Cybersecurity Policy Awareness Model

3.8.1 Description of Research Hypothesis Table

Drawing from the established theoretical foundation from Section 2.9 (refer to the conceptual model and hypotheses), this research proposes a conceptual model to understand employee CCB within the specific context of SA HEIs. This model goes beyond existing research by integrating the institutional cybersecurity environment with PMT and TPB in a SA HEI context. The model proposed focuses on understanding the factors that influence employees' cybersecurity behaviours within SA HEIs. By testing the following hypotheses (H1-H9), this study aims to validate the model and provide valuable insights into these influencing factors. Following Mark et al.'s (2023) recommendations, these hypotheses will be tested using data collected from employees within SA HEIs, and the results will be presented and discussed in detail in Chapter 5 (See Table 5 for detailed hypotheses).

Table 5: ***Proposed Hypotheses for the Conceptual Model***

No	Hypothesis
H1	Cybersecurity awareness positively impacts employees' attitudes, which leads to CCB**.**
H2	Organisational policies positively affect subjective norms towards performing CCB.
H3	Employees' experience positively affects perceived behavioural control towards performing CCB.
H4	Attitude towards cybersecurity has a positive impact on performing CCB.
H5	Subjective norms have a positive impact on performing CCB.
H6	Perceived behavioural control has a positive impact on performing CCB.
H7	Threat appraisal positively impacts employees' CCB.
H8a	Cybersecurity response efficacy has a positive impact on CCB.
H8b	Cybersecurity self-efficacy has a positive impact on CCB.
H9	Cybersecurity policy awareness will positively impact employees' CCB.

3.8.2 Research Instrument: Survey Questionnaire

The study employed a survey questionnaire as the primary tool for data collection. This questionnaire was adapted from the published literature (i.e., Safa et al., 2015; Li et al., 2019) and modified to address employee cybersecurity behaviours context within SA HEIs specifically. The questionnaire comprised various sections, each focusing on a specific construct within the conceptual model. Participants were asked to respond to a series of statements using a Likert scale, typically ranging from "Strongly Disagree" to "Strongly Agree". This approach allowed researchers to gauge participants' perceptions and attitudes towards various aspects of cybersecurity. Table 6 provides a detailed breakdown of the questionnaire, outlining the constructs measured and the corresponding sample items used.

Table 6: ***Research Survey Questionnaire adapted (e.g., Safa et al., 2015)***

Construct	Items
Cybersecurity Awareness (CA)	**CA1**: I know the potential cybersecurity threats that could impact my work. **CA2**: I possess sufficient knowledge about the cost of cybersecurity breaches to my institution. **CA3**: I understand the risk of cybersecurity incidents to my institution. **CA4**: I keep myself informed and updated on cybersecurity threats and cybersecurity awareness best practices. **CA5**: I share cybersecurity knowledge with colleagues to increase awareness.
Institution Cybersecurity Policy (ICP)	**ICP1**: Cybersecurity policies and procedures are significant in my institution/organisation. **ICP2**: Cybersecurity policies and procedures impact my behaviour. **ICP3**: Cybersecurity policies and procedures have attracted my attention. **ICP4**: Behaviour in line with institutional cybersecurity policies and procedures is of value in my institution/organisation.
Cybersecurity Experience (CEI)	**CEI1**: My cybersecurity experience improves my ability to have safe behaviour in terms of cybersecurity. **CEI2**: I am involved with cybersecurity and care about my behaviour at work. **CEI3**: My cybersecurity experience helps to organise and assess Cybersecurity threats. **CEI4**: I can sense the cybersecurity threat level due to my experience in this domain. **CEI5**: I perform cybersecurity-compliant behaviour due to my experience. **CEI6**: I possess the suitable capability to manage

	cybersecurity risk due to my experience.
Attitude (ATT)	**ATT1**: Cybersecurity-compliance behaviour is essential. **ATT2**: Cybersecurity-conscious care behaviour is usually beneficial. **ATT3**: Practicing cybersecurity compliance behaviour is usually helpful. **ATT4**: I have positive views about changing users' Cybersecurity behaviour to conscious care. **ATT5**: My attitudes toward cybersecurity compliance behaviour are positive.
Subjective Norms (SN)	**SN1**: Cybersecurity policies in my institution/organisation are significant for my coworkers. **SN2**: My coworkers' cybersecurity behaviour influences my behaviour. **SN3**: My institution's/organisation's cybersecurity culture influences my behaviour. **SN4**: My supervisor's Cybersecurity behaviour influences my behaviour.
Perceived Behavioural Control (PBC)	**PBC1**: I believe that cybersecurity compliance behaviour is a relatively straightforward practice. **PBC2**: My experiences help me have careful behaviour in cybersecurity. **PBC3**: For me, following cybersecurity policies and procedures is easy. **PBC4**: Cybersecurity-compliance behaviour is an accessible and achievable practice.
Threat Appraisal (TA)	**TA1**: To reduce the risk, I must avoid opening unexpected and out-of-context emails. **TA2**: I could fall victim to different attacks if I do not follow cybersecurity policies. **TA3**: My data's cybersecurity will be ineffective if I do not comply with cybersecurity policies.

	TA4: Hackers (Cybercriminals) attack with different methods, and I should be careful in this dynamic environment.
Cybersecurity Response Efficacy (CRE)	**CRE1**: Complying with the information security policies in my organisation will keep security breaches down. **CRE2**: If I comply with information security policies, the chance of information security breaches occurring will be reduced. **CRE3**: Careful compliance with information security policies helps to avoid security problems.
Cybersecurity Self-efficacy (CSE)	**CSE1**: I possess the necessary skills to protect my institution and private data. **CSE2**: I possess the expertise to protect my institution and private data. **CSE3**: I think the protection of my data is in my control in terms of cybersecurity violations. **CSE4**: I can prevent cybersecurity violations.
Cybersecurity Compliance Behaviour (CCB)	**CCB1**: I follow the recommendations of security experts in my cybersecurity manner. **CCB2**: I consider its consequences before taking any action affecting cybersecurity. **CCB3**: I talk with cybersecurity experts before doing anything related to cybersecurity. **CCB4**: I consider my previous cybersecurity experience to avoid repeating similar or prior mistakes.

3.9 CONCLUSION

Building upon the identified literature gaps, this study proposes a conceptual model for investigating the factors influencing employees' CCB in HEIs. The model integrates TPB and PMT to understand employee motivations, attitudes, and perceived control over cybersecurity practices. The proposed conceptual model and hypotheses provide a framework for investigating the relationship between various factors and CCB in HEIs. This framework guides the development of the following research hypotheses presented in the chapter. This study

aims to contribute valuable insights to cybersecurity awareness in HEIs by investigating these hypotheses. The findings will inform effective strategies for promoting employee cybersecurity compliance behaviour and ultimately strengthen these institutions' overall security posture.

4 RESEARCH DESIGN AND METHODOLOGY

4.1 INTRODUCTION

The previous chapter explored the existing literature and theories that underpin cybersecurity research within the information systems domain. This chapter introduces the research methodology that guides this study and the selected research design, serving as the roadmap to achieving the research goals and answering the research questions. Research methodology encompasses the techniques and procedures used to gather, process, and analyse data related to a specific research question or hypothesis (Crotty, 1998). This aligns with Ngulube's (2021) and PEDIAA's (2017) assertions, emphasising the comprehensive nature of research methodology, which involves procedures, processes, data collection, and analysis tools. Also, research design, as explained by Tobi et al. (2017), describes the overarching structure of an academic research project, providing a framework to achieve the research objectives.

This study focuses on cybersecurity awareness and behaviour within South African (SA) Higher Education Institutions (HEIs) to identify factors influencing Cybersecurity-Compliance Behaviour (CCB). The research methodology drew upon Saunders et al.'s (2023) research onion framework to provide a structured approach to research design. Specifically, this study employed a causal-comparative research design (Babbie, 2010; Creswell, 2015). This design is well-suited for exploring the effects of independent variables, such as educational background, on a dependent variable, like cybersecurity compliance behaviour, through comparisons of multiple groups within SA HEIs. For instance, we will utilise this causal-comparative design to examine how factors like educational background and other variables influence employee cybersecurity compliance behaviour within SA HEIs. By comparing employee groups with different educational backgrounds, we can gain a deeper understanding of the potential influence of this factor on cybersecurity compliance behaviour.

4.2 SAUNDERS' RESEARCH ONION

Saunders et al. (2023) developed the research onion framework, a valuable tool for researchers to visualise and systematically approach the different aspects of research methodology. As illustrated in the onion diagram (see Figure 5), the research onion comprises six layers, each building upon the previous one. These layers guide researchers through key

decisions they must make when designing their research strategy (Saunders et al., 2023), as outlined below.

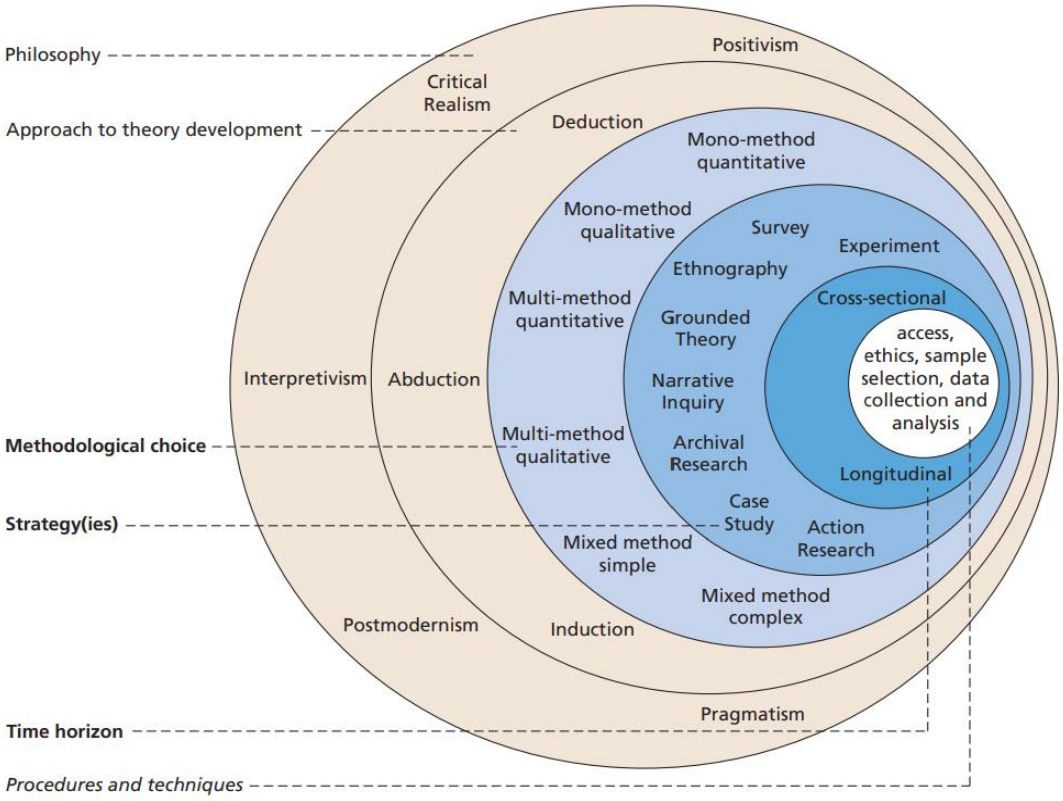

Figure 5: Saunders Research Onion Model. Source: Saunders et al. (2023, p. 177).

Therefore, this research methodology drew upon Saunders et al.'s (2023) research onion framework to provide a structured approach to research design. This chapter is organised following the research onion layers:

- **Research Philosophy (Section 4.3):** This section will explicitly state the study's philosophical underpinnings (e.g., positivism).
- **Research Approach (Section 4.4):** This section will outline the broad research strategy, such as quantitative or qualitative.
- **Research Strategy (Section 4.5):** This section explores the data collection methods chosen (i.e., surveys).
- **Research Choices (Section 4.6):** This section will focus on the practical decisions within the chosen research strategy, such as sampling techniques and data analysis methods.

- **Time Horizon (Section 4.7):** This section will consider the timeframe for conducting the research.
- **Data Collection Methods (Section 4.8):** This section details the techniques and procedures used to gather data (e.g., survey instruments).

In addition to the above structure, the following sections elaborate on data analysis procedures (Section 4.9), ethical considerations (Section 4.10) and the chapter conclusion (Section 4.11).

4.3 RESEARCH PHILOSOPHY

Every research project is grounded in a specific set of philosophical assumptions guiding the knowledge acquisition approach. These assumptions encompass ontological, epistemological, and methodological viewpoints, each playing a distinct role in shaping the research process and its outcomes (Saunders et al., 2019). They guide our perspectives on various aspects of the world (Danermark et al., 2002). These foundational philosophies translate into interpretive frameworks such as positivism, constructivism, pragmatism and transformative research.

This section explores the research philosophy that underpins this study, focusing on positivism (Holden & Lynch, 2006). *Positivism* is a philosophical stance that emphasises knowledge acquisition through objective observation and measurement (Bryman, 2021). This aligns well with research that employs scales to measure technology and attitudes (Rosen et al., 2013). Furthermore, the positivist paradigm suits the study's objectives, which are to investigate the factors influencing employees' cybersecurity awareness and behaviour in SA HEIs and to identify effective strategies for improving cybersecurity measures (Hair et al., 2016).

Positivism posits that reality exists independently of human observation and is subject to examination through scientific methods (Saunders et al., 2023; Bryman, 2021). Herein, the research delved into the objective reality of cybersecurity awareness and behaviour among employees in SA HEIs. The study systematically and objectively explored this reality using survey questionnaires to gather quantitative data on employee CCB and its influencing factors. By adopting the positivist paradigm, the study validated its commitment to aligning with its objectives and adhering to scientific methods. This approach provides a robust framework for investigating the multifaceted cybersecurity realms in SA HEIs.

The selection of positivism as the research philosophy establishes a foundation for employing a quantitative approach and survey methods in subsequent sections. This aligns with the research goals of uncovering the factors influencing cybersecurity compliance behaviour and proposing strategies for improvement.

4.4 RESEARCH APPROACH

This study employed a quantitative approach aligned with a positivist paradigm because it emphasises robust empirical evidence for testing and explaining relationships between variables (Saunders et al., 2019). This relationship is more robust when used amid predetermined, highly structured data collection methods (Mark et al., 2023). This aligns with similar studies such as Le Grange (2018), which advocate for evidence-confirmatory research.

Numerical data and statistical analysis are central to quantitative methods, enabling the investigation of connections between the research variables outlined in the conceptual model (see Figure 3) (Saunders et al., 2019). Additionally, quantitative research typically uses an approach that collects and analyses data to test existing theories, such as the TPB and PMT employed for this study.

Therefore, this study implemented quantitative analysis through survey questionnaires to assess the targeted relationships and test theories (e.g., TPB and PMT) against data collected from SA HEI employees. This approach provided insights into the research phenomena. Furthermore, probability sampling techniques ensured the unbiased generalisability of the findings (Saunders et al., 2019).

This section explains the chosen approach (quantitative) and how it aligns with the research philosophy (positivism) discussed earlier. It highlighted the importance of robust evidence, predetermined data collection methods, numerical data, and statistical analysis, which are all hallmarks of quantitative research.

4.5 RESEARCH STRATEGY

This section outlined the study’s research strategy, a set of procedures that guides a researcher’s thoughts and efforts (Saunders et al., 2019). This systematic approach to

conducting research yields high-quality results and enables comprehensive reporting. Research strategies represent a logical thinking approach involving drawing conclusions from specific incidents or observations (Creswell & Creswell, 2017) and guiding data collection methods to achieve research objectives (Mark et al., 2023). Considering this study's research questions and goals, a survey strategy was chosen as the primary method for data collection (Hair et al., 2017b). Surveys are a popular method in social science research for gathering quantitative data from large samples and enabling statistical analysis (Bryman & Bell, 2015; Mccusker & Gunaydin, 2015).

This study utilised an online questionnaire, known for its efficiency and accuracy in collecting data from geographically dispersed populations (Fowler, 2014; Sepehr et al., 2014). Online questionnaires minimise researcher influence during data collection and promote objectivity (Saunders et al., 2019). Survey research involves administering standardised questionnaires or interviews to a sample group (Bryman & Bell, 2015). This approach is particularly suitable for this study as it allows for the collection of quantitative data on employee cybersecurity awareness, behaviours, and the factors influencing them (Hair et al., 2017b).

As a result, the researcher selected and used a survey strategy for the study's data collection to achieve the research goals (Hair et al., 2017b). This choice aligns with the confirmatory research approach (Saunders & Lewis, 2012) and is consistent with positivists' preference for large-scale sample surveys (Saunders et al., 2019; Bhattacherjee, 2017). The survey employed an online questionnaire, considered the most accurate and efficient method for gathering data from a broad, geographically diverse sample (Fowler, 2014; Sepehr et al., 2014). This approach ensures objectivity by minimising the researcher's influence during data collection (Mark et al., 2023). Survey research involves collecting data from a sample of individuals using standardised questionnaires or interviews (Bryman & Bell, 2015). This approach is well-suited to this study as it supports collecting quantitative data on employees' cybersecurity awareness and behaviour and the influencing factors (Hair et al., 2017b).

4.6 RESEARCH CHOICES

Having established a structured research approach and outlined the research questions and objectives, this chapter delved into the specific choices to gather and analyse data. These

choices, including the research instrument, measurement tool, and sampling strategy, directly influence the data quality and generalisability of the research findings.

This research employed a structured approach to gather and analyse data to achieve the research objectives (Goddard & Mellvile, 2004), which involved clearly defined research questions, a specific data collection method, and a systematic analysis process. The chosen research design ensures the objectivity and reliability of the findings. The research objectives outline the specific goals this study aims to achieve. These objectives are formulated based on the identified research problem and relevant literature review findings. They provide a clear direction for the research and guide the data collection and analysis processes. The research employed a specific data collection method to gather the necessary information. This method was carefully selected based on the research objectives and the nature of the data required. The chosen method ensures the validity and reliability of the collected data.

The research used systematic data analysis to interpret and make sense of the collected data. This process involves employing appropriate statistical techniques or quantitative analysis methods, depending on the type of collected data. The chosen analysis approach ensured the objectivity of the research findings, which eventually validated or revised the theories, as the steps involved in the research are illustrated in (Figure 5).

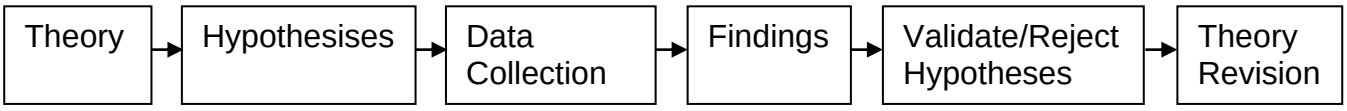

Figure 6: Research Steps (Tracy, 2019; Bhattacherjee, 2017)

Therefore, herein, the researcher starts with the general theory suggesting a relationship between cybersecurity awareness and behaviour, then develops hypotheses (See Table 5) that test these relationships. The hypotheses are then tested using data collected from the study. For example, the following hypothesis was developed: Employees with higher cybersecurity awareness are more likely to engage in cybersecurity-compliant behaviours. This approach requires formulating research theories and hypotheses to test and analyse the collected data (Saunders et al., 2019) and consists of five stages:

Stage 1: Identifying theories and Formulating the research question or hypothesis

- Integrate the organisation’s cybersecurity environment with TPB and PMT to formulate a framework for investigating employees' cybersecurity behaviour. This framework

provides a model of the factors influencing cybersecurity awareness and behaviour among employees in SA HEIs. The researcher can use this framework to formulate a research question or hypothesis about the factors influencing cybersecurity behaviour.

Stage 2: Reviewing the literature

- Adopting hypotheses from cybersecurity and general IS literature. The researcher reviewed cybersecurity literature to identify previously proposed hypotheses used to develop the research hypotheses.

Stage 3: Developing the research design

- The researcher developed a research design to collect data for hypothesis testing. The researcher used a survey instrument to collect data from employees in SA HEIs. The data was then analysed using statistical methods to test the hypotheses.

Stage 4: Collecting the data

- The researcher collected and analysed research data to test the hypotheses. The results of the data analysis determine whether the hypotheses are supported or refuted.

Stage 5: Analysing the data

- Validating or refuting the hypotheses. The results of the data analysis determine whether the hypotheses are supported or refuted.

Consequently, this research employed the five-stage process commonly found in quantitative research (Saunders et al., 2019; Hatch, 2012), which is iterative as the researcher may revisit stages as needed (Bhattacherjee, 2012). For example, the research questions might be refined based on the insights from the literature review or data collection phase.

4.7 TIME HORIZON

This study employed a cross-sectional design, collecting data from SA HEI employees between December 2023 and February 2024 to investigate factors influencing their cybersecurity awareness and behaviour (Saunders et al., 2019; Bhattacherjee, 2012). This approach aligns well with the survey methodology, capturing a snapshot of employees' current perceptions and cybersecurity practices during the study.

Rationale for Data Collection Period: Data collection occurred between December 2023 and February 2024 to minimise potential seasonal variations in employee workload or computer system usage patterns that might influence responses.

Limitations of the Time Frame: A cross-sectional design offers a valuable starting point but cannot capture changes in perceptions or behaviour over time. Future research might consider a longitudinal design to explore these dynamics.

4.8 DATA COLLECTION

This study used a questionnaire to gather quantitative data on employees' cybersecurity awareness and behaviour and the influencing factors (Aguinis & Vandenberg, 2014). The questionnaire (Table 5) included questions on employees' level of cybersecurity awareness, their perception of cybersecurity risk, their experience with cybersecurity training programs, and their perception of their organisation's cybersecurity culture (Nagle & Pope, 2013). To ensure anonymity and comply with POPIA, the survey excluded all demographic questions except for education level. For simplicity, the survey began with questions on education level and cybersecurity policy awareness (Bhattacherjee, 2012).

4.8.1 Target Audience and POPIA Compliance

In adhering to the POPIA, the researcher ensured the target audience comprised employees directly involved with computer usage. This alignment minimised collecting irrelevant personal information, such as names, ages, or institutional details (Bates & Cozby, 2012). The survey design excluded personal identifiers, and respondents were not asked to provide any information that could reveal their identity.

To achieve this targeted approach, the researcher secured permission from the management of the participating SA HEIs to collaborate with their Human Resource (HR) departments or designated representatives. Institution HR departments and general management typically maintain comprehensive employee lists (Saunders et al., 2019) that include job roles and details on computer usage. By collaborating with these departments, the researcher ensured the survey only reached employees whose positions directly involved IT or computer usage. This aligned with the research objectives and minimised the risk of collecting irrelevant personal information. We did not directly communicate with any potential respondents. Instead, after informing the institutions about the survey requirements and target audience, the survey materials were shared only with HR or designated sections within the institutions for internal distribution to the appropriate employees.

4.8.2 Survey Distribution Process

Following ethical approval from the institution's management board (Appendix A), the researcher collaborated with SA HEIs' management for survey distribution within these institutions. This collaboration focused on utilising management-assigned departments, like HR, to ensure access to the target population and maximise response rates (Sheehan, 2001; Saunders et al., 2019).

1. Identifying Target Participants

The researcher collaborated with the HR departments or management-assigned departments of participating SA HEIs to identify potential participants. These departments maintain comprehensive employee lists, allowing for the selection of a representative sample that aligns with the research objectives. The researcher then established inclusion criteria to focus on employees with direct or indirect involvement in computer usage (Saunders et al., 2019; Sheehan, 2001).

2. Distribution Channels

The researcher distributed Qualtrics survey link through management-assigned departments that identified employees through two primary channels:

- **Email:** An institutionally personalised email invitation was emailed to the HR or management-assigned departments, which redistributed it to potential participants (i.e., employees) through their internal distribution channels. The email explained the study's purpose, ensured anonymity and confidentiality of responses, and included the survey link. This widely used online survey distribution approach leveraged institutional email systems' reach and efficiency (Sheehan, 2001).
- **Mobile Phones (Optional):** Collaborating with the participating HEIs, the researcher coded the link to be accessible from mobile phones and advised the institutions as such. This offers an additional channel for employees who cannot access personal computers to complete the survey (Saunders et al., 2023). It is important to note that this mobile phone option campaign was optional.

3. Communication and Reminders

As Saunders et al. (2019) recommend, the researcher sends reminders to the management-assigned departments of the participating institutions to maintain participant engagement; a

communication plan was implemented throughout the data collection period. This plan included:

- **Initial Welcome Email:** Upon survey launch, an introductory email outlining the study's objectives and the importance of their contribution was sent to all potential participants.
- **Reminder Emails:** Gentle reminder emails were sent at pre-determined intervals to encourage participation from those who may have not responded initially.
- **Survey Completion Thank You:** After the participant completed the survey, an automated thank-you message was sent to express appreciation for their time and contribution.

4. Control Measures

The researcher implemented several control measures to ensure data quality and integrity:

- **Anonymous Survey Link:** An anonymous survey link was generated for each participating HEI, allowing researchers to track participation rates from different institutions.
- **Participant Screening:** The Qualtrics platform was configured to limit participation to one completed survey per individual, preventing duplicate responses.
- **Question Logic:** The survey was designed with logical branching and skip logic, ensuring respondents only answered questions once.

This comprehensive survey preparation and distribution approach ensured that respondents were informed and engaged, leading to smoother and more successful data collection.

4.8.3 Sampling

This study investigated cybersecurity awareness and behaviour among employees in SA HEIs. Employees within these institutions emerged as the default study population, ensuring the findings are generalisable. Quantitative research (Saunders et al., 2019, pp. 296-297) typically uses two primary sampling techniques: probability and non-probability sampling. The former employs randomisation to ensure that all members of a sampling frame have an equal chance of selection. In contrast, the latter selects participants from a quota system. In survey-based studies, probability sampling is cost-effective and precise, producing generalisable results (Neuman, 2011).

This study employed simple random sampling, a probability sampling technique, to target employees from various departments or roles within the HEIs who utilise computers and other digital devices as part of their official responsibilities (Saunders et al., 2019). Given this study's focus on employee cybersecurity behaviour, the survey officially targets employees who use computers and other digital devices. Thus, those without such responsibilities or who decline participation are excluded. This study employed a simple random sampling approach (Hair et al., 2017; Bhattacherjee, 2012), which accords each member of the population with an equal selection chance for the study (Anderson, 2019). This method ensures unbiased selection and simplifies the sampling process, making it suitable for situations with a homogeneous population (Mark et al., 2023), like in SA HEIs. Thus, with permission from the relevant institutional management, a comprehensive list of employees will be used as the sampling frame, a list of all elements in the target population (Saunders et al., 2019). In this study, the frame will ensure that all employees have an equal opportunity to participate in the survey.

4.8.4 Research Instrument

Online questionnaires are a popular data collection method in modern research due to their convenience, efficiency, and ability to gather extensive data from a diverse pool of participants (Saunders et al., 2019; Hair et al., 2017; Bhattacherjee, 2012). Unlike paper-based surveys, online questionnaires eliminate physical distribution, reduce administrative expenses, and enable remote data collection without geographical constraints. Also, online questionnaires enhance data accuracy through automated entry, mitigating human error (Saunders et al., 2019). Similar to prior cybersecurity research (Li et al., 2019; Safa et al., 2015), this study used online questionnaires to collect data on cybersecurity awareness and behaviour and their influencing factors. This aligns with the confirmatory survey method recommended for exploring and elucidating relationships between research variables (Saunders et al., 2019; Hair et al., 2017; Bhattacherjee, 2012). The choice is also justified by their suitability for efficient quantitative data collection from a diverse participant pool (Hair et al., 2017).

The research instrument was a comprehensive questionnaire to facilitate systematic data collection (Saunders et al., 2019). The introductory section informed participants about the study's purpose, title, and ethical considerations, adhering to recommendations by Hair et al. (2017) and Saunders et al. (2019). It also assured them of the study's approval by the University of Pretoria (UP) and the Faculty of Engineering, Built Environment, and IT Ethics

Committee (EBIT). The first section focused on collecting demographic information, a crucial aspect for describing the sample and ensuring its representativeness of the larger population (Saunders et al., 2019). Complying with POPI Acts and UP EBIT policies regarding personal information collection, this section collected data on education level and awareness of the cybersecurity policy.

To explore the factors influencing employee cybersecurity behaviour in SA HEIs, the survey instrument was adapted from prior research instruments on cybersecurity (Safa et al., 2015; Li et al., 2019), following the UP's questionnaire policy. This adaptation involved careful selection and modification of questions to ensure their relevance to the specific context of this study (see Section 3.7.2 for details). Specific constructs like "cybersecurity awareness", "security policy", "cybersecurity experience", "attitude", "subjective norms", "perceived behavioural control" "threat appraisal", "response efficacy", and "self-efficacy", along with questions on "cybersecurity-compliant behaviour", were adapted from various publications (i.e., Li et al., 2019; Safa et al., 2015; Herath & Rao, 2009a; Ifinedo, 2012; Johnston & Warkentin, 2010). Notably, questions assessing "cybersecurity policy awareness" were adapted explicitly from Li et al. (2019) to better reflect the unique policy landscape within SA HEIs.

Explanation of Adaptation: While the original instruments by Safa et al. (2015) and Li et al. (2019) provided a strong foundation, the researcher adapted them to reflect better the unique employee roles and challenges within SA HEIs. This involves revising existing questions for clarity and relevance to this study population (Saunders et al., 2019). Moreover, new questions were added to capture specific aspects of cybersecurity awareness relevant to the settings of SA HEIs. The questionnaire was designed to be easily accessible to participants through an emailed hyperlink. This approach aligns with Saunders et al.'s (2019) recommendations and ensures compatibility with various devices, including computers and mobile phones. The careful selection of questions and format within the instrument was guided by the study's key objectives, focusing on achieving clarity and effectiveness in data collection. The specific questions featured in the instrument (see Table 6).

4.8.5 Measurement

A questionnaire is a central data collection instrument in survey research, often using closed-ended questions like the Likert scale (Saunders et al., 2019). In this study, the survey questionnaire evaluated employees' awareness and CCB and related factors using a 5-point

Likert scale (1 = Strongly Disagree, 5 = Strongly Agree), a widely used method for measuring attitudes and opinions (Hair et al., 2017b). A 5-point scale was chosen due to its ability to capture a range of opinions, offer clear response options, facilitate statistical analysis, and minimise potential midpoint bias (Hair et al., 2017; Boone & Boone, 2012). This format aligns with the previous focus on cybersecurity behaviour (Safa et al., 2015) and ensures that the collected data is appropriate for statistical analysis to address the research objectives.

A sample size calculator was used to determine a precise sample for the study's investigation. The sampling confidence interval represents the confidence level in the population's selection of an answer within a specified range (Hair et al., 2017b). The margin of error determines the extent to which survey results align with the views of the overall population. A smaller margin of error indicates a closer approximation to the precise answer at a given confidence level. Determining the appropriate sample size for representativeness involves various methods and formulas that hinge on factors such as research design, statistical analyses, expected effect size and confidence levels (Charan et al., 2021). Several studies have endorsed using power analysis for sample size calculation to ensure the population subset provides sufficient information to draw representation and conclusions (Hair et al., 2017; Ringle et al., 2018). Thus, this study used a sample size calculator to determine an appropriate sample size of 384 employees (SurveyMonkey, 2019). This sample size maintains a 95% confidence level with a 5% margin of error and adheres to the criteria for accurately representing the broader population (Saunders et al., 2019; Hair et al., 2016b).

Thus, the study utilised Cochran's sample size formula to determine the required sample size. Employing a 95% confidence level (Z-score = 1.96), a standard deviation of 0.5, and a margin of error of 5% (0.05), the sample size was calculated using the Cochran formula:

n = (Z-score) ^2 * Standard Deviation * (1 - Standard Deviation) / (Margin of Error) ^2

Where:
n is the sample size
Z-score is the critical value for the chosen confidence level (i.e., 1.96)
Standard deviation is the standard deviation of the population proportion (i.e., 0.5)
The margin of error is the desired/acceptable margin of error (i.e., 0.05)

n = (1.96) ^2 * 0.5 * (1 - 0.5) / (0.05) ^2

Thus, this resulted in a 384-sample size, deemed adequate as it aligns with prior cybersecurity studies employing PMT and TPB models and the study's cross-sectional nature.

4.8.6 Pilot-testing

Designing a questionnaire is a complex process that requires careful planning (Campanelli, 2008). The researcher pilot-tested the questionnaire to ensure it was easy to understand and complete and to identify potential data capture or collection errors. This process helped to confirm the validity and reliability of the data, which is essential for making inferences and generalisations about employees in SA HEIs (Saunders et al., 2019).

The size and frequency of the pilot test were determined by the research questions, objectives, project scale, available resources, and questionnaire design (Saunders et al., 2019). Perneger et al. (2014) recommend a sample size of 30 participants for pilot-testing questionnaires. This study's pilot tests focused on 30 participants, which were deemed sufficient for meaningful inferences and assessing the questionnaire's potential. The pilot-test evaluation was guided by Yellow and Bell (2014), which considered factors such as completion time, clarity of instructions and questions, respondent challenges, omitted details, layout, and feedback.

The researcher employed multiple questionnaire delivery and collection strategies, including questionnaire length, appearance, delivery methods, contact procedures, content quality, and communication (Anseel et al., 2010). These strategies attracted timely, high response rates.

The Qualtrics platform facilitated the questionnaire's design, offering features such as bullet points, text boxes, and automatic user-friendliness (Boas et al., 2020; Cardella et al., 2018). The survey was delivered through various platforms to accommodate diverse participants, with multiple communications and reminders sent to address inquiries and ensure successful data collection. This comprehensive approach guarantees questionnaire quality, validity, and reliability while facilitating data collection from a broader audience.

4.9 DATA ANALYSIS

Data analysis is a crucial step in research, where collected data is examined, interpreted and used to validate proposed hypotheses and draw meaningful conclusions (Saunders et al., 2019). This study employs both descriptive and inferential statistics for analysis.

4.9.1 Data Analysis with PLS-SEM

Partial least squares structural equation modelling (PLS-SEM) with SmartPLS 4.0 software was chosen for data analysis and hypothesis testing for its specific advantages in this context: This study employed PLS-SEM for data analysis, which aligns well with the study's research design and data characteristics.

Advantages of PLS-SEM

- **Accommodates Smaller Sample Sizes:** PLS-SEM is well-suited for smaller sample sizes, which is particularly relevant for this study, as 283 usable responses were obtained from participants within SA HEIs (Hair et al., 2022).
- **Handles Non-normal Data:** Real-world data often deviates from perfect normality. PLS-SEM exhibits robustness towards non-normality (Hair et al., 2012), making it suitable for analysing data collected from various sources, including surveys.
- **Focuses on Prediction:** Since this study aims to predict and understand the factors influencing cybersecurity-compliant behaviour, PLS-SEM's prioritisation of prediction aligns well with this objective (Hair et al., 2017).

Additionally, PLS-SEM offers several advantages that are particularly relevant to this research:

- **Formative Constructs:** This study included critical formative constructs such as cybersecurity awareness, policies, and prior experience. PLS-SEM effectively accommodates these, providing a more accurate representation of their influence.
- **Confirmatory Nature:** Given the study's aim to comprehensively examine and confirm cybersecurity awareness and behaviour, PLS-SEM offers valuable insights into causal relationships between variables.
- **Flexibility:** PLS-SEM's ability to handle small or large sample sizes and non-normally distributed data (Hair et al., 2017) aligns with the characteristics of this research data.

Limitations of PLS-SEM

- **Limited Hypothesis Testing:** While offering valuable insights into relationships and predictive power, PLS-SEM has limitations in rigorously testing specific hypotheses. This method may only be suitable for studies partially confirming or rejecting pre-established theoretical predictions.
- **Black Box Issues:** Compared to other SEM techniques, PLS-SEM can be less transparent in pinpointing the specific sources of variance within the model. While providing an overall understanding of relationships, it may not readily reveal the exact pathways of influence between constructs (Hair et al., 2017).

4.9.2 Data Cleaning and Analysis Procedures

Data analysis followed established procedures and statistical tests outlined in MacKenzie et al. (2011) to minimise and test for common method bias (CMB). Findings suggest that CMB is not a significant concern for this research.

- **Data Cleaning:** Missing or inconsistent data were identified and rectified before analysis, ensuring data integrity (Pallant, 2016).
- **Descriptive Statistics:** Descriptive measures of central tendency (means, medians) and dispersion (standard deviations, ranges) were used to summarise the data's primary features (Field, 2013). Visual representations like histograms and scatter plots also aided data exploration.
- **Data Analysis and Descriptive Statistics:** Descriptive and frequency analyses (Hair et al., 2017) using SPSS and applied PLS-SEM method using SMART PLS-4 to test relationships between variables and test the study's hypotheses. SMART-PLS is a well-substantiated method for estimating complex cause-effect-relationship models in business research (Gudergan et al., 2008; Ringle et al., 2022).

4.9.3 Reliability and Validity

Scale reliability and validity are crucial factors for ensuring meaningful and dependable research results (Sürücü & Maslakçi, 2020). Therefore, the following measures were implemented to guarantee that the study's findings are reliable and valid:

- **Reliability:** Cronbach's alpha assessed the questionnaire's internal consistency, with a value exceeding the 0.7 acceptable threshold (Sürücü & Maslakçi, 2020; Nunnally, 1978).
- **Content Validity:** The questionnaire underwent scrutiny by experts and supervisors to ensure it accurately measures the intended constructs (Sürücü & Maslakçi, 2020; Polit & Beck, 2006).
- **Construct Validity:** Confirmatory factor analysis was conducted to evaluate the questionnaire's underlying structure and verify its accurate measurement of the intended constructs (Hair et al., 2017).

This study strives to ensure data accuracy, questionnaire reliability and alignment of research objectives with the questionnaire design by employing these rigorous data analysis procedures and reliability and validity assessments. Table 7 provides a synopsis of this study's research methodology and data analysis.

Table 7: ***Research Design and Methodology Summary***

Category	Characteristics
Research Philosophy	Positivism - focuses on objective measurement and observable data to investigate and explain real-world phenomena.
Research Approach	Quantitative approach - emphasises collecting and analysing numerical data to test hypotheses and arrive at generalisable conclusions.
Research Strategy	Survey methodology - utilises questionnaires to collect data from a large sample of SA HEI employees.
Research Choices	Sampling: Simple random sampling was used to select employees from various departments who use computers. Data Analysis: Statistical techniques, including descriptive statistics and PLS-SEM, were used using SmartPLS software.
Time Horizon	Cross-sectional—Data was collected from December 2023 to February 2024 to capture a snapshot of employees' current perceptions and practices.
Data Collection	An online questionnaire was distributed through SA HEIs' management and HR departments. The questionnaire used Qualtrics and included a mix of question formats (e.g., five-point Likert scale) to gather quantitative data on cybersecurity awareness and behaviour.
Data Analysis	Descriptive statistics summarise the data (e.g., means and frequencies). PLS-SEM tests the relationships between variables in the research model.

4.10 ETHICS

This research upholds rigorous ethical principles, adhering to informed consent, anonymity, confidentiality, and data security as outlined in the UP-EBIT ethics standards, literature and legislation (e.g., Saunders et al., 2019; POPIA Act). The study received ethics approval from the UP-EBIT Faculty Committee for Research Ethics and Integrity on November 30, 2023 (reference number EBIT/244/2023).

HEIs participatory approval: As stated in the Ethics approval, the study first sought management approval from the participating HEIs before realising the survey link to the institution for employees' participation.

Informed Consent: Respondents provided informed consent through a detailed information sheet explaining the study, their rights, potential risks, and commitment to upholding anonymity and confidentiality (Bryman, 2021). Participation was voluntary and withdrawable at any time without repercussions.

Anonymity and Confidentiality: Data was pseudonymised using unique codes instead of names and stored securely on password-protected servers. Specific measures addressed online survey anonymity, such as using an anonymous platform that avoids embedding IP addresses (Resnik, 2015). All data was handled according to the principle of least privilege, with access granted only to authorised individuals.

Data Privacy and Legislation: The study adhered to the POPIA by not collecting personal identifiers (South African Government, 2019). The researcher also obtained management approval and consent from participating SA HEIs and relevant institutions (Resnik, 2015).

Ethical Conduct: Throughout the research process, ethical considerations are paramount to:

- **Protect participant rights and well-being:** This includes addressing any unforeseen ethical concerns promptly and transparently (Bryman, 2021).
- **Maintain research integrity:** Ethical practices ensure the validity and credibility of the research findings (Field, 2013).

This approach ensured participant privacy by refraining from collecting personally identifiable information (PII), which was unnecessary for the study's aims. This balanced the ethical imperative of protecting participants with the research objective of acquiring crucial data required for the investigation.

4.11 CONCLUSION

This chapter outlined the research design and methodology adopted, rooted in the research onion's framework. The study adopts a positivist stance and objectivist ontological and employs a survey research strategy. It follows a quantitative approach with a confirmatory purpose. It uses an online questionnaire to collect data on employees' cybersecurity awareness and its influencing factors within SA HEIs. Qualtrics and SPSS-29 were used for data collection, cleaning and description. Ethical considerations uphold the research integrity and protect respondents and organisations.

The researcher used a cross-sectional survey implemented across SA HEIs and employed SMART-PLS-4 to test the study's research hypotheses. The study utilised a simple random probability sampling technique, with a sample of employees using computers within the SA HEIs. Data was collected between January and February 2024 through an online questionnaire distributed on Qualtrics software. The next chapter presents the data analysis and research findings.

5 INTERPRETATION AND DISCUSSION OF FINDINGS

5.1 INTRODUCTION

The preceding chapter details the research design and methodology employed in this study. Following the detailed data collection process in chapter three, this chapter analyses the data and presents the findings concerning the research objective. This quantitative survey investigated factors influencing cybersecurity awareness and behaviour among South African (SA) Higher Education Institutions (HEIs) employees. Following Boas et al. (2020), the survey questionnaire was developed and distributed online using Qualtrics, a versatile platform for online surveys and statistical analysis (Boas et al., 2020; Qualtrics, n.d.-a). A pilot test involving 30 participants from the target population provided valuable feedback that led to revisions, primarily shortening specific questions.

The researcher designed and distributed the survey online using the versatile Qualtrics platform (Boas et al., 2020; Qualtrics, n.d.-a) and yielded 399 initial responses from SA HEI employees between January and February 2024. After data cleaning to ensure quality and address missing values, a final sample of 283 usable responses remained. Further, since the study employed SmartPLS for data analysis, it adheres to the 10-times rule (Hair et al., 2017, 2022). The rule recommends a minimum sample size of 10 times the number of structural or This quantitative survey investigated factors influencing formative indicators to a particular construct in a model. The proposed model has nine paths. Thus, at least 90 sample sizes are required for the analysis. This study's 283-sample size surpasses established minimums for various analytical approaches and aligns with recommendations for SmartPLS analysis (Hair et al., 2018; Hair et al., 2017; Guilford, 1954).

Initial data analysis using IBM SPSS (Version 29) involved checking for missing values and establishing normality, resulting in a final dataset of 283 complete and usable responses (Lane, 2003). This sample size further aligns with recommendations for SmartPLS analysis (Hair et al., 2017), requiring a minimum of 144 observations for an 80% statistical power in detecting R-squared values of at least 0.10 with a 5% error probability.

The remainder of the chapter is structured as follows: Demographic representation of data, Descriptive statistics, Demographic effects on explanatory variables, Presentation of structural equation modelling, and chapter conclusion.

5.2 DEMOGRAPHICS OF RESPONDENTS

This study obtained demographics about the respondents' education level to better understand the factors influencing employee cybersecurity behaviour within SA HEIs. Research suggests a positive correlation between an individual's educational level and cybersecurity awareness (Aivazpour & Rao, 2020; Wiley et al., 2020). In student contexts, studies by Fatokun et al. (2019) and Kovacevic et al. (2020) further highlight that the educational level is a significant factor in mediating cybersecurity behaviours. Thus, understanding the educational background of our respondents is crucial as the research objectives explore the factors influencing employee cybersecurity behaviour within SA HEIs. By analysing the respondents' educational background alongside other variables, the study can determine the relative influence of education on employee cybersecurity behaviour.

Respondents' Education

The sample comprised employees with diverse educational backgrounds within the SA HEIs. Most respondents held a bachelor's degree qualification (44.9%, n = 127), suggesting a population with a solid foundation in academic knowledge. This was followed by employees with Certificate/Diploma qualifications (30.7%, n = 87), depicting a focus on applied skills and vocational training. Master's degrees (13.4%, n = 38) and Doctoral degrees (4.6%, n = 13) comprised sizable portions of the sample, suggesting a representation of higher-level education. The remaining respondents (5.9%, n = 17) held other qualifications categorised as "other," indicating a degree of heterogeneity within the sample. This varied distribution of educational backgrounds among participants within SA HEIs will be further analysed to explore its potential connection to cybersecurity within these institutions (see Table 8).

Table 8*: Respondents' Education*

Factor	Frequency	Percentage (%)
Higher school	4	1.4%
Certificate/Diploma	87	30.7%
Bachelor's Degree	127	44.9%
Master's Degree	38	13.4%
Doctoral Degree	13	4.6%
Other	17	5.9%

Note *N* =283

5.2.1 Cybersecurity Policy Awareness

Responses concerning cybersecurity policy awareness revealed a spectrum of familiarity among employees within SA HEIs, as responses indicated. Over 41% (n = 116) reported being aware of a cybersecurity policy within their institutions. This suggests that many employees within SA HEIs operate within institutions that prioritise cybersecurity measures. However, a substantial portion (47.3%, n = 134) were unsure of the existence of such policies, highlighting a potential gap in awareness or communication within some institutions. A smaller group (11.7%, n = 33) confirmed the absence of a formal cybersecurity policy, indicating a possible area for improvement in certain institutional practices. Figure 7 provides visual representations of respondents' cybersecurity policy awareness distribution. Each pie chart slice corresponds to a distinct cybersecurity policy awareness category: aware, unaware and unsure.

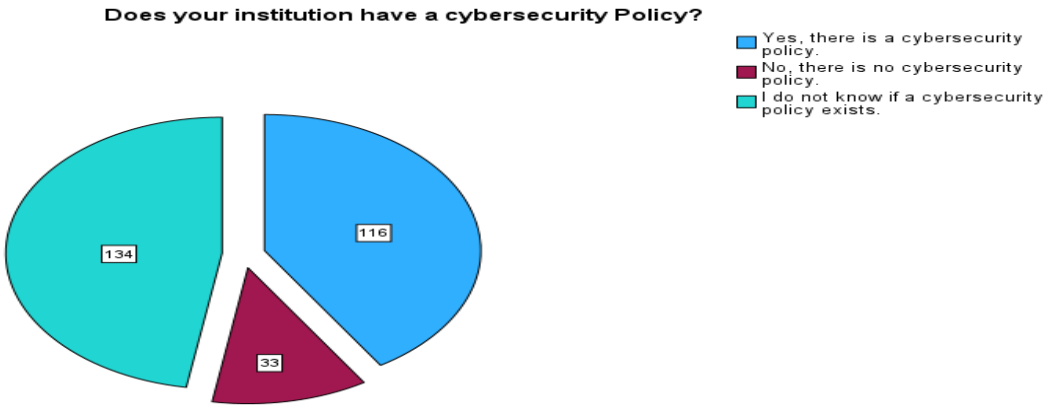

Figure 7: Graphical Representation of Cybersecurity Policy Awareness

5.3 DESCRIPTIVE STATISTICS

The survey yielded 283 usable responses from SA HEIs employees. Descriptive statistics were employed to analyse data on ten key variables, namely Cybersecurity Awareness (CA), Institution Cybersecurity Policy (ICP), Cybersecurity Experience (CEI), Attitude (ATT), Subjective Norm (SN), Perceived Behavioural Control (PBC), Threat Appraisal (TA), Cybersecurity Response Efficacy (CRE), Self-efficacy (CSE) and Cybersecurity-Compliant Behaviour (CCB). Table 9 summarises each variable's central tendency, dispersion and range.

The mean (M) represents the average score for each variable, reflecting the central tendency. The standard deviation (SD) depicts the variability of responses around the mean, with higher values indicating greater spread. Additionally, the table includes the minimum and maximum values encountered for each variable, providing context regarding the data's range. The study used a five-point Likert scale ranging from 1 ("strongly disagree") to 5 ("strongly agree") to gauge participants' perceptions. This information is essential for interpreting the descriptive statistics and drawing meaningful conclusions about the data's distribution and central tendencies across all ten variables. Table 9 presents the descriptive statistics for the key variables used in the study. The variables represent the constructs within the conceptual model investigating employee CCB in SA HEIs (Table 9). The table includes:

Table 9*: Descriptive Statistics for Key Variables*

Factor	Minimum	Maximum	Mean	Standard Deviation	Interpretation
CA	1.00	5.00	3.4290	0.854	Neutral
ICP	1.00	5.00	3.4779	0.855	Neutral
CEI	1.00	5.00	3.1031	0.934	Neutral
ATT	1.00	5.00	4.0537	0.705	Slightly agree
SN	1.00	5.00	3.3348	0.867	Neutral
PBC	1.00	5.00	3.6608	0.700	Slightly agree
TA	1.00	5.00	4.0883	0.669	Slightly agree
CRE	1.00	5.00	4.1578	0.681	Slightly agree
CSE	1.00	5.00	3.2951	0.894	Neutral
CCB	1.00	5.00	3.5901	0.760	Slightly agree

Note *N* =283

Factor: Abbreviated label for each variable. **Minimum**: The lowest score obtained on the five-point Likert scale (ranging from 1 “strongly disagree” to 5 “strongly agree”). **Maximum**: The highest score was obtained on the Likert scale. **Mean**: Each variable’s average score reflects the central tendency. **Standard Deviation**: The variability of responses around the mean, with higher values indicating greater dispersion of data points. **Interpretation**: A brief description of the central tendency based on the mean score (e.g., neutral, slightly agree).

Key Observations from Demographics Analysis

The data reveals a relatively neutral stance on cybersecurity within SA HEIs, with most variables (e.g., CA, ICP) scoring between 3 and 4 on a 5-point Likert scale (neutral range). This suggests a potential need to emphasise cybersecurity awareness and behaviour within these institutions further. However, interestingly, the analysis of education level and policy awareness revealed no statistically significant differences (see Section 5.3.1 for details).

5.3.1 Education Level Impact on Cybersecurity Policy Awareness

Table 10 presents a post hoc analysis of Tukey’s Honestly Significant Difference (HSD) conducted to explore potential differences in cybersecurity policy awareness among employees with varying highest education levels (High School, Certificate/Diploma, Bachelor’s Degree, Master’s Degree, Doctoral Degree and Other). The analysis answers the question: “Does your institution have a cybersecurity policy?

The table displays the mean difference in policy awareness scores between each pair of education levels (columns I and J). The corresponding standard error (Std. Error) and significance level (Sig.) are also reported. A significance level greater than 0.05 (indicated by values close to 1) suggests no statistically significant difference in policy awareness between the education levels.

Table 10*: Education Level Impact Cybersecurity Policy Awareness*

(I) Highest Education Level	(J) Highest Education Level	Mean Difference	Std. Error	Sig.
High School	Certificate/Diploma	-0.365	0.48	0.974
	Bachelor's Degree	-0.36	0.477	0.975
	Master's Degree	-0.303	0.494	0.99
	Doctoral Degree	-0.173	0.537	1
	Other	0.179	0.532	0.999
Certificate/Diploma	High School	0.365	0.48	0.974
	Bachelor's Degree	0.005	0.131	1
	Master's Degree	0.062	0.183	0.999
	Doctoral Degree	0.192	0.279	0.983
	Other	0.544	0.27	0.339
Bachelor's Degree	High School	0.36	0.477	0.975
	Certificate/Diploma	-0.005	0.131	1
	Master's Degree	0.058	0.174	0.999
	Doctoral Degree	0.187	0.273	0.984
	Other	0.539	0.264	0.324
Master's Degree	High School	0.303	0.494	0.99
	Certificate/Diploma	-0.062	0.183	0.999
	Bachelor's Degree	-0.058	0.174	0.999
	Doctoral Degree	0.13	0.302	0.998
	Other	0.481	0.294	0.573
Doctoral Degree	High School	0.173	0.537	1
	Certificate/Diploma	-0.192	0.279	0.983
	Bachelor's Degree	-0.187	0.273	0.984
	Master's Degree	-0.13	0.302	0.998
	Other	0.352	0.362	0.926
Other	High School	-0.179	0.532	0.999
	Certificate/Diploma	-0.544	0.27	0.339
	Bachelor's Degree	-0.539	0.264	0.324

	Master's Degree	-0.481	0.294	0.573
	Doctoral Degree	-0.352	0.362	0.926

Key Findings on the Impact of Education on Cybersecurity Policy Awareness:

While literature shows a positive correlation between education and cybersecurity awareness (Aivazpour & Rao, 2020; Wiley et al., 2020), our data suggests a different scenario. This could be attributed to several factors, particularly the potential influence of institutional efforts:

- **Institutional Cybersecurity Awareness Programs:** HEIs with varying education levels among employees may cultivate a uniform level of cybersecurity policy awareness through standardised training programs. These programs ensure that all staff, regardless of their educational background, possess a baseline understanding of cyber threats and policies. For instance, organisations like SA HEIs often adhere to frameworks like NIST SP 800-16, which recommends basic cybersecurity literacy and policy awareness for all employees (Toth et al., 2014).
- **Cybersecurity Culture:** A robust institutional cybersecurity culture that emphasises the importance of policy adherence and secure practices can significantly influence employee behaviour across all education levels (Wolak et al., 2017). This culture is fostered through various means, such as leadership commitment, ongoing communication, and security awareness campaigns. Even employees with lower educational backgrounds might exhibit assertive cybersecurity behaviour if the institutional culture emphasises security best practices.
- **South African Regulatory Environments** (i.e., POPIA) advise organisations like HEIs to implement measures to safeguard personal information. Regardless of employees' education level, cybersecurity policy awareness can be crucial in achieving this, validating similar policy awareness levels observed across groups (see Table 10).

The following section delves into the data analysis procedure, noting other factors that might influence cybersecurity policy awareness. The results and discussion will reflect these factors.

5.4 DATA ANALYSIS PROCEDURES

This study analysed the quantitative data using SmartPLS 4 (Ringle et al., 2022) software for partial least squares structural equation modelling (PLS-SEM). The choice of PLS-SEM was justified by its effectiveness in causal relationship research (Byrne, 2001) and its ability to address challenges often encountered in social and business science research, such as small sample sizes and non-normal data (Hair et al., 2022, 2017). The analysis followed a two-stage approach, a widely accepted PLS analysis reporting style, as studies suggested (Chin, 2010):

1. Measurement Model Assessment: This stage evaluates the constructs' reliability, validity, and associated variables to validate them before model analysis. It involved examining indicators like loadings, composite reliability (CR) and average variance extracted (AVE) to ensure the measures accurately captured their intended constructs.

2. Structural Model Assessment: This stage analyses the relationships between the constructs hypothesised in the research conceptual model. It involved estimating path coefficients, assessing their significance, and evaluating the model's overall fit using various indices.

Following these two stages, researchers can ensure a robust and reliable data analysis using PLS-SEM. The measurement model assessment is presented next.

5.4.1 Measurement Model Assessment – Reliability and Validity

This section assessed the reliability and relationships between the constructs and their measurement items. It adhered to the guidelines set by Hair et al. (2022) to ensure all constructs achieve acceptable levels of reliability and validity. The reliability and validity of the measurement model are assessed by examining (1) indicator reliability, (2) internal consistency reliability, (3) convergent reliability, (4) discriminant validity and (5) multicollinearity assessment.

Indicator Reliability

Indicator reliability or Factor Loadings represent the associations between the constructs and their measurement variables, measured by examining item loadings. It is the extent to which each item (i.e., CE1, TA2) in the correlation matrix correlates with the principal component (Hair et al., 2022). A recommended 0.6 threshold (Hair et al., 2022; Chin et al., 2008; Gefen & Straub, 2005) indicates a strong association and satisfactory indicator reliability. All 43 indicator loadings exceeded this threshold, signifying a strong association between individual items (e.g., CE1, CE2, TA1, TA2) and their respective constructs (e.g., Cybersecurity Awareness, Self-efficacy). Thus, all items are retained for the following assessment (Table 11).

Internal Consistency Reliability

- Cronbach's Alpha (α) is the traditional criterion that measures internal consistency but is considered a conservative approach (Hair et al., 2022).
- Composite Reliability (CR) also measures internal consistency and is recommended by Hair et al. (2022) for a more comprehensive evaluation. It complements α's limitations and vice versa.

Table 11 presents the reliability and validity measures for the key constructs employed in the study's conceptual model. These measures assess the internal consistency (reliability) and convergent validity of the constructs used to investigate employee CCB within SA HEIs. Both α and CR and two CR options (rho_a and rho_c) were used to generate a more robust reliability measurement. All constructs surpassed the minimum thresholds of 0.7 for α and 0.70 for CR, demonstrating adequate internal consistency and convergent validity. The results for FL, α, CR values, and AVE (Table 11).

Table 11*: Loadings, Reliability and Validity of Constructs*

Constructs	Loadings	Alpha	CR (rho_a)	CR (rho_c)	AVE
Cybersecurity Awareness		0.86	0.87	0.90	0.65
CA1	0.78				
CA2	0.84				
CA3	0.83				
CA4	0.85				
CA5	0.71				
Institution Cybersecurity Policy		0.86	0.88	0.91	0.71
ICP1	0.85				
ICP2	0.85				
ICP3	0.81				
ICP4	0.86				
Cybersecurity Experience		0.92	0.92	0.94	0.72
CEI1	0.74				
CEI2	0.75				
CEI3	0.90				
CEI4	0.88				
CEI5	0.90				
CEI6	0.89				
Attitude		0.93	0.93	0.95	0.78
ATT1	0.83				
ATT2	0.92				
ATT3	0.92				
ATT4	0.83				
ATT5	0.90				
Subjective Norms		0.89	0.91	0.92	0.75
SN1	0.83				
SN2	0.85				
SN3	0.91				
SN4	0.88				
Perceived Behavioural Control		0.82	0.84	0.88	0.65
PBC1	0.64				
PBC2	0.85				

PBC3	0.88				
PBC4	0.84				
Threat Appraisal		0.87	0.87	0.91	0.72
TA1	0.80				
TA2	0.89				
TA3	0.88				
TA4	0.83				
Response Efficacy		0.90	0.90	0.94	0.84
CRE1	0.89				
CRE2	0.93				
CRE3	0.93				
Self-Efficacy		0.86	0.86	0.91	0.71
CSE1	0.89				
CSE2	0.86				
CSE3	0.78				
CSE4	0.84				
Cybersecurity-Compliant Behaviour		0.87	0.88	0.91	0.71
CCB1	0.87				
CCB2	0.89				
CCB3	0.78				
CCB4	0.83				

Multicollinearity Assessment

Multicollinearity, which refers to excessive intercorrelations among independent variables, can lead to inaccurate estimates of path coefficients and inflated standard errors in structural models (Hair et al., 2017). This study assesses multicollinearity using Variance Inflation Factors (VIFs) (Fornell & Bookstein, 1982). VIF values above 3.3 generally indicate potential multicollinearity concerns (Hair et al., 2017). As depicted, All VIF values in the current model are below 1.33, suggesting no significant multicollinearity issues within the model (Table 12).

Table 12: ***Multicollinearity Statistics (VIF) for Indicators***

Independent Variable	VIF
CA -> ATT	1.00
ICP -> SN	1.00
CEI -> PBC	1.00
ATT -> CCB	2.43
SN -> CCB	1.33
PBC -> CCB	2.64
TA -> CCB	2.65
CRE -> CCB	2.63
CSE -> CCB	1.70

Convergent Validity

Convergent validity assesses the degree to which multiple items within a construct measure the same underlying concept. The Average Variance Extracted (AVE) value serves as an indicator, targeting a desired minimum threshold of 0.5 (Fornell & Larcker, 1981; Hair et al., 2017). The current study's convergent validity is based on AVE values, which show that all constructs exhibit AVE values exceeding 0.5, suggesting convergent validity. Table 13 presents the convergent and discriminant validity measures for the key constructs employed in the study's conceptual model.

Discriminant Validity

The following assessment is the discriminant validity, which represents the degree to which the measures of different concepts are distinct (i.e., do not reflect other variables as two more concepts are unique). This study employs Two criteria to assess validity. First, the Fornell-Larcker Criterion, the square root of AVE for each construct, should be higher than its correlations with other constructs (Table 13).

Table 13: ***Discriminant validity (Fornell-Larcker Criterion)***

Constructs	CA	ICP	CEI	ATT	SN	PBC	TA	CRE	CSE	CCB
CA	***0.80***									
ICP	0.62	***0.84***								
CEI	0.63	0.58	***0.85***							
ATT	0.49	0.52	0.51	***0.88***						
SN	0.31	0.54	0.46	0.43	***0.87***					
PBC	0.60	0.51	0.71	0.63	0.44	***0.81***				
TA	0.40	0.39	0.38	0.65	0.29	0.59	***0.85***			
CRE	0.37	0.33	0.36	0.67	0.35	0.54	0.74	***0.91***		
CSE	0.47	0.43	0.66	0.37	0.33	0.63	0.39	0.36	***0.84***	
CCB	0.55	0.44	0.61	0.58	0.38	0.72	0.64	0.58	0.61	***0.84***

Bold and italics on the diagonal are AVE's square root, while the off-diagonals are correlations.

All diagonal elements in the table fulfil this criterion, confirming discriminant validity. Second, discriminant validity was tested using the Heterotrait Monotrait (HTMT) procedure. According to Henseler et al. (2015), (≥0.90) is the most conservative threshold value of the HTMT ratio for checking discriminant validity. This procedure measures the ratio of between-construct (heterotrait) and within-construct (Monotrait) correlations. All HTMT values fall below the conservative 0.90 threshold (Henseler et al., 2015), further supporting discriminant validity (see Table 14).

Table 14: ***Discriminant validity (Heterotrait-Monotrait)***

Constructs	CA	ICP	CEI	ATT	SN	PBC	TA	CRE	CSE	CCB
CA										
ICP	**0.73**									
CEI	0.71	**0.65**								
ATT	0.54	0.58	**0.54**							
SN	0.34	0.59	0.49	**0.46**						
PBC	0.70	0.60	0.80	0.72	**0.52**					
TA	0.46	0.45	0.42	0.73	0.32	**0.70**				
CRE	0.42	0.37	0.39	0.74	0.39	0.63	**0.84**			
CSE	0.55	0.49	0.75	0.40	0.36	0.76	0.44	**0.40**		
CCB	0.64	0.51	0.68	0.64	0.43	0.84	0.73	0.65	**0.70**	

Shaded boxes are the standard reporting format for the HTMT procedure.

5.4.2 Structural Model Assessment

The structural model examines the hypothesised relationships between the constructs within the research framework, which integrate the institution's cybersecurity environment with TPB and PMT. It analyses and tests the relationship between all constructs, also known as causal relationships, to denote the theoretical structure between the constructs (Hair et al., 2017b). This section evaluates the model's fit and the significance of the path coefficients using a one-tailed Bias-Corrected and Accelerated (BCa) bootstrapping procedure with 5000 samples (Hair et al., 2022, 2019, 2017; Streukens & Leroi-Werelds, 2016) in SmartPLS 4. This approach was used to calculate path coefficients and R-squared values and assess significance at a level of $\alpha = 0.05$ (Hair et al., 2017; Ringle et al., 2015). The analysis considers 283 sample sizes.

The structural model's analysis is divided into three parts: (1) R^2 (explanatory power), Q^2 (predictive relevance), and path coefficients (relationship strength and direction).

Goodness-of-Fit Measures

A well-specified measurement model (assessed by AVE and CR, see Table 11) provides the foundation for reliable path coefficients and overall model fit. This section evaluates the structural model's fit using R-squared (R^2), Adjusted R-squared, and Q-squared (Q^2) in SmartPLS 4.

- R-squared (R^2) and Adjusted R-squared:

- **R-squared (R^2)**: R^2 represents the variance explained in each endogenous construct by the independent constructs, reflecting the model's predictive power (Hair et al., 2017). Generally, an R^2 value of 0.1 or above indicates acceptable power (Falk & Miller, 1992). As shown in Table 15, all R^2 values exceed this threshold. For instance, the R^2 value for CCB (0.635) suggests that the model explains 63.5% of the variance in this construct. **Adjusted R^2** accounts for model complexity and is slightly lower. The adjusted R^2 value for CCB was 0.627, slightly lower due to the consideration of model complexity. Similarly, R^2 and adjusted R^2 values were calculated for other endogenous constructs (see Table 15).

- **Q-squared (Q^2)**: Q^2 assesses and establishes the predictive relevance of the endogenous constructs (Hair et al., 2017a; Richter et al., 2016). A Q^2 value greater than

zero indicates good value reconstruction and model predictive relevance (Hair et al., 2017). The table below displays significant predictive relevance for the constructs. For example, Q^2 values for CCB range from 0.311 to 0.504, indicating moderate to strong predictive ability. Similarly, the range of Q^2 values for constructs (i.e., SN and PBC) suggests moderate predictive relevance (Table 15).

Table 15*: Q Square and R Square predictive values*

Construct	Q^2predict	R-squared	Adjusted R-squared
CCB	Range: 0.311 - 0.504	0.635	0.627
ATT	Range: 0.134 - 0.234	0.241	0.239
SN	Range: 0.108 - 0.303	0.292	0.289
PBC	Range: 0.150 - 0.434	0.504	0.502

Significance of Path Coefficients

Path coefficients represent the strength and direction of relationships between constructs. The P-value value represents the probability of observing the obtained results by chance (Bhattacherjee, 2012). A p-value less than 0.05 suggests that the observed relationship is statistically significant. Hair et al. (2017) suggest path coefficient thresholds of 0.20 to 0.30. Table 16 displays the path coefficients for each hypothesised relationship. Notably, the relationships between Cybersecurity Experience (CEI) and Perceived Behavioural Control (PBC) ($\beta = 0.71$, $p < 0.002$) and between Self-Efficacy (CSE) and CCB ($\beta = 0.247$, $p < 0.002$) are significant.

Table 16*: Path Coefficient*

Path	Path Coefficient
CA -> ATT	0.491
ICP -> SN	0.54
CEI -> PBC	0.71
ATT -> CCB	0.05
SN -> CCB	0.031
PBC -> CCB	0.33
TA -> CCB	0.247
CRE -> CCB	0.088
CSE -> CCB	0.24

The structural model assessment results indicate that the model has acceptable predictive power and relevance. The hypothesised relationships between the constructs are statistically significant and contribute to explaining the variance in CCB.

5.4.3 Hypothesis Tests

The hypotheses in the study's structural model test the proposed relationships among Cybersecurity Awareness (CA), Institution Cybersecurity Policy (ICP), Cybersecurity Experience (CEI), Attitude (ATT), Subjective Norm (SN), Perceived Behavioural Control (PBC), Threat Appraisal (TA), Cybersecurity Response Efficacy (CRE), Self-efficacy (CSE) and Cybersecurity-Compliant Behaviour (CCB) (Figure 8). The hypothesis test reveals several significant findings regarding the factors influencing employees' cybersecurity-compliant behaviour (CCB) in SA HEIs. The summary of the hypothesis test is presented (Table 17). This table summarises the hypothesis testing result to examine the relationships between the study's independent variables and employee CCB within SA HEIs. Also, provide the following information for each hypothesis:

Path Coefficient (β) is the standardised regression coefficient and represents the independent variable's relative influence on CCB when all variables are standardised.
Std Deviation: The standard deviation of the path coefficient.

T-statistic is the test statistic used to assess the null hypothesis that there is no relationship between the independent and dependent variables.

The **P-value** represents the significance level associated with the t-statistic. Values less than 0.05 indicate a statistically significant relationship, supporting the hypothesis. Values greater than 0.05 indicate non-significant relationships, suggesting the hypothesis is unsupported. **Decision** indicates whether the hypothesis was supported or not supported based on the p-value.

Supported Hypotheses

H1: Cybersecurity awareness has a positive and significant relationship with attitude towards cybersecurity (β = 0.49, p = 0.000). This indicates that respondents (i.e., employees) with higher cybersecurity awareness are likelier to have positive attitudes towards cybersecurity practices. **H2**: Institutional cybersecurity policies positively and significantly influence subjective norms surrounding CCB (β = 0.54, p = 0.000). This suggests that having clear and well-established cybersecurity policies within SA HEIs can foster positive social pressure and expectations for employees to engage in CCB.

H3: Employees' cybersecurity experience has a statistically significant positive impact on perceived behavioural control regarding CCB (β = 0.71, p = 0.000), signifying that employees with significant cybersecurity experience feel more confident and capable of performing CCB effectively. **H6**: Perceived behavioural control has a positive and significant relationship with CCB (β = 0.33, p = 0.000), indicating that employees who feel confident in their ability to perform CCB are likelier to engage in such behaviours.

H7: Threat appraisal positively and significantly influences CCB (β = 0.25, p = 0.000). This suggests that when employees perceive a higher level of cyber threat, they are likelier to adopt CCB practices to mitigate the threat. **H8b**: Cybersecurity self-efficacy is positively and significantly associated with CCB (β = 0.24, p = 0.000). This finding aligns with H3, highlighting that employees with higher confidence in their ability to handle cybersecurity situations are likelier to engage in CCB.

However, the following three hypotheses were found insignificant and thus unsupported:

H4: Attitude towards cybersecurity does not significantly impact CCB (β = 0.05, p = 0.410). Although previous research suggests a positive link, these findings indicate that employees' attitudes alone may not directly translate into CCB in the SA HEIs. **H5**: Subjective norms do not significantly influence CCB (β = 0.03, p = 0.483). This suggests that peer pressure or social expectations might not be a strong and independent motivator for CCB within SA HEIs, highlighting the need to explore alternative factors beyond social influence. **H8a**: Cybersecurity response efficacy does not significantly relate to CCB (β = 0.09, p = 0.179). This implies that employees' perceptions of their cyber-threats responding ability do not directly and effectively translate into engaging in CCB within this study's context.

This result supports the proposed model of relationships between the institution's cybersecurity environments, which comprises cybersecurity awareness, policy, experience, TPB, PMT and self-reported cybersecurity behaviour. Cybersecurity awareness is a positive driving force behind positive attitude, as policy positively contributes to subjective norms (i.e., workplace social pressure and expectations). Cybersecurity experience is a positive predictor of PBC towards CCB, signifying that employees feel more confident and competent in handling CCB if they possess related experience. Threat appraisal and self-efficacy are related to more CCB. This validates the protection motivation theory and the theory of planned behaviour as valuable conceptual frameworks for explaining employees' cybersecurity behaviour. The following section analyses the link between cybersecurity policy awareness and employees' CCB.

Table 17*: Hypothesis Testing Result*

Hypothesis	Path Coefficient (β)	Std Deviation	T-statistic	p-value	Decision
H1: CA → ATT	0.49	0.05	9.31	0.00	Supported
H2: ICP → SN	0.54	0.06	9.35	0.00	Supported
H3: CEI → PBC	0.71	0.04	20.51	0.00	Supported
H4: ATT → CCB	0.05	0.06	0.83	0.41	Not Supported
H5: SN → CCB	0.03	0.04	0.7	0.48	Not Supported
H6: PBC → CCB	0.33	0.07	4.95	0.00	Supported
H7: TA → CCB	0.25	0.07	3.59	0.00	Supported
H8a: CRE → CCB	0.09	0.07	1.34	0.18	Not Supported
H8b: CSE → CCB	0.24	0.05	4.59	0.00	Supported

Table 17 summarises the result of hypothesis testing conducted to examine the relationships between various constructs in this study. This table provides statistical evidence to support or refute the proposed relationships.

Figure 8 visually represents the results from a bootstrapping procedure applied to your PLS-SEM analysis. Bootstrapping is a statistical technique used to examine the model's robustness and the significance of the relationships between the constructs.

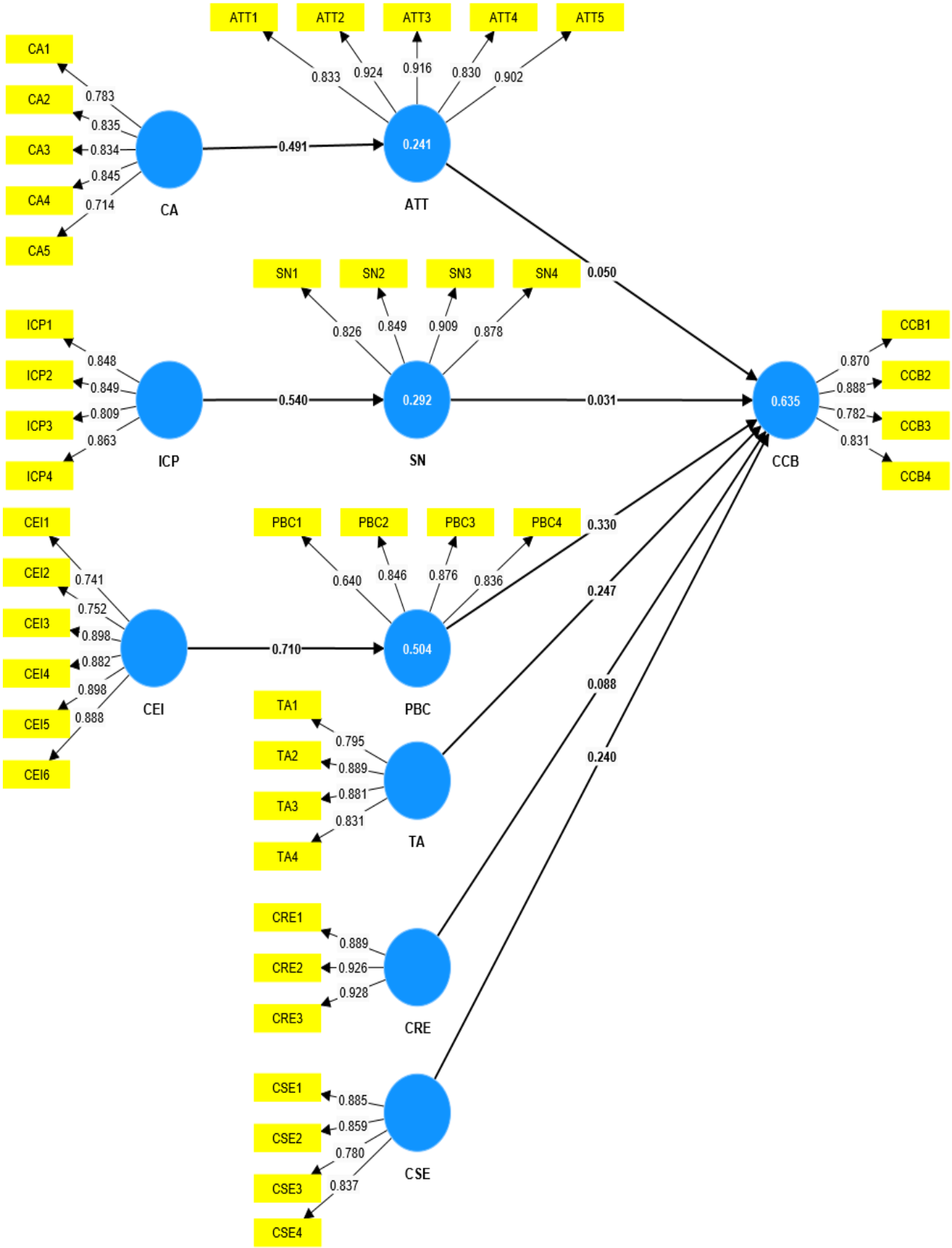

Figure 8: PLS-SEM Bootstrapping - Structural Model Evaluation

Key Findings

Table 17 reveals several significant relationships between the constructs (p-value < 0.05):

- **H1, H2, H3, H6, H7, and H8b:** These hypotheses were supported, indicating positive relationships between various constructs influencing cybersecurity behaviours or intentions.
- **H4, H5, and H8a:** These hypotheses were not supported, suggesting no statistically significant relationships between the proposed constructs in these cases.

5.5 CYBERSECURITY POLICY AWARENESS

This section applies the ten theory-based constructs identified in previous sections, including CA, ICP, CEI, ATT, SN, PBC, TA, CSE, CRE, and CCB. The hypotheses focus on the relationship between cybersecurity policy awareness and employees' cybersecurity-compliant behaviour. Responses to the study's survey instrument regarding the "institution's explicit cybersecurity policy" show that over 41% of the respondents confirmed their institutions have a cybersecurity policy (Yes, 41%, n = 116), over 11% confirmed no (No, 11.7%, n = 33), and over 47% were unsure (47.3%, n = 134), as depicted in section 5.2.1 (see Figure 7).

The researcher conducted ANOVA or analysis of variance in (SPSS 29) to analyse the impact of cybersecurity policy awareness on employees' cybersecurity-complaint behaviour. The independent variable was cybersecurity policy awareness, represented in three groups that responded to the question, "Does your institution have a cybersecurity policy?": (a) Yes (employees who reported institutions having a cybersecurity policy), (b) No (employees who reported no policy), and (c) Don't know (employees who don't know or are unsure about the existence of a policy). The dependent variable was the ten-theory-based constructs. The F statistics for ten constructs range between 3.11 and 23.04, and all are statistically significant at $p < 0.05$ (Table 18). The results of the ANOVA indicated a statistically significant effect of cybersecurity policy awareness on employees' belief about cybersecurity and self-reported cybersecurity-complaint behaviour, supporting the proposed Hypothesis 9.

Table 18 presents the results of an Analysis of Variance (ANOVA) test conducted between groups. This test is likely used to investigate whether statistically significant differences exist in the means of specific constructs (variables) across different groups.

Table 18*: ANOVA – Between Groups*

Constructs	Mean	F	Sig.
CA	11.10	16.93	0.00
ICP	13.32	20.80	0.00
CEI	17.39	23.04	0.00
ATT	4.42	9.43	0.00
SN	4.16	5.72	0.00
PBC	5.52	12.16	0.00
TA	2.55	5.90	0.00
CRE	1.42	3.11	0.046
CSE	11.12	15.30	0.00
CCB	8.91	17.21	0.00

ANOVA tests the null hypothesis that all group means are equal without identifying which specific groups differ from each other. Thus, after the ANOVA test showed a significant result, the post hoc (Tukey's HSD) tests determined which specific group differences were significant, contributing to the overall significant result in the ANOVA (Field, 2018). For example, when multiple pairwise comparisons are made, these tests control for the increased risk of Type I error. They help prevent drawing false conclusions about group differences and provide a more nuanced understanding of the data.

Therefore, the researcher conducted a post hoc test with Turkey's HSD to compare and analyse the differences in cybersecurity complaint behaviour in the three sub-groups. Table 18 presents the results of multiple comparisons that analyse the differences in various cybersecurity-related factors based on employees' cybersecurity policy awareness within their institutions. The factors analysed are CA, ICP, CEI, ATT, SN, PBC, TA, CRE, CSE and CCB.

Cybersecurity Awareness (CA) - Comparing three groups

Respondents (i.e. employees) who were aware of cybersecurity policies ("Yes" group) had significantly higher mean scores compared to those who don't know ("No" group) on all measures except for perceived barriers, where there was no significant difference. The "Yes" group also showed significantly higher mean scores on all measures than the "Don't Know"

group except for perceived barriers and self-efficacy, where there was no significant difference.

Institution Cybersecurity Policy (ICP) - Comparing three groups
Employees who were aware of cybersecurity policies (“Yes” group) had significantly higher mean scores on all measures compared to those who reported No (“No” group) and those who don’t know (“I don’t know” group) except for perceived barriers, where there was no significant difference. The “No” and “I do not know” groups did not significantly differ on any measure.

Cybersecurity Experience (CEI) - Comparing three groups
Employees who were aware of cybersecurity policies (“Yes” group) had significantly higher mean scores compared to those who reported No (“No” group) and those who don’t know (“I don’t know” group) on all measures except for perceived barriers, where there was no significant difference. The “No” and “I do not know” groups did not significantly differ on any measure.

Attitude (ATT) - Comparing three groups
Employees who were aware of cybersecurity policies (“Yes” group) had significantly higher mean scores on all measures compared to those who reported No (“No” group) and those who don’t know (“I don’t know” group) except for perceived barriers, where there was no significant difference. The “No” and “I do not know” groups did not significantly differ on any measure.

Subjective Norm (SN) - Comparing three groups
Employees who were aware of cybersecurity policies (“Yes” group) had significantly higher mean scores on all measures except perceived barriers, where there was no significant difference, compared to those who reported No (“No” group) and those who were don’t know (“I don’t know” group). The “No” and “I do not know” groups did not significantly differ on any measure.

Perceived Behavioural Control (PBC) - Comparing three groups.
Employees who were aware of cybersecurity policies (“Yes” group) had significantly higher mean scores on all measures compared to those who reported No (“No” group) and those who don’t know (“I don’t know” group) except for perceived barriers, where there was no significant difference. The “No” and “I do not know” groups did not significantly differ on any measure.

Threat Appraisal (TA) - Comparing three groups

Employees who were aware of cybersecurity policies (“Yes” group) had significantly higher mean scores on all measures compared to those who reported No (“No” group) and those who don’t know (“I don’t know” group) except for perceived barriers, where there was no significant difference. The “No” and “I do not know” groups did not significantly differ on any measure.

Cybersecurity Response Efficacy (CRE) - Comparing three groups

Employees who were aware of cybersecurity policies (“Yes” group) had significantly higher mean scores on all measures compared to those who reported No (“No” group) and those who don’t know (“I don’t know” group), except for perceived barriers, where there was no significant difference. The “No” and “I do not know” groups did not significantly differ on any measure.

Self-efficacy (CSE) - Comparing three groups

Employees who were aware of cybersecurity policies (“Yes” group) had significantly higher mean scores on all measures compared to those who reported No (“No” group) and those who don’t know (“I don’t know” group) except for perceived barriers, where there was no significant difference. The “No” and “I do not know” groups did not significantly differ on any measure.

Cybersecurity-Compliant Behaviour (CCB) - Comparing three groups

Employees who were aware of cybersecurity policies (“Yes” group) had significantly higher mean scores on all measures compared to those who reported No (“No” group) and those who did not know (“I don’t know” group) except for perceived barriers, where there was no significant difference. The “No” and “I do not know” groups did not significantly differ on any measure.

Post Hoc Multiple Comparisons

Table 19 presents the post hoc multiple comparison results following a significant ANOVA test. This analysis builds upon the (ANOVA – Between Groups) findings in Table 18.

Table 19*: Post Hoc Multiple Comparison Result: Cybersecurity Policy Awareness*

	No/Yes		G1	No/Don't Know		G2	Yes/Don't Know		G3
Variables	MeanDiff.	Std.Error	Sig.	MeanDiff.	Std.Error	Sig.	Mean Diff.	Std.Error	Sig.
CA	0.30	0.16	0.15	0.597*	0.10	0.001	-0.30	0.16	0.14
ICP	0.55695*	0.16	0.000	0.64*	0.10	0.001	0.08	0.16	0.86
CEI	0.44296*	0.17	0.003	0.75*	0.11	0.001	0.30	0.17	0.17
ATT	0.38067*	0.14	0.001	0.35*	0.09	0.001	-0.03	0.13	0.98
SN	0.35377*	0.11	0.000	0.30	0.17	0.17	-0.35377*	0.11	0.00
PBC	0.42122*	0.09	0.001	0.20	0.13	0.27	-0.42122*	0.09	0.01
TA	0.28644*	0.08	0.000	0.12	0.13	0.62	-0.28644*	0.08	0.00
CRE	0.20351*	0.09	0.05	0.19	0.13	0.32	-0.20351*	0.09	0.05
CSE	0.59139*	0.11	0.001	0.40349*	0.17	0.04	-0.59139*	0.11	0.01
CCB	0.51618*	0.09	0.001	0.44623*	0.14	0.00	-0.51618*	0.09	0.01

The mean difference is significant at the 0.05 level. G1, G2 and G3 signify three CPA groups

The results of the comparisons of the three groups suggest that employees' cybersecurity policy awareness (CPA) within institutions is associated with more positive attitudes, beliefs and behaviours related to cybersecurity. Therefore, HEIs must consider implementing and promoting cybersecurity policies to improve employees' cybersecurity awareness and CCB.

5.6 DISCUSSION OF FINDINGS

This study investigated the factors influencing CCB among employees in SA HEIs by using PLS-SEM with bootstrapping to test the proposed hypotheses within the conceptual model. The study introduced a model informed by the TPB and PMT, two prominent theories in cybersecurity research. These theories were integrated with the concept of an institution's cybersecurity environment, including cybersecurity awareness, policy and experience to inform employee CCB. The resulting model demonstrated strong predictive power in explaining employee intention and motivation to adopt CCB. The model was validated using data collected from 283 SA HEI employees (see Figure 3), as the measurement model assessment demonstrates that the constructs possess acceptable reliability and validity, suggesting that the items effectively capture the intended constructs. This paves the way for further analysis,

where the structural model will be examined to determine the relationships between the identified factors and their influence on the CCB of employees within SA HEIs.

5.6.1 Key Findings Summary

This study investigated the factors influencing employees' cybersecurity behaviour within A HEIs. By integrating the TPB and PMT with the concept of an institution's cybersecurity environment, the study identified two crucial influences on CCB. First, the institutional cybersecurity environment encompasses policy, awareness and experience. Second, the institutional influence through constructs like subjective norms (perceptions of colleagues' expectations). Both factors significantly enhance employees' cybersecurity behaviour by fostering intrinsic or extrinsic motivation.

5.6.2 Finding Analysis

The study's findings regarding the influence of psychological factors on CCB are consistent with prior research by Ifinedo (2012) and Farooq et al. (2019). The role of self-efficacy and threat appraisal in cybersecurity decision-making and compliance has been highlighted by Kimpe et al. (2022) and Sulaiman et al. (2022). These studies underscore the significance of CCB formation as a proactive strategy to bolster employee cybersecurity behaviour in SA HEIs. Given the inherent openness of HEIs computer networks and the vulnerabilities of the internet, proactive measures are necessary to prevent cybersecurity incidents.

This study demonstrates how CCB emerges from an institution's cybersecurity environment, encompassing cybersecurity awareness training, established policies and opportunities to gain practical experience. This environment forms a foundation for employee CCB by equipping them with the knowledge and confidence to engage in secure practices. These findings offer valuable guidance for institutional leadership seeking to enhance CCB. Firstly, the pervasiveness of cyber threats underscores the importance of compliant behaviour in mitigating employee security risks. Secondly, the study reinforces the notion that technology alone cannot guarantee cybersecurity; a robust safeguard measure requires a combination of technological measures and a culture of CCB.

The study's adoption of the TPB and PMT theories, which are well-established in cybersecurity research, strengthens its contribution to the field. These frameworks illuminate how an institution's cybersecurity environment shapes employee behaviour. The findings supported the following hypotheses and addressed the research questions highlighted in section 1.5:

Institutional Cybersecurity Environment: This environment encompasses cybersecurity awareness, policy, and experience, as validated by H1, H2, and H3. Increased cybersecurity awareness has consistently positively impacted attitudes and CCB (Haeussinger & Kranz, 2013; Safa et al., 2015; Nifakos et al., 2021). This study's findings (H1) affirm this notion, indicating that a well-established institutional cybersecurity environment fosters intrinsic and extrinsic motivation, ultimately leading to enhanced CCB.

Similarly, effective cybersecurity policies play a significant role in shaping subjective norms and guiding employee perceptions of colleagues' expectations regarding cybersecurity behaviour, as supported by previous research (Cheng et al., 2013; Safa et al., 2015; Brown & Johnson, 2019; Nifakos et al., 2021). These findings underscore the role of explicit and well-communicated policies in fostering a security culture that provides a sense of security and guidance conducive to CCB.

Moreover, cybersecurity experience (H3) enhanced knowledge, boosting employee confidence in their ability to perform cybersecurity tasks effectively. This finding aligns with prior studies (Tøndel et al., 2014; Safa et al., 2015; Li et al., 2019) and echoes the importance of training programs that Khan et al. (2023) highlighted in developing confidence and skills for handling cybersecurity incidents.

Regarding H6, the study aligns with the core principles of the Theory of Planned Behaviour (TPB) (Ajzen, 1991), showing that Perceived Behavioural Control (PBC)—an individual's belief in their capability to perform cybersecurity behaviours—significantly influences CCB. This underscores that employees who perceive themselves as capable of performing CCB are more likely to engage in such behaviours, consistent with Safa et al.'s (2015) findings in cybersecurity research.

Psychological Factors: Hypotheses (H7) Self-efficacy and (H8b) Threat appraisal emerged as significant predictors of CCB, consistent with PMT's propositions (Rogers, 1975). This

suggests that employees with higher self-confidence (self-efficacy) in their cybersecurity skills and a heightened perception (threat appraisal) of cyber threats are more likely to engage in secure cybersecurity practices. These findings align with previous studies that emphasise the motivating effect of threat severity on adopting protective measures (Padayachee, 2012; Vance et al., 2012; Safa et al., 2015; Sommestad et al., 2015; Verkijika, 2018). As Sommestad et al. (2015) also posited, cybersecurity awareness campaigns can be tailored to highlight the potential consequences of cyberattacks to strengthen threat perception. Furthermore, self-efficacy also has a strong influence on CCB, reinforcing existing cybersecurity research underscoring the importance of self-confidence in cybersecurity decision-making and compliance (Warkentin et al., 2016; Li et al., 2019; De Kimpe et al., 2022; Sulaiman et al., 2022). Therefore, this indicates that employees who believe in their ability to perform safe cybersecurity practices are likelier to adopt such behaviours.

Also, H9 was supported and aligns with the research by Li et al. (2019), who found a significant relationship between policy awareness and CCB. These findings suggest that establishing a clear and accessible cybersecurity policy and ensuring employees are aware of the policy can contribute to positive employee cybersecurity beliefs and CCB. One potential mechanism for this effect might be that awareness increases employees' understanding of cybersecurity threats and the consequences of non-compliance, as recently highlighted (Zhang et al., 2021; Aldawood & Skinner, 2019). Further, it increases trust in the organisation's commitment to protecting information assets, as Yang et al. (2020) posited.

Subjective Norms (H5): Unexpectedly, the study found no significant impact between subjective norms (perceptions of colleagues' expectations) and CCB in SA HEIs. This finding partially contradicts previous research (Cheng et al., 2013; Safa et al., 2015) and differs from Garcia et al.'s (2020) study, highlighting social pressure's role in HEIs. Herein, perhaps social influence plays a less significant role, highlighting the need to explore alternative motivators for CCB. It is possible that other factors, such as coping appraisal variables (threat severity, anticipated regret), might hold more sway over employee cybersecurity behaviour in this specific environment (Tsai et al., 2016; Sommestad et al., 2015; Van Bavel et al., 2019).

Neither attitude nor response efficacy significantly impacted CCB. On attitude, this contradicts Safa et al.'s (2018) findings that employees aware of the policy generally reported more positive attitudes; it aligns with Menard et al.'s (2017) and could be attributed to limitations in

SA HEIs' cybersecurity efforts, as recent studies suggested. Ntloedibe et al. (2024) found that a lack of awareness training could hinder employees' understanding of cyber threats and best practices, weakening the link between attitude and cybersecurity behaviour. Similarly, Brown and Johnson (2019) identified a positive impact of stringent policy enforcement on user compliance. These findings suggest that SA HEIs can strengthen the relationships between these constructs and CCB by implementing targeted interventions, such as enhancing cybersecurity training programs and reviewing policy enforcement mechanisms.

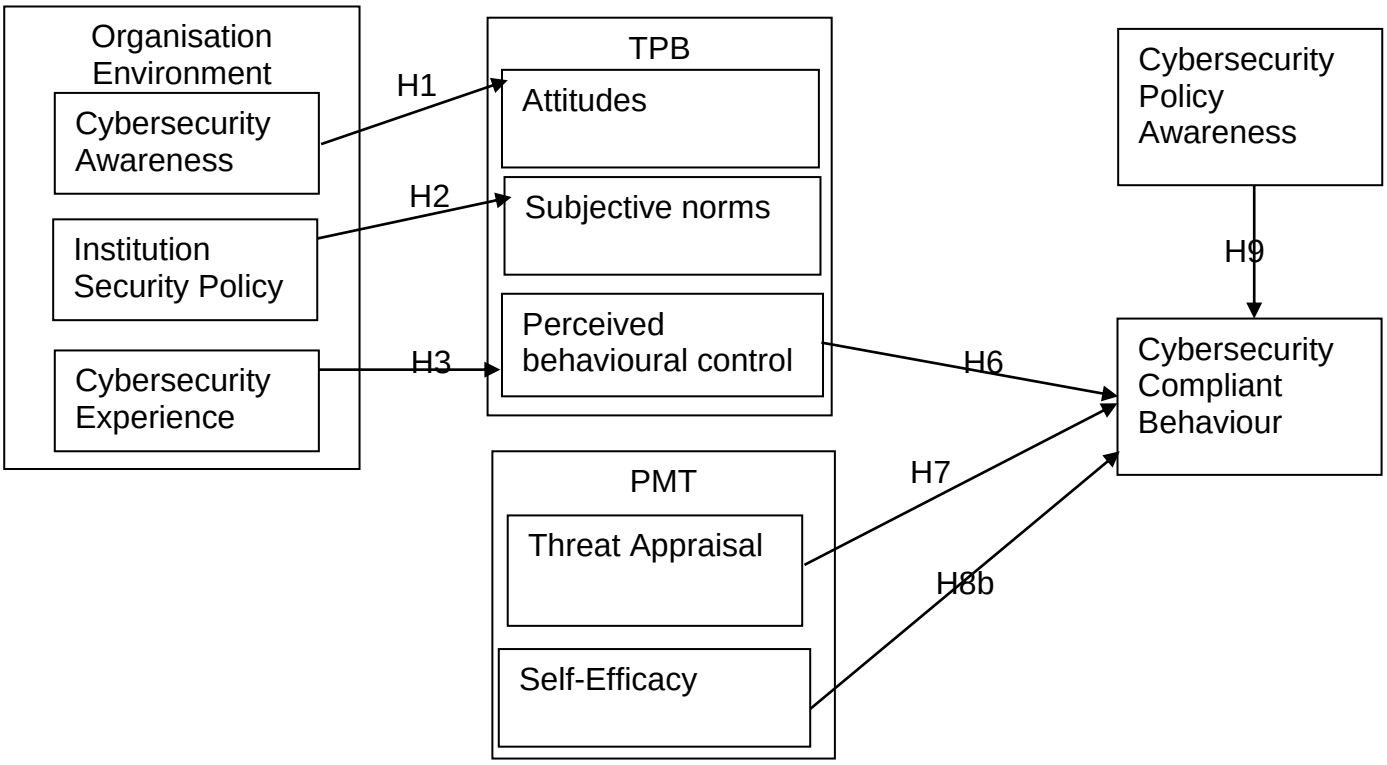

Figure 9: Validated Research Model

Key Findings

Figure 9 depicts the validated research model using data from employees in SA HEIs, with lines representing significant positive relationships between constructs (p-value < 0.05). The model validated the influence of institutional cybersecurity environment (awareness, policy, experience and policy awareness) and psychological factors (perceived behavioural control, threat appraisal and self-efficacy) on employee CCB.

Therefore, institution leaders should implement and deliver regular communications stressing the importance of cybersecurity breaches and the fact that such threats can lead to institutional

vulnerability and the disclosure of private information. Keeping employees updated on cybersecurity and increasing their knowledge in this domain significantly affects their behaviour. In addition, ensuring the availability of explicit cybersecurity policies and procedures is another effective approach to preventing cybersecurity breaches. Cybersecurity policies and procedures should be clear, concise, and accessible for all employees.

Connection to Framework

The positive outcomes of the measurement model assessment establish a strong foundation for further analysis. The established reliability and validity of the constructs ensure confidence in accurately representing the intended theoretical concepts. This aligns with the research objective of identifying factors influencing employee cybersecurity awareness and behaviour within SA HEIs.

Furthermore, the chosen constructs, such as cybersecurity awareness (CA), attitude (ATT), perceived behavioural control (PBC), self-efficacy (CSE), and threat appraisal (TA), directly correspond to the combined framework of the Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT). These theories posit that individuals' intentions to engage in specific behaviours, like cybersecurity-compliant behaviour (CCB), are influenced by their attitudes, subjective norms, perceived behavioural control, and threat appraisal.

The successful establishment of these constructs through the measurement model assessment demonstrates the potential of this research to contribute to the existing knowledge within the field of cybersecurity in SA HEIs. The study can shed light on their influence on employees' CCB by analysing the relationships between these constructs in the structural model. This aligns with the research objective of determining factors influencing employee cybersecurity awareness and behaviour.

5.7 CONCLUSION

This chapter analysed data collected from employees within the SA HEIs to explore the factors influencing employees' cybersecurity-compliant behaviour (CCB). The study adopted a novel framework integrating the TPB and PMT with an institution's cybersecurity environment concept, encompassing cybersecurity awareness, policy and experience.

The data analysis used PLS-SEM with bootstrapping, which yielded several key findings. The institutional cybersecurity environment, including awareness programs, established policies, and opportunities to gain experience, emerged as a significant factor influencing CCB. This environment not only equips employees with knowledge but also instils confidence in them to make secure choices, thereby empowering them in the realm of cybersecurity.

Furthermore, psychological factors such as self-efficacy (confidence in cybersecurity skills) and threat appraisal (perception of cyber threats) were identified as significant predictors of CCB. Employees with higher self-efficacy and a stronger perception of cyber threats are likelier to engage in CCB. Interestingly, the study found no significant relationship between subjective norms (perceptions of colleagues' expectations) and CCB in this context. This finding warrants further exploration to understand the influence of social dynamics within HEIs on employee cybersecurity behaviour.

Data analysis provides a foundation for understanding how various factors influence CCB amongst employees within the SA HEIs. These findings provided valuable guidance for SA HEIs in developing targeted interventions to strengthen their cybersecurity posture. By building a strong institutional cybersecurity environment, fostering employee self-efficacy and threat appraisal and exploring alternative social motivators, HEIs can create a culture of cybersecurity compliance and mitigate cyber risks.

6 CONCLUSIONS AND RECOMMENDATIONS

6.1 INTRODUCTION

The previous chapter rigorously analysed the study's data, presenting the results objectively and discussing the research findings and objectives to conclude the study. It comprehensively outlined the methodologies employed to achieve the research goals and objectives. Building upon the foundation laid by earlier chapters, which covered the introduction, literature review, methodology, and detailed data analysis, this chapter concludes with comprehensive discussions of the research's implications, limitations, and recommendations. The rest of the chapter is structured as follows:

Section 6.2 revisits the research objectives and questions, critically evaluating how they addressed the research purpose. Section 6.3 explores the research's contributions, detailing how the findings advance the understanding of information systems within South African (SA) higher education institutions (HEIs). Sections 6.4 and 6.5 delve into the implications for academic research and practical applications, establishing connections to the broader body of knowledge in information systems and their relevance to SA HEIs. Section 6.6 critically examines the limitations encountered during the research process, offering valuable insights and paving the way for future studies. Section 6.7 encapsulates the recommendations derived from the research findings, providing actionable insights for stakeholders in academia and beyond. Lastly, Section 6.8 offers a comprehensive report summary, summarising key findings, implications, and the significance of the study's contributions.

6.2 ADDRESSING RESEARCH OBJECTIVES AND QUESTIONS

The study's main objective was to investigate how cybersecurity awareness and related factors influence employee cybersecurity behaviour in SA HEIs, focusing on identifying effective strategies for enhancing cybersecurity measures (Section 1.4). The following were employed in this study to address the objective:

Creating a Conceptual Model: The study created a testable model that integrated two well-established cybersecurity research theories (TPB and PMT) with the concept of an institution's cybersecurity environment. The model examined how cybersecurity awareness, policy, and

experience within the institutional environment influence employee attitudes, subjective norms, perceived behavioural control, threat appraisal and self-efficacy, which lead to CCB.

Hypothesis Testing and Model Validation: PLS-SEM analysis validated and confirmed significant relationships between several constructs that lead to employees' CCB, supporting the proposed conceptual framework (see Section 5.1.2 and Figure 3). These findings offer insight into the multifaceted influences on employee CCB within SA HEIs and pave the way for addressing the research questions discussed below.

Main Research Question: How do cybersecurity awareness and other factors influence employee cybersecurity behaviour (CCB) in SA HEIs?
This study investigated the multifaceted influences of cybersecurity awareness and other factors on employee CCB in SA HEIs. The study identified factors from the institutional cybersecurity environment and PMT's and TPB's psychology factors that significantly impact employees' CCB. The below outlines how these factors impact CCB within the HEIs:

The Institutional Cybersecurity Environment
Cybersecurity Awareness (H1), the study found a positive relationship between cybersecurity awareness and employee CCB. This suggests that institutions offering effective awareness programs that equip employees with the knowledge and skills to identify and respond to cyber threats can ultimately influence their secure cybersecurity behaviour within the SA HEIs.

Cybersecurity Policies (H2): The study found a positive relationship between cybersecurity policies and CCB, indicating that defined policies enable employees to make informed security-related decisions. Therefore, having clear and accessible security policies establishes expectations and guidelines that guide employees' behaviour.

Cybersecurity Experience (H3): The study found a positive relationship between cybersecurity experience and CCB, suggesting that hands-on learning can contribute to more secure employee behaviour. This suggests that employees who gained practical experience through cybersecurity incidents or training exercises will likely develop a deeper understanding of cyber threats and their potential consequences.

Cybersecurity Policy Awareness (H9): Awareness of the institution's cybersecurity policies is crucial for ensuring cybersecurity compliance behaviour. The study confirmed a positive relationship between cybersecurity policy awareness and CCB, highlighting the importance of effective communication strategies to ensure employees remain informed about these policies.

Psychological Factors (TPB & PMT)

Perceived Behavioural Control (H6): This factor refers to employees' belief in their ability to perform specific cybersecurity behaviours. The study shows a positive relationship between perceived behavioural control and CCB. Thus, when employees are confident in their ability to handle cybersecurity incidents, they are more likely to engage in secure practices. Threat Appraisal (H7): Employees' perception of the severity and likelihood of cyber threats can influence their behaviour. The study found a positive correlation between threat appraisal and CCB. Thus, employees who are cognisant of and recognise the potential consequences of cyberattacks are likelier to embrace secure practices to mitigate these risks.

Self-efficacy (H8b) refers to employees' confidence in their cybersecurity skills and abilities. This study found a positive relationship between self-efficacy and CCB. Employees who believe in their ability to handle cybersecurity challenges are more likely to exhibit secure behaviour.

Addressing Sub-questions

RSQ1: What cybersecurity awareness programs are currently available in SA HEIs? This study investigates the programs offered, and the findings support the importance of such programs in fostering positive attitudes towards CCB. This is validated by hypothesis (H1), which suggests that increased awareness leads to positive attitudes towards CCB and strengthens the argument for investigating the effectiveness of these programs.

As the study's scope does not focus on designing and exploring the specific programs offered in SA HEIs, the findings provide valuable insights into program design effectiveness and inform future research in developing more impactful cybersecurity awareness initiatives. For example, surveying IT security personnel or interviewing employees can be a starting point.

RSQ2: How can current employee cybersecurity awareness levels in SA HEIs be effectively measured?

This study focused on factors influencing employee CCB, highlighting the importance of effective cybersecurity awareness programs (H1) and employee cybersecurity policies awareness (H9). These findings highlight the importance of improving current employees' awareness levels within SA HEIs. Future research can gain valuable insights into the effectiveness of existing programs and identify areas for enhancement by focusing on measuring these awareness levels. For example, developing and applying standardised surveys that focus on assessing cybersecurity knowledge could provide a basis for evaluating the effectiveness of current programs that inform the design of future interventions to improve employee CCB.

RSQ3: What factors influence employees' cybersecurity awareness and behaviour in SA HEIs?

The findings revealed that the institutional cybersecurity environment and psychological factors significantly influence employees' CCB. This environment, encompassing cybersecurity awareness programs (H1), clearly defined security policies (H2) and policy awareness (H9), and cybersecurity experience (H3), fosters positive CCB. Likewise, PMT and TPB psychological factors, including perceived behavioural control (H6), heightened threat appraisal (H7), and strong self-efficacy (H8b), also directly and significantly influence employee CCB.

RSQ4: What challenges impede the effectiveness of cybersecurity awareness programs and practices in SA HEIs?

The study addresses important gaps in current cybersecurity strategies by exploring the challenges impeding the effectiveness of cybersecurity awareness programs and practices in SA HEIs. The findings related to subjective norms (H5), attitude (H4) and response efficacy (H8a) indicate that there are challenges in motivating employees to adopt secure practices due to limitations in existing cybersecurity approaches within SA HEIs. Thus, these necessitate alternative factors and interventions to improve the effectiveness of cybersecurity awareness programs. Future research can gain valuable insights into how SA HEIs can enhance their cybersecurity posture by addressing the identified issues and focusing on the identified challenges.

The study's findings provide valuable insights into the multifaceted nature of employee CCB in SA HEIs. Institutions can significantly improve their cybersecurity posture by implementing a

comprehensive approach that addresses the identified factors and explores opportunities for improvement in cybersecurity awareness programs and practices.

6.2.1 Key Finding Summary

The study's key findings contribute to a deeper understanding of employees' CCB in SA HEIs, directly addressing the research objectives:

- **Institutional Cybersecurity Environment:** This study highlights the importance of a robust institutional cybersecurity environment and structure, including policy, awareness training and opportunities to gain practical experience (Section 1.1 & 5.1.2). These factors equip employees with the knowledge and confidence to engage in secure practices. The data analysis showed that cybersecurity awareness, policy awareness and experience positively influence CCB, underscoring institutions' critical role in shaping employee cybersecurity-related behaviour (Section 5.1.2).
- **Psychological Factors:** This study shows consistencies with previous research by demonstrating the influence of psychological factors like self-efficacy and threat appraisal on CCB (Ifinedo, 2012; Farooq et al., 2019; De Kimpe et al., 2022; Sulaiman et al., 2022). As hypothesised (see Table 4), employees with an elevated perception of cyber threats and greater self-belief in their ability to perform secure actions were likelier to exhibit CCB (see Section 5.1.2).
- **Subjective Norms and Response Efficacy:** The result did not find a significant impact of subjective norms (perceptions of colleagues' expectations) on CCB in SA HEIs, as response efficacy (perceived ease of performing desired cybersecurity behaviours) did not significantly influence CCB (Section 5.1.2). These findings suggest that social influence and confidence in the effectiveness of specific actions play a less prominent role in this context relative to other factors. Future studies are required to explore alternative motivators for CCB in SA HEIs.
- These findings improve understanding of employee CCB in SA HEIs and further inform the development of effective strategies to enhance employee cybersecurity behaviour.

6.3 CONTRIBUTIONS

This study contributes to the cybersecurity research in SA HEIs and the information systems body of knowledge by:

Providing a comprehensive model: The study developed a model that integrated PMT and TPB with factors found within the institutional cybersecurity environment and offers a holistic understanding by identifying five key factors that influence employees' CCB. This framework is valuable for researchers and institutions seeking to improve their cybersecurity structure by providing a data-driven approach to understanding and achieving employee behaviour.

Validating the influence of key factors: This study demonstrates and validates the importance of psychological factors such as perceived behavioural control, threat appraisal and self-efficacy and the institutional cybersecurity environment (i.e., cybersecurity awareness, policy awareness and experience) in shaping employees' CCB. This acquired knowledge informs the development of targeted interventions, including training programs that focus on building self-efficacy and threat awareness, to improve employees' behaviours regarding cybersecurity issues.

Identifying areas for further exploration: Some results regarding subjective norms and response efficacy establish a need for further studies to inquire into alternative motivators beyond social pressure and how institutions can improve the perceived effectiveness of their cybersecurity efforts. Exploring the influence of organisational culture on CCB could also be a valuable area for future investigation.

6.4 IMPLICATION FOR RESEARCH

This study makes three significant contributions to cybersecurity research. Firstly, it proposed a conceptual framework that integrates the institution's cybersecurity environment with TPB and PMT to validate the relationships among cybersecurity awareness, policy, employees' cybersecurity experience, attitude, subjective norms, perceived behavioural control, threat appraisal, self-efficacy, response efficacy and cybersecurity-compliant behaviour.

The results confirm several key findings: (a) cybersecurity awareness significantly enhances employees' positive attitudes towards cybercrimes; (b) cybersecurity policies serve as a guide for employees, establishing subjective norms within institutions; (c) employees' cybersecurity experience positively affects their perceived behavioural control, influencing their cybersecurity-compliant behaviour. These findings validate previous research regarding the factors that motivate employees to comply with cybersecurity policy in the workplace, aligning with the nature of cybersecurity motivation for risk mitigation and threat reduction.

Secondly, this study acknowledges and contributes to addressing the inconsistencies and limitations identified in previous research. For instance, Zahedi et al. (2015) highlighted response efficacy as the primary coping factor, contrasting with Warkentin et al.'s (2016) emphasis on self-efficacy. In addition, studies have reported varying results with PMT, often citing a lack of moderating constructs (Schuetz et al., 2020) and identified inadequacies in certain TPB factors (Karlsson et al., 2018; Sommestad et al., 2019). This study extends traditional TPB and PMT frameworks by introducing the concept of 'institutional cybersecurity' as a determinant influencing employee behaviour to address these gaps.

Third, this study proposes that some ambiguous results involving TPB/PMT and cybersecurity may be due to the exclusive use of behavioural intention or likelihood of future behaviour as the criterion measure. While using behavioural intention is reasonable in research aiming to change employee behaviour, the relationship among variables that affect intentions may differ from those that determine current beliefs and behaviours. Thus, this study assesses employees' current cybersecurity behaviour by asking them to self-report their engagement in specific behavioural activities, noting that accounts of behaviour are subject to biases (Vance et al., 2014). This approach provides a view of the relationship between concurrent beliefs and actions, which researchers and institutions can employ to develop interventions and policies (Chowdhury et al., 2020).

Lastly, this study investigates the relationship between employees' cybersecurity policy awareness and perceptions of the institution's cybersecurity environment. This includes cybersecurity awareness, policy, experience, attitudes, subjective norms, perceived behavioural control, threat appraisal, self-efficacy, response efficacy and CCB. The results offer a new dimension to evaluating employees' CCB, potentially extending previous research in workplaces and employee belief factors. Specifically, the results indicate that when

employees are aware of their institution's policy, they are better equipped to cope with cybersecurity incidents in the workplace.

6.5 IMPLICATION FOR PRACTICE

Building upon the study's findings, which directly addressed the research objective, this section offers practical guidance for SA HEIs seeking to enhance employees' CCB. The proposition of a more holistic approach towards cybersecurity management offers contributions applicable to managing employees' security behaviour that go beyond just theory. Cybersecurity issues are increasingly pivotal challenges for many organisations despite the advancements in cybersecurity technology (Li et al., 2019; Whitman & Mattord, 2018). This highlights the importance of successful cybersecurity policy implementation and organisational strategies as the foundation for successfully implementing technological solutions (Ponemon Institute, 2018; McCormac et al., 2017).

Institutions should consider cybersecurity a top management issue, elevating it to strategic and priority levels. This ensures cybersecurity responsibility is institution-wide (i.e., all employees are involved) and not just the technical responsibility of technical or cybersecurity/information officers. As reported in this study (see section 4.4), the significant difference in security behaviour between employees aware and unaware of cybersecurity policies highlights institutional management's need for proactive measures. These measures include:

- **Support from Top Management and Involvement:** Top management support and involvement in cybersecurity policy implementation are key to success. Employees often follow cues and gain awareness from regular cybersecurity awareness programs, especially when mandatory and monitored at the management level. Thus, a digitally secure workplace starts with a well-defined cybersecurity policy and awareness program championed and monitored by management.
- **Regular Security Awareness Programs:** Institutions should implement periodic and regular (annually, quarterly or needs-driven) cybersecurity awareness programs to cultivate positive employee attitudes toward cybersecurity. These programs can be particularly beneficial for those who may have overlooked or disregarded such policies.

- **User-Friendly Security Materials:** Cybersecurity procedures, guidelines, and policies should be written concisely and user-friendly to ensure comprehension and compliance by all employees, regardless of technical background.
- **Ongoing Communication and Reminders:** Regular communication is key. Institutions should regularly disseminate information security tips, advice, and reminders to keep employees engaged and motivated to practice secure behaviours.
- **Supportive Learning Environment:** Creating an effectively supportive institutional cybersecurity environment is essential as it offers opportunities for employees to gain exposure to emerging security technologies and develop their cybersecurity skills and knowledge (Caldwell, 2013; Jeske & van Schaik, 2017).
- **Monitoring and Improvement:** As over 41% of employees confirmed their institutions have a cybersecurity policy, 47% were unsure. This highlights a potential gap in policy communication or accessibility. Therefore, HEIs must prioritise effective communication strategies and continuously monitor the effectiveness of their awareness programs. By bridging the gap between policy-aware and unaware employees through ongoing improvement, institutions can create a more secure environment.

Additional Considerations

Interestingly, the study's data reveals that employee education level does not significantly impact their awareness of cybersecurity policies. This positive finding may be attributed to the guidelines the POPI Act set forth, which informs and ensures a policy communication baseline level across all staff regardless of educational background. This highlights the importance of clear, well-defined and consistently communicated cybersecurity policies for effective cybersecurity awareness, which HEIs can leverage and maintain to cultivate positive employee cybersecurity behaviour and ultimately foster a more secure institution technology environment. Further, following the comprehensive approach, this study outlines and addresses the institutional cybersecurity environment and psychological factors. Institutions can bolster positive employee cybersecurity behaviour and strengthen the overall cybersecurity structure of institutions.

6.6 STUDY LIMITATIONS AND SUGGESTIONS FOR FUTURE WORKS

This study successfully addressed its research objectives but experienced some limitations that offer valuable insights for future research, which include:

Measurement Limitations:

- **Self-reported Behaviour:** The study employed self-reported cybersecurity behaviour as the primary measure, which is susceptible to self-report bias. Future research should explore methods to capture actual cybersecurity actions rather than relying solely on self-reported behaviour (although many studies have used this approach successfully).

Timeframe Limitations:

- The study's cross-sectional design limits the establishment of causal relationships due to the time constraint. Further research using longitudinal studies could explore how policy awareness or training program changes might impact CCB over time.

Generalisability Limitations:

- **Context Specificity:** The study focused exclusively on SA HEIs. Future research can investigate the role of cybersecurity behaviour in broader contexts, including social networks, community structures, and their evolution (Kapoor et al., 2018).

Future Research Opportunities:

- **Motivating Policy Compliance:** While the study identified employee awareness of cybersecurity programs as influential, it did not explore procedures for motivating employees to learn and implement cybersecurity policies. One potential area of future research is developing employee cybersecurity awareness programs and creating feasible procedures to enhance policy implementation.
- **Mixed-Methods Approach:** This study employed a quantitative approach, limiting the capture of employee voices. Future research could benefit from adopting mixed methods, collecting quantitative and qualitative data from multiple sources (e.g., surveys and interviews) to achieve triangulation and enhance reliability and validity.
- **Framework Validation:** The developed conceptual framework could be further validated by applying it to multiple case studies and including a larger, more diverse group of research participants from various contexts. This would strengthen the generalisability and validity of the research findings.
- **User Behaviour and Ethics:** The study highlights the importance of employee behaviour in safeguarding institutional cybersecurity. Future research could delve deeper into the role of user behaviour and ethical conduct in cyberspace. While humans play a central role in cybersecurity, this study did not quantify their specific level of

influence. Future investigations could explore other factors influencing CCB within the workplace.

6.7 RECOMMENDATIONS

Cybersecurity research offers opportunities for collaboration and knowledge sharing within the community of cybersecurity professionals in SA HEIs rather than just individual pursuits. Thus, researchers, institutions and government entities should collaborate to address several areas that warrant future investigations, which include but are not limited to:

1. **Applicability in Broader contexts**: Conduct similar studies at different institutions to explore and ascertain the applicability of this study's findings across various SA HEIs. Obtaining and comparing results across diverse contexts can validate the robustness of identified factors influencing cybersecurity behaviour.
2. **Institutional Culture**: Investigating the institutions' cultural influence on employees' cybersecurity behaviour can illuminate how institutional norms, values, and practices shape cybersecurity attitudes and practices, which can inform tailored interventions to foster a cybersecurity-conscious culture.
3. **Longitudinal Research**: Conducting longitudinal research to capture changes in cybersecurity behaviour over a long period can track the effectiveness of cybersecurity awareness programs and policies longitudinally and provide insights into their sustainability and long-term impact on employee behaviour.
4. **Specified Interventions**: Designing and evaluating targeted cybersecurity training interventions based on the identified factors influencing cybersecurity behaviour can assess their effectiveness in improving employees' cybersecurity awareness and practices and guide the development of evidence-based training programmes.
5. **Comparative Analysis**: Comparing the effectiveness of different cybersecurity awareness programs and policies across SA HEIs can identify best practices and lessons from successful implementations, which can inform policy development and enhance cybersecurity measures.
6. **Technological Approach**: Investigating the role of technological measures, tools, and solutions in influencing employees' cybersecurity behaviour can provide insights into enhancing the technical aspects of cybersecurity within institutions.

6.8 CONCLUSION

This study has comprehensively investigated the factors influencing employees' cybersecurity behaviour in SA HEIs. The study's framework enhances our understanding of CCB within SA HEIs by integrating established theories with institutional cybersecurity environments. The findings underscore the critical role of these environments and contribute to the IS body of knowledge by identifying key institutional and psychological factors impacting CCB. The validated conceptual model provides a holistic view of these relationships, offering valuable insights for researchers and institutions aiming to strengthen their cybersecurity frameworks.

The study's limitations and recommendations for future research highlight areas for further exploration and development aimed at enhancing cybersecurity effectiveness within SA HEIs. Fostering a robust cybersecurity environment within SA HEIs is crucial. Therefore, empowering employees through targeted interventions like awareness training, transparent policies, and practical experience opportunities can help mitigate cybersecurity risks. These strategies align with recommendations from previous research and contribute to a broader effort to enhance cybersecurity across organisations. Lastly, this research advances the researcher's understanding of CCB in SA HEIs. It provides practical guidance for institutional leadership seeking to foster a more secure digital environment, ultimately contributing to a more secure cyberspace for HEIs and beyond.

7 REFERENCES

Abdel-Aziz, A. A., Abdel-Salam, H., & El-Sayad, Z. (2016). The role of ICTs in creating the new social public place of the digital era. *Alexandria Engineering Journal*, *55*(1), 487–493. https://doi.org/10.1016/j.aej.2015.12.019

Accenture. (2024). N/A. Retrieved from https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa

Administrator, T. (n.d.). Important Notice Regarding TUT Cyber Security Incident. Retrieved from https://www.tut.ac.za/index.php/cyber-security-incident

Aguinis, H., & Vandenberg, R. J. (2014). An Ounce of Prevention Is Worth a Pound of Cure: Improving Research Quality before Data Collection. *Annual Review of Organizational Psychology and Organizational Behavior*. Annual Reviews Inc. https://doi.org/10.1146/annurev-orgpsych-031413-091231

Ajzen, I. (1991). The theory of planned behavior. *Organisational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology and Health*. https://doi.org/10.1080/08870446.2011.613995

Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, *2*(4), 314–324. https://doi.org/10.1002/hbe2.195

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Future Internet*. MDPI AG. https://doi.org/10.3390/fi11030073

Al-Emran, M., Mezhuyev, V., & Kamaludin, A. (2019). PLS-SEM in Information Systems Research: A Comprehensive Methodological Reference. In *Advances in Intelligent Systems and Computing* (Vol. 845, pp. 644–653). Springer Verlag. https://doi.org/10.1007/978-3-319-99010-1_59

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Applied Sciences (Switzerland)*. MDPI. https://doi.org/10.3390/app13095700

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information (Switzerland)*, *11*(2). https://doi.org/10.3390/info11020121

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers and Security*, *98*. https://doi.org/10.1016/j.cose.2020.102003

Alsmadi, D., Maqousi, A., & Abuhussein, T. (2022). Engaging in cybersecurity proactive behavior: awareness in COVID-19 age. *Kybernetes*. https://doi.org/10.1108/K-08-2022-1104

Alsmadi, D., Maqousi, A., & Abuhussein, T. (2022). Engaging in cybersecurity proactive behavior: awareness in COVID-19 age. *Kybernetes*. https://doi.org/10.1108/K-08-2022-1104

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 613–643. https://doi.org/10.2307/25750694

Anderson, S. F. (2019). Best (but oft forgotten) practices: Sample size planning for powerful studies. *American Journal of Clinical Nutrition*, *110*(2), 280–295. https://doi.org/10.1093/ajcn/nqz058

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and Employees' Differing Responses to Security Approaches. *Journal of Computer Information Systems*, *59*(3), 197–210. https://doi.org/10.1080/08874417.2017.1318687

Bhagattjee, P., Govuza, A., & Westcott, R. (2021). Regulating the Fourth Industrial Revolution - South Africa's Cybercrimes Bill is signed into law. Cliffe Dekker Hof meyr.

Bhattacherjee, A. (2012). *Social Science Research: principles, methods, and practices*. *Book 3.* (pp. 1–147). Florida: University of South Florida. Retrieved from http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, 87–97. https://doi.org/10.1016/j.chb.2018.05.023

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers and Security*, *86*, 350–357. https://doi.org/10.1016/j.cose.2019.07.003

Boone, H. N., & Boone, D. A. (2012). Analyzing Likert data. *Journal of Extension*, *50*(2). https://doi.org/10.34068/joe.50.02.48

Bryman, A., & Bell, E. (2015). Business research methods: Oxford University Press. *American Journal of Sociology*.

Bryman, A., Clark, T., Foster, L., & Sloan, L. (2021). Bryman's Social Research Methods. *Oxford*, 670. Retrieved from https://books.google.com/books/about/Bryman_s_Social_Research_Methods.html?hl=nl&id=QJg5EAAAQBAJ

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Quarterly Special Issue Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness1. Source: MIS Quarterly (Vol. 34, p. 39).

Cascio Ramiro, W. & M. (2016). How Technology Is Changing Work and Organisations. Annual Review of Organizational Psychology and Organizational Behavior. 3. 349-375. *ResearchGate*. Retrieved from https://www.researchgate.net/publication/299400943_How_Technology_Is_Changing_Work_and_Organizations http://files/88/299400943_How_Technology_Is_Changing_Work_and_Organizations.html

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

Charandura, K. (2022). Cybersecurity in the Education Industry. Retrieved from https://www.grantthornton.co.za/Newsroom/cybersecurity-in-the-education-industry/

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information and Management*, *55*(8), 1049–1060. https://doi.org/10.1016/j.im.2018.05.011

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Information (Switzerland), 13(4). https://doi.org/10.3390/info13040192

Chigada, J. (2023). Towards an aligned South African national cybersecurity policy framework.

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. Computers and Security, 97. https://doi.org/10.1016/j.cose.2020.101931'

Clark, M. A., Espinosa, J. A., & DeLone, W. H. (2020). Defending organizational assets: A preliminary framework for cybersecurity success and knowledge alignment. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (Vol. 2020-January, pp. 4283–4292). IEEE Computer Society. https://doi.org/10.24251/hicss.2020.524

Coman, C., Țîru, L. G., Meseșan-Schmitz, L., Stanciu, C., & Bularca, M. C. (2020). Online teaching and learning in higher education during the coronavirus pandemic: Students' perspective. *Sustainability (Switzerland)*, *12*(24), 1–22. https://doi.org/10.3390/su122410367

Costa, L. P. da S., & Figueira, A. C. R. (2016). Risco político e internacionalização de empresas: uma revisão bibliográfica Political risk and companies' internationalization: a literature review. *Cad. EBAPE.BR*, *10*(4), 75–99. Retrieved from http://www.scielo.br/pdf/cebape/v15n1/1679-3951-cebape-15-01-00063.pdf%0Ahttp://dx.doi.org/10.1590/1679-395156933

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers and Security*, *48*, 281–297. https://doi.org/10.1016/j.cose.2014.11.002

Darvell, M. J., Walsh, S. P., & White, K. M. (2011). Facebook tells me so: Applying the theory of planned behavior to understand partner-monitoring behavior on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *14*(12), 717–722. https://doi.org/10.1089/cyber.2011.0035

De Bruyn, M. (2014). The Protection Of Personal Information (POPI) Act - Impact On South Africa. *International Business & Economics Research Journal (IBER)*, *13*(6), 1315. https://doi.org/10.19030/iber.v13i6.8922

De', R. K., Pandey, N., & Pal, A. (2020). Virtual classrooms in times of COVID-19: A review of the literature. International Journal of Educational Research Open, 1, 100011. doi: 10.1016/j.ijedro.2020.100011

Department of Justice and Constitutional Development. (2013). Protection of Personal Information Act 4 of 2013. Pretoria, South Africa: Government Printer. (n.d.). Retrieved 24 April 2023, from https://www.gov.za/documents/protection-personal-information-act

Dhawan, S. M., Gupta, B. M., & Elango, B. (2021). Global Cyber Security Research Output (1998–2019): A Scientometric Analysis. *Science and Technology Libraries*, *40*(2), 172–189. https://doi.org/10.1080/0194262X.2020.1840487

DTPS. (2017). *National e-Government Strategy and Roadmap*. *Government Gazette* (p. 84). Government Printing Works.

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior ever follows intention?: A validation of the Security Behavior Intentions Scale (SeBIS). In *Conference on Human Factors in Computing Systems – Proceedings* Field, A. P. (2018). Discovering (pp. 5257–5261). Association for Computing Machinery. https://doi.org/10.1145/2858036.2858265

Ehiane, S. O., Olofinbiyi, S. A., & Mkhize, S. M. (2023). *Cybercrime and challenges in South Africa*. *Cybercrime and Challenges in South Africa* (pp. 1–240). Springer Nature. https://doi.org/10.1007/978-981-99-3057-9

Eltahir, M. E., & Ahmed, O. S. (2023). Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan. Information Sciences Letters, 12(1), 171–183. https://doi.org/10.18576/isl/120113

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers and Security*, *80*, 74–89. https://doi.org/10.1016/j.cose.2018.09.002

Farheen Ansari, M. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *International Research Journal of Engineering and Technology (IRJET)*, *9*(4), 1–6. Retrieved from www.irjet.net

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. In *Journal of Physics: Conference Series* (Vol. 1339). Institute of Physics Publishing. https://doi.org/10.1088/1742-6596/1339/1/012098

Field, A. P. (2018). Discovering statistics using IBM SPSS statistics: 5th edition. *SAGE Publications, Inc.* Retrieved from http://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf

Fonseca, R. S., & van Wyk, J. A. (2021). Cybersecurity in South Africa: Status, governance, and prospects. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 591–607). Taylor and Francis Inc.

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Furnell, S., & Shah, J. N. (2020). Home working and cyber security – an outbreak of unpreparedness? Computer Fraud & Security, 2020(8), 6–12. https://doi.org/10.1016/s1361-3723(20)30084-1

Giovannella, C. (2021). Effect induced by the covid-19 pandemic on students' perception about technologies and distance learning. In Smart Innovation, Systems and Technologies (Vol. 197, pp. 105–116). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-15-7383-5_9

Goddard, W., & Melville, S. (2004). *Research methodology: An introduction*. Juta and Company Ltd.

Govender, P. (2024). Tshwane University of Technology suffered massive data breach after its computer systems were hacked. Retrieved from https://www.news24.com/news24/southafrica/news/tshwane-university-of-technology-suffered-massive-data-breach-after-its-computer-systems-were-hacked-20240212

Hair Jr., J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)*. *SAGE Publications, Inc.* (p. 385).

Hair Jr., J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017b). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107. https://doi.org/10.1504/ijmda.2017.10008574

Hair, Sarstedt, M., Matthews, L. M., & Ringle, C. M. (2016b). Identifying and Treating Unobserved Heterogeneity with FIMIX-PLS: part I – Method. *European Business Review*, *28*(1), 63–76.

Hair. (2017). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Thousand Oaks. *Sage*, 165.

Haleem, A., Javaid, M., Qadri, M. A., & Suman, R. (2022). Understanding the role of digital technologies in education: A review. *Sustainable Operations and Computers*, *3*, 275–285. https://doi.org/10.1016/j.susoc.2022.05.004

Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. Computers and Security, 87. https://doi.org/10.1016/j.cose.2019.101594

Hoxha, A. (2021). Culture of Security: An interdisciplinary analysis of the potential risks, threats, safety, and behavior, in the realm of cybersecurity for private users of the BankID-system.

Ince, L. P. (1976). How Behavior Means. *American Journal of Psychotherapy*, *30*(3), 501–502. https://doi.org/10.1176/appi.psychotherapy.1976.30.3.501a

Institute, P. (2020). 2020 Cost of Insider Threats. *Available Online: Https://Www.Observeit.Com/Costof- Insider-Threats*.

Iriqat, Y. M., Ahlan, A. R., & Molok, N. N. A. (2019). Information security policy perceived compliance among staff in palestine universities: An empirical pilot study. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT 2019 – Proceedings* (pp. 580–585). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JEEIT.2019.8717438

ITU. (2020). *Global Cybersecurity Index 2020 - Measuring commitment to cybersecurity*. *ITU Publications* (p. 78). Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITUPublications. (2020). *Global Cybersecurity Index 2020*. *itu.int*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Jaeger, L. (2018). Information security awareness: Literature review and integrative framework. In Proceedings of the Annual Hawaii International Conference on System Sciences (Vol. 2018-January, pp. 4703–4712). IEEE Computer Society. https://doi.org/10.24251/hicss.2018.593

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research*, *22*(1). https://doi.org/10.2196/16775

Jalali, M., Bruckes, M., Westmattelmann, D., & Schewe, G. (2019). Why Employees (Still) Click on Phishing Links: An Investigation in Hospitals. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3317498

Johl, C., Flowerday, S., & Von Solms, R. V. S. (2016). INFORMATION TECHNOLOGY GOVERNANCE PROCESS MATURITY IN HIGHER EDUCATION INSTITUTIONS IN SOUTH AFRICA. South African Journal of Higher Education, 27(3). https://doi.org/10.20853/27-3-268

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, /*28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kadir, M. R. A., Norman, S. N. S., Rahman, S. A., Ahmad, A. R., & Bunawan, A. A. (2016). Information security policies compliance among employees in Cybersecurity Malaysia. In *Proceedings of the 28th International Business Information Management Association Conference - Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth* (pp. 2419–2430). International Business Information Management Association, IBIMA.

Kearns, G. (2015). Countering mobile device threats: A mobile device security model. Journal of Forensic & Investigative Accounting, 8(1), 157–167. Retrieved from http://www.nacva.com/jfia

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

Khatib, R., & Barki, H. (2022). How different rewards tend to influence employee non-compliance with information security policies. *Information and Computer Security*, *30*(1), 97–116. https://doi.org/10.1108/ICS-01-2021-0008

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, *8*, 125140–125148. https://doi.org/10.1109/ACCESS.2020.3007867

Kruger, H. A., Drevin, L., Flowerday, S., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. In *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*. https://doi.org/10.1109/ISSA.2011.6027505

Kumar, P., & Nanda, P. (2020). Digital transformation in higher education: A review of the literature. Journal of Education and e-Learning research, 7(2), 123-132. doi: 10.20448/journal.509.2020.72.123.132

Kumar, V., & Reinartz, W. (2016). Creating enduring customer value. *Journal of Marketing*, *80*(6), 36–68. https://doi.org/10.1509/jm.15.0414

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 2978–2987). https://doi.org/10.1109/HICSS.2013.192

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

Lee, C. S., & Kim, D. (2023). Pathways to Cybersecurity Awareness and Protection Behaviors in South Korea. *Journal of Computer Information Systems*, *63*(1), 94–106. https://doi.org/10.1080/08874417.2022.2031347

Lee, D., Lallie, H. S., & Michaelides, N. (2023). The impact of an employee's psychological contract breach on compliance with information security policies: intrinsic and extrinsic motivation. *Cognition, Technology and Work*, *25*(2–3), 273–289. https://doi.org/10.1007/s10111-023-00727-5

Lee, H., & Lim, H. (2019). Awareness and Perception of Cybercrimes and Cybercriminals. The International Journal of Cybersecurity Intelligence and Cybercrime, 2(1), 1–3. https://doi.org/10.52306/02010119uyib64

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives′ decision to adopt antimalware software. *European Journal of Information Systems*, *18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, *24*(6), 479–502. https://doi.org/10.1111/isj.12037

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, pp. *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, *30*(2), 255–279. https://doi.org/10.1108/ICS-06-2021-0091

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150. https://doi.org/10.1016/j.chb.2018.11.002

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

McIlwraith, A. (2021). Information security and employee behaviour: How to reduce risk through employee education, training and awareness. *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness* (pp. 1–195). Taylor and Francis. https://doi.org/10.4324/9780429281785

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers and Security*, *75*, 147–166. https://doi.org/10.1016/j.cose.2018.01.020

Miraja, B. A., Persada, S. F., Prasetyo, Y. T., Belgiawan, P. F., & Redi, A. A. N. P. (2019). Applying protection motivation theory to understand Generation Z students intention to comply with educational software anti piracy law. *International Journal of Emerging Technologies in Learning*, *14*(18), 39–52. https://doi.org/10.3991/ijet.v14i18.10973

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2). https://doi.org/10.3390/s22020538

Mitrovic, Z., Thakur, C., & Palhad, S. (2023). Towards Building Cybersecurity Culture in TVET Colleges in South Africa. In *2023 IST-Africa Conference, IST-Africa 2023*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.23919/IST-Africa60249.2023.10187852

Mogoane, S. N., & Kabanda, S. (2019). Challenges in Information and Cybersecurity program offering at Higher Education Institutions (Vol. 12, pp. 202–190). EasyChair. https://doi.org/10.29007/nptx

Morilla-Luchena, A., Munoz-Moreno, J. L., Chaves-Montero, A., & Vazquez-Aguado, O. (2021). Virtual education during the COVID-19 pandemic: A qualitative study of students' experiences. International Journal of Educational Research Open, 2, 100025. doi: 10.1016/j.ijedro.2021.100025

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach. *Journal of the Association for Information Systems*, *23*(1), 196–236. https://doi.org/10.17705/1jais.00723

Nagle, T., & Pope, A. (2013). Understanding social media business value, a prerequisite for social media selection. *Journal of Decision Systems*, *22*(4), 283–297. https://doi.org/10.1080/12460125.2014.846543

Nasir, A., Abdullah Arshah, R., & Rashid Ab Hamid, M. (2018). The Significance of Main Constructs of Theory of Planned Behavior in Recent Information Security Policy Compliance Behavior Study: A Comparison among Top Three Behavioral Theories. *International Journal of Engineering & Technology*, *7*(2.29), 737. https://doi.org/10.14419/ijet.v7i2.29.14008

NCPF. (2015). The National Cybersecurity Policy Framework (NCPF) For South Africa - 2015. *Government Gazette*, (39475), 1–30. Retrieved from http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf

Ncubukezit, T. (2022). Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. International Conference on Cyber Warfare and Security, 17(1), 395–403. https://doi.org/10.34190/iccws.17.1.51

Ng, W. (2015). *New Digital Technology in Education*. *New Digital Technology in Education*. Springer International Publishing. https://doi.org/10.1007/978-3-319-05822-1

Ngulube, P. (Ed.). (2021). *Handbook of research on mixed methods research in information science*. IGI Global.
Ntloedibe, T., Foko, T., & Segooa, M. A. (2024). Cloud leakage in higher education in South Africa: A case of University of Technology. *South African Journal of Information Management*, *26*(1), 10.
Oates, B. J. (2006). *Researching Information Systems and Computing.* London: SAGE Publications Ltd.
Odun-Ayo, I., Alagbe, O., & Yahaya, J. (2021). A systematic mapping study of security, trust and privacy in clouds. *Bulletin of Electrical Engineering and Informatics*, *10*(3), 1598–1610. https://doi.org/10.11591/eei.v10i3.1887
Öłütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002
Park, Y. S., Konge, L., & Artino, A. R. (2020). The Positivism Paradigm of Research. *Academic Medicine*. Lippincott Williams and Wilkins. https://doi.org/10.1097/ACM.0000000000003093
PEDIAA. (2017). Difference Between Research Methods and Research Design | Definition, Features, Comparison. Retrieved October 13, 2023, from https://pediaa.com/differencebetween-research-methods-and-research-design/
Pelling, E. L., & White, K. M. (2009). The theory of planned behavior applied to young people's use of social networking web sites. *Cyberpsychology and Behavior*, *12*(6), 755–759. https://doi.org/10.1089/cpb.2009.0109
Perera, S., Jin, X., Maurushat, A., & Opoku, D. G. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, *9*(1). https://doi.org/10.3390/informatics9010028
Perwej, Dr. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04
Pieczywok, A. (2021). Cyber threats and challenges targeting man versus his education. Cybersecurity and Law, 1(1), 225–236. https://doi.org/10.35467/cal/133799
Pieterse, H. (2021). The Cyber Threat Landscape in South Africa: A 10-Year Review. *The African Journal of Information and Communication*, *28*. https://doi.org/10.23962/10539/32213
Ponemon Institute LLC. (2016). 2016 Cost of Data Breach Study: Global Analysis. *2016 Cost of Data Breach Study: Global Analysis*, (June), 31. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
Ponemon, L., & Danahy, J. (2018). The 2017 state of endpoint security risk report. Technical Report. *Ponemon Institute*. https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends.
Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2023). A systematic analysis of failures in protecting personal health data: A scoping review. *International Journal of Information Management*, *74*, 102719.
Porcedda, M. G. (2018). Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Computer Law and Security Review*, *34*(5), 1077–1098. https://doi.org/10.1016/j.clsr.2018.04.009
Potgieter, P. (2019). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms. (2019). A Case Study at Central University of Technology.
Protection of Personal Information Act 4 of 2013 | South African Government. (n.d.). Retrieved from https://www.gov.za/documents/protection-personal-information-act

Rajesh Chandarman, & Brett Van Niekerk. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication (AJIC)*, (20). https://doi.org/10.23962/10539/23572

Rao, A. R., & Dave, R. (2019). Developing hands-on laboratory exercises for teaching STEM students the internet-of-things, cloud computing and blockchain applications. In *2019 9th IEEE Integrated STEM Education Conference, ISEC 2019* (pp. 191–198). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ISECon.2019.8882068

Resnik, D. B. (2015). Glossary of Commonly Used Terms in Research Ethics. *National Institute of Environmental Health Science, National Institutes of Health*. Retrieved from https://www.medicres.org/glossary-of-commonly-used-terms-in-research-ethics.html

Richardson, R. (2007). Csi. *FBI Computer Crime and Security Survey*.

Richet, J. L. (2022). How cybercriminal communities grow and change: An investigation of ad-fraud communities. *Technological Forecasting and Social Change*, *174*. https://doi.org/10.1016/j.techfore.2021.121282

Ringle, C. M., Sarstedt, M., Mitchell, R., & Gudergan, S. P. (2020). Partial least squares structural equation modeling in HRM research. *International Journal of Human Resource Management*, *31*(12), 1617–1643. https://doi.org/10.1080/09585192.2017.1416655

Risk-Based Security. (2020). *The 2019 Year-End Report Data Breach QuickView* (Report). https://edtechmagazine.com/higher/article/2020/08/tips-reducing-key-remote-learning-security-risks-perfcon. Accessed 12 December 2023.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rysavy, M., & Michalak, J. (2020). Impact of COVID-19 on higher education: Students' attitudes towards e-learning. Journal of Human Behavior in the Social Environment, 30(4), 452-461. https://doi.org/10.1080/10911359.2020.1773258

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organisations. Computers in Human Behavior, 57, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Cybersecurity education: Bridging the gap between academia and industry. Computers & Security, 75, 122–135. https://doi.org/10.1016/j.cose.2018.01.012

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

Sample Size Calculator: Understanding sample sizes | SurveyMonkey. (n.d.). Retrieved from https://www.surveymonkey.com/mp/sample-size-calculator/

Saunders Mark, Lewis Philip & Thornhill Adrian. (2023). *Saunders Research Methods*. *Research Methods for Business Students* (Vol. 9th Edition, pp. 1–852). Pearson.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2023). *Research methods for business students* (9th ed.). Pearson.

Saunders, M., Lewis, P. and Thornhill, A. (2012). Methods for Business Students. Pearson Education Ltd., Harlow. *Methods for Business Students. Pearson Education Ltd., Harlow.*

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students by Mark Saunders, Philip Lewis and Adrian Thornhill 8th edition. Research Methods For Business Students*.

Schwarzmüller, T., Brosi, P., Duman, D., & Welpe, I. M. (2018). How does the digital transformation affect organisations? Key themes of change in work design and

leadership. *Management Revue*, *29*(2), 114–138. https://doi.org/10.5771/0935-9915-2018-2-114
Sepehr, F., Bertasi, F., Di Noto, V., & Paddison, S. J. (2014). Ab Initio Study and Vibrational Spectroscopy of Imidazolium Based Ionic Liquids with Dissolved δ-MgCl 2. *ECS Meeting Abstracts*, *MA2014-01*(23), 1029–1029. https://doi.org/10.1149/ma2014-01/23/1029
Serrat, O. (2023). Information and Communication Technology in Organizations: Impacts and Implications. In Digital Solutions (pp. 13–28). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-7253-9_2
Sheehan, K. (2001). E-mail survey response rates: A review. *Journal of Computer-Mediated Communication*. Wiley Blackwell. https://doi.org/10.1111/j.1083-6101.2001.tb00117.x
Shingange, J. G. (2022). Problematizing the South African cybersecurity policy landscape (Doctoral dissertation, Stellenbosch: Stellenbosch University).
Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management and Computer Security*. https://doi.org/10.1108/IMCS-08-2012-0045
Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, *23*(2), 200–217. https://doi.org/10.1108/ICS-04-2014-0025
Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063
Steyn, A. A. (2015). *Incorporating technology into South African entrepreneurial training*. University of Pretoria (South Africa).
Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information (Switzerland)*, *13*(9). https://doi.org/10.3390/info13090413
Sürücü, L., & Maslakçi, A. (2020). Validity and Reliability in Quantitative Research. *Business & Management Studies: An International Journal*, *8*(3), 2694–2726. https://doi.org/10.15295/bmij.v8i3.1540
Toth, P., Klein, P., Toth, P., & Klein, P. (2014). A Role-Based Model for Federal Information Technology / Cybersecurity Training NIST Special Publication 800-16 A Role-Based Model for Federal Information Technology / Cybersecurity Training. *Nist Sp 800-16*, *1*(Draft).
Trim, P. R. J., & Lee, Y. I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, *83*, 224–238. https://doi.org/10.1016/j.indmarman.2019.04.003
Tvaronavičienė, M., Plėta, T., Casa, S. D., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, *2*(4), 802–813. https://doi.org/10.9770/ird.2020.2.4(6)
Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers and Security*, *109*. https://doi.org/10.1016/j.cose.2021.102387
Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*. MDPI AG. https://doi.org/10.3390/fi13020039
Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Verizon: Data Breach Investigations Report 2020. (2020). *Computer Fraud & Security*, *2020*(6), 4–4. https://doi.org/10.1016/s1361-3723(20)30059-2
Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers and Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008
Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*. https://doi.org/10.1016/j.dss.2019.113160
von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025
Vrhovec, S., Bernik, I., & Markelj, B. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign.*Computers and Security*,*125*. https://doi.org/10.1016/j.cose.2022.103038
Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*, 11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633
Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267–284. https://doi.org/10.1057/ejis.2010.72
Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning, 11. Retrieved from www.cengage.com.
Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*. https://doi.org/10.1016/j.ijinfomgt.2022.102520
Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005
Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behavior, pp. 84, 375–382. https://doi.org/10.1016/j.chb.2018.02.019
Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, *16*(6), 448–484. https://doi.org/10.17705/1jais.00399
Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269