DEVELOPING A PROTOCOL FOR EFFECTIVE CYBERSECURITY INFORMATION SHARING: A HUMAN-CENTRIC APPROACH FOR SMALL AND MEDIUM ENTERPRISES IN SOUTH AFRICA

MATIPA RICKY NGANDU

Dissertation submitted in fulfilment of the requirements for the Degree

MASTER IN INFORMATION TECHNOLOGY

in the

Department of Information Technology
Faculty of Engineering, Built Environment and Information Technology
at the
Central University of Technology, Free State

Supervisor: Dr Ntima Mabanza
Co-supervisor: Dr Gardner Mwansa

2025

DECLARATION OF INDEPENDENT WORK

DECLARATION WITH REGARD TO

INDEPENDENT WORK

I, MATIPA RICKY NGANDU, identity number _____ and student number _____, do hereby declare that this research project submitted to the Central University of Technology, Free State for the Master of Information Technology, is my own independent work; and complies with the Code of Academic Integrity, as well as other relevant policies, procedures, rules and regulations of the Central University of Technology, Free State; and has not been submitted before to any institution by myself of any other person in fulfilment (or partial fulfilment) of the requirements for the attainment of any qualification.

24/09/2025

_____ _____

SIGNATURE OF STUDENT **DATE**

DEDICATION

This dissertation is dedicated to my beautiful wife and wonderful children, for supporting me over the long hard nights and very early mornings. Your love and sacrifices continue to motivate me.

ACKNOWLEDGEMENTS

The efforts culminating to this point could not have been achieved without the support from:

- Almighty God, family, friends, and work colleagues who continuously provided motivation when frustrations arose.
- The excellent team of academic and non-academic staff at CUT, who not only acted professionally but were always ready and willing to assist in the progress of this journey.
- Dr N. Mabanza, my supervisor, and Dr G. Mwansa, my co-supervisor. Your guidance, patience, and encouragement are things for which I am grateful and will aspire to emulate when I one day become a supervisor to Master's and Doctoral candidates.
- My employer, particularly the HR division for benefits at WSU, and the funding and grants office at CUT for graciously sponsoring me throughout my studies. This endeavour would have been far more challenging without your support.

Thank you is not always enough; in this instance, it serves as a small token of my immense appreciation for getting me to this point and beyond. Thank you.

ABSTRACT

Cybersecurity remains a serious concern for Small and Medium Enterprises (SMEs) in South Africa. Despite their significant contributions to the national economy and job creation, SMEs are becoming increasingly susceptible to cyber threats, including phishing, ransomware, business email compromise (BEC), and data breaches. Although Cybersecurity Information Sharing (CIS) has been globally recognised as a critical mechanism for enhancing organisational resilience, SMEs frequently encounter obstacles to effective participation, such as low awareness, limited resources, a lack of skills, and pervasive mistrust. Despite the existence of regulatory frameworks like the Protection of Personal Information Act (POPIA) and the Cybercrimes Act, adherence remains inconsistent, and SMEs still lag behind in implementing effective CIS practices. This gap highlights the necessity for a socio-technical, human-centric approach specifically designed for the SME context.

This research study aimed to develop a human-centric CIS protocol that integrates behavioural, socio-cultural, psychological, technological, and regulatory dimensions, placing trust at its core. A key emphasis was placed on understanding how human factors, such as motivation, social impact, and self-efficacy, affect SMEs' willingness and capacity to participate in CIS. A comprehensive literature review of existing frameworks for CIS (such as NIST, NISTIR 7621, ISO/IEC 27032, and NIST 80018) revealed that they mainly focus on technical and policy aspects, often overlooking behavioural dynamics, which leaves SMEs without clear guidance to address organisational and behavioural challenges.

Guided by Social Cognitive Theory (SCT), the study examined how individual capabilities, organisational norms, perceived outcomes, and external policy and technological environments influence SMEs' cybersecurity decisions. A pragmatist paradigm, utilising an explanatory sequential mixed-methods design, was employed. The quantitative phase surveyed 21 SMEs to assess knowledge, capability, self-efficacy, social persuasion, and outcome expectations in relation to CIS participation. The qualitative phase involved semi-structured interviews with 10 participants to explore socio-cultural constraints, trust dynamics, and organisational practices. SCT was utilised to guide the development of a human-centric CIS protocol, ensuring that it incorporates behavioural, socio-cultural, psychological, technological, and regulatory aspects. The developed CIS protocol was tested by six experts from research, decision-making, and technical backgrounds to ensure practical relevance and applicability.

The study achieved four objectives: (1) identifying human factors associated with effective CIS; (2) examining how policy and technology interact with these factors; (3) developing a protocol tailored to the realities of South African SMEs; and (4) evaluating its effectiveness. Findings indicate that trust, peer influence, and supportive policy environments are critical enablers of CIS participation. SMEs with

higher self-efficacy and confidence in cybersecurity practices demonstrated a greater willingness to share information. Persistent barriers, including the lack of standardised reporting tools, inadequate technical infrastructure, and organisational mistrust, continue to hinder adoption.

This research contributes both theoretically and practically. Theoretically, it extends SCT's applicability to cybersecurity by demonstrating how behavioural and environmental factors jointly shape SMEs' engagement with CIS. Practically, it delivers a human-centric CIS protocol that addresses behavioural, organisational, and policy barriers, providing actionable guidance for SMEs, policymakers, and industry associations. The findings highlight the need for targeted training, stronger policy integration, and trust-building initiatives to foster sustained CIS participation. Ultimately, this study strengthens SME resilience in South Africa's digital economy and lays the groundwork for future research on sector-specific and regional variations in CIS practices.

PUBLICATIONS RESULTING FROM RESEARCH

I. A conference paper titled "*Enabling SME Participation in Cybersecurity Information Sharing: A Human-centric, Socio-technical Model*" was submitted to the 4th World Conference on Information Systems for Business Management (ISBM) – 2025 (https://isbm.ict4sd.org/) on 11 July 2025 ("Accepted for full paper presentation and proceedings publication").

TABLE OF CONTENTS

LIST OF TABLES

TABLE OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

AI	Artificial Intelligence
BEC	Business Email Compromise
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act
CTIS	Cyber Threat Information Sharing
CIS	Cybersecurity Information Sharing
GDPR	General Data Protection Regulation
MISP	Malware Information Sharing Platform
AIS	Automated Indicator Sharing
NIST	National Institute of Standards and Technology
POPIA	Protection of Personal Information Act
SCT	Social Cognitive Theory
SMEs	Small and Medium Enterprises
STIX	Structured Threat Information Expression
TAM	Technology Acceptance Model
TAXII	Trusted Automated Exchange of Indicator Information
TOE	Technology-Organisation-Environment
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
HCA	Hierarchical Cluster Analysis

1 CHAPTER ONE: INTRODUCTION AND BACKGROUND

1.1 Introduction

The increasing frequency of cyber incidents worldwide has intensified concerns about cybersecurity (World Economic Forum, 2025). Similarly, Small and Medium Enterprises (SMEs) have become targets of sophisticated cyberattacks. According to an Allianz commercial report, data breaches at SMEs rose by 152% globally in 2021, compared to a 75% increase at larger companies during the same period (Allianz, 2023). This trend may indicate that SMEs are increasingly appealing to cybercriminals due to their low levels of cyber resilience, which are influenced by their limited cybersecurity resources and expertise. According to the Council for Scientific and Industrial Research (CSIR), cybercrime has a significant negative impact on the economy, costing South Africa an estimated R2.2 billion a year (Mzekandaba, 2023). This costly consequence of cyber vulnerability within the South African economy is concerning, as it has the potential to rise further and have long-term negative impacts on growth. Despite the fact that cyber incidents are more likely to go unnoticed or may not be reported among South African SMEs, this does not exempt them from the negative impact of cybercrime (Kabanda, Tanner & Kent, 2018). Therefore, it is important for all stakeholders in the South African economy, especially SMEs, to find sustainable strategies to reduce the surge in cyberattacks that continue to negatively impact South Africa. In South Africa, SMEs are considered vital for economic growth and job creation, particularly at a time of high unemployment. Their substantial contribution to the economy makes them a key sector, highlighting the importance of prioritising efforts to strengthen their cyber resilience.

In recent years, SMEs have increasingly integrated Information and Communication Technology (ICT) into their operations. Unfortunately, this rapid adoption of technology has rendered them more vulnerable to cyberattacks (Kent, Tanner & Kabanda, 2016; Medoh & Telukdarie, 2022). These cyberattacks have resulted in financial losses, operational delays, reputational damage, and even permanent shutdowns (Mugwagwa, Bhero & Chibaya, 2024). Improving cybersecurity resilience for SMEs is crucial, and one promising strategy is Cybersecurity Information Sharing (CIS). CIS facilitates the sharing of practical intelligence regarding threats, vulnerabilities, and effective practices among community members, thereby enhancing organisational readiness (Paggio, Bafoutsou & Sarri, 2021).

In South Africa, legislation requires organisations and government bodies to share threat information promptly and within a reasonable timeframe. Organisations must demonstrate adherence by creating and applying relevant policies and technologies that facilitate cyber threat information sharing (CTIS) (Pieterse, 2021). Both open-source and commercial threat information sharing technologies and

platforms such as: the Malware Information Sharing Platform (MISP); Structured Threat Information Expression (STIX); Trusted Automated Exchange of Indicator Information (TAXII) protocols and; Automated Indicator Sharing (AIS), have been used to support CIS processes (van Haastrecht et al., 2021; MISP, 2025). While these tools offer SMEs an opportunity to meet legislative requirements, their effective use depends on access to technical expertise for implementation, maintenance, and operation.

However, participation in CIS among SMEs is not at the expected levels in South Africa and globally, despite the existing laws, policies, and technologies (Lewis et al., 2014; Ring, 2014; Cano, 2019; Sangari, Dallal & Whitman, 2022). Furthermore, Koepke (2017) notes that the low level of adoption can be attributed to the fact that participation in CIS declines as an organisation grows, resulting in minimal involvement from SMEs. South African SMEs face significant challenges in adopting cybersecurity measures and information sharing practices. Some practical examples of these challenges include limited budgets, lack of management support, negative attitudes towards cybersecurity, absence of security policies and risk management strategies, and technical and resource constraints (Kent, Tanner & Kabanda, 2016; Kabanda, Tanner & Kent, 2018; Moeti, Langa & Sigama, 2023). In a general study by Koepke (2017), it was found that most SMEs do engage in information-sharing communities or participate in CIS due to their inability to build trust in the system. However, Benz & Chatterjee (2020) advocate for the idea that SMEs should receive guidance on optimising their resources to participate effectively in information-sharing initiatives.

Based on the earlier discussion, there is a need to examine an alternative perspective to improve CIS adoption among SMEs. Currently, the structural enablers provided by laws, policies, and technologies are insufficient. Therefore, addressing human-centric barriers such as trust, knowledge, perceived risks, cultural attitudes, and organisational readiness may lead to improved CIS adoption. This research investigates the human factors that influence CIS participation, examines how policies and technologies interact with these factors, and develops a human-centric CIS protocol for SMEs. The protocol will be validated to assess its efficacy in improving CIS participation, thereby enhancing SME cybersecurity resilience.

Different key concepts used in this study are defined in the glossary of terms, see Appendix A.

1.2 Research problem

SMEs are underrepresented in cybersecurity partnerships, including CIS initiatives, which undermines collective cyber defence, especially in supply chains and regional economic networks. Unlike large companies, SMEs frequently suffer from constrained and non-existent cybersecurity budgets, lack of

management support, negative attitudes towards cybersecurity, absence of security policies and risk management strategies, technical and resource constraints, lack of specialised cybersecurity teams, insufficient awareness, limited leadership involvement, and concerns about competitive risk (Kent, Tanner & Kabanda, 2016; Koepke, 2017; Kabanda, Tanner & Kent, 2018; Chidukwani, Zander & Koutsakis, 2022; El-Hajj & Mirza, 2024).

South African SMEs are increasingly targeted by cyberattacks, resulting in financial loss, operational delays, reputational damage, and even permanent shutdowns (Mugwagwa, Bhero & Chibaya, 2024). This presents a significant barrier to progress and development that the South African economy needs, especially in this time of high unemployment. SMEs must play a more active role in improving their cyber resilience posture to reduce the negative impacts of cybercrime. CIS participation presents an opportunity for SMEs to meet legal compliance requirements while also offering clear benefits, including cost savings and enhanced cyber resilience (Yang, Kwon & Lee, 2020). However, SMEs' participation remains low due to significant barriers, such as insufficient trust, limited skills, and financial constraints (Kent, Tanner & Kabanda, 2016). Existing frameworks focus on technological and procedural solutions, leaving human factors underexplored (Parsons et al., 2010; Al-Alawi et al., 2021). Hence, the current research study aims to fill this gap by developing a human-centric protocol that addresses behavioural, cognitive, and organisational factors to improve CIS adoption among SMEs.

1.3 Research questions

The following four research questions are formulated in accordance with the problem statement:

1) What human factors are associated with effective CIS?
2) How do policies and technologies influence human factors associated with CIS?
3) What protocol can be implemented to achieve reciprocal CIS amongst SMEs?
4) What is the efficacy of the protocol in achieving reciprocal CIS?

1.4 Research aim and objectives

This study aimed to develop a human-centric protocol that enhances reciprocal CIS among SMEs. Experts validated the resulting protocol to determine its effectiveness in enhancing CIS within SMEs. This was accomplished by pursuing a specific set of four objectives:

1) Determine human factors associated with effective CIS – This objective aimed to establish the critical human factors that promote or hinder SME participation in CIS. The approach taken:

    - Carried out a comprehensive literature review to identify human factors that act as promoters and barriers to CIS participation.
    - Determined a suitable theoretical framework to underpin the study.
    - Carried out a quantitative survey among SMEs to capture perceptions and behaviours regarding CIS participation.

    The outcome of the first objective:

    - A baseline (literature-informed) interaction model that centres on human factors influencing effective CIS participation amongst SMEs in South Africa.

2) Examine policy and technology's influence on human factors – The aim of this objective was to link macro-level enablers (laws, policies, platforms such as MISP/STIX/TAXII/AIS) to micro-level adoption obstacles.

    The approach taken:

    - Used current literature to map how laws, policies, and CIS technologies interact with human factors.

    The outcome of the second objective:

    - A protocol based on literature that can be implemented to promote successful CIS amongst SMEs in South Africa. This will assist to get a clear understanding of how structural enablers impact CIS adoption.

3) Develop a human-centric CIS protocol customised for SMEs.

    The approach taken:

    - Conducted qualitative interviews with SMEs to deeply understand quantitative survey findings.
    - Design using Social Cognitive Theory (SCT), the theoretical framework (self-efficacy, outcome expectations, social persuasion) and baseline literature-informed protocol (developed based on current literature) in objective 2.

- Integrated policy/technology affordances with trust-building, simplified reporting, and incentives.

The outcome of the third objective:

- A step-by-step guide for SMEs to improve CIS participation,

4) Evaluate the efficacy of the proposed protocol improving CIS amongst SMEs - The aim of this objective was to determine if the protocol truly enhances SMEs' willingness and capability to share information.

The approach taken:

- Conducted expert validation of the protocol's practicality, scalability, and effectiveness.

The outcome of the fourth objective:

- Evidence of the improved CIS behaviour among SMEs.

1.5 Research methodology

This study adopted a pragmatist paradigm, utilising an explanatory sequential mixed-methods approach, guided by SCT. The approach began with a quantitative phase involving data collection and analysis, followed by a qualitative phase designed to further explore and explain the quantitative findings. The method and purpose of the quantitative phase were to administer a closed-ended questionnaire via Google Forms to a sample identified through the snowball sampling technique. Descriptive and inferential statistics, such as Spearman's Rank Correlation and Hierarchical Cluster Analysis (HCA), were used to analyse the data gathered during this phase. The purpose of this quantitative phase was to assist in achieving Research Objectives 1 and 2. The qualitative phase involved conducting semi-structured interviews with a subset of purposively selected participants identified from the quantitative phase. Thematic analysis was employed to analyse the data collected during this phase, which contributed towards accomplishing Research Objectives 2 and 3. The study improved the validity and reliability of its findings and attained a thorough grasp of the human factors influencing CIS participation by using SCT in the data collection instrument development and interpretation process and by integrating relevant secondary data from various sources. Chapter 3 provides a detailed discussion of the research method and the rationale behind the methodological choices made.

1.6 Research limitations

This study uses both primary and secondary data to assist in the development of a protocol aimed at improving CIS participation among SMEs. Nevertheless, the following limitations of the study must be acknowledged when interpreting the findings:

- Firstly, the relatively small sample sizes in both the quantitative and qualitative phases may limit the generalisability of the findings beyond the specific context of retail SMEs in the Eastern Cape.
- Secondly, geographic focus (limited to the Eastern Cape province) and sectoral focus (SMEs in the retail sector) may not fully capture the cybersecurity dynamics of SMEs in other regions or rural areas, nor those highly regulated industries.
- Thirdly, the cross-sectional design restricts observation of long-term CIS behaviour changes or the sustained adoption of the proposed CIS protocol.
- Lastly, the protocol evaluation was based solely on experts' feedback, without input from government or regulatory policy stakeholders, which may have affected its alignment with national cybersecurity strategies and compliance frameworks.

1.7 Research contribution

This study underscores the significance of cybersecurity for stakeholders within the SME value chain. It adds to the expanding body of knowledge by developing a human-centric protocol to enhance effective CIS among SMEs. The research examines the interplay between human factors, technology, policies, and procedures, providing practical guidance for improving cyber resilience. The protocol encourages SMEs to actively participate in reciprocal CIS by addressing critical areas such as trust, awareness, reporting mechanisms, technical support, and management commitment. Strengthening cybersecurity in SMEs can ultimately benefit the wider economy. Consequently, this research study offers both theoretical and practical contributions:

- Theoretical: This study extends SCT to cybersecurity behaviours, linking cognitive (perceptions of risk), environmental (policies, organisational support), and behavioural (trust-based decisions) factors to CIS adoption.
- Practical: This study provides SMEs with a human-centric protocol that addresses and strengthens trust, awareness, reporting, technical support, and management commitment.
- Policy Implications: This study offers insights for regulators and policymakers on how laws, regulations, and incentives can enhance CIS engagement and collaboration among SMEs.

- Sector-specific Guidance: This study identifies sector-specific, human-centred barriers and motivations for CIS within SMEs, enabling future research interventions.

1.8 Dissertation structure

This dissertation is divided into six chapters as illustrated in Figure 1.1.

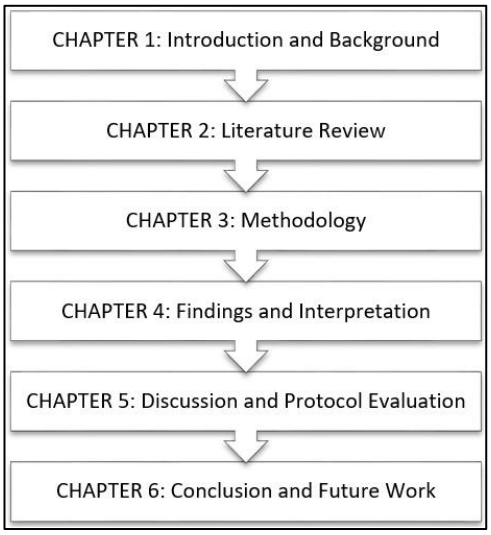


Figure 1-1: Outline of the dissertation

A brief summary of the different topics that will be discussed in each of the six chapters, as shown in Figure 1.1 above, will now be provided.

Chapter 1 introduces the research study by outlining the research problem, objectives, and questions. It further explains the research design and methodology, acknowledges the study's limitations, and highlights its potential contributions. The chapter closes with an overview of the dissertation structure.

Chapter 2 provides the literature review. It begins with an overview of the key concepts and theories relevant to the study, with a particular focus on cybersecurity and CIS within SMEs in South Africa. The chapter identifies existing research gaps and critically evaluates prior studies in relation to the research problem. It then presents SCT, the theoretical framework adopted to underpin the study, and explains how SCT is applied to understand human behaviour in cybersecurity practices. The chapter concludes by consolidating the theoretical and empirical foundations that guide the study's research design and objectives.

Chapter 3 outlines the research methodology used in the study. It details the research design, including the explanatory sequential mixed-methods approach, and justifies the choice of methods. The chapter describes the data collection process, the instruments used (questionnaires and semi-structured

interviews), the sampling techniques, and the data analysis procedures. Ethical considerations are also addressed.

Chapter 4 presents the findings of the study, beginning with an overview of the quantitative results, including descriptive statistics, reliability testing, and inferential analysis. It then moves to the qualitative findings, derived from thematic analysis of semi-structured interview data. The chapter also integrates both data sets to provide a comprehensive understanding of the factors influencing CIS among SMEs. In this chapter, tables and figures are used to present key trends, correlations, and thematic insights. The chapter concludes with a summary of the findings and their implications for the research objectives.

Chapter 5 provides an in-depth discussion and interpretation of the research findings presented in Chapter 4. It relates the results to the existing literature, linking the study's outcomes to SCT. The chapter also highlights the significance of the findings in the context of the research problem, objectives, and questions. It examines the implications for practice, policy, and future research, offering insights into how SMEs can enhance their participation in CIS. The chapter concludes with the study's overall contributions.

Finally, Chapter 6 is the conclusion chapter that summarises the key findings of the study. It revisits the research objectives, reflecting on how the study addressed the research problem and questions. The chapter highlights the theoretical, methodological, and practical contributions of the research. It provides recommendations for future research, policy development, and practice. The chapter concludes with a reflection on the study's overall impact on understanding and improving CIS among SMEs.

1.9 Summary

This chapter introduced the study by outlining the growing cybersecurity challenges facing SMEs in South Africa and the significant economic implications of their vulnerability to cyberattacks. It established the research problem by demonstrating that, despite the availability of laws, policies, and technologies intended to support CIS, SME participation remains markedly low due to human, organisational, and resource-related constraints. The chapter articulated the research aim, questions, and objectives, emphasising the need for a human-centric protocol that addresses behavioural, socio-cultural, psychological, technological, and regulatory influences on CIS adoption. An overview of the explanatory sequential mixed-methods approach was provided, together with a discussion of the study's limitations and anticipated contributions. The chapter concluded with an outline of the dissertation structure, showing how each chapter builds towards the development and evaluation of the proposed CIS protocol.

The next chapter presents the literature review, which examines the human, technological, policy, and organisational factors that influence SME cybersecurity behaviour. It also introduces the theoretical framework underpinning the study, thereby establishing the conceptual foundation for the empirical investigation that follows.

2 CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The introduction chapter outlined the state of CIS among SMEs in South Africa and identified the gap that this study seeks to address. Building on that foundation, this chapter (i.e., Chapter 2) critically reviews and synthesises existing literature on CIS, focusing on the human, policy, and technological dimensions shaping SME participation. Chapter 2 provides an overview of the cybersecurity landscape in relation to SMEs. It reviews relevant policies, technological platforms, and frameworks within the South African context while emphasising the importance of human factors in shaping participation. The chapter introduces SCT as a lens to understand how personal, social, and environmental influences interact with CIS behaviours. It establishes the groundwork for subsequent discussions on developing a human-centric CIS protocol tailored to SMEs. Drawing on this synthesis, the chapter lays the foundation for a literature-informed protocol that links policies, technologies, and human factors to CIS participation. In doing so, it justifies the need for a human-centric CIS protocol tailored to SMEs and positions the study to address the identified gap. The next section explores the cyberthreat landscape confronting SMEs, establishing the contextual backdrop for these challenges.

2.2 Cyberthreat landscape

The European Union Agency for Cybersecurity [ENISA] (2022) defines the cyberthreat landscape as the current state and range of cybersecurity risks faced by organisations, individuals, and governments. European Union Agency for Cybersecurity [ENISA] (2022) highlights six key aspects of this landscape: (1) Threat types, such as malware, phishing, distributed denial-of-service (DDoS) attacks, data breaches, and business email compromise (BEC); (2) threat actors, including cybercriminals, hacktivists, nation-state actors, insider threats, and script kiddies; (3) vulnerabilities in software, hardware, networks, or human processes that can be exploited; (4) attack techniques and tools, such as social engineering, zero-day exploits, and automated hacking tools; (5) emerging technological trends, including artificial intelligence (AI), advanced persistent threats, and the Internet of Things (IoT); and (6) regional and sector-specific threats, which vary according to local vulnerabilities.

As stated by INTERPOL (2024), the threat landscape in Africa includes BEC; phishing scams via traditional and social media; romance scams; pig butchering scams that blend cryptocurrency investment fraud with romance scams; and mobile phone scams encompassing mobile phishing attacks and banking trojans. There is an increase in the trend of cybercrime-as-a-Service, with cybercriminals

collaborating to target companies (INTERPOL, 2024). Cybercriminals have taken notice of the rise in generative AI usage, utilising the advantages of large language models to facilitate new types of cyberattacks (INTERPOL, 2024).

In alignment with the previous points, Pieterse (2021) noted that there is an ongoing rise in global cyberattacks, and South African SMEs face similar vulnerability issues to cyberattacks as larger organisations do. Thus, the current study focuses on the cyberthreat environment for SMEs in South Africa (SA).

2.2.1 South Africa's cyberthreat environment

In South Africa, SMEs are defined according to sector-specific thresholds, typically considering two key metrics, namely, the number of employees (between 10 and 250 employees) and annual turnover (a maximum of R220 million) (Ayandibu & Houghton, 2017). SMEs play a critical role in the economy, contributing approximately 34% to the Gross Domestic Product and employing around 60% of the workforce in the country (Ayandibu & Houghton, 2017). They provide 60–70% of employment, particularly for unskilled and semi-skilled workers (Abor & Quartey, 2010; Enaifoghe & Vezi-Magigaba, 2023). Operating in diverse sectors such as retail, services, manufacturing, and agriculture, they often function under resource-constrained and informal management structures. Various methods exist for classifying SMEs in South Africa. This research study focused exclusively on SMEs that utilise ICT in their operations (Cant & Wiid, 2016), as cybercriminals infiltrate and access SMEs via digital systems. While SMEs are flexible and adaptive to market changes, their limited technological and cybersecurity capacity makes them particularly vulnerable to cyber threats, highlighting the importance of implementing effective human-centric CIS protocols to enhance resilience.

Common cyberattacks targeting South African SMEs include phishing, ransomware, and BEC attacks. Phishing remains the most prevalent, with 61% of SMEs reporting attempted phishing incidents in the past year, often leading to compromised credentials or financial losses (Mcanyana, Brindley & Seedat, 2020). Ransomware attacks are increasingly common, affecting 27% of SMEs in 2020, which incurred average financial losses of over ZAR 150,000 per incident, underscoring the critical vulnerability of SMEs with limited IT resources (Mzekandaba, 2023). BEC attacks exploit social engineering tactics, with South African SMEs reporting unauthorised fund transfers and fraud losses exceeding ZAR 200 million annually (Cline, 2025). These threats illustrate that SMEs operate in a high-risk cyber environment and underscore the urgent need for human-centric CIS mechanisms that address behavioural, organisational, and technological factors to enhance resilience.

Accenture's report on South Africa's threat environment highlights worrying trends: malware incidents rose by 22% in the first quarter of 2019 compared to the same period in 2018; Android devices were the second most targeted by banking malware; cybercriminals increasingly exploited mobile phones for cryptocurrency mining and mobile banking fraud; and card-not-present fraud on South African-issued credit cards remained the leading contributor to fraud losses (Mcanyana, Brindley & Seedat, 2020). For SMEs, already operating with limited resources, these threats create significant vulnerabilities, undermining their ability to secure investments in digital transformation.

Cele & Kwenda (2024) argue that SMEs are seen as attractive targets for cybercriminals due to several factors: they frequently lack the resources necessary for advanced cybersecurity measures; SME employees are more likely to be exploited due to insufficient training and inadequate security protocols; SMEs struggle to meet compliance requirements like the POPIA due to associated costs and complexities; while SMEs utilise cloud-based digital solutions, they often lack the technical knowledge needed to secure these environments, thus making them more vulnerable; and the absence of government support in strengthening their cybersecurity infrastructure leads to increased risks from cyberthreats.

Furthermore, the arrival of the Fourth Industrial Revolution (4IR) has brought forth many emerging technologies, including Artificial Intelligence, the Internet of Things, 5G, Blockchain, Robotics, Virtual Reality, Cloud Computing, and Big Data, to name just a few. To respond to these challenges and ensure their survival in the 4IR era, many SMEs are currently incorporating various emerging technologies (such as, Cloud Computing) into their everyday operations. However, the integration of these new 4IR technologies has created new kinds of vulnerabilities for SMEs, primarily due to their lack of expertise in adequately protecting their environments. Limited government support exacerbates these challenges, putting SMEs at a greater disadvantage. The next section, Section 2.3, builds on this discussion by linking the SME cyberthreat landscape to the specific barriers they encounter in implementing cybersecurity measures.

2.3 SME cybersecurity challenges and barriers

Pieterse (2021) indicates that the cyberthreat landscape in South Africa is deteriorating due to a variety of factors, including inadequate investment in cybersecurity, a sluggish legislative response to combat cybercrime, insufficient awareness of cyberthreats, an accelerated adoption of digital solutions, and a growing perception among cybercriminals that South Africa presents an accessible target. SMEs are particularly vulnerable, characterised by limited cybersecurity initiatives and a plethora of publicly

documented attacks that highlight their susceptibility. In response to these challenges, Pieterse (2021) proposes adopting a defence-in-depth approach, fostering a security-focused cyber culture, leveraging threat intelligence, prioritising compliance, enhancing collaboration and reporting, and preparing for inevitable cyberattacks. While Pieterse (2021) study can be viewed as a positive step toward tackling SMEs' cyber threat landscape issues, it offers little guidance on how to effectively implement mitigation strategies under the approach of collaboration and reporting, which is the primary concern in CIS and the focus of this study.

Research in specific sectors reinforces these concerns. For instance, Jideani et al. (2018) examined the cybersecurity environment of South Africa's e-retail sector and found that SMEs often do not have the infrastructure, resources, or expertise required to address cybercrime or conduct security assessments. Unlike larger corporations that can rely on dedicated specialised IT teams, SMEs often struggle to adopt comprehensive and effective security measures. Kent, Tanner & Kabanda (2016) similarly found that the adoption of certain cybersecurity measures by SMEs was affected by their organisational readiness. The four primary factors influencing how SMEs perceive and execute cybersecurity include budget constraints, organisational complexity, management attitudes towards security, and available expertise in implementing security measures. Their findings highlight that SMEs frequently prioritise compliance over building genuine resilience, leaving them vulnerable to targeted attacks such as credit card fraud, bank account compromise, identity theft, and phishing schemes.

Kabanda, Tanner & Kent (2018) identify two categories, internal and external factors, into which the challenges and barriers discussed in this section are categorised. Internal barriers include budget limitations, weak management support, lack of IT security expertise, outdated systems, and difficulties complying with regulatory requirements (Sukumar, Mahdiraji & Jafari-Sadeghi, 2023). External factors include poor cyber hygiene, novice users, reliance on pirated software, limited awareness of adversarial tactics, increased bandwidth availability, gaps in IT education, and socio-cultural constraints (Chidukwani, Zander & Koutsakis, 2022). These factors compound SMEs' cybersecurity vulnerabilities, making them attractive targets for cybercriminals.

Despite the severity of these challenges, research suggests they can be mitigated through reciprocal processes such as CIS. Yet, as Chidukwani, Zander & Koutsakis (2022) note, most existing literature focuses heavily on the identify and protect functions of cybersecurity, with far less emphasis on detect, respond, and recover. Since CIS is situated within this underexplored space, it highlights a critical limitation of purely technological defences: while advanced tools can block some attacks, they are far

less effective against social engineering that exploits psychological and organisational weaknesses. Hence, further research is needed to determine how SMEs can leverage it to strengthen resilience and overcome systemic barriers. The barriers highlighted show that SME adoption of cybersecurity measures is not only constrained by technical or resource limitations but is also deeply shaped by human behaviours, organisational practices, and regulatory expectations. Thus, a human-centred approach to CIS becomes vital. Section 2.4 examines how these human, organisational, technological, and policy-related influences interact to shape SMEs' participation in CIS.

2.4 Human and institutional influences on CIS

This section examines how human, organisational, technological, and regulatory factors collectively shape SMEs' engagement in CIS. While technical frameworks establish necessary structures, their effectiveness ultimately depends on how individuals and organisations interpret, adopt, and operationalise them within specific contexts. By integrating bottom-up behavioural dynamics with top-down regulatory pressures, this section provides a holistic perspective on the drivers and barriers influencing CIS participation among SMEs.

2.4.1 Human and behavioural factors

Human factors relate to the behavioural, socio-cultural, psychological, and cognitive processes that shape how individuals interact with systems (Pollini et al., 2022). These factors include user habits, security awareness, and beliefs about risk and convenience (Triplett, 2022). Even when users are aware of appropriate security behaviours, they may disregard them due to perceived inconvenience or role-specific constraints. Psychological dynamics, including heuristics such as reliance on expert advice or easily accessible information, also influence decision-making (Fard Bahreini, Cenfetelli & Cavusoglu, 2022). Behaviours that contradict cybersecurity best practices are particularly common in SMEs, where resources are limited. The behavioural tendencies discussed do not operate in isolation; they are reinforced or discouraged by the socio-cultural and organisational norms within which SMEs function.

2.4.2 Socio-cultural and organizational norms

Organisational values and cultural norms strongly influence employees' willingness to engage in CIS (Herath, Khanna & Ahmed, 2022). Policies signal expected behaviours; however, if they are viewed as impractical or overly burdensome, employees may disregard them (Pollini et al., 2022). Effective CIS requires alignment between organisational culture and technological or policy interventions (Abzakh & Althunibat, 2023). SMEs embedded in trusted peer networks or communities are more likely to share

threat intelligence, as reciprocal trust and perceived mutual benefit reduce reluctance (Pala & Zhuang, 2019; Collier et al., 2023). These organisational and cultural influences interact closely with the technological tools that enable or constrain CIS practices.

2.4.3 Influence of technology

Technology plays a dual role in influencing user behaviour. Automated platforms and standardised sharing languages can streamline information exchange and foster trusted environments (Koepke, 2017). However, automation may also reduce attentiveness, thereby creating a false sense of security (Mohammed, Benson & Saridakis, 2020). While advanced systems support monitoring, sophisticated threat analysis and decision-making continue to necessitate human oversight (Montasari, Hosseinian-Far & Hill, 2018). Trust in CIS technologies is, therefore, essential, as SMEs must feel confident that shared data is secure, authentic, and useful (Pienta, Tams & Thatcher, 2020). Nevertheless, technology alone cannot drive participation; its effectiveness depends on alignment with regulatory and policy frameworks that shape organisational obligations and behaviours.

2.4.4 Regulatory and policy frameworks

At a higher level, laws and policies attempt to shape cybersecurity behaviours by mandating compliance and reporting. Global instruments such as the General Data Protection Regulation (GDPR) and the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) impose strict breach reporting requirements (Data Protection Act 2018, 2018; Comizio et al., 2023). In South Africa, the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act (POPIA) create obligations to disclose cyber incidents within a “reasonable time” (South African Government, 2013, 2020). These laws aim to promote accountability and improve resilience by ensuring timely information flows (Johnson et al., 2016). However, SMEs often fall short of compliance due to limited resources, low awareness, and fears of reputational harm (Koepke, 2017; Pieterse, 2021). The persistent gap between regulatory intent and SME practice underscores the importance of human-centric approaches that bridge formal mandates with behavioural realities.

2.4.5 Bridging the gap: human-centric compliance

The literature reveals a persistent gap between the intent of laws and the realities of SME participation. Formal mandates alone do not overcome the psychological, cultural, and organisational barriers that discourage CIS. SMEs may perceive compliance as burdensome or irrelevant if they underestimate their attractiveness as cyber targets (Kabanda, Tanner & Kent, 2018). Therefore, regulatory frameworks must

be supplemented with trust-building measures, incentives, and supportive processes that address the human dimension of compliance. Only by embedding behavioural and socio-cultural considerations into legal and policy frameworks can SMEs be meaningfully encouraged to participate in CIS. These insights highlight the interplay of human, organisational, technological, and regulatory influences, all of which converge to shape how SMEs approach CIS.

Human behaviour, organisational culture, technological tools, and legal frameworks are interdependent forces that shape CIS participation. A human-centric approach that integrates bottom-up behavioural insights with top-down regulatory measures is necessary to reduce barriers and build trust. This integrated perspective emphasises the importance of designing CIS protocols that reflect both the lived realities of SMEs and the structural imperatives of regulation. The next section will focus directly on CIS, examining its role, benefits, and limitations for SMEs as both a strategic necessity and a collaborative practice.

2.5 Cybersecurity Information Sharing

2.5.1 Human and organisational dimensions of CIS

The sharing of sensitive cybersecurity intelligence is increasingly recognised as a cornerstone of collective defence and rapid incident response. Since SMEs face the same types of attacks as large organisations, active participation in CIS is crucial for improving their security posture (Johnson et al., 2016). However, this decision is not straightforward; it is shaped by human factors such as trust, organisational culture, and perceived risks, as well as the ability of technology and policy to bridge gaps and foster collaboration (Pienta, Tams & Thatcher, 2020). To achieve cyber resilience, SMEs must establish a positive cybersecurity culture where technical controls, human behaviour, and effective policy frameworks function together (Glaspie & Karwowski, 2018). Cyber resilience further depends on aligning incident response procedures with business continuity processes to ensure organisational survival during and after cyber incidents (Cichonski et al., 2012). In this sense, CIS requires not only resilient technologies but also skilled people and sustainable policy structures (Johnson et al., 2016).

CIS is essential because it enables organisations to learn from shared experiences of threats and vulnerabilities, creating opportunities for proactive rather than reactive security practices. The reciprocal exchange of cyber threat intelligence builds collective defence capacity and allows organisations to detect and respond to incidents more quickly (Bahar, Muqeem & Pattnaik, 2024). For SMEs in particular,

CIS can reduce resource gaps by leveraging the insights of others. Yet, the success of such sharing depends on addressing the human and organisational dynamics that shape the willingness to contribute.

2.5.2 Regulatory developments and compliance obligations

In South Africa, the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013 (POPIA) impose strict reporting obligations on service providers and organisations handling personal data (South African Government, 2020). Despite these legislative developments, evidence suggests that laws alone have not led to higher participation in CIS among SMEs. Changing behaviour requires more than mere compliance; it necessitates addressing the cultural, economic, and knowledge barriers that influence adoption.

2.5.3 CIS platforms and technological ecosystem

Alongside regulation, the technological ecosystem for CIS has matured. Advanced threat information-sharing platforms such as Splunk, CrowdStrike, IBM X-Force, OpenCTI, and MISP are available commercially and as open-source options for SMEs to collect, cross-reference, and share cyber threat intelligence at scale (Sonwani et al., 2022). These platforms provide both technical indicators and aggregated intelligence that support investigative and defensive activities (Alaeifar et al., 2024). However, adoption challenges persist. Issues such as interoperability, network scalability, data privacy concerns, and a lack of standardised sharing protocols hinder effectiveness (Sauerwein et al., 2017; Serini, 2024). For SMEs in particular, cost constraints, shortages of technical expertise, and uncertainty about how shared information will be used often discourage participation. Current research on SMEs and CIS remains underdeveloped, limiting understanding of the barriers they face and the support they require (Alaeifar et al., 2024).

2.5.4 Strategic approaches to CIS

At the strategic level, CIS is shaped by two interrelated considerations: cybersecurity risk strategy and information-sharing strategy (Zhang, Goel & Williamson, 2024). Risk strategies reflect an organisation's tolerance for risk, whether through acceptance, balancing costs and risks, or proactive risk reduction (Mizrak, 2023). In turn, information-sharing strategies range from selective sharing with trusted partners to balanced or extensive sharing across networks, and even to futile sharing that adds little value (Zhang et al., 2018). For SMEs, the challenge lies in balancing confidentiality concerns with the benefits of collaboration. Achieving balanced or extensive sharing is particularly important in the current threat

landscape, but this requires overcoming barriers such as trust deficits, reputational concerns, and a lack of incentives.

2.5.5 Towards a human-centric CIS model

While CIS clearly offers significant benefits, its implementation remains complex. Laws and platforms establish an enabling environment, but they do not directly change behaviour (Watney, 2024). The level of risk tolerance, trust in stakeholders, and internal capabilities of SMEs ultimately determine their willingness to engage. Addressing persistent barriers such as data privacy concerns, insufficient standards, and weak collaboration mechanisms requires a more cohesive strategy. Integrating technological innovation with supportive policies, while simultaneously embedding human factor protocols that address trust, motivation, and organisational culture, is essential for achieving effective CIS (Colabianchi et al., 2025). Without this human-centric approach, SMEs are likely to remain underrepresented in CIS ecosystems, thereby weakening collective resilience against an increasingly hostile cyber threat environment.

2.6 Availability and suitability of CIS protocols for SMEs

Expanding on the broader challenges of CIS participation discussed in Section 2.5, it is important to assess the availability and suitability of existing information-sharing protocols for SMEs. Existing research indicates that SMEs in developing economies, such as South Africa, face multiple barriers, including limited resources, insufficient technical expertise, and restricted access to advanced cybersecurity tools (Kabanda, Tanner & Kent, 2018; Armenia et al., 2021). Pawar & Palivela (2022) also observe that many SME leaders are unaware of how to create effective cyber-risk strategies, resulting in their unpreparedness to improve their security posture.

Several international frameworks, such as ISO/IEC 27032 and NIST 800-150, provide recognised guidelines for enhancing organisational cybersecurity resilience. However, SMEs remain hesitant to adopt these frameworks, often perceiving themselves as unlikely targets of cyberattacks or lacking the capacity to implement these complex standards (Hoong, Rezania & Baker, 2024). Another key reason for this hesitancy is that these frameworks were primarily designed for larger, resource-rich organisations and are not tailored to the operational realities of SMEs, which typically have limited IT staff, budgets, and cybersecurity expertise (El-Hajj & Mirza, 2024). The complexity and formal documentation requirements of these standards can be overwhelming, and the technical language and procedures are often perceived as inaccessible. Additionally, SMEs in South Africa face contextual

challenges, such as uneven digital infrastructure, high cybercrime rates, and sector-specific regulatory pressures, which reduce the perceived relevance and practicality of adopting generic frameworks (Mugwagwa, Bhero & Chibaya, 2024). These barriers underscore the need for a human-centric approach to cybersecurity, where frameworks and protocols are simplified, locally contextualised, and aligned with SMEs' capacities and operational realities, enhancing their likelihood of adoption.

This mismatch highlights the critical need for tailored solutions. For SMEs in South Africa, the absence of a context-specific and resource-sensitive CIS protocol has left them vulnerable. Developing a human-centric framework that reflects the realities of SMEs is, therefore, essential to fostering greater participation in information sharing and improving cybersecurity resilience.

2.7 Frameworks for CIS

As outlined in Section 2.6, existing cybersecurity frameworks often lack suitability for SMEs not only because of their complexity and resource-intensive requirements, but also due to factors such as limited technical expertise, low awareness of regulatory obligations, poor alignment with SME business processes, insufficient organisational support, and the perception that cybersecurity measures are costly or irrelevant to their immediate business needs. Nonetheless, frameworks, guidelines, and protocols remain essential in providing structured approaches to managing cybersecurity risks, creating common standards for communication, and improving cyber resilience across organisations. For SMEs, the challenge lies not only in adopting these frameworks but also in aligning them with their limited resources, technical expertise, and organisational cultures (Chidukwani, Zander & Koutsakis, 2022). This section reviews the state of CIS frameworks and their applicability to SMEs.

2.7.1 National Institute of Standards and Technology (NIST) frameworks and SME adaptations (NISTIR 7621)

One of the most widely referenced frameworks is the NIST Cybersecurity Framework (CSF), originally designed for critical infrastructure in the United States (US). It offers a structured approach to identifying, protecting, detecting, responding to, and recovering from cyber incidents (Moore, 2022). While it is flexible enough to be adapted beyond large infrastructure, its complexity can present adoption challenges for smaller organisations. Recognising this, NIST developed NISTIR 7621 Small Business Information Security, a guideline tailored for US-based SMEs. It covers systems and network security, physical and personnel security, and disaster recovery (Taşkın & Sandıkkaya, 2023). However, scholars argue that its abstract nature often limits practical uptake, as SMEs struggle to translate broad

recommendations into concrete practices (AL-Dosari & Fetais, 2023; Moeti, Langa & Sigama, 2023). Importantly, NISTIR 7621 emphasises general information security but provides little direction on the mechanisms of CIS (Mmango & Gundu, 2023).

2.7.2 Global guidelines for cybersecurity and information sharing (ISO/IEC 27032 and NIST 800-150)

Complementary to NISTIR 7621, ISO/IEC 27032 establishes international guidelines to improve cybersecurity by bridging gaps across information, network, and internet security (ISO 27032, 2012). It promotes resilience, situational awareness, and a stronger cybersecurity culture (Arenas, Palomino & Mansilla, 2023). Similarly, the NIST 800-150 Guide to Cyber Threat Information Sharing provides practical steps for organisations to exchange cyber threat intelligence effectively and securely. It highlights the benefits of collaboration, including improved situational awareness, coordinated incident response, and enhanced trust networks (Johnson et al., 2016; Wei, Kong & Zhao, 2017). Despite these contributions, both frameworks tend to overlook SME-specific constraints such as limited skills, compliance costs, and human factors like trust, motivation, and risk tolerance, which strongly influence CIS behaviour (Aferudin & Ramli, 2022).

2.7.3 Automated approaches to CIS frameworks

Recent scholarship has turned to automated CIS frameworks as a way to overcome existing limitations. Automated approaches facilitate a timely exchange of structured threat intelligence, often supported by blockchain technology to address trust and privacy concerns (Purohit et al., 2020; Riesco, Larriva-Novo & Villagra, 2020). Game-theoretic models further incentivise participation in CIS platforms by aligning organisational self-interest with collective security benefits (Tosh et al., 2015; Xie et al., 2020). While these innovations are promising, they also raise new challenges regarding the reliability, accuracy, and contextual relevance of shared data (Haque & Krishnan, 2021). Beyond automation, the concept of situational awareness has emerged as a central theme across frameworks, providing another lens for understanding how shared intelligence enhances decision-making.

2.7.4 Situational awareness and threat intelligence models

A recurring concept across CIS frameworks is situational awareness, defined as the ability to comprehend and act upon the cyber threat environment using shared intelligence (Serini, 2024). SMEs with higher situational awareness are more likely to adopt preventive controls and contribute to community resilience (Renaud & Ophoff, 2021). However, participation among SMEs remains low due to the predominance of manual, resource-intensive sharing processes and persistent fears of exposing

sensitive data (Wagner et al., 2019; Shojaifar & Fricker, 2020). Models such as Zhao & White (2012) group-centric Secure Information Sharing emphasise trust, privacy safeguards, and community-based governance; yet, their successful implementation demands reliable coordination mechanisms that are often beyond SMEs' capacity.

2.7.5 Types and levels of threat intelligence

Another dimension of CIS frameworks is the type of threat intelligence shared, which ranges from strategic (executive-level decision support) to operational (threat actor behaviours), tactical (technical attack details), and technical (malware signatures and vulnerabilities) (Leszczyna & Wróbel, 2019; Pawar et al., 2024). While this categorisation helps standardise exchanges, its rigidity struggles to keep pace with the rapidly evolving threat landscape that often requires blended or cross-level intelligence (Möller, 2023).

2.7.6 Human and organisational dimensions of CIS frameworks

Beyond technical and procedural considerations, human factors remain critical. Studies show that organisational support, perceived behavioural control, and subjective norms strongly influence employee commitment to CIS, often outweighing trust alone (Safa & Von Solms, 2016; Bishop, Asquith & Morgan, 2025). Lewis et al. (2014) further proposed a taxonomy indicating that SMEs share information selectively depending on its perceived business impact, operational benefits, or reputational risks. These behavioural insights underscore that even the most sophisticated frameworks cannot succeed without addressing the psychological, social, and organisational dimensions of information sharing.

In summary, although a range of CIS frameworks exists, from general guidelines such as ISO/IEC 27032 and NISTIR 7621 Small Business Guidance to advanced threat-sharing platforms like MISP, these solutions often fail to meet the contextual needs of South African SMEs (Clark & Mujeye, 2025). This failure is multifaceted: international frameworks are typically complex, resource-intensive, and designed for larger organisations with dedicated IT staff and budgets, which most SMEs in South Africa lack (Chidukwani, Zander & Koutsakis, 2024). They also assume regulatory and infrastructural conditions that differ from the South African context, including POPIA compliance, limited ICT access in rural areas, and sector-specific operational constraints. Cultural and socio-economic factors, such as trust in technology, fear of reputational damage, and informal business practices, are similarly overlooked. To date, very few frameworks have been tailored specifically for South African SMEs, leaving a critical gap in locally relevant guidance. Addressing this gap is necessary because SMEs operate under unique

conditions, including limited resources, informal management structures, and sector-specific risk profiles. Human-centric CIS protocols that integrate behavioural, socio-cultural, psychological, technological, and policy considerations are, therefore, essential to make CIS adoption feasible, sustainable, and sensitive to the realities of South African SMEs. By embedding human factors, resource constraints, and sector-specific needs into practical, scalable models, such protocols can transform CIS from a largely aspirational practice into a viable mechanism for enhancing cybersecurity resilience.

2.8 Developing a literature-informed protocol for effective cybersecurity information sharing

2.8.1 Integrating insights from the literature

The development of a CIS protocol tailored to SMEs in South Africa requires an integration of insights into their unique challenges, the role of human factors, the strengths and limitations of existing frameworks, and the influence of policies and procedures. Section 2.4 highlighted that SMEs remain disproportionately vulnerable due to resource scarcity and limited expertise. It further established that laws and policies mandate reporting but do not adequately influence SME behaviour, with compliance gaps persisting due to underreporting and perceived burdens. Section 2.5 emphasised the importance of CIS for collective resilience but noted that adoption is undermined by barriers such as a lack of trust, awareness, and incentives. Section 2.6 demonstrated that most existing protocols and standards are designed with larger enterprises in mind and therefore lack applicability in the SME context. Section 2.7 reviewed prominent frameworks such as NIST 800-150 and ISO/IEC 27032, showing that while they provide useful structures, they overlook the behavioural and organisational factors shaping participation. Taken together, these literature findings underscore the need for a preliminary human-centric CIS protocol that is sensitive to the realities of SMEs.

2.8.2 Trust as a central principle

Central to the design of a human-centric CIS protocol is the concept of trust. Existing literature consistently demonstrates that trust not only motivates participation but also underpins the effectiveness of all other dimensions of information sharing (Safa & Von Solms, 2016; Collier et al., 2023). A trust-centric perspective ensures that SMEs view CIS not as a regulatory burden but as a collaborative practice with tangible security benefits. Trust, therefore, serves as the unifying principle across the five critical concepts distilled from the review: behavioural, socio-cultural, psychological, technological, and regulatory. Trust-building mechanisms, such as anonymised data sharing and the establishment of

trusted peer networks, directly align with this dimension, providing the foundational component of the proposed protocol.

2.8.3 Behavioural dimension

The behavioural dimension relates to how SMEs perceive risks and benefits, as well as their willingness to share information. Participation is strengthened when SMEs possess situational awareness and can link knowledge to actionable behaviour, supported by clear incentives (Safa & Von Solms, 2016; Solansky & Beck, 2021). This behavioural perspective underpins the protocol component of simplifying and incentivising information sharing, ensuring that SMEs are supported in acting on their awareness with reduced burden and clear rewards.

2.8.4 Socio-cultural dimension

The socio-cultural dimension reflects the influence of community norms, peer networks, and industry collaboration. Studies on human behaviour show that SMEs are more likely to share threat intelligence when embedded within trusted communities or sector-specific networks (Pala & Zhuang, 2019; Collier et al., 2023). The emphasis on community norms and peer networks informs the protocol's focus on fostering a collaborative culture and ensuring psychological safety, enabling SMEs to share information more openly.

2.8.5 Psychological dimension

The psychological dimension emphasises the need for environments that minimise the fear of exposure or reputational damage while promoting a sense of psychological safety. Approaches such as applying heuristics and developing non-punitive sharing environments have been shown to encourage openness (Lewis et al., 2014; Schinagl & Paans, 2017; Staneiu, 2022). This dimension reinforces the protocol element of creating psychologically safe environments and peer-to-peer learning structures, encouraging SMEs to participate without fear of reputational harm.

2.8.6 Technological dimension

The technological dimension necessitates platforms that reduce the burden of participation by facilitating semi-automated, secure, and trust-focused sharing. Modern solutions, such as blockchain-enabled or semi-automated systems, provide methods to enhance reliability and mitigate privacy concerns (Purohit et al., 2020; van Haastrecht et al., 2021). Technological enablers, including secure platforms and semi-

automated reporting mechanisms, directly correspond to the protocol's component aimed at lowering the burden of participation while safeguarding trust.

2.8.7 Regulatory dimension

Finally, the regulatory dimension involves aligning laws, policies, and procedures with SME contexts by providing standardised communication mechanisms and clearer compliance pathways (Koepke, 2017; Chidukwani, Zander & Koutsakis, 2022). This regulatory perspective relates to the protocol element of ensuring legal and ethical guidelines, thereby making compliance pathways clearer and more relevant for SMEs. Taken together, the behavioural, socio-cultural, psychological, technological, and regulatory dimensions discussed in sections 2.8.1 to 2.8.7 provide the scaffolding for a trust-centric protocol.

2.8.8 Towards a trust-centric protocol

Taken together, the behavioural, socio-cultural, psychological, technological, and regulatory dimensions suggest that an effective SME-focused CIS protocol must move beyond technical or legal prescriptions to integrate human factors as active design elements. Trust emerges as the unifying principle that shapes behavioural, socio-cultural, psychological, technological, and regulatory influences into a coherent framework. The preliminary protocol, informed by Chapter 2, positions elements for the establishment of trust-building mechanisms not as isolated factors but as the thread linking the simplification and incentivisation of information-sharing processes, fostering a collaborative culture and safety, ensuring legal compliance and ethical guidelines, and providing ongoing support and feedback. Figure 2.1 illustrates how the listed elements interact within a trust-centric model for CIS, offering both a synthesis of the reviewed literature and a foundation for protocol development that will be refined in subsequent empirical stages.

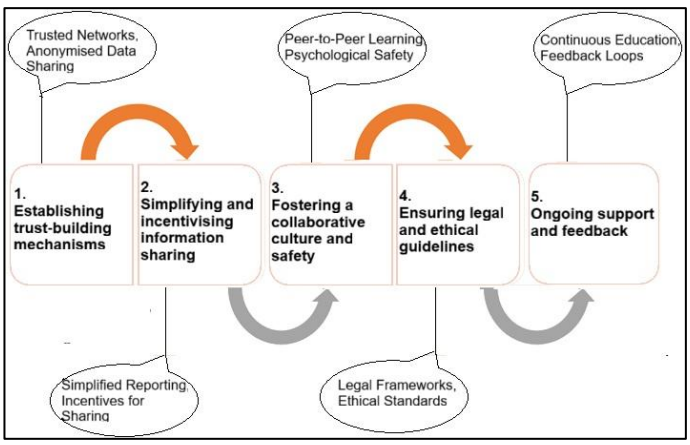


Figure 2-1: Protocol to foster effective CIS amongst SMEs in South Africa

The protocol illustrated in Figure 2.1 consists of five components: establishing trust-building mechanisms, simplifying and incentivising information sharing, fostering a collaborative culture and safety, ensuring legal and ethical guidelines, and providing ongoing support and feedback. These five specified components operate as a dynamic cycle in which each component reinforces the next. *Establishing trust-building mechanisms* forms the entry point, as SMEs are unlikely to share information without confidence in the security and integrity of exchanges. Once trust is established, *simplified processes and incentives* reduce participation burdens and highlight tangible benefits, encouraging broader engagement. This leads to the cultivation of a *collaborative culture and psychological safety*, where SMEs view sharing as a mutually supportive practice rather than a risk. To sustain this culture, *legal and ethical guidelines* provide clarity, accountability, and alignment with regulatory expectations, reducing uncertainty and fostering consistency. Finally, *ongoing support and feedback* ensure that SMEs continuously adapt, learn, and refine their participation, feeding back into trust and strengthening the overall cycle of effective CIS.

This preliminary protocol serves as a baseline that will be refined in the empirical stages of this research to develop a human-centric protocol that can lead to reciprocal CIS among SMEs. The next section, 2.9, will discuss the theoretical framework. The theoretical framework discussed in the next section will be used to study human factors, thereby operationalising the preliminary protocol.

2.9 Theoretical framework

A theoretical framework provides the foundation for structuring research, guiding data collection, and informing analysis by linking research problems to key variables and relevant theories (Grant & Osanloo, 2014; Salawu et al., 2023). It functions as a blueprint that shapes how phenomena are understood and how findings contribute to knowledge. In this study, the framework is central to explaining the human factors that influence SME participation in CIS. Since the aim is to develop a human-centric protocol, the framework must capture the behavioural, social, and contextual influences that underpin CIS behaviour.

Human behaviour models are widely applied in information systems research to explain adoption, technology use, and decision-making (Venkatesh et al., 2003). Eight prominent models have informed past studies: the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB), the Technology Acceptance Model (TAM), SCT, Motivational Model (MM), and the Innovation Diffusion Theory (IDT). These are reviewed below to justify the adoption of SCT for this study.

2.9.1 Common human behaviour models in information systems

Theory of Reasoned Action (TRA): TRA posits that behaviour is predicted by attitudes, subjective norms, and intentions (Kuo, Roldan-Bau & Lowinger, 2015). While useful, TRA assumes behaviour is rational and intentional, overlooking habit and environmental constraints (Taherdoost, 2018).

Theory of Planned Behaviour (TPB): TPB extends TRA by adding perceived behavioural control, reflecting how individuals' sense of ability shapes intentions (Ajzen, 1985). Its limitation is that it neglects emotional, cultural, and unconscious influences.

Technology Acceptance Model (TAM): TAM adapts TRA with the constructs of perceived usefulness and ease of use, which shape adoption intentions (Davis, 1989; Venkatesh et al., 2003). TAM has been widely applied but overlooks organisational norms and contextual pressures that compel usage beyond individual perceptions (Ang, Ramayah & Amin, 2015).

Social Cognitive Theory (SCT): SCT views behaviour as a dynamic interplay between personal factors, behaviour, and environment (Bandura, 1986). Its constructs of self-efficacy, outcome expectations, social persuasion, and reciprocal determinism make it particularly suited for explaining human-centric cybersecurity behaviours (Middleton, Hall & Raeside, 2019).

Motivational Model (MM): MM distinguishes between intrinsic (enjoyment) and extrinsic (usefulness) motivations (Ryan & Deci, 2000). Its weakness lies in generalisation, assuming homogeneity of motivations across individuals.

Innovation Diffusion Theory (IDT): IDT explains the adoption of innovations through characteristics of adopters, innovations, and communication processes (Rogers, 2003). It is useful for understanding diffusion over time but is limited in predicting individual behavioural drivers in complex environments (Taherdoost, 2018).

In sum, while TRA, TPB, TAM, MM, and IDT each contribute to understanding adoption behaviour, SCT provides a more holistic account by recognising the reciprocal interaction of human, technological, and environmental factors. For this reason, SCT is adopted as the theoretical framework for this study.

2.9.2 SCT as a framework

SCT conceptualises behaviour through reciprocal determinism, which is the dynamic interaction of personal factors, behaviour, and environment (Bandura, 1982, 1986). Its emphasis on self-efficacy is

critical, as an SME's willingness to share information is strongly tied to confidence in their ability to create, report, and share intelligence securely (Schunk & DiBenedetto, 2023). SCT also highlights observational learning, where SMEs model behaviours from peers within trusted networks (Ika Tamrin, Norman & Hamid, 2021). Figure 2.2 illustrates the adapted SCT framework, highlighting six interrelated components that shape SMEs' participation in CIS:

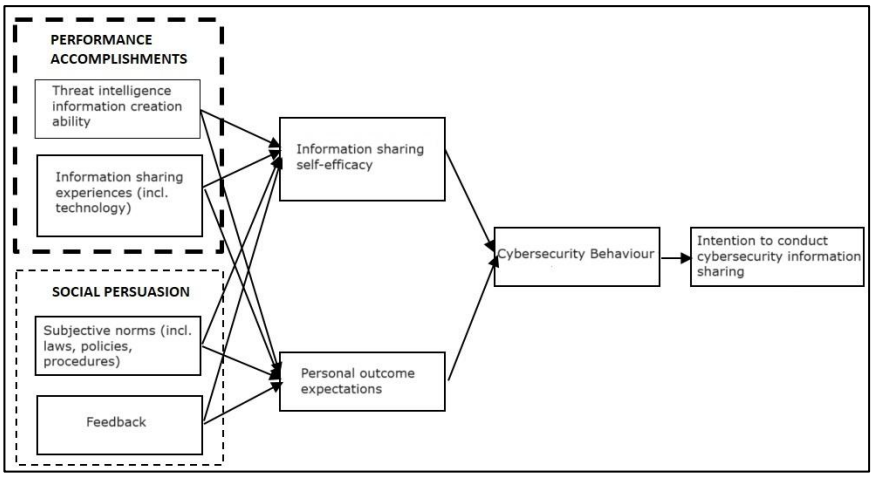


Figure 2-2: Theoretical framework (Ika Tamrin, Norman & Hamid, 2021)

Here is a brief explanation of each of the six interrelated components of the SCT framework shown in Figure 2.2 above:

- Performance accomplishments: ability to create and share threat intelligence based on past experiences;
- Social persuasion: subjective norms and feedback that reinforce behaviour;
- Information sharing self-efficacy: confidence in the ability to share effectively;
- Personal outcome expectations: internal motive to share effectively drawn from awareness of the benefits and risks of CIS;
- Cybersecurity behaviour: best practices guiding when, how, and with whom to share;
- Intention to conduct CIS: the decision to engage in actual sharing practices.

Additionally, the explanation regarding how each of the six interconnected SCT framework components mentioned above interacts with one another is provided below:

The process begins with *performance accomplishments*, where SMEs build competence through their ability to create and share threat intelligence based on prior experiences. These accomplishments provide both confidence and practical skills. Similarly, *social persuasion* operates alongside

performance accomplishments by exerting external reinforcement through *subjective norms* such as laws, policies, industry expectations, and feedback mechanisms from peers or regulators.

Both performance accomplishments and social persuasion contribute to *information sharing self-efficacy* and *personal outcome expectations*. Together, they shape SMEs' confidence in their capacity to share effectively (self-efficacy) and influence their internal motivations by weighing the benefits and risks of CIS (outcome expectations). This stage is critical as it integrates experiential, social, and motivational influences.

When these drivers are strong, they directly inform *cybersecurity behaviours*. At this stage, SMEs demonstrate concrete practices regarding when, how, and with whom to share threat intelligence. Such behaviours are influenced by efficacy and expectations but are also tested and refined through actual engagement in CIS activities.

Finally, cybersecurity behaviours lead to *intention to conduct CIS*, representing the decision point where SMEs commit to sharing information in practice. Intention reflects the culmination of prior experiences, reinforcements, confidence, and motivations, consolidating them into an actionable choice.

The adapted SCT model presents a progressive pathway in which accomplishments and persuasion feed into efficacy and expectations, which in turn guide behaviours that ultimately shape intention. By emphasising these interactions, the model demonstrates that SME participation in CIS is not driven by a single factor but rather by the integration of experiential, social, psychological, and behavioural influences. This sequential flow reinforces the trust-centric protocol outlined in Section 2.8, highlighting how experiential and social foundations build towards efficacy, behaviour, and intention, thereby operationalising trust within SME information-sharing practices.

SCT has been widely applied across diverse domains, including health communication, organisational behaviour, and cybersecurity. It has been used to explain security policy compliance (Johnston, Wech & Jack, 2000), doxing behaviour (Smolnik, Croasdell & Jennex, 2024), and employee awareness of security threats (Cashin & Ifinedo, 2014). In cybersecurity contexts, SCT effectively accounts for how environmental factors such as policies and reporting platforms; personal factors such as efficacy and motivation; and social norms influence behaviour.

By adopting SCT, this study situates itself within a robust behavioural tradition that not only explains why SMEs may resist or under-report incidents but also provides actionable insights for protocol design.

SCT thus offers the theoretical underpinning necessary to connect the literature-informed CIS protocol (Section 2.8) with the empirical investigation that follows, ensuring that behavioural, social, and motivational dynamics are embedded in the framework for SMEs to participate in CIS.

2.10 Summary

The literature review highlights the urgent need for a human-centric approach to CIS, as SMEs face escalating threats such as phishing, ransomware, and BEC. While digital adoption enables SMEs to pursue growth and competitiveness, it simultaneously exposes them to increasingly sophisticated risks, including cybercrime-as-a-service and AI-enabled attacks. Despite regulatory mandates such as POPIA, GDPR, and CIRCIA, participation in CIS remains limited. SMEs are constrained by internal barriers, such as limited expertise, budget restrictions, and weak management support, as well as external challenges, including poor cyber hygiene and socio-cultural constraints. Human factors, ranging from behavioural inconsistencies and organisational norms to psychological barriers of mistrust, emerge as decisive in shaping CIS engagement. Although frameworks like NIST 800-150 and ISO/IEC 27032 provide technical guidance, they fail to account for trust, usability, and SME-specific realities.

This review therefore identifies five interrelated domains: behavioural, socio-cultural, psychological, technological, and regulatory. These must be addressed through a human-centric CIS protocol, with trust as the central integrating element. SCT is the adopted theoretical framework, as it explains how personal, environmental, and behavioural factors interact to shape cybersecurity decision-making. Collectively, this positions the study to contribute a socio-technical protocol that integrates governance, human behaviour, and enabling technologies to strengthen SME resilience through effective CIS. The next chapter outlines the research methodology used to investigate the SME retail sector in the Eastern Cape, providing empirical grounding for the literature-informed protocol and deeper insight into the human and contextual influences shaping CIS participation.

3 CHAPTER THREE: METHODOLOGY

3.1 Introduction

This chapter presents the research design and methodology employed to address the study's research questions and objectives outlined in Chapter 1. The discussion begins by establishing the study's philosophical stance, with pragmatism adopted as the guiding paradigm. It then details the research design, including the rationale for selecting a mixed-methods approach. Subsequent sections describe the population, sampling strategies, and data collection and analysis procedures, illustrating how these choices collectively ensure the collection of reliable, valid, and ethically sound data. The chapter concludes with a discussion of validity and reliability, outlining the measures implemented to enhance the robustness and trustworthiness of the study's findings. The methodological choices made in this chapter collectively support the rigorous design and validation of a human-centred CIS protocol tailored for SMEs.

3.2 Research philosophy

Research philosophy defines the assumptions about knowledge and reality that guide a study's approach (Saunders, Lewis & Thornhill, 2016), shaping methodological choices and ensuring alignment with the research questions. To determine the most appropriate philosophical lens for this study, the researcher first examined the major philosophies commonly considered for research studies in information systems and information technology, which include positivism, interpretivism, critical realism, and pragmatism (Adam, 2014; Swaleh & Wabwoba, 2025).

Positivism treats knowledge as objective and measurable, supporting quantitative methods (Karupiah, 2022); however, it is limited in capturing social meaning and contextual nuance (Ryan, 2018). Interpretivism emphasizes subjective, socially constructed knowledge, valuing meaning and context over generalisation (Scauso, 2020). Its limitations include challenges in replicability and establishing broad validity. Critical realism recognises an independent reality while acknowledging that knowledge is socially mediated (Elder-Vass, 2021; Smith, 2023). Critics argue that its abstract nature may render it dehumanising. Pragmatism prioritises practical solutions and actionable knowledge, allowing the integration of multiple methods to address complex real-world problems (Kelly & Cordeiro, 2020). Although it has been critiqued for potential relativism, where validity may vary across contexts, this limitation can be mitigated through triangulation and methodological rigour, ensuring findings are credible, cross-validated, and grounded in multiple sources of evidence.

After reviewing these paradigms and considering the study's focus on developing a human-centric CIS protocol for SMEs, pragmatism was selected as the guiding philosophy. The pragmatic philosophy enables the combination of quantitative and qualitative data to capture the complex human factors influencing SME participation, supporting a methodology that is both rigorous and practically relevant.

3.3 Research design

A research design provides a structured blueprint for conducting a study, guiding decisions on sampling, data collection, analysis, and the management of bias and validity (Creswell & Creswell, 2018; Dannels, 2018). Research designs are broadly categorised into three types: quantitative, qualitative, and mixed-methods (Creswell & Creswell, 2018). To select the design most appropriate for this study and closely aligned with the chosen pragmatic paradigm, the researcher reviewed the characteristics, applications, advantages, and limitations of each type of research design.

3.3.1 Quantitative

Quantitative research designs focus on measuring variables and testing relationships through structured data collection, providing statistical rigor and generalisable insights. They are closely associated with the post-positivist paradigm, emphasising objective measurement to identify trends, attitudes, or behaviours (Fowler, 2014; Panke, 2024). Common quantitative designs include surveys, experiments, and causal-comparative studies. The advantages of quantitative research include statistical rigour, larger sample coverage, and efficiency in data collection (Rahman, 2016; Ghafar, 2023). However, the limitations are that quantitative methods only present snapshots of phenomena, thereby lacking depth and overlooking respondents' experiences (Rahman, 2016). Furthermore, quantitative research may struggle to provide explanations for specific behaviours and typically offers only a broad understanding of the topic under investigation (Ghafar, 2023).

3.3.2 Qualitative

Qualitative research designs, in contrast, prioritise understanding participants' experiences and the meanings they attach to phenomena, thereby offering depth and contextual richness. Qualitative research design is regarded as flexible and particularly advantageous for studying social phenomena, aiming to explore participants' perspectives and interpretations of their environment (Malagon-Maldonado, 2014; Creswell & Creswell, 2018). Common strategies associated with qualitative research designs include case studies, phenomenology, grounded theory, and narrative research (Astalin, 2013). Qualitative research design is especially beneficial when investigating topics with limited existing information or when seeking to comprehend complex phenomena from participants' viewpoints

(Malagon-Maldonado, 2014). Advantages include rich, nuanced insights, cultural sensitivity, and a deeper understanding of complex social processes (Lee, 2024). Limitations encompass potential researcher bias, small sample sizes, and challenges in generalising findings (Mwita, 2022). Data collection and analysis can be labour-intensive and time-consuming, and researcher subjectivity may influence interpretation, thereby complicating the achievement of objectivity (Mwita, 2022; Lee, 2024).

3.3.3 Mixed-methods

Mixed-methods designs integrate both quantitative and qualitative research methods to provide a more comprehensive understanding of phenomena. This approach allows researchers to capture numerical trends while also exploring the nuanced perspectives of participants (Harrison, 2024). Mixed-methods research design addresses complex research questions that cannot be fully answered by a single method (Aramo-Immonen, 2013; Sharma et al., 2023). The advantages of using mixed-methods research design include triangulation for validity, a richer understanding, and adaptability to emerging findings (Grace, Banson & Saraf, 2023; Harrison, 2024). It enables researchers to adjust their methods as new insights emerge, fostering iterative exploration (Gerzso & Riedl, 2024).

Table 3.1 below provides a comparison of the key characteristics of the three types of research designs: quantitative, qualitative, and mixed-methods research design, along with how these three research designs correspond with the research philosophies, strategies, and methods.

Table 3-1: Comparative overview of qualitative, quantitative, and mixed-methods approaches and their alignment with research philosophies, strategies, and methods (Creswell & Creswell, 2018: 17)

Tend to or typically…	Qualitative Approaches	Quantitative Approaches	Mixed Method Approaches
Use these philosophical assumptions	Constructivist / transformative knowledge claims	Postpositivist knowledge claims	Pragmatic knowledge claims
Employ these strategies of inquiry	Phenomenology, grounded theory, ethnography, case study, and narrative	Surveys and experiments	Sequential, convergent and transformative
Employ these methods	Open-ended questions, emerging approaches, text or image data	Closed-ended questions, predetermined approaches, numeric data (may include some open-ended questions)	Both open- and closed-ended questions, both emerging and predetermined approaches, and both quantitative and qualitative data and analysis
Use these practices of research as the researcher	Positions him- or herself	Tests or verifies theories or explanations	Collects both quantitative and qualitative data
	Collects participant meanings	Identifies variables to study	Develops a rationale for mixing

	Focuses on a single concept or phenomenon	Relates variables in questions or hypotheses	Integrates the data at different stages of inquiry
	Brings personal values into the study	Uses standards of validity and reliability	Presents visual pictures of the procedures in the study
	Studies the context or setting of participants	Observes and measures information numerically	Employs the practices of both quantitative and qualitative research
	Validates the accuracy of the data	Uses unbiased approaches	
	Makes interpretations of the data	Employs statistical procedures	
	Creates an agenda for change or reform		
	Collaboration with the participants		
	Employs text analysis procedures		

Based on the discussion in Sections 3.3.1 – 3.3.3 and supported by Table 3.1 above, the study employed a mixed-methods research design. Table 3.1 further illustrates how adopting mixed methods aligns with a pragmatic philosophy for understanding knowledge.

Various designs exist for mixed-methods research. These include the convergent parallel design, in which quantitative and qualitative data are collected and integrated simultaneously; the explanatory sequential design, where a quantitative phase is followed by qualitative exploration; and the exploratory sequential design, where qualitative findings inform subsequent quantitative testing (Creswell & Creswell, 2018; Sharma et al., 2023). The explanatory sequential mixed-methods research design was selected to capture both numerical trends and nuanced perspectives of SMEs. This design closely aligns with the study's pragmatic philosophy and supports the development of a human-centric CIS protocol that reflects both quantitative evidence and the complex human factors influencing CIS adoption. Moreover, this explanatory sequential mixed-methods research design aligns with the research objectives outlined in Chapter 1 and facilitates a systematic integration of quantitative and qualitative data to develop a human-centric CIS protocol. Figure 3.1 presents a comprehensive methodological

process diagram for the study, summarising how the implementation process of the explanatory sequential mixed-methods design was utilised.

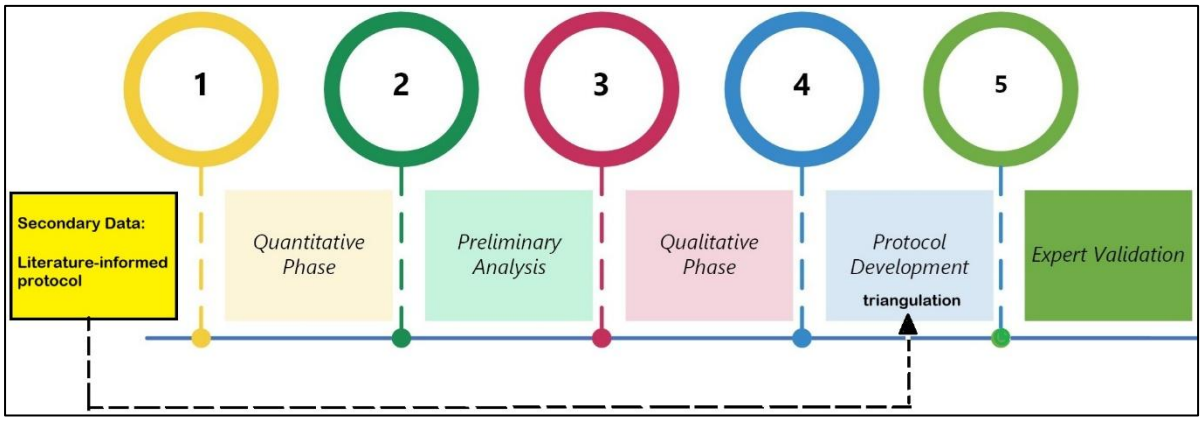


Figure 3-1: Methodological process diagram

As shown in Figure 3.1 above, the process begins with the analysis of secondary data, resulting in a literature-informed protocol. The sequential explanatory process then proceeded through the following five steps:

1) *Quantitative Phase* – Quantitative data were collected from a sample of SMEs operating in the Eastern Cape, South Africa, to identify statistically significant human, organisational, and technological factors that influence the adoption of CIS practices among SMEs.
2) *Preliminary Analysis* – The quantitative data were analysed to determine patterns and trends, providing evidence to inform the Qualitative phase.
3) *Qualitative Phase* – Qualitative data were subsequently collected from SMEs that participated in the quantitative phase to explore the identified phenomena in greater depth, capturing participants' experiences, perceptions, and contextual factors that influence participation in CIS.
4) *Protocol Development* – Quantitative findings were contextualised and enriched through qualitative insights. These primary data were integrated with the literature-informed protocol to develop a human-centric CIS protocol that reflects both measurable outcomes and an in-depth understanding of human factors, guided by SCT.
5) *Expert Validation* – The protocol was evaluated by subject-matter experts. Feedback from this validation was integrated to refine the protocol and enhance its applicability and effectiveness in promoting SME participation in CIS.

This structured process ensured that the final protocol was both evidence-based and responsive to the practical realities of SMEs. It combined the strengths of quantitative measurement with the depth of

qualitative insight, ensuring that the research outcomes are credible, contextually relevant, and practically useful. The next section outlines the population and sampling techniques employed to select participants for both the quantitative and qualitative phases of the study.

3.4 Population and sampling techniques

The study population comprised SMEs operating in South Africa, particularly those situated in the Eastern Cape. The focus was on SMEs in the services sector that have incorporated ICT into their operations. Participants were selected from urban areas in the Eastern Cape, specifically the Buffalo City Metropolitan Municipality and the Nelson Mandela Bay Metropolitan Municipality.

Sequential mixed-methods research designs allow for multiple strategies for selecting participants. As stated by Collins, Onwuegbuzie & Jiao (2007), these can be classified as:

- Identical samples, where the same participants are involved in both the quantitative and qualitative phases;
- Parallel samples, where different participants are selected for each phase, but all are drawn from the same population;
- Nested samples, where participants selected for one phase represent a subset of those involved in the other phase; and
- Multilevel samples, where two or more sets of samples are obtained from different levels of the study.

For this study, a nested sampling design was adopted to satisfy the requirements of both research phases outlined in Section 3.3.3. In the quantitative phase, participants were required to be managers, owners, or officers of SMEs operating in the Eastern Cape, with sufficient knowledge of their organisation's operations to respond to the structured questionnaire. In the qualitative phase, participants were selected from those who completed the quantitative phase and were willing to provide additional insights through semi-structured interviews, ensuring an in-depth exploration of the phenomena identified statistically. Nested sampling was considered suitable for this study as it allows for the integration of both quantitative and qualitative data by selecting interview participants from the original survey respondents, thereby enhancing continuity, contextual understanding, and explanatory power of the sequential design (Creswell & Plano Clark, 2018). This approach ensures that qualitative insights directly reflect the patterns and behaviours identified in the quantitative phase, improving the overall validity and coherence of the findings. Teddlie & Yu (2007) note that typical quantitative sampling

techniques used in mixed-methods research include simple random sampling, systematic sampling, stratified sampling, cluster sampling, snowball sampling, and purposive sampling (quantitative phase), while qualitative sampling commonly involves purposive (judgement) sampling, snowball sampling, and maximum variation sampling.

3.4.1 Quantitative sampling techniques in mixed-methods research

The following represents a brief overview of the common quantitative sampling techniques used in mixed-methods research:

- Simple random sampling: Every individual in the population has an equal chance of selection. For example, SMEs could be assigned numbers, and participants randomly drawn to minimise selection bias (Teddlie & Yu, 2007).
- Systematic sampling: Participants are selected at regular intervals from a population list, such as every 10th SME (Teddlie & Yu, 2007).
- Stratified sampling: Ensures proportional representation from distinct subgroups, such as industry sub-sectors or years of operation (Teddlie & Yu, 2007).
- Cluster sampling: Appropriate when populations are geographically dispersed. Entire clusters (such as, metropolitan regions) are randomly selected to reduce resource requirements (Teddlie & Yu, 2007).
- Snowball sampling: Particularly relevant when access to participants is limited. Initial participants refer others, enabling the researcher to reach SMEs that may not be listed in formal networks (Teddlie & Yu, 2007; Bryman, 2016).
- Purposive sampling (quantitative phase): Used as a supplementary strategy when participants must meet specific inclusion criteria, such as operating in the retail sector, having adopted ICT, and being located in urban metropolitan areas (Etikan, 2016).

The first (quantitative) phase, as outlined in the methodological process diagram in Figure 3.1, employed snowball sampling. This sampling technique was chosen for the first phase due to barriers in accessing SME populations and the hidden nature of SMEs within urban communities. To ensure methodological rigour and relevance to the research aims, explicit inclusion criteria were applied when selecting SMEs from the retail sector. SMEs were included in the study if they met the following criteria:

- SME Classification: The business had to meet the South African National Small Enterprise Act thresholds for SME classification, based on sector-specific turnover, number of employees, and asset value.
- Use of ICT in Core Operations: The SME had to actively use ICT systems such as point-of-sale applications, cloud services, e-commerce platforms, online banking, or digital communication tools. This ensured direct relevance to cybersecurity and CIS practices.
- Exposure to Cybersecurity Issues: SMEs needed to have encountered basic cybersecurity concerns (such as, phishing attempts, suspicious emails, system downtime, or interaction with IT support). This criterion ensured participants could meaningfully engage with CIS-related questions.
- Willingness to Participate: Participation was voluntary and contingent upon agreement to complete the survey and/or qualitative interviews.
- Sectoral and Geographic Alignment: Only SMEs operating in the Eastern Cape retail sector were eligible, ensuring contextual relevance to the study.

Target respondents included SME managers, owners, or officers, as these individuals possess strategic knowledge and a holistic understanding of the organisation. The intended sample size was 25 (N=25), which is considered acceptable for exploratory quantitative studies in contexts with limited populations and accessibility (Kianpour et al., 2019; Shojaifar & Fricker, 2020). Ultimately, 22 responses were received. While this sample is small, it aligns with exploratory research in social and behavioural studies, where the focus is on understanding phenomena rather than achieving statistical generalisability (Saunders, Lewis & Thornhill, 2016; Creswell & Creswell, 2018). Small sample sizes are deemed appropriate for identifying patterns, relationships, and human factors in specific contexts, particularly when complemented by qualitative follow-up, as in an explanatory sequential design (Ivankova, Creswell & Stick, 2006). The emphasis of the quantitative phase was, therefore, on uncovering the human factors influencing CIS adoption among SMEs in the Eastern Cape, rather than generating findings that can be generalised across all South African SMEs. Small samples are common in cybersecurity research due to limited access to organisations, confidentiality constraints, and niche focus areas, such as SME cybersecurity behaviour (Neuman, 2011; Ifinedo, 2012). Despite limited generalisability, small-sample studies can yield valuable insights when justified by exploratory aims, research context, and the use of robust analytical techniques (Kianpour et al., 2019; Shojaifar & Fricker, 2023). Triangulating quantitative and qualitative data further strengthens the reliability of findings (Crotty & Daniel, 2022).

3.4.2 Qualitative sampling techniques in mixed-methods research

The third (Qualitative) phase, as per Figure 3.1, aimed to explore and contextualise findings from the quantitative phase. Common qualitative sampling techniques include:

- Purposive sampling: Participants are selected based on characteristics relevant to the research objectives. Clear selection criteria and a diverse participant range are recommended to reduce bias (Etikan, 2016; Nyimbili & Nyimbili, 2024).
- Snowball sampling: Useful for accessing hard-to-reach populations, where participants refer other potential participants within their network (Teddlie & Yu, 2007).
- Maximum variation sampling: A subtype of purposive sampling where participants are deliberately selected to capture diverse perspectives (such as, SMEs that do and do not participate in CIS), providing richer contextual understanding (Patton, 2015).

For this study, purposive sampling was employed in the qualitative phase to ensure that participants with relevant experience and knowledge of CIS practices in SMEs were included, allowing for an in-depth exploration of the identified phenomena. Participants were drawn from the initial quantitative sample based on their engagement in CIS, ensuring representation of both participating and non-participating SMEs. This approach enabled a deeper exploration of the findings from the first phase. A total of 10 participants was targeted for interviews, consistent with recommendations for achieving thematic saturation in exploratory qualitative research (Guest, Bunce & Johnson, 2006).

The next section, 3.5 Data Collection Method, outlines the procedures employed to gather and integrate these data across the quantitative and qualitative phases.

3.5 Data collection method

Explanatory sequential mixed-methods studies employ distinct data collection methods for the quantitative and qualitative phases. Quantitative data collection typically involves surveys, questionnaires, and secondary data analysis (Ivankova, Creswell & Stick, 2006). Surveys and questionnaires use structured, closed-ended questions to gather numerical data, enabling the identification of trends and patterns. Their advantages include efficiency in reaching large populations and ease of statistical analysis, while limitations include reduced depth and limited contextual understanding. Secondary data analysis involves examining existing datasets or records to complement survey findings. This method is cost-effective and time-efficient but provides limited control over data accuracy or relevance (Ivankova, Creswell & Stick, 2006).

Qualitative data collection commonly employs interviews, focus groups, case studies, and document analysis. Interviews and focus groups allow for an in-depth exploration of themes or patterns identified during the quantitative phase, providing rich contextual insights (Jackson-Gordon & Plano Clark, 2024). Focus groups additionally generate diverse perspectives through discussion, although responses may be influenced by group dynamics. Document analysis involves reviewing textual materials, such as policies, emails, or training manuals, to triangulate findings and provide a deeper contextual understanding. Limitations include reliance on the availability and quality of documents.

For this study, the quantitative phase employed a closed-ended questionnaire administered online via Google Forms. Respondents were identified through snowball sampling, a technique appropriate for accessing SMEs that may not be listed in formal databases or networks. Data from this phase informed the following secondary objectives:

- Secondary objective 1: Determine human factors associated with effective CIS.
- Secondary objective 2: Examine policy and technology's influence on human factors associated with CIS.

The qualitative phase employed semi-structured interviews conducted either face-to-face or via online platforms (such as, WhatsApp, MS Teams, Zoom), depending on participant convenience. Participants were identified through purposive sampling, drawn from the first phase sample to ensure representation of SMEs that do and do not participate in CIS. The intended qualitative sample size was 10 participants, which is sufficient for achieving data saturation in exploratory studies of small, specialised populations (Guest, Bunce & Johnson, 2006). This phase provided rich, contextual insights into the human factors influencing CIS adoption and addressed secondary objectives 2 and 3:

- Secondary objective 2: Examine policy and technology's influence on human factors associated with CIS.
- Secondary objective 3: Develop a protocol for SMEs seeking to implement policies and technology interventions that optimize CIS.

This nested data collection approach ensured that quantitative findings were complemented and enriched by qualitative insights, providing a comprehensive understanding of human factors affecting CIS adoption.

3.5.1 Evaluation of the protocol

The expert validation phase, as outlined in Figure 3.1, addresses secondary objective 4 of this study. Its purpose was to evaluate the efficacy of the developed CIS protocol. This evaluation was conducted

through a survey of six purposefully selected cybersecurity experts, chosen for their expertise in cybersecurity and experience with SMEs (Creswell & Creswell, 2018). To ensure a rigorous and transparent selection process, explicit inclusion criteria were used to identify experts suitable for evaluating the protocol. Experts were required to meet the following criteria:

- Domain-Specific Expertise: Each expert needed specialised knowledge in at least one of the following: cybersecurity operations or governance, information systems research, cybersecurity policy or regulation, SME cybersecurity management, or threat intelligence frameworks such as MISP, STIX, TAXII, or AIS.
- Minimum Professional Experience: Experts had to possess at least five years of experience in a relevant cybersecurity or ICT field.
- Role Relevance: Eligible experts included cybersecurity analysts, information security managers, ICT decision-makers, researchers, system architects, and consultants.
- Familiarity with SMEs or CIS: Preference was given to experts who had direct professional experience working with SMEs or with CIS initiatives.
- Independence: Experts were drawn from outside the SME participant pool to ensure objectivity.

The expert panel represented research, decision-making, and technical perspectives, providing comprehensive feedback on the protocol's clarity, applicability, and effectiveness in achieving the study's aims. The survey instrument, presented in Appendix G, comprised both closed-ended and open-ended questions, enabling the collection of quantitative ratings and qualitative insights (Creswell & Plano Clark, 2018). This dual approach allowed for a thorough assessment and informed refinement of the protocol.

3.5.2 Ethical considerations

This study adhered to rigorous ethical standards to protect the rights, privacy, and well-being of all participants. Ethical clearance was formally granted by the Central University of Technology Research Ethics Committee, with the certificate issued on 31 May 2024 (see Appendix B). Prior to participation, each individual received a detailed consent form explaining the study's objectives, their expected contributions, and the voluntary nature of their involvement (see Appendix C). Participants were assured of their right to withdraw at any stage, with any previously collected data managed according to a jointly agreed decision. Confidentiality was maintained through the use of pseudonyms, and participants' identities were never disclosed without explicit consent.

3.6 Data collection instrument development

The development of the data collection instruments for this study was guided by SCT, the research objectives (Section 1.4), and the research questions (Section 1.3). SCT provides a theoretical lens to examine the dynamic interaction between individual behaviour, environmental factors, and expected outcomes in the context of CIS among SMEs. This theoretical underpinning ensured that the instruments captured both behavioural and cognitive dimensions of CIS, while also considering organisational and environmental influences.

The instruments were designed to gather both quantitative measures of knowledge, behaviour, intention, and literacy, as well as qualitative insights into experiences, perceptions, and organisational context. Research Objectives 1, 2, and 3 were addressed through Phase One and Phase Two of the explanatory sequential mixed-methods approach, while Research Objective 4 required a specialised instrument to collect expert evaluations of the CIS protocol. The resulting instruments are provided in Appendices D, E, and F: the quantitative survey, qualitative interview guide, and expert evaluation instrument, respectively.

3.6.1 Integration of SCT, research objectives, and questions

The study systematically mapped SCT constructs to the research objectives and questions to ensure construct validity and theoretical alignment. The mapping is summarised as follows:

- *Performance Accomplishments (Threat Intelligence Creation & Information Sharing Experiences):* Guided questions regarding past knowledge of cyber threats, incident reporting, and information sharing experiences. These questions addressed the objective of understanding individual capabilities and engagement in CIS.
- *Social Persuasion (Subjective Norms & Feedback):* Informed questions on trust, peer influence, and management support. These questions aligned with the objective of assessing environmental and peer influences on CIS behaviour.
- *Information Sharing Self-Efficacy:* Informed questions about confidence in identifying, assessing, and sharing cyber threats, supporting objectives related to perceived ability and readiness to participate in CIS.
- *Personal Outcome Expectations:* Guided questions on organisational culture, perceived benefits, and barriers to sharing, aligning with objectives focused on evaluating motivators and the perceived value of CIS.

- *Cybersecurity Behaviour and Intention to Share:* Informed behavioural and compliance-based questions, addressing objectives related to predicting engagement in CIS and identifying areas for improvement.

This mapping ensured that each SCT construct was operationalised into specific, measurable items while remaining aligned with the study's overarching objectives.

3.6.2 Instrument development process

The development of data collection instruments followed a structured, three-phase process:

a) Quantitative Instrument (Survey):
   - Developed to capture SCT-informed constructs, SME demographic information, and cybersecurity literacy and practices.
   - The survey items were derived from Phase One analysis and designed to measure knowledge, behaviour, intention, and self-efficacy.
   - Items employed Likert scales, Yes/No, and categorical response formats to allow statistical analysis of relationships between constructs and CIS engagement.
   - The finalised survey instrument is provided in Appendix E.

b) Qualitative Instrument (Interview):
   - Developed to capture in-depth, open-ended insights regarding experiences, barriers, motivations, and organisational culture.
   - Phase Two guided the development of interview questions that probed SCT constructs while eliciting rich contextual data on CIS behaviours.
   - Questions addressed performance accomplishments, social persuasion, self-efficacy, personal outcomes, and cybersecurity behaviours.
   - Interviews were semi-structured, allowing flexibility to explore emergent themes while maintaining consistency across respondents.
   - Probes and follow-up questions were included to ensure depth and contextual relevance.
   - The resulting interview guide is presented in Appendix F.

c) Expert Evaluation Instrument (Survey):
   - Developed to evaluate the efficacy of the CIS protocol in addressing the study's objectives.

- The cybersecurity experts who participated in the evaluation were selected based on their SME experience and subject-matter expertise. They assessed the protocol for clarity, applicability, and potential impact.
- The instrument included both closed-ended questions for quantifiable assessment and open-ended questions for qualitative feedback, allowing triangulation of expert perspectives.
- Iterative refinement ensured that the evaluation instrument captured all relevant dimensions of protocol performance.
- The finalised expert evaluation instrument is provided in Appendix G.

This three-phase approach allowed for systematic integration of SCT constructs, research objectives, and questions, while maintaining methodological rigour and enhancing the instruments' relevance and applicability.

3.6.3 Pilot testing

Pilot testing is a critical step in research, as it provides an initial evaluation of data collection instruments to ensure alignment with study objectives and to identify potential issues with question clarity, structure, and flow (Creswell & Creswell, 2018). It also allows the researcher to assess participant fatigue resulting from instrument length or cognitive demand (Bearman, 2019). Pilot testing should involve participants similar to the intended research sample, with feedback used to refine the instrument before full deployment (Bearman, 2019; Williams-Mcbean, 2019).

For this study, three individuals, comprising one manager and two officers of an SME, completed the two data collection instruments under conditions similar to the planned research environment. They evaluated the instruments for issues such as length, clarity, structure, and flow. Their feedback informed the following revisions:

- Length: Sections and questions were summarised to reduce perceived length.
- Clarity and language: Missing response options in the quantitative instrument were identified and corrected.
- Flow and engagement: Adjustments ensured smooth progression and minimised participant fatigue.

- The finalised instruments, incorporating all pilot feedback, are presented in Appendices D and E.

Refer to Appendices D and E to view the final and complete data collection instruments used in this explanatory sequential mixed-methods study.

3.6.4 Replicability and transparency

The structured mapping of SCT constructs to research objectives and research questions, combined with a phased development approach, ensures transparency and reproducibility. Conducting a pilot test guarantees the completeness and effectiveness of data collection instruments. Future researchers can replicate the instruments by following the same mapping procedure, iterative refinement, and validation processes. Clear documentation of item derivation and pilot testing procedures provides a replicable framework for data collection in similar contexts.

3.7 Data analysis technique

In explanatory sequential mixed-methods research, data analysis techniques must align with the type and purpose of the collected data (Creswell & Plano Clark, 2018). The quantitative phase, as illustrated in Figure 3.1, employed a survey questionnaire, making statistical analysis the most appropriate approach to derive meaningful insights from numerical data, investigate trends, and examine relationships (Field, 2018). Quantitative analysis was conducted using descriptive statistics to summarise key characteristics of the data, including measures of central tendency (mean, median, mode), and inferential statistics to examine relationships between variables (Creswell & Creswell, 2018). Descriptive statistics provided an overview of cybersecurity knowledge, CIS engagement, and SME policy perceptions, ensuring an understanding of data distribution before applying inferential techniques. Reliability analysis using Cronbach's alpha assessed the internal consistency of the dataset and engagement measures, ensuring the reliability of the constructs.

Inferential analysis included Spearman's Rank Correlation, which was used to examine relationships between SCT-related constructs (self-efficacy, trust, leadership support, feedback, legal compliance, recognition) and CIS engagement. Additionally, Hierarchical Cluster Analysis (HCA) identified natural groupings of SMEs, informing actionable recommendations in the CIS protocol. All quantitative analyses were performed using IBM SPSS (version 29.0.2.0), which was selected for its suitability for Likert-scale data and handling of small sample sizes.

The qualitative phase, as depicted in Figure 3.1, employed semi-structured interviews that were analysed using qualitative techniques. Two common approaches to qualitative analysis are content analysis, which organises textual data to quantify themes or concepts for comparative purposes, and thematic analysis, which identifies, organises, and interprets patterns and themes within qualitative data (Evans & Lewis, 2018). For this study, thematic analysis was selected to provide a detailed and contextual understanding of trust concerns, organisational barriers, and motivators for participation in the CIS. By coding responses according to SCT constructs, thematic analysis facilitated a systematic exploration of factors influencing behaviour while maintaining a connection to quantitative findings. The qualitative analysis was conducted using Microsoft Excel, ensuring a structured, transparent, and replicable process.

The integration of quantitative and qualitative analyses within a mixed-methods framework enhances the rigor, validity, and applicability of the findings, offering a comprehensive understanding of the CIS among SMEs (Creswell & Plano Clark, 2018). Quantitative results provided statistical insights into patterns and associations, while qualitative findings contextualised these results, revealing nuanced behavioural, organisational, and social factors that shape CIS practices. This combined approach strengthens evidence-based recommendations for the development of the CIS protocol.

3.8 Validity and reliability

3.8.1 Validity

In mixed-methods research, validity ensures that findings are credible, trustworthy, and reflective of real-world phenomena. To strengthen validity in this study, the researcher employed methodological triangulation by integrating quantitative surveys, semi-structured interviews, and expert evaluations. By systematically comparing insights across these diverse sources, the researcher was able to cross-verify results and capture a comprehensive understanding of CIS among SMEs (Fetters, Curry & Creswell, 2013). This triangulated approach not only enhances confidence in the conclusions but also mitigates the limitations inherent in relying on a single method, ensuring that the findings accurately represent the complexities of the studied context (Denzin, 2012; Creswell & Creswell, 2018).

3.8.2 Reliability

Reliability addresses the consistency and reproducibility of results (Zohrabi, 2013). To ensure robust reliability, the researcher methodically documented all research procedures, facilitating future replication. The internal consistency of quantitative instruments was evaluated using Cronbach's alpha, confirming that constructs were measured stably across the sample (Tavakol & Dennick, 2011). For

qualitative data, reliability was reinforced through data triangulation, comparing multiple perspectives to ensure consistency in identified patterns and themes (Fetters, Curry & Creswell, 2013). By deliberately integrating these strategies, this study ensures that both quantitative and qualitative findings are dependable, interpretable, and meaningful, ultimately supporting credible conclusions about factors influencing CIS engagement in SMEs.

3.9 Summary

Chapter 3 presented the research methodology employed to address the study's overarching aim of developing and evaluating a human-centric protocol for enhancing CIS among SMEs. The study utilised an explanatory sequential mixed-methods design, informed by a pragmatic research philosophy. Initially, quantitative data were gathered through a closed-ended questionnaire to investigate the impact of human, technological, and policy-related factors on CIS participation among SMEs. The collected data were analysed using descriptive statistics, reliability tests, and inferential methods, including Spearman's Rank Correlation and HCA, to identify patterns and classify SMEs based on their behaviour. Subsequently, qualitative data were obtained through semi-structured interviews with selected SMEs to explore and contextualise the statistical findings. The interview data were subjected to thematic analysis, facilitating a deeper understanding of participants' experiences, perceptions, and the contextual factors influencing CIS adoption. Sampling strategies were customised for each phase: snowball sampling was utilised for the quantitative survey to reach SMEs within relevant networks, while purposive sampling was employed for the qualitative interviews to ensure participants possessed direct experience and knowledge of CIS practices. The research was grounded in SCT, which guided the design of the instruments and the interpretation of human behavioural constructs. Ethical approval was obtained, and pilot testing was conducted to validate the instruments. The subsequent results chapter will present the quantitative findings, detailing key patterns, correlations, and clusters, before integrating the qualitative insights to provide a comprehensive understanding of SME engagement in CIS and inform protocol development, concluding with the findings from the evaluation of the resulting protocol by experts.

4 CHAPTER FOUR: FINDINGS AND INTERPRETATION

4.1 Introduction

This chapter presents the findings of the study in alignment with the research objectives outlined in Chapter 1. As detailed in Chapter 3, an explanatory sequential mixed-methods approach was employed, combining quantitative and qualitative analyses, with a focus on understanding SME engagement in CIS in South Africa. The findings aim to identify the human factors influencing CIS, examine the role of policy and technology, and further refine the literature-informed protocol presented in Chapter 2 into a human-centric model that promotes reciprocal CIS among SMEs.

Chapter 4 is structured to first present quantitative results, which describe SME demographics, awareness levels, technical capabilities, and patterns of CIS participation. Statistical analyses, including reliability (Cronbach's Alpha), correlation (Spearman's Rank), and cluster analysis (HCA), are presented alongside an interpretation of observed patterns in line with SCT. Secondly, qualitative findings are presented to provide an in-depth understanding of SME perceptions, motivations, and organisational realities that underpin CIS engagement. These qualitative insights are structured around SCT constructs of performance accomplishments, social persuasion, self-efficacy, outcome expectations, cybersecurity behaviour, and intention to share. Thirdly, to close this chapter, Section 4.4 integrates quantitative and qualitative findings to provide a holistic understanding of intention-behaviour alignment, barriers, and enablers, while Section 4.5 summarises the key findings and implications for the design of a human-centric CIS protocol.

4.2 Quantitative findings and interpretation

This section presents the quantitative findings of the study, structured to deliver both descriptive and inferential insights into SME engagement with CIS. The analyses encompass SME demographic profiling, assessment of awareness, evaluation of technical aspects, reliability testing, correlation analysis, and hierarchical clustering of behavioural profiles. The aim is to identify the human, organisational, and technical factors influencing CIS participation and to establish a foundation for integrating qualitative findings in subsequent sections. The findings facilitate the identification of SME behavioural profiles, intention–behaviour gaps, and critical factors influencing effective CIS participation.

4.2.1 SME demographics and profile

The purpose of the demographics and profile questions was to collect general information about SMEs, including their decision-makers, to gain insight into their business characteristics. The study captured a

diverse sample of 22 SMEs across multiple sectors, organisational sizes, years in operation, IT capacities, and geographic locations. Table 4.1 shows that the respondents who participated in the study varied in their staff roles, ranging from technical positions (such as, IT Technician (4.5%), Cybersecurity Specialist (4.5%), Security Analyst (9.1%)) to managerial and customer-facing roles (such as, Managing Partner (4.5%), Manager (13.6%), Customer Consultant (22.7%)). The number of Customer Consultants was dominant, followed by Managers, Security Analysts, and Information Officers. This distribution reflects a diverse set of perspectives and presents a balanced view between technical and non-technical staff, which is important for understanding the different insights and responsibilities related to CIS.

Table 4-1: Job roles in SME

Item	N	%
Technician	1	4,5%
Managing Partner	1	4,5%
IT Technician	1	4,5%
Director	1	4,5%
Cybersecurity Specialist	1	4,5%
Customer consultant	5	22,7%
IT Specialist	1	4,5%
Center Manager	1	4,5%
Court clerk	1	4,5%
Worker	1	4,5%
Security Analyst	2	9,1%
Manager	3	13,6%
Information officer	2	9,1%
Cybersecurity officer	1	4,5%

As shown in Table 4.2, gender representation was evenly split, with 50% male and 50% female respondents. This balance indicates that insights on CIS behaviour and intentions were gathered from a representative sample of both genders, minimising gender bias in profiling SME cybersecurity practices.

Table 4-2: Gender

Item	N	%
Male	11	50,0%
Female	11	50,0%

Table 4.3 shows that respondents reported varying levels of IT knowledge, with 13.6% indicating no knowledge, 18.2% limited knowledge, and 18.2% moderate knowledge. In contrast, 18.2% reported extensive knowledge, while 31.8% described themselves as experts. This variation reflects a diverse range of technical competencies within SMEs, which may influence both confidence and the capacity to engage in CIS effectively. Moreover, respondents with higher IT knowledge are likely to have greater familiarity with cyber incidents and CIS processes, potentially enhancing their participation and proactive engagement in cybersecurity practices.

Table 4-3: Level of IT knowledge

Item	N	%
None	3	13,6%
Limited knowledge	4	18,2%
Moderate knowledge	4	18,2%
Extensive knowledge	4	18,2%
Expert knowledge	7	31,8%

Table 4.4 shows that cybersecurity-specific knowledge among respondents varied considerably. A small proportion reported no knowledge (13.6%) or limited knowledge (18.2%), while the largest group indicated moderate knowledge (31.8%). Smaller proportions reported extensive knowledge (18.2%) or expert knowledge (13.6%). This variation underscores that cybersecurity awareness is unevenly distributed across SMEs, which has implications for their readiness to identify cyber incidents and create incident reports. Uneven awareness levels may also influence SME participation and engagement in CIS initiatives.

Table 4-4: Level of knowledge in cybersecurity

Item	N	%
None	4	18,2%
Very little knowledge	3	13,6%
Limited knowledge	1	4,5%
Moderate knowledge	7	31,8%
Extensive knowledge	4	18,2%
Expert knowledge	3	13,6%

As reported in Table 4.5, SMEs were drawn from diverse sectors, with the majority coming from computer and electronics retail (22.7%), internet and catalogue retail (18.2%), superstores (18.2%), pharmacies (13.6%), and other retail or service sectors. This sectoral diversity provides a broad context

for understanding how CIS engagement might vary based on operational focus, customer interaction, and reliance on technology.

Table 4-5: Sector of SME

Item	N	%
Computer and electronics retail	5	22,7%
Convenience stores	1	4,5%
Home improvement retail	1	4,5%
Internet & catalogue retail	4	18,2%
Multi-line retail	1	4,5%
Restaurants	1	4,5%
Superstores	4	18,2%
Pharmacy	3	13,6%
Financial	1	4,5%
Other	1	4,5%

Table 4.6 reveals that SMEs were geographically distributed, with the largest representation from Bizana (36.4%) and East London (31.8%), followed by Gqeberha (13.6%), Kokstad (9.1%), and Mthatha (9.1%). Regional differences may influence exposure to cybersecurity threats, access to technical resources, and opportunities for sharing threat intelligence within networks.

Table 4-6: City of operation

Item	N	%
Gqeberha	3	13,6%
East London	7	31,8%
Kokstad	2	9,1%
Mthatha	2	9,1%
Bizana	8	36,4%

As shown in Table 4.7, the majority of SMEs had been in operation for 3–5 years (36.4%) or 6–10 years (27.3%), while 22.7% had been operating for less than 2 years and 13.6% for over 15 years. This range reflects both emerging and established SMEs, suggesting that experience and organisational maturity may influence both awareness and engagement in CIS practices.

Table 4-7: SME years in operation

Item	N	%
less than 2 years	5	22,7%
3-5 years	8	36,4%
6-10 years	6	27,3%
Over 15 years	3	13,6%

Table 4.8 indicates that most SMEs were small, with 63.6% employing fewer than 10 staff members, while 36.4% had between 51 and 250 employees. This distribution is relevant because organisational size may affect the formalisation of processes, internal IT support, and the ability to participate in structured CIS activities. Smaller SMEs may lack IT and security personnel, impacting their CIS readiness compared to larger SMEs, which may have better IT and security capacity.

Table 4-8: Number of employees

Item	N	%
Below 10	14	63,6%
51 - 250	8	36,4%

As reported in Table 4.9, 50% of SMEs had dedicated IT personnel involved in security, while the remaining 50% did not. This indicates that half of the SMEs may lack specialised internal capacity to manage cybersecurity threats, potentially affecting their operational readiness and willingness to participate in CIS.

Table 4-9: IT personnel in security

Item	N	%
Yes	11	50,0%
No	11	50,0%

The demographic profiling of respondents and SMEs reveals a heterogeneous landscape in terms of technical expertise, operational maturity, and sectoral and regional contexts. SMEs exhibit a mix of technical and managerial perspectives, alongside varying IT and cybersecurity competencies, which suggests differing levels of confidence and ability to engage in CIS practices. Smaller organisations, particularly those with fewer than 10 employees or without dedicated IT security personnel, may face capacity constraints that limit their active participation in information sharing, despite potentially high awareness or intention. Sectoral and regional differences indicate that context-specific barriers, such as

access to resources or exposure to cyber threats, are likely to influence engagement. Collectively, this profiling provides a characterisation of the SME population, forming a foundation for interpreting behavioural intentions, information-sharing patterns, and designing tailored interventions to improve CIS adoption.

4.2.2 SME awareness, challenges, and technical aspects

This section presents the descriptive findings regarding the approximate level of SME awareness of CIS, the obstacles they encountered in participating, and the technical aspects of their operational readiness. The data provides insight into the readiness and constraints of SMEs in adopting CIS practices. Figure 4.1 illustrates that 59.09% of respondents expressed extreme concern for the security of their company assets, whereas only 13.64% reported no concern.

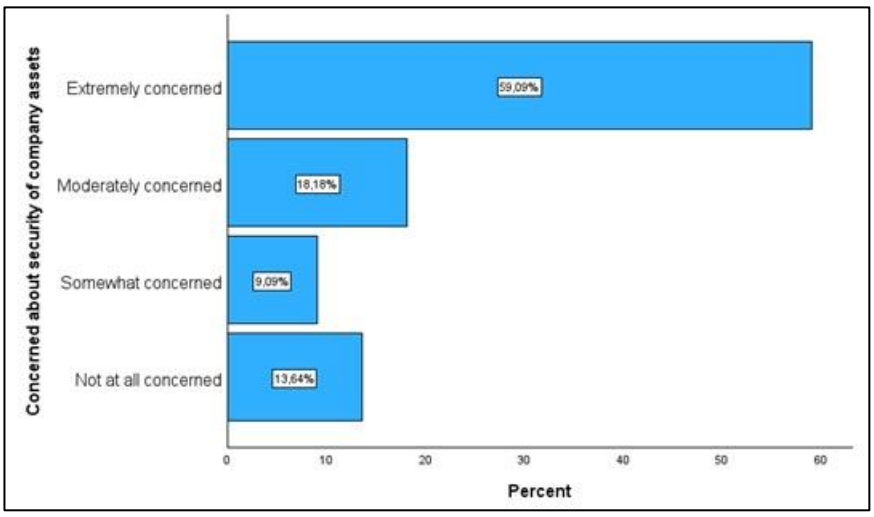


Figure 4-1: Concerned about company assets

This high level of awareness underscores the perceived criticality of digital asset protection for SME continuity. The job roles in Table 4.1 help contextualise these responses; participants in technical and security roles, such as IT Technicians, Cybersecurity Specialists, and Security Analysts, likely contributed to higher levels of concern, reflecting their exposure to organisational risks. Similarly, managerial and customer-facing staff demonstrated awareness, suggesting a holistic recognition of asset vulnerability across SME hierarchies.

Figure 4.2 presents respondents' self-assessed CIS knowledge. A majority (54.55%) considered themselves knowledgeable, 36.36% reported lacking CIS knowledge, and 9.09% were uncertain. CIS knowledge is a key indicator of whether SMEs can engage meaningfully in threat intelligence sharing. Moreover, the level of CIS knowledge is often influenced by the presence of dedicated IT or cybersecurity staff, which can enhance an SME's capacity to participate in CIS initiatives.

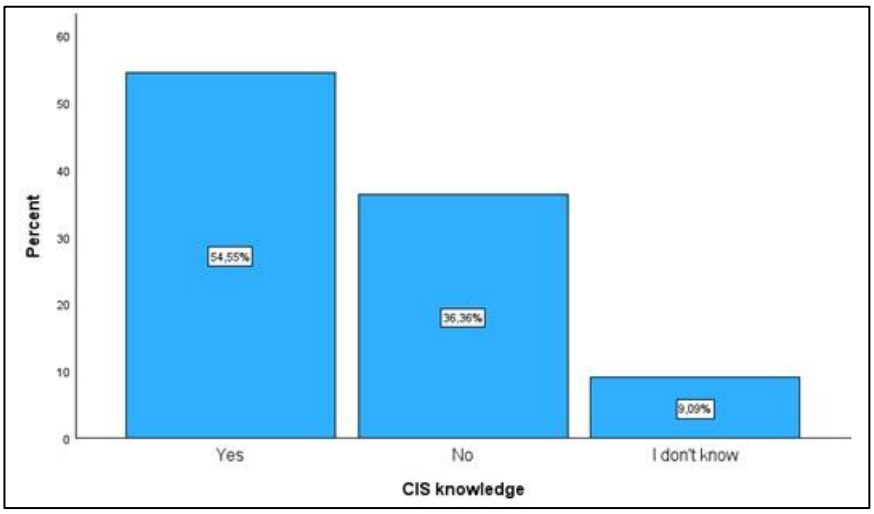


Figure 4-2: CIS knowledge

In Table 4.10, respondents' understanding of what constitutes a cyber incident varied: 63.6% confirmed their knowledge, 31.8% lacked awareness, and 4.5% were unsure. SMEs with dedicated IT or security personnel, as reflected in Table 4.9, were more likely to demonstrate familiarity and the ability to recognise incidents, highlighting the role of technical expertise in CIS readiness.

Table 4-10: Cyber incident knowledge

Item		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	14	63,6	63,6	63,6
	No	7	31,8	31,8	95,5
	I don't know	1	4,5	4,5	100,0
	Total	22	100,0	100,0	

Sector and geographical distribution further contextualise awareness levels. SMEs operating in computer and electronics retail, internet retail, and superstores (Table 4.5) reported higher familiarity with the CIS and increased awareness of cyber incidents compared with other sectors, likely reflecting their exposure to technology-driven threats. Similarly, SMEs based in urban centres such as East London and Gqeberha (Table 4.6) were more likely to access cybersecurity resources, whereas SMEs located outside urban centres, such as Bizana, reported greater uncertainty regarding incidents and reporting structures.

Table 4.11 shows that 54.5% of SMEs reported not having experienced a cyberattack, 22.7% confirmed prior attacks, and 22.7% were unsure.

Table 4-11: SME cyberattacked

Item		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	5	22,7	22,7	22,7
	No	12	54,5	54,5	77,3
	Maybe	5	22,7	22,7	100,0
	Total	22	100,0	100,0	

Given the prevalence of cyber threats, it is unlikely that over half of these SMEs have truly avoided attacks. This is likely due to underreporting, limited incident detection, or low awareness of cyber risks within the organisation. The high proportion of respondents unsure about prior attacks further highlights gaps in monitoring, record-keeping, and cybersecurity readiness. These findings indicate that SMEs may overestimate their cyber resilience and underappreciate the need for proactive threat intelligence sharing, which directly impacts their engagement in CIS initiatives.

At the sector level, Table 4.12 indicates that 45.5% of respondents acknowledged sector-level cyberattacks, while 40.9% reported none, and 13.6% were uncertain. The contrast between organisational and sector-level perceptions may suggest underreporting or limited internal awareness of cybersecurity events. SMEs with fewer employees (Table 4.8) and those operating for less than five years (Table 4.7) were particularly likely to be uncertain, suggesting that organisational maturity and workforce size influence perceptions of cyberattacks.

Table 4-12: Sector cyberattacked

Item		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	10	45,5	45,5	45,5
	No	9	40,9	40,9	86,4
	Maybe	3	13,6	13,6	100,0
	Total	22	100,0	100,0	

The ability to generate cyber incident reports is essential for effective CIS. Table 4.13 demonstrates that 40.9% of respondents could create reports, while 50% could not, and 9.1% were unsure. Figure 4.3 further confirms this, showing that only 45.5% of respondents reported proficiency in creating reports. These findings are linked to the respondents' technical roles (Table 4.1) and IT knowledge (Tables 4.3–4.4). SMEs with dedicated IT or security personnel reported higher competence in reporting.

Table 4-13: Can create cyber incident report

Item		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	9	40,9	40,9	40,9
	No	11	50,0	50,0	90,9
	I don't know	2	9,1	9,1	100,0
	Total	22	100,0	100,0	

Figures 4.3 and 4.4 reveal internal and external reporting pathways. Internally as reported in Figure 4.3, management and organisational structures received equal recognition (33.36%), while IT was identified by 27.27%.

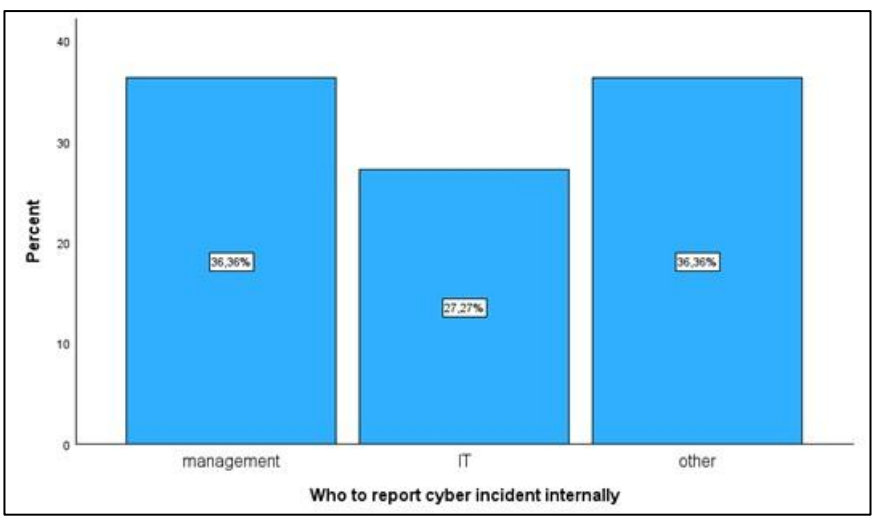


Figure 4-3: Who to report cyber incident internally

Externally as reported in Figure 4.4, 63.64% of SMEs share reports with third parties, 27.27% with other stakeholders, and 9.09% within collaborative communities.

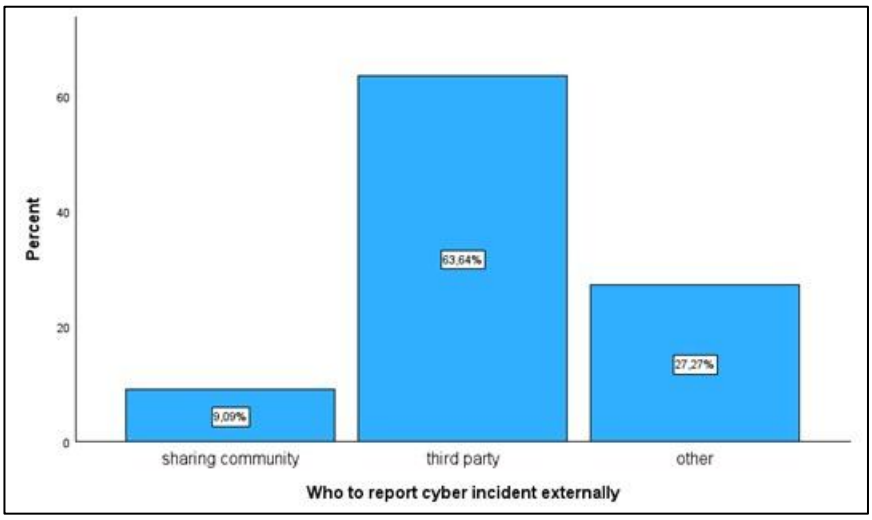


Figure 4-4: Who to report cyber incident externally

The absence of standardised reporting protocols, as indicated in Table 4.14, where 63.6% of SMEs reported lacking a standardised reporting format and only 36.4% reported having one, highlights procedural gaps that may undermine the effectiveness of CIS.

Table 4-14: Standardised reporting format

Item		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	8	36,4	36,4	36,4
	No	14	63,6	63,6	100,0
	Total	22	100,0	100,0	

Without standardisation, the clarity, consistency, and usability of shared information are compromised, limiting SMEs' ability to contribute meaningfully to broader CIS initiatives. This finding underscores the need for clearly defined reporting procedures to enhance the effectiveness and reliability of threat intelligence sharing.

Figure 4.5 shows that 36.4% of respondents found access to CIS platforms difficult, while 22.7% reported it as very difficult. In contrast, 18.2% found access easy, 4.5% very easy, and 18.2% were neutral.

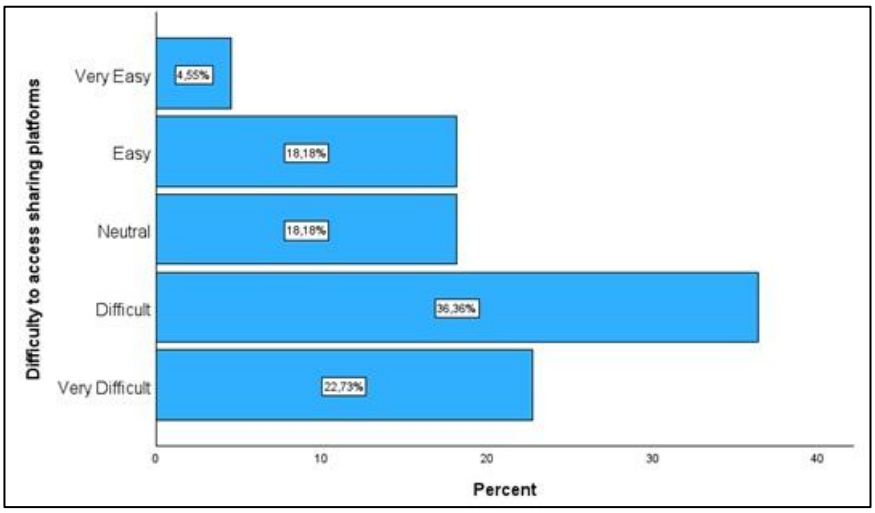


Figure 4-5: Difficulty in accessing sharing platforms

These responses highlight technical barriers that are compounded by procedural gaps. Table 4.14 shows that 63.6% of SMEs lack a standardised reporting format, limiting the clarity, consistency, and usability of shared information. Knowledge disparities further exacerbate these challenges; as illustrated in Figures 4.2 and Table 4.4, while some SMEs report moderate to expert knowledge in CIS and cybersecurity, a substantial proportion indicate limited or no understanding. The combination of limited platform access, uneven procedural standardisation, and variable knowledge levels underscores the multifaceted barriers that hinder effective CIS participation among SMEs. These findings suggest that both structural and human factors, which include IT capacity, procedural readiness, and cybersecurity literacy, must be addressed to enable meaningful engagement in information-sharing initiatives.

Notably, Figure 4.6 shows that 50% of respondents did not perceive participation in CIS as challenging, despite the access difficulties highlighted in Figure 4.5 and the procedural gaps in Table 4.14. In contrast, 31.82% acknowledged challenges, and 18.18% were uncertain.

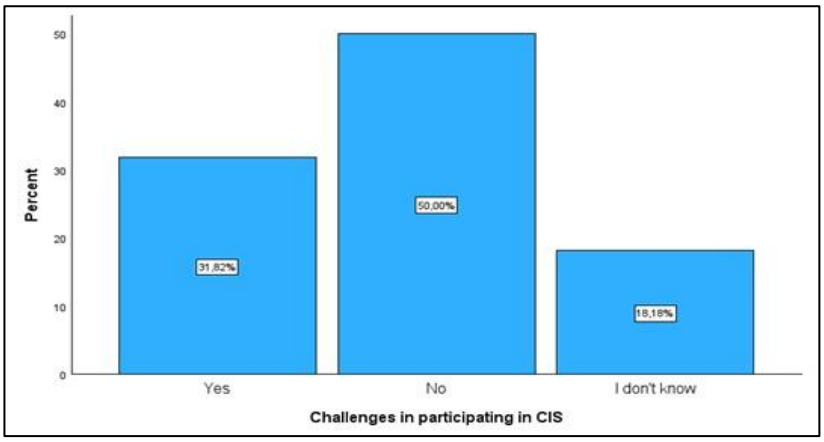


Figure 4-6: Challenges in participating in CIS

These findings suggest that organisational characteristics, such as IT knowledge, the presence of dedicated security personnel (Table 4.9), and SME size (Table 4.8), mediate perceived difficulties. They distinguish between actual technical and procedural barriers and those that are perceptual. Consequently, both tangible factors (platform access, reporting standards, cybersecurity knowledge) and organisational context shape SME engagement in CIS.

Table 4.15 highlights respondents' perspectives on enhancing CIS, with 59.1% indicating a need for improvement, 18.2% believing that no improvements are required, and 22.7% expressing uncertainty.

Table 4-15: Improvements needed in CIS within SME

Item		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	13	59,1	59,1	59,1
	No	4	18,2	18,2	77,3
	Maybe	5	22,7	22,7	100,0
	Total	22	100,0	100,0	

The strong majority underscores that SMEs recognise current CIS processes as insufficiently robust or accessible. Key areas for improvement drawn from the findings include standardising reporting procedures, increasing platform accessibility, and enhancing cybersecurity awareness. This demonstrates that SMEs not only acknowledge existing gaps but are also willing to take action to strengthen their participation in CIS initiatives.

The findings from SME demographics (Tables 4.1–4.9), technical knowledge, and reporting capabilities provide a nuanced understanding of CIS readiness. Key implications include:

- Technical capability as a determinant of CIS engagement: SMEs with IT and cybersecurity expertise, or dedicated security personnel, are more likely to engage in CIS activities, identify incidents, and create reports.
- Organisational maturity and size matter: Larger SMEs and those with longer operational histories demonstrate higher procedural readiness and reporting confidence.
- Sectoral and geographic influences: Exposure to technology-intensive sectors and urban operating environments enhances cyber awareness and CIS familiarity.

- Procedural gaps and standardisation need: Limited standardised reporting formats and inconsistent internal/external reporting pathways indicate structural weaknesses that must be addressed to optimise CIS participation.
- Baseline for inferential analysis: These descriptive insights provide context for subsequent inferential analyses, such as Spearman's Rank Correlation and Hierarchical Cluster Analysis, highlighting the convergence of human factors, organisational characteristics, and behavioural patterns in shaping SME CIS behaviour.

4.2.3 Reliability analysis (Cronbach's alpha)

Reliability analysis was conducted to assess the internal consistency of the survey instruments used to measure constructs related to CIS among SMEs. Cronbach's alpha coefficients were calculated for all key constructs to determine whether the items within each scale consistently measured the intended concept. As Taber (2018) notes, the interpretation of Cronbach's alpha values is context-dependent and can be evaluated as illustrated in Table 4.16. A threshold of $\alpha \geq 0.70$ was considered acceptable for research reliability (Nunnally & Bernstein, 1994; Tavakol & Dennick, 2011).

Table 4-16: Interpretation of Cronbach's Alpha values

Cronbach's Alpha (α)	Interpretation
≥ 0.90	Excellent reliability (very strong internal consistency)
0.80 - 0.89	Good reliability
0.70 - 0.79	Acceptable reliability (suitable for exploratory research)
0.60 - 0.69	Questionable reliability (low internal consistency)
< 0.60	Poor reliability (not suitable for research)

The initial reliability assessment identified several variables that contributed minimally to overall consistency. The variables removed were: *Number of IT personnel* (+0.026), *Experience* (+0.018), *Age* (+0.014), *Confidence in ability to share CIS externally* (+0.008), and *Highest Qualification* (+0.012). These variables were eliminated not merely on statistical grounds, but also after careful theoretical consideration. For example, *Number of IT personnel* reflects organisational size rather than individual behavioural intent to participate in CIS; its inclusion could have introduced construct-irrelevant variance, potentially diluting measures of human-centric CIS behaviours (DeVellis, 2017). Similarly, *Experience* and *Highest Qualification* capture demographic characteristics that, while informative for descriptive purposes, do not directly contribute to the operationalisation of constructs such *as Information Sharing Self-Efficacy or Cybersecurity Behaviour. As reflected in Table 4.17, removing these variables enhanced internal consistency without undermining the theoretical scope of the constructs.*

Table 4-17: Resulting Cronbach Alpha values from refinement of dataset

Pre-refinement

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,665	,728	83

Post-refinements

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,735	,781	79

Pre-refinement, the Cronbach's alpha value of 0.665 indicated questionable reliability, which could compromise the precision of inferential analyses if left unaddressed (Tavakol & Dennick, 2011). Post-refinement, the Cronbach's alpha increased to 0.735, reflecting acceptable reliability. Although one construct, *Information Sharing Activity*, had an alpha of 0.692 (borderline), it was retained due to its theoretical importance in capturing actual CIS behaviours. Retaining borderline constructs is supported in exploratory SME studies, where removing conceptually relevant items could reduce content validity (Field, 2018).

Following these refinements, variables were grouped according to the SCT framework underpinning this study. Table 4.18 represents the Cronbach's alpha values for these SCT-aligned constructs, with these calculated results confirming the reliability of each grouping.

Table 4-18: Variable groupings in alignment with SCT

#	Adapted SCT Element / Sub-element	New Construct	Variables in Construct	Cronbach's Alpha
1	Intention to Conduct CIS	CIS Intention	SMEintentiontosharethreatinformationexternally, Intentiontosharethreatinformationinternally, SMEpromotessharing, Recommendotherstoshare	0.853
2	Information Sharing Experiences	Governance Preparedness	SMEPolicyoncybersecurity, SMEDisasterRecoveryPlanforcyberattacks	0.850
3	Cybersecurity Behaviour	Cybersecurity Best Practice Engagement	ApplyCybersecuritybestpractice, EvidenceofCISactivityinsector	0.837
4	Information Sharing Self-Efficacy	Operational Sharing Confidence	ConfidenceinabilitytoshareCISinternally, ConfidenceinabilitytoshareCISexternally	0.809
5	Personal Outcome Expectations	Cyber Resilience Outcome Beliefs	BeliefCISwithinSMEcanimproveresilience, confidentCISimprovesresilience, confidentcommunityCISimprovesresilience, BelieveCISwithotherSMEsimrpovesresilience	0.777
6	Information Sharing Experiences	Information Sharing Activity	Frequencyofreportinginternally, Frequencyofreportingexternally, Experienceinsharingthreatinformationinternally, Experienceinsharingthreatinformationexternally	0.692

7	Social Persuasion	Subjective Norms	Peersexpecttoshare, LikelihoodtosharewithotherSMEreciprocity, Likelihoodtoreportincidentifarule, ManagementinvestinCIS, ManagementsupprtCIS	0.771

All SCT-aligned constructs demonstrate reliability ranging from acceptable to good, confirming that the survey items consistently measure the intended concepts. The borderline reliability of the *Information Sharing Activity* construct is acknowledged, but its retention ensures content validity in capturing actual CIS behaviours, which is central to understanding the human factors influencing SME participation.

In conclusion, the critical refinement and reliability assessment ensure that only constructs with sufficient internal consistency are included in subsequent inferential analyses, while descriptive variables are retained selectively to contextualise the findings. This approach balances statistical rigour with theoretical fidelity, enhancing the overall validity of the dataset and supporting robust insights into CIS adoption among SMEs.

4.2.4 Spearman's rank correlation analysis

Spearman's Rank Correlation Coefficient (Rs) was used to examine the strength and direction of monotonic relationships between key SCT-aligned constructs related to CIS among SMEs. This non-parametric approach was chosen due to the ordinal nature of several variables and deviations from normality in the dataset (Field, 2018). Correlation analysis helps identify potential associations that may inform the behavioural mechanisms underpinning CIS participation. Table 4.19 presents the constructs used in the correlation analysis, aligned with the adapted SCT framework.

Table 4-19: Constructs used in Spearman's Rank Correlation Analysis

#	Adapted SCT Element / Sub-element	New Construct	Variables in Construct
1	Intention to Conduct CIS	CIS Intention	SMEintentiontosharethreatinformationexternally, Intentiontosharethreatinformationinternally, SMEpromotessharing, Recommendotherstoshare
3	Cybersecurity Behaviour	Cybersecurity Best Practice Engagement	ApplyCybersecuritybestpractice, EvidenceofCISactivityinsector
4	Information Sharing Self-Efficacy	Operational Sharing Confidence	ConfidenceinabilitytoshareCISinternally, ConfidenceinabilitytoshareCISexternally
5	Personal Outcome Expectations	Cyber Resilience Outcome Beliefs	BeliefCISwithinSMEcanimproveresilience, confidentCISimprovesresilience, confidentcommunityCISimprovesresilience, BelieveCISwithotherSMEsimrpovesresilience

7	Social Persuasion	Subjective Norms	Peersexpecttoshare, LikelihoodtosharewithotherSMEreciprocity, Likelihoodtoreportincidentifarule, ManagementinvestinCIS, ManagementsupprtCIS

R_s values were interpreted using contextually informed thresholds (Cohen, 2013), where,

- $R_s > 0.7$ represents a strong relationship
- $0.4 \leq R_s < 0.7$ represents a moderate positive relationship
- $0.2 \leq R_s < 0.4$ represents a weak positive relationship
- $R_s \approx 0$ represents no correlation
- $R_s < 0$ represents negative correlation

Conventional guidance categorises $R_s \geq 0.70$ as strong, $0.40 \leq R_s < 0.70$ as moderate, and $R_s < 0.40$ as weak; these were critically assessed in the context of SME CIS behaviour. Moderate correlations may still reflect meaningful behavioural associations given the multifactorial nature of CIS adoption, where intention, confidence, norms, and organisational context interact. Table 4.20 shows correlations between construct variables with strong positive correlations ($R_s > 0.60$).

Table 4-20: Strong Positive Spearman's Rank Correlations ($R_s > 0.60$)

Variable Pair	Spearman R_s	Interpretation
Recommendotherstoshare *correlation with* BeliefCISwithinSMEcanimproveresilience	0.73	SMEs that believe sharing improves resilience are more likely to advocate sharing
SMEpromotessharing *correlation with* BeliefCISwithinSMEcanimproveresilience	0.69	Perceived organisational benefit predicts proactive encouragement
ApplyCybersecuritybestpractice *correlation with* EvidenceofCISactivityinsector	0.72	Good practice is aligned with observed external CIS activity
Recommendotherstoshare *correlation with* Peersexpecttoshare	0.65	Strong peer norms relate to internal promotion of sharing

These strong correlations confirm SCT propositions that outcome expectations and social persuasion mechanisms significantly influence sharing intentions and advocacy. SMEs perceiving CIS benefits internally or at the sector level demonstrate higher proactive engagement, consistent with prior literature (Bandura, 1986; Siponen, Adam Mahmood & Pahnila, 2014).

Table 4.21 shows moderate correlations, which are numerically lower than strong correlations, but still represent meaningful behavioural enablers in SMEs. These results underscore that CIS adoption is influenced by multiple interacting factors rather than a single determinant.

Table 4-21: Moderate Positive Spearman's Rank Correlations ($0.40 \leq R_s \leq 0.60$)

Variable Pair	Spearman R_s	Interpretation
Intentiontosharethreatinformationinternally correlation with BeliefCISwithinSMEcanimproveresilience	0.63	Internal sharing intention linked to resilience beliefs
SMEpromotessharing correlation with BelieveCISwithotherSMEsimrpovesresilience	0.60	Sharing advocacy is tied to belief in collective resilience
Recommendotherstoshare correlation with ManagementinvestinCIS	0.40	Internal investment signals promote peer engagement
SMEintentiontosharethreatinformationexternally correlation with Intentiontosharethreatinformationinternally	0.53	Internal and external sharing intentions co-occur

Notably, the correlation between *ConfidenceinabilitytoshareCISinternally* and *ApplyCybersecuritybestpractice* was −0.69, suggesting that confidence in internal sharing does not necessarily translate to observable best-practice engagement. Similarly, *ManagementsupprtCIS* correlations were low or negative across several intention variables, indicating potential gaps between symbolic managerial support and functional influence on CIS behaviour.

These nuanced results highlight that high self-efficacy or perceived management support does not automatically ensure behavioural execution, reinforcing the importance of considering contextual and social mechanisms alongside individual beliefs (Bandura, 1986; Johnston & Warkentin, 2010).

Spearman's correlation analysis demonstrates that SCT-aligned constructs related to outcome expectations and subjective norms are most strongly associated with CIS intention and advocacy. Moderate or weak correlations provide insight into subtle enablers or barriers in SME cybersecurity behaviour, informing subsequent cluster analyses. By interpreting correlations contextually rather than applying thresholds mechanistically, this study preserves theoretical integrity while revealing key human factors driving CIS participation.

4.2.5 Hierarchical Cluster Analysis (HCA)

HCA was conducted to identify distinct behavioural profiles of SMEs based on their engagement with CIS. HCA is suitable for this study as it allows for the identification of naturally occurring groupings within small sample datasets, providing insight into heterogeneous patterns of intention and activity without assuming prior knowledge of cluster membership (Everitt et al., 2011; Hair et al., 2019). Ward's linkage

method was applied using squared Euclidean distance to minimise within-cluster variance and ensure maximally distinct clusters (Ward, 1963).

Table 4.22 lists the constructs used for HCA. Two key domains of CIS intention and Information Sharing Activity were included to capture both attitudinal and behavioural dimensions aligned with SCT (Bandura, 1986).

Table 4-22: Constructs used in Hierarchical Cluster Analysis (HCA)

#	Adapted SCT Element / Sub-element	New Construct	Variables in Construct
1	Intention to Conduct CIS	CIS Intention	SMEintentiontosharethreatinformationexternally, Intentiontosharethreatinformationinternally, SMEpromotessharing, Recommendotherstoshare
6	Information Sharing Experiences	Information Sharing Activity	Frequencyofreportinginternally, Frequencyofreportingexternally, Experienceinsharingthreatinformationinternally, Experienceinsharingthreatinformationexternally

The resulting dendrogram in Figure 4.7 revealed three distinct SME clusters. A 3-point interpretive scale (Low = 1.00–2.33; Medium = 2.34–3.66; High = 3.67–5.00) was applied to facilitate meaningful interpretation of cluster means, consistent with previous SME behavioural research where Likert-type data is treated ordinally (Boone & Boone, 2012).

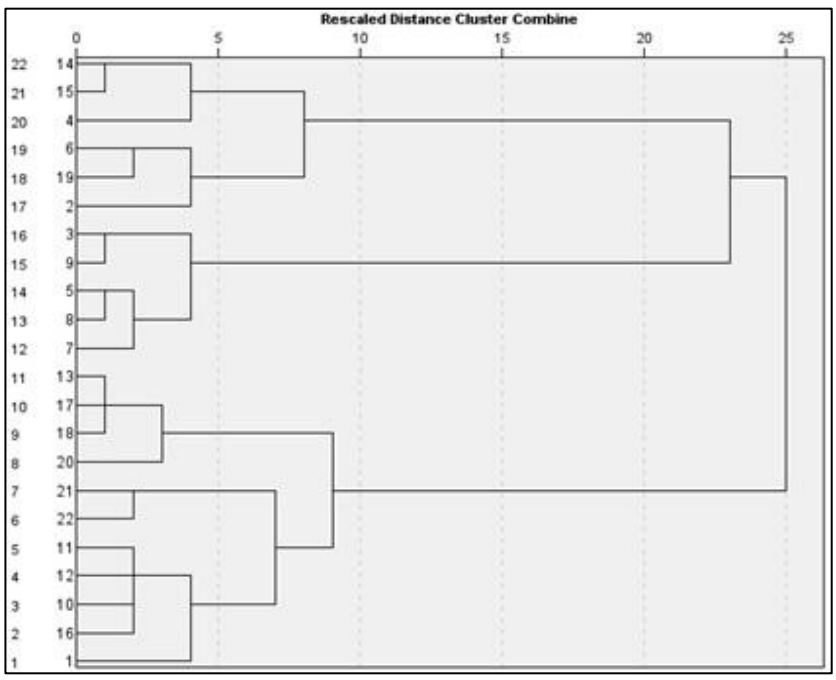


Figure 4-7: Dendrogram using Ward Linkage

Based on Table 4.23, cluster profiles are presented as follows:

- Cluster 1: High intention (Mean = 4.52) but low CIS activity (Mean = 1.59). These SMEs exhibit a pronounced intention–behaviour gap, aligning cognitively with CIS values but failing to operationalise sharing behaviourally. Possible explanations include limited internal capacity, lack of structured processes, or low self-efficacy in executing CIS practices.
- Cluster 2: Medium intention (Mean = 2.67) and moderate activity (Mean = 2.54). SMEs in this cluster appear to engage in CIS episodically or reactively, potentially driven by compliance pressures or external mandates rather than intrinsic motivation.
- Cluster 3: High intention (Mean = 4.40) and high activity (Mean = 3.65). SMEs in this cluster represent the ideal engagement profile, demonstrating alignment between intention and behaviour and exhibiting strong operational participation in CIS.

Table 4-23: Summary of Cluster Profiles

Cluster	CIS Sharing Intention (Mean)	Information Sharing Activity (Mean)	Interpretation
Cluster 1	4.52 (avg. across 4 items)	1.59 (avg. across 4 items)	High intention, but ***low actual sharing activity***. These SMEs likely advocate CIS but may lack internal capacity or confidence.
Cluster 2	2.67	2.54	Lowest intention and mid-level activity. Possibly ***compliance-driven*** or externally mandated reporting.
Cluster 3	4.4	3.65	***High engagement cluster***. SMEs in this group are both willing and operationally active in threat sharing.

The HCA highlights the heterogeneity of SME participation in CIS. Clusters 1 and 2 reveal barriers to converting intention into action, including occasional engagement and intention–behaviour gaps, while Cluster 3 represents SMEs for which positive attitudes and actual behaviours are well-aligned. These findings reinforce SCT propositions that perceived outcome benefits, social persuasion, and self-efficacy are critical determinants of CIS engagement (Bandura, 1986; Johnston & Warkentin, 2010). Table 4.24 presents an integrated inferential analysis of nuanced insights into SME engagement with CIS.

Table 4-24: Integrated inferential summary of SME CIS engagement

Construct / SCT Element	Key Correlations (Spearman R_s)	Cluster Profile	Interpretation
CIS Intention	Recommendothers to share ↔ Belief CIS improves resilience (0.73)	Cluster 1: High intention, low activity	SMEs motivated to share but behaviourally inactive; indicates intention–behaviour gap.
	SMEpromotessharing ↔ Belief CIS improves resilience (0.69)	Cluster 2: Medium intention, moderate activity	Advocacy linked to perceived organisational benefit; episodic/reactive engagement.
Cybersecurity Behaviour	ApplyCybersecuritybestpractice ↔ Evidence of CIS activity (0.72)	Cluster 3: High intention, high activity	Observed external CIS activity reinforces good practice; attitude-behaviour alignment.
Information Sharing Self-Efficacy	Confidence internal ↔ ApplyCybersecuritybestpractice (-0.69)	Cluster 1	High self-efficacy does not guarantee engagement; intention alone is insufficient.
Outcome Expectations / Personal Beliefs	SMEpromotessharing ↔ Believe CIS with other SMEs improves resilience (0.60)	Cluster 2	Perceived sector-level benefits drive advocacy; partially aligned behaviour.
Subjective Norms / Social Persuasion	Recommendothers to share ↔ Peersexpecttoshare (0.65)	Cluster 3	Strong peer norms promote proactive CIS engagement.
Organisational Support	Recommendothers to share ↔ Management invests in CIS (0.40)	Cluster 2	Management influence exists but is weaker; may not fully drive active sharing.

The strong correlations in Table 4.24 reveal that outcome expectations (perceived resilience benefits) and social persuasion (peer norms) are the primary drivers of sharing intention, aligning with SCT propositions that beliefs about outcomes and social influence shape behaviour (Bandura, 1986). However, the negative correlation between self-efficacy and actual best practice engagement highlights a critical intention–behaviour gap, suggesting that confidence alone does not guarantee execution, especially in SMEs with limited resources or procedural knowledge. HCA further identifies heterogeneity among SMEs: Cluster 1 demonstrates high intention but low activity, indicating motivational constraints but operational challenges; Cluster 2 shows episodic engagement, likely influenced by external compliance pressures; and Cluster 3 represents the ideal profile with alignment between intention and action. These findings imply that effective CIS interventions must address both human factors (beliefs, peer influence) and structural enablers (capacity, tools, managerial support) to translate intention into consistent behaviour.

The descriptive and inferential analyses collectively suggest that policy and technological supports are crucial for bridging the intention–behaviour gap. SMEs with high intention but low activity may benefit from standardised reporting tools, capacity-building, and peer-sharing mechanisms to operationalise

their CIS commitment. Furthermore, HCA results provide a foundation for targeted interventions, allowing CIS protocols to be tailored to SMEs according to their readiness and behavioural profiles. However, it is important to note that statistical clustering identifies patterns but not causality, highlighting the necessity of the subsequent qualitative phase to explore organisational interpretations, motivations, and contextual realities influencing CIS engagement.

4.3 Qualitative results

Qualitative results were obtained through a thematic analysis guided by Braun & Clarke (2006) six-phase framework. This framework was selected for its flexibility and suitability for small datasets, enabling a rigorous and structured examination of interview data. Data were manually coded in Microsoft Excel, facilitating systematic organisation, categorisation, and theme development (Bree & Gallagher, 2016).

For each interview question, open coding was employed to identify recurring concepts, terms, and phrases, consistent with Corbin & Strauss (2012) definition of open coding as the process of breaking down data into discrete units for examination. This was followed by axial coding, which grouped codes into categories and identified relationships between them (Charmaz, 2006). Themes were iteratively refined to ensure alignment with the study's theoretical framework based on SCT, ensuring both methodological and theoretical coherence.

The qualitative findings are presented in alignment with the SCT constructs underpinning this study: performance accomplishments, social persuasion, self-efficacy, personal outcome expectations, cybersecurity behaviour, and intention to share cybersecurity information. Each interview question is presented with corresponding participant extracts, supported by graphical frequency representations of responses. Where appropriate, qualitative findings are interpreted alongside quantitative results to highlight convergences and divergences, with particular attention to the barriers influencing the intention–behaviour gap.

4.3.1 Describe a cyber threat incident that has affected your company.

Participant narratives revealed a spectrum of cyber incident experiences, ranging from phishing attacks compromising credentials to malware affecting point-of-sale systems. For example, one participant described:

> "*I received an email from a bank asking me to update my account details by clicking on the link. I entered my login credentials only to discover it was a fake website*" (Participant 01).

Another participant reported a malware attack that impacted operations:

> "*Malware Attack on my Retail Store. The attacker gained access to the store's Point-of-Sale system through a phishing email that was opened by an employee. The email contained a malicious link that downloaded malware onto the POS system*" (Participant 08).

Several participants (Participants 03 and 04) reported no direct experience of cyber incidents, highlighting variation in threat exposure across SMEs.

These narratives provide insight into performance accomplishments, a key construct of SCT, illustrating that prior experience with cyber threats shapes SMEs' perceived ability to engage in CIS. However, the qualitative variation in how incidents were recognised, managed, and articulated suggests that experience alone does not guarantee effective CIS participation. SMEs with a high intention to share threat information often lacked structured reporting procedures, reflecting a gap between motivation and actionable capacity. These findings reinforce the segmentation observed in the HCA, where SMEs with high intention (Cluster 1) frequently lacked the procedural capacity to translate that intention into action. The foundational role of threat experience in shaping performance accomplishments is revealed through this question, while also illustrating that experience alone is insufficient without structured reporting and organisational support.

For this finding, raw responses were coded for incident type (such as, phishing, malware, none), linked to SCT constructs (performance accomplishments, self-efficacy), and grouped into themes such as threat recognition and procedural readiness. Triangulation with quantitative findings confirmed that SMEs' experiences of cyber incidents are foundational but insufficient on their own to drive CIS engagement, reinforcing the need for structured reporting and organisational support.

4.3.2 How do you create an incident report?

SME approaches to creating incident reports varied widely, reflecting differing levels of procedural maturity. Some participants described structured processes, such as template-based reporting, while others relied on informal notifications to management or immediate technical interventions. For instance, one participant explained:

> "*Specifying the date and time of the incident, and the type of incident. And then describe the incident in detail*" (Participant 01).

Another detailed a multi-step template process:

> "1. Gather information; 2. Fill out incident report template; 3. Conduct an investigation; 4. Document findings; 5. Review and revise; 6. Submit report" (Participant 05).

In contrast, some participants reported simpler, informal approaches:

> "*By notifying store management immediately*" (Participant 08),
>
> "*I notify and involve relevant stakeholders, such as management, IT, and security*" (Participant 09).

These narratives illustrate considerable variation in procedural competence and maturity, highlighting that SMEs with a high intention to share information may lack the structured capacity to do so effectively. While some participants described structured documentation processes, others lacked clarity or relied on informal communication. SCT constructs, particularly self-efficacy and reciprocal determinism, are evident: personal confidence, behavioural routines, and the organisational environment interact to influence CIS engagement. These findings support quantitative data indicating low confidence and capability in report creation, with mean scores below 1.6. The absence of standardised reporting formats or templates further explains the behavioural gap observed in Cluster 1, where a high intention to share does not translate into action. The lack of standardised reporting protocols contributes to low self-efficacy and reporting confidence, demonstrating that SCT's reciprocal determinism applies: personal factors, behaviour, and the environment interact to influence CIS engagement. Therefore, incident reporting practices must be strengthened through training, procedural standardisation, and organisational support to enable SMEs to participate effectively in CIS.

Responses in this section were coded according to reporting approach (structured, general, informal) and mapped to SCT constructs: procedural competence → self-efficacy; communication behaviours → outcome expectations; organisational support → environmental factors. Triangulation with quantitative data confirmed that procedural variation underpins the gap between high intention and actual CIS participation. Strengthening incident reporting through formalised templates, staff training, and organisational support is essential for enabling effective SME engagement.

4.3.3 How do you or your company stay informed about cybersecurity threats?

Participants described a variety of methods for remaining informed about cybersecurity threats, reflecting differing access to and reliance on external knowledge sources. Some SMEs engaged with specialists:

"*Engage with cybersecurity experts, either through the appointment of a cyber expert to the board*" (Participant 02).

While others sought knowledge through professional events:

"*By attending cybersecurity conferences*" (Participant 07).

Digital channels, including websites and social media, were also cited:

"*Cybersecurity websites and social media*" (Participant 08).

Some SMEs referred to government sources:

"Government agencies, they monitor government agencies" (Participant 09).

These responses reveal how SMEs perceive and access threat intelligence. Differences in information-seeking behaviour reflect variations in organisational resources, IT expertise, and environmental awareness. SCT constructs are evident: vicarious learning is observed in engagement with experts and conferences, while environmental cues and perceived norms influence attention to social media and government sources. Access to timely, relevant information appears to strengthen confidence and preparedness, which correlates with quantitative measures of cyber readiness and HCA clusters showing segmentation in SME engagement.

The responses to this question were coded based on source type (experts, conferences, digital media, government) and linked to SCT constructs: expert engagement → vicarious learning; information from social and governmental sources → environmental cues; proactive behaviours → self-efficacy. Triangulation with quantitative results confirmed that SMEs relying on diverse threat intelligence sources showed higher confidence in CIS engagement. Encouraging SMEs to access multiple information channels is likely to enhance awareness, preparedness, and subsequent CIS participation.

4.3.4 What are the barriers to sharing with other SMEs?

Participants highlighted multiple barriers to sharing cybersecurity threat information with other SMEs, revealing the complex interplay of relational, organisational, and environmental factors. Concerns around confidentiality and competitive advantage were frequently cited:

"*I think businesses may hesitate to share information that they think is confidential. Also, they might fear sharing info could lead to a loss of competitive advantage. Lastly, businesses have different goals and priorities so they may not align with each other*" (Participant 01).

Technical limitations and capability gaps were also mentioned:

"*Evolving threats. Lack of cybersecurity capabilities*" (Participant 02).

Trust issues were explicitly reported:

"*There is no trust*" (Participant 03).

Some participants expressed uncertainty regarding barriers:

"*I'm not sure*" (Participant 04).

A few participants noted organisational misalignment with sharing protocols:

"*Some retail stores won't accept the sharing of threat information due to protection of icon*" (Participant 08).

These responses reveal that trust deficits, competitive pressures, and structural constraints limit CIS participation despite expressed willingness. SCT constructs are evident: self-efficacy is reduced when SMEs perceive insufficient capability or authority to share, and outcome expectations are moderated by fears of reputational or financial loss. The qualitative themes complement quantitative analyses, showing that managerial support, policy presence, and social norms strongly influence sharing behaviour. HCA segmentation illustrates that highly engaged SMEs (Cluster 3) navigate these barriers more effectively, whereas SMEs in Cluster 1 are inhibited by perceived risks.

Responses were coded into relational barriers (trust, competition), technical barriers (capabilities, access), and regulatory/environmental barriers. Reflexivity was maintained by reflecting on prior experience in SME cybersecurity practices and cross-checking interpretations with the quantitative findings. Triangulation with survey and HCA data confirmed that these barriers materially affect whether SMEs translate sharing intentions into action, highlighting the importance of trust-building, technical support, and policy guidance to facilitate CIS engagement.

4.3.5 What challenges have you encountered in sharing initiatives?

Participants reported a variety of challenges in engaging with CIS initiatives, highlighting the interplay of technical, organisational, and relational factors. While some participants indicated no significant challenges, others described substantial obstacles:

"*No challenge yet*" (Participant 01).

Trust and reputational concerns emerged prominently:

"*Cultural and Trust Challenges: 1. Building trust: Establishing trust among participating organizations is crucial for effective threat information sharing. 2. Fear of reputational damage:*

Organizations may be reluctant to share threat information if they fear it could damage their reputation or compromise their competitive advantage" (Participant 02).

Technical limitations and infrastructure issues were also noted:

"*Technical problems*" (Participant 04).

Resource constraints were frequently cited, particularly in smaller SMEs:

"*Lack of resources, participating in threat information sharing initiatives may require significant resources*" (Participant 07).

"*Resource constraints, our store may lack the necessary resources to participate in threat information sharing initiatives*" (Participant 08).

These narratives illustrate that SMEs face multifaceted barriers to CIS participation. Technical limitations reduce their practical ability to engage, resource scarcity constrains sustained involvement, and trust deficits undermine their willingness to share. SCT constructs are apparent: environmental factors (infrastructure, resources, organisational support) interact with personal determinants (self-efficacy, perceived outcomes) to shape behaviour. High-intention SMEs in Cluster 1 frequently struggle to convert intention into action due to systemic constraints, underscoring the importance of supportive conditions for behavioural enactment.

Challenges were categorised into technical (infrastructure, platform usability), relational (trust, reputational concerns), and organisational (resource constraints, managerial support) categories. Reflexivity was upheld by considering the researcher's prior engagement with SME cybersecurity initiatives and the potential influence of the interview setting on participants' disclosures. Triangulation with survey findings and HCA clusters reinforced the connection between systemic barriers and observed behaviour patterns.

4.3.6 Why does your organisation engage in CIS?

Participants highlighted multiple motivations for engaging in CIS, reflecting both practical and strategic considerations. Across responses, themes of risk mitigation, incident management, collaborative security, and threat awareness emerged, underscoring SMEs' focus on resilience and preparedness:

"*To gain a more complete understanding of the threats the organisation may face*" (Participant 02).

"*To help other businesses know when an incident is about to occur and get ready to manage the risk*" (Participant 03).

"*Sharing threat information can help reduce the risk of cyberattacks, physical robberies, or other security incidents*" (Participant 05).

"*To improve their security*" (Participant 07).

"*Improve incident reports*" (Participant 10).

Participants' narratives reveal that engagement in CIS is largely driven by anticipated benefits, including enhanced organisational resilience, improved incident management capabilities, and mutual support within the SME community. These motives align with quantitative findings showing that perceived benefits are the strongest predictor of CIS participation, corroborated by Spearman correlations linking the belief in resilience improvement with actual sharing behaviour. SMEs in Cluster 3, who consistently demonstrated sharing behaviours, articulated the most coherent strategic rationale, suggesting that clarity of purpose supports the translation of intention into action.

From an SCT perspective, these responses illustrate the role of outcome expectations: SMEs engage in CIS when they anticipate tangible benefits for themselves and their network, reinforcing self-efficacy and shaping behaviour. Motives are thus not merely individual but socially embedded, reflecting reciprocal determinism between environmental cues (peer practices, threat awareness), personal factors (perceived risk and benefit), and behavioural enactment.

Responses were coded into categories reflecting risk management, collaborative advantage, and incident readiness. Reflexivity was applied by considering the researcher's prior engagement with SMEs and awareness of potential social desirability in responses. Cross-validation with quantitative clusters and Spearman correlation results enhanced credibility.

4.3.7 Benefits from CIS participation?

Participants described several tangible benefits derived from engaging in CIS, reflecting both operational and relational gains. Key themes included enhanced incident response, strengthened trust and communication, optimised resource allocation, and improved cybersecurity capability. While a few participants did not report benefits, most recognised CIS as contributing to organisational resilience and collective security:

"*You can easily respond to incidents, businesses can collectively strengthen their defences against cyber threats*" (Participant 01).

"*We built trust among our businesses in the community*" (Participant 05).

"*Improved resource allocation. Threat information sharing helps my organisation allocate resources more effectively, reducing waste and improving overall efficiency*" (Participant 06).

"*Employee training on cybersecurity best practices is essential*" (Participant 08).

"*No response*" (Participant 04).

Participants' narratives indicate that CIS participation extends beyond mere information exchange, fostering collaborative learning, operational efficiency, and organisational trust. These benefits reinforce quantitative evidence linking perceived resilience gains with advocacy and the intention to share. SMEs in Cluster 3, who consistently demonstrate high engagement, articulated these advantages most clearly, suggesting that recognition of tangible benefits sustains participation and supports a positive feedback loop in CIS adoption.

These findings exemplify positive reinforcement, where observable benefits enhance self-efficacy and encourage continued behavioural enactment. The interplay between environmental factors (peer engagement, organisational support), personal factors (perceived efficacy and trust), and behavioural outcomes illustrates reciprocal determinism, highlighting the conditions necessary for sustained CIS participation.

Responses were coded into categories representing operational improvement, relational trust, and knowledge/skill development. Reflexivity involved considering the potential influence of social desirability and prior researcher engagement with SMEs.

4.3.8 Lessons from past CIS participation?

Participants reflected on lessons learned from prior CIS engagement, highlighting both positive outcomes, such as increased resilience and collaboration, and negative experiences, including trust breaches and accountability concerns. Illustrative responses include:

"*In terms of physical lessons I learnt that threat information sharing contributes to a safer and more secure community, benefiting businesses and customers, and the negative lesson is that you may not be trusted and later be blamed to be the one who caused the cyber threats when they occur*" (Participant 05).

"*Regular employee training on cybersecurity best practices, such as avoiding suspicious emails and attachments, can help prevent similar incidents*" (Participant 06).

"*By establishing a governance structure to oversee threat information sharing*" (Participant 09).

"*Address confidentiality and trust*" (Participant 10).

The narratives illustrate that SMEs derive actionable knowledge from prior CIS participation, which strengthens organisational preparedness and collaborative capability. Conversely, negative experiences such as breaches of trust, poor data quality, or unclear governance constrain behavioural enactment and help explain the intention–action gap observed in Cluster 1 SMEs. These insights reveal the dual role of past experience as both a motivator and a potential inhibitor in CIS engagement.

Lessons learned influence outcome expectations, which, in turn, shape self-efficacy and the translation of intention into action. Positive reinforcement from successful collaboration fosters confidence and encourages future participation, while adverse experiences may lower self-efficacy or create caution in sharing behaviours. This exemplifies reciprocal determinism, where personal experiences, organisational environment, and behavioural responses interact continuously.

Responses were coded into themes of risk awareness/training, trust/confidentiality, governance, and financial impact. Reflexivity involved acknowledging that participants' narratives could be influenced by hindsight bias and organisational pride.

4.3.9 How do you assess trustworthiness of others?

Trust emerged as a central consideration in SMEs' decisions to share threat information. Participants described assessing trustworthiness through multiple cues, including industry reputation, information quality, collaborative relationships, and security certifications. Illustrative responses include:

> "*Consider the business's reputation within the industry. And check if the business holds relevant security certifications*" (Participant 01).
>
> "*I'm not sure*" (Participant 03).
>
> "*By building a relationship with the business before sharing threat information*" (Participant 05).
>
> "*By checking collaborative security initiatives*" (Participant 08).
>
> "*Establish a clear communication channel*" (Participant 10).

SMEs rely on both formal and informal indicators to gauge trustworthiness. High-engagement SMEs (Cluster 3) appear to utilise structured trust cues, such as certifications or established collaborative networks, while low-engagement SMEs (Cluster 1) express caution or uncertainty, despite their intentions to participate. This demonstrates that the perceived credibility of peers mediates CIS engagement, influencing whether intentions translate into actual sharing behaviours.

Trust assessment reflects the environmental and social determinants that shape behavioural enactment. Structured trust cues enhance self-efficacy by providing confidence in safe engagement, whereas

ambiguous or informal trust signals can inhibit participation. These dynamics exemplify SCT's principle of reciprocal determinism, where personal perceptions, social environment, and behaviour interact to influence engagement in CIS initiatives.

Responses were coded into themes of information quality, communication channels, reputation, and collaborative relationships. Reflexivity was applied by acknowledging that participants' self-reported trust criteria may be influenced by social desirability or prior engagement experience.

4.3.10 What influences trust in other SMEs?

SMEs reported that the establishment of trust in peers is influenced by both business/security factors and reputation/motivation, with participants emphasising transparency, compliance, mutual benefit, and prior performance. Illustrative responses include:

> "*Industry standing and past performances. And also, security certificate*" (Participant 01).
>
> "*Trust factors: 1. Established relationships, 2. Clear communication and transparency, 3. Mutual benefit. Distrust factors: 1. Lack of transparency, 2. Poor security track record, 3. Competitive interests*" (Participant 02).
>
> "*I'm not sure*" (Participant 04).
>
> "*By building business factors and security factors*" (Participant 06).
>
> "*Compliance, some private hospitals have relevant regulations and standards*" (Participant 09).

SMEs consider trust to be a multidimensional construct that incorporates both formal and informal cues. Transparency, adherence to security protocols, demonstrated reliability, and mutually beneficial outcomes enhance confidence in sharing threat information. Low-engagement SMEs (Cluster 1) remain hesitant due to distrust or competitive concerns, while high-engagement SMEs (Cluster 3) actively utilise structured trust-building practices to mitigate perceived risks. This demonstrates that trust is not purely an individual judgment but is shaped by social norms, relational histories, and governance clarity.

Trust formation aligns with reciprocal determinism: environmental factors (such as, governance clarity, sector norms), social influences (peer behaviour and expectations), and personal perceptions (belief in peers' reliability) collectively shape behavioural engagement. Positive experiences with trustworthy peers reinforce self-efficacy and outcome expectations, which increase the likelihood of active CIS participation.

Responses were coded under transparency, reputation, relational history, mutual benefit, and compliance. Reflexivity was applied to acknowledge the influence of participants' prior CIS experiences and social desirability on their responses.

4.3.11 How does management support CIS?

Management support for CIS was reported to manifest in various forms, including training and awareness, active leadership involvement, incentives, and collaborative engagement. Participants described both structured initiatives and less formalised signals of support:

> "*There's an emphasis on collectively contributing to security of the industry. The management supports building strong relationships and partnerships with other businesses*" (Participant 01).
>
> "*I'm not sure*" (Participant 03).
>
> "*By active engagement and encouragement*" (Participant 05).
>
> "*By producing trainings and meetings about cyber security*" (Participant 07).
>
> "*Leadership were involved in this matter*" (Participant 10).

SMEs experience management support along a continuum, ranging from clear, structured engagement to ambiguous or minimal involvement. High-engagement SMEs (Cluster 3) report tangible leadership initiatives, such as regular training, formal encouragement, and visible participation in security programmes that reinforce intention and enable action. In contrast, Clusters 1 and 2 display passive or inconsistent managerial engagement, which correlates with gaps between intention and actual CIS behaviour.

Management support operates as a key environmental determinant. Formalised leadership, awareness initiatives, and recognition mechanisms enhance SMEs' self-efficacy and reinforce positive outcome expectations, facilitating behavioural enactment. Conversely, unclear or inconsistent signals weaken confidence and limit CIS participation, demonstrating SCT's assertion that behaviour emerges from the interaction of personal, behavioural, and environmental factors.

Responses were coded under training/awareness, leadership engagement, incentives, collaboration, and clarity of support. Reflexive consideration acknowledged that participants' interpretations of managerial support are influenced by organisational culture and prior experience with CIS initiatives.

4.4 Integration of quantitative and qualitative findings

Using a convergence coding matrix, the qualitative and quantitative results were integrated. Themes identified in the quantitative analysis (such as, cluster-based engagement and Spearman correlations) were systematically compared with qualitative codes derived from SME interviews (such as, trust cues, lessons learned, management support). The integration process explicitly captured both convergent findings (areas of agreement between qualitative and quantitative findings) and divergent insights (where qualitative and quantitative findings differed, such as underreporting of incidents or distrust), providing a more comprehensive understanding of CIS engagement.

The integration revealed that SME CIS participation is shaped by experiential learning, trust, outcome expectations, and organisational support. High intention alone is insufficient; active engagement requires procedural capacity, managerial involvement, and technological resources. The SCT constructs of self-efficacy, trust, and perceived benefit emerged as primary determinants, moderated by technological and policy enablers that influence the translation of intention into action.

4.4.1 Convergence and divergence

The integration of quantitative and qualitative findings reveals both points of convergence and divergence, providing a more nuanced understanding of SME CIS engagement. Convergence is evident in the consistent identification of trust, perceived benefit, and self-efficacy as primary predictors of CIS participation. Across both datasets, SMEs in Cluster 3, characterised by high engagement, consistently demonstrate structured reporting practices, employ clear trust cues, and receive visible managerial support. These high-engagement SMEs also reflect strong outcome expectations, such as improved incident response, increased resilience, and enhanced collaboration, which are reinforced in both survey correlations and participant narratives. This alignment between quantitative and qualitative evidence supports the central SCT premise that self-efficacy, perceived benefit, and trust drive behavioural engagement when supported by conducive environmental factors.

Divergences emerge in several key areas. Quantitative results suggest low incident reporting across Clusters 1 and 2; however, qualitative interviews reveal that underreporting is often deliberate, motivated by fear of reputational damage or distrust of peers. This illustrates that low observable behaviour does not necessarily indicate a lack of intention or awareness. Furthermore, some SMEs in Clusters 1 and 2 did not perceive immediate benefits from CIS participation, providing an explanation for the gap between high reported intention and low actual activity. The qualitative findings also uncover subtle psychological and relational barriers, such as fear of negative judgement, competitive concerns, and uncertainty about

governance structures, which are not fully captured by survey instruments. These divergences underscore the importance of complementing quantitative indicators with rich qualitative insights to capture the full spectrum of behavioural determinants.

4.4.2 Integrated interpretation

Table 4.25 synthesizes the quantitative and qualitative findings by categorising barriers to CIS participation into three interrelated domains: psychological, organisational, and external or environmental.

Table 4-25: SCT-Aligned Barrier Model for SME CIS

Barrier Type	Specific Barriers	Quantitative Evidence	Qualitative Evidence	Cluster Impact
Psychological	Low self-efficacy	Low confidence scores in reporting tasks; low engagement in Cluster 1	Participant 08: informal reporting, unsure of templates	Cluster 1
	Fear of reputational damage	High correlation between risk perception and low sharing	Participant 02: concerns about business image	Cluster 1
	Low perceived benefit	Perceived benefit weaker in Clusters 1 & 2	Participant 05: does not see immediate value	Cluster 1 & 2
Organisational	Lack of structured reporting protocols	Low standardisation; ad hoc incident reporting	Participant 05 (template-based), Participant 08 (informal)	Cluster 1 & 2
	Limited managerial support	Managerial involvement positively correlated with intention	Participant 01, 03, 07: limited leadership engagement	Cluster 1
	Resource constraints	Time, technical capacity, and staff shortages correlated with low engagement	Participant 04, 08: insufficient staff/time	Cluster 1 & 2
External / Environmental	Technological limitations	System/infrastructure challenges correlated with low sharing	Participant 02, 07: technical issues	Cluster 1 & 2
	Regulatory uncertainty	Regulatory clarity positively correlated with participation	Participant 09: confusion over compliance	Cluster 1 & 2
	Competitive pressures	Competitive risk negatively correlated with sharing	Participant 06: competitor risk	Cluster 1

Psychological barriers, including low self-efficacy, fear of reputational damage, and limited perceived benefits, constrain SMEs' motivation and confidence to actively participate in CIS. For instance, participants expressed hesitation to report incidents due to concerns about business image or uncertainty over reporting procedures, which directly impacts the engagement of Cluster 1 SMEs. Organisational barriers, such as the absence of structured reporting protocols, limited managerial support, and resource constraints, reduce procedural capacity and impede the translation of intention into action. SMEs lacking formal training, leadership involvement, or accessible templates demonstrate

inconsistent or ad hoc reporting behaviour, further illustrating this gap. External/environmental barriers, including technological limitations, regulatory uncertainty, and competitive pressures, shape the broader environmental context, influencing whether SMEs feel secure and supported in participating.

Additionally, the varying effects of these barriers across clusters are highlighted in Table 4.25. Cluster 3 SMEs, representing the fully engaged group, have largely overcome these barriers through strong procedural systems, structured trust-building practices, and managerial engagement. In contrast, Cluster 1 SMEs demonstrate high intention but low behavioural enactment, with barriers in all three domains constraining participation. Cluster 2 SMEs show moderate engagement, often affected by resource and technical limitations, illustrating that barriers interact dynamically with internal motivation and external support.

This integrated interpretation aligns with SCT by confirming that intention alone is insufficient; self-efficacy, trust, and perceived benefits must interact with organisational and environmental enablers for actual behaviour to occur. Qualitative insights provide additional explanatory depth, showing that communication quality, collaborative norms, and past experience mediate engagement. SMEs with prior CIS experience articulate lessons learned, improved risk awareness, and collaborative trust, reinforcing positive outcome expectations and strengthening future participation.

From a practical perspective, Table 4.25 informs the design of targeted, human-centric CIS interventions. For Cluster 1 SMEs, strategies should prioritise procedural guidance, structured reporting templates, active managerial involvement, and technology enablement to bridge the intention–behaviour gap. Reinforcing trust, demonstrating tangible benefits, and clarifying regulatory expectations address both psychological and relational barriers. Cluster-specific strategies allow for nuanced interventions that accommodate variations in SME confidence, resources, and engagement histories, ensuring that CIS behaviour can be strengthened across diverse organisational contexts. By explicitly integrating quantitative and qualitative findings and linking them to SCT constructs, Table 4.25 serves as a comprehensive reference model for understanding and mitigating barriers to SME CIS participation.

4.5 Summary

Chapter 4 presented a detailed analysis that integrated quantitative and qualitative data using an explanatory sequential mixed-methods approach. Key behavioural, technological, and policy-related factors influencing SME CIS engagement were identified. Quantitative results validated SCT-aligned constructs, including outcome expectations, social persuasion, and self-efficacy, as strong predictors of

CIS intention and activity, while hierarchical cluster analysis revealed three distinct behavioural profiles reflecting varying levels of engagement and operational capacity.

Qualitative interviews expanded on these findings by identifying nuanced barriers, trust dynamics, reporting practices, and the role of management support. Together, these results confirmed that SCT constructs play a central role in shaping SME engagement and demonstrated how organisational and external enablers moderate the translation of intention into action. The proposed SCT-aligned barrier model synthesises these insights, emphasising the psychological, organisational, and external factors that contribute to persistent intention–behaviour gaps, particularly among Cluster 1 SMEs.

The integration of findings achieves the first two research objectives by identifying human factors associated with effective CIS participation and examining the influence of policy and technology on these factors. Chapter 5 will leverage these insights to guide the development and evaluation of a human-centric, policy-aligned, and technologically supported CIS protocol for SMEs. Collectively, the findings provide both theoretical and practical clarity, offering a robust foundation for interventions designed to improve SME participation in CIS and to bridge the observed intention–behaviour gaps.

5 CHAPTER FIVE: DISCUSSION AND PROTOCOL EVALUATION

5.1 Introduction

This chapter interprets the findings from Chapter 4 with the aim of fulfilling the third and fourth objectives of this study: the third objective seeks to refine a human-centric CIS protocol for SMEs that integrates policy, technological, and behavioural interventions, while the fourth objective evaluates the protocol's efficacy in addressing SME-specific cybersecurity challenges. The discussion integrates quantitative results (HCA clusters, correlations) and qualitative insights to provide a comprehensive understanding of the human factors, trust, and organisational behaviours influencing CIS participation. Guided by SCT, this chapter examines how personal, environmental, and behavioural factors interact to shape SMEs' cybersecurity practices. Importantly, the findings are interpreted in the South African context, and more specifically, the Eastern Cape regional context, considering socio-economic constraints, infrastructural limitations, and regulatory gaps that influence SME participation in cybersecurity information sharing. The chapter further positions the refined protocol in relation to existing frameworks (such as, NIST, NISTIR 7621, ISO/IEC 27032, and NIST 800-18) and highlights innovations, scalability, and adaptability to emerging technologies.

The structure of the chapter is as follows: Section 5.2 presents an interpretation of key findings; Section 5.3 introduces the refined human-centric CIS protocol; Section 5.4 details the protocol evaluation through expert feedback; and Section 5.5 concludes the chapter.

5.2 Interpretation of key findings

As indicated earlier, the interpretation of key findings from this study is done through the lens of SCT, mapping how its constructs of performance accomplishments, social persuasion, self-efficacy, and outcome expectations help explain SME behaviour in CIS. By integrating quantitative clusters, qualitative themes, and SCT principles, this discussion situates SMEs' experiences within the broader South African socio-economic, infrastructural, and policy environment, while highlighting practical implications for the proposed human-centric CIS protocol.

5.2.1 Performance accomplishments

The findings reveal a critical gap between knowledge and structured action: while many SMEs report awareness of cyber incidents (63.6%), far fewer can create formal reports (40.9%) or use standardised templates (36.4%). Qualitative insights indicate a reliance on informal procedures, ad hoc tools, or

undocumented practices. This gap suggests that SMEs may understand cybersecurity risks conceptually but lack procedural mastery, aligning with SCT's emphasis on mastery experiences in building self-efficacy (Bandura, 1986) and supported by practical learning theories (Kobis, 2021). SMEs' inability to operationalise knowledge indicates that knowledge alone is insufficient; procedural guidance, practice, and structured frameworks are critical. This presents a key barrier to effective CIS participation, particularly in South Africa, where resource constraints and a fragmented ICT landscape compound procedural gaps (Kabanda, Tanner & Kent, 2018; Chidukwani, Zander & Koutsakis, 2022). Based on the finding that SMEs possess conceptual awareness of cyber incidents but lack the procedural mastery to translate this into formal reporting, the protocol should prioritise training programmes that provide repeated, guided practice, standardise reporting procedures, and facilitate incremental skill development. By explicitly fostering mastery experiences, SMEs can translate knowledge into consistent, actionable CIS behaviours.

5.2.2 Social persuasion (subjective norms and feedback)

Trust, peer expectations, and management support have a strong influence on CIS participation. Correlations, such as $R_s = 0.65$ between peer expectations and sharing behaviours, indicate that SMEs respond to perceived social obligations. However, qualitative data point to inconsistent management involvement and trust deficits as barriers. These results highlight that CIS behaviour is not purely individualistic but socially embedded. SCT suggests that social persuasion, modelling, and feedback influence self-efficacy and engagement (Bandura, 1986). SMEs' reliance on peer credibility and management cues indicates that interventions must leverage social networks and trusted relationships, particularly in SMEs where formal governance structures are weak. It can therefore be construed that social persuasion is a critical lever for CIS uptake. Based on the finding that SMEs respond strongly to external cues, such as peer norms and feedback, a protocol aimed at promoting CIS participation should innovatively embed peer-led initiatives, mentoring structures, and trusted communities to strengthen normative influence, reinforce positive behaviour, and overcome mistrust. In the South African context, where scepticism towards external authority may exist, building internal social reinforcement mechanisms is particularly pertinent (Lewis et al., 2014; Safa & Von Solms, 2016).

5.2.3 Information sharing self-efficacy

Although SMEs report confidence in sharing (internally and externally), negative correlations ($R_s = -0.69$) reveal that self-perceived competence does not always translate into best practice. Qualitative evidence suggests overconfidence, reliance on informal processes, or inadequate tools. This finding

highlights the "knowledge-behaviour gap," a phenomenon that SCT explains as arising when self-efficacy is misaligned with actual ability (Nabavi, 2012). SMEs may feel confident but operate without proper scaffolding or supportive infrastructure, leading to inconsistent CIS behaviours. This presents a subtle but crucial insight: interventions must address both perceived competence and structural enablers in order to be effective. This aligns with Bandura (1986), Nabavi (2012), and SME studies on procedural scaffolding (Kent, Tanner & Kabanda, 2016; Kabanda, Tanner & Kent, 2018), but diverges from knowledge-only framings (Koepke, 2017; Fard Bahreini, Cenfetelli & Cavusoglu, 2022) by showing that confidence must be scaffolded with tools, practice, and feedback. Considering the finding that SMEs often display overconfidence in their ability to share information despite procedural and structural weaknesses, protocol measures should include safe environments for practice, heuristic-informed guidance, and real-time feedback loops, ensuring that confidence is grounded in capability. This nuanced perspective emphasises that promoting CIS participation is not simply about knowledge dissemination but requires bridging perception with action (Nabavi, 2012; Triplett, 2022).

5.2.4 Outcome expectations

Belief in CIS benefits correlates strongly with sharing intention (R_s = 0.73) and advocacy (R_s = 0.69). Interviews emphasise improved incident response, trust-building, and resource efficiency as motivators. SCT suggests that anticipated outcomes guide behavioural intention (Nabavi, 2012; Middleton, Hall & Raeside, 2019). SMEs are motivated not merely by obligation but by expected resilience and operational benefits. This provides evidence that perceived utility, tangible benefits, and reward structures are central to motivating CIS engagement. Furthermore, the findings highlight that even when SMEs are aware of protocols, their adoption is contingent on perceived efficacy and advantage. Based on the finding that SMEs' willingness to share externally is shaped by perceived benefits and fears of reputational harm, the protocol must ensure easy-to-use, standardised reporting tools and clear communication of CIS benefits, reinforcing outcome expectations. It should also embed incentive structures, anonymised sharing options, and reassurance mechanisms that make the benefits of participation outweigh the perceived risks. This aligns with Pala & Zhuang (2019) and Skopik, Settanni & Fiedler (2016), who note that trust, incentives, and inter-organisational dynamics drive SME participation. In practice, this means interventions should explicitly demonstrate "what's in it for the SME", combining risk mitigation with operational efficiency.

5.2.5 Cybersecurity behaviour and intention to share

Positive correlations between behaviour and sector CIS activity (R_s = 0.72), and between internal and external sharing intentions (R_s = 0.53), indicate alignment of motivation and action. However, qualitative findings show that consistency relies on clear procedures and leadership reinforcement. This suggests that behaviour is both intention-driven and context-sensitive. SCT emphasises that reinforcement and environmental support stabilise behaviour (Bandura, 1986). SMEs' reliance on leadership signals and procedural clarity illustrates the need for structural enablers alongside individual motivation. Consistent behaviour is therefore dependent on the alignment of environmental cues, capability, and intention. This aligns with Bandura (1986), Safa & Von Solms (2016), Kent, Tanner & Kabanda (2016), Kabanda, Tanner & Kent (2018), Pala & Zhuang (2019), Collier et al. (2023), and Johnson et al. (2016), but diverges from compliance- or technology-only positions (ISO 27032, 2012; Koepke, 2017; Sauerwein et al., 2017; Chidukwani, Zander & Koutsakis, 2022; Serini, 2024) by demonstrating that intention converts to consistent action only when leadership cues and procedural clarity are present. Based on the finding that consistent CIS behaviour depends not only on intention but also on leadership reinforcement and procedural clarity, the protocol should clearly define roles, responsibilities, and reporting lines, integrate national legislation, and provide feedback mechanisms to reinforce consistent engagement. This nuanced understanding ensures that interventions are holistic, combining motivational, structural, and social dimensions.

5.2.6 Cluster profiles synthesis

Three clusters emerged as presented in the findings:

1) High intention / low behaviour – intention-to-action gap
2) Moderate engagement – reactive/compliance-driven participation
3) High intention / high behaviour – alignment of motivation with capacity

The cluster profiles reveal that SMEs are diverse, and CIS adoption is highly context-dependent. SCT helps explain this variance: capability, observational learning, social support, and outcome expectations interact differently across clusters (Bandura, 1986). The presence of intention–behaviour gaps (Cluster 1) emerge as a critical insight: even motivated SMEs (Cluster 3) may fail to act without scaffolding, resources, or social reinforcement. With this in mind, namely the finding that SMEs fall into distinct clusters ranging from high intention/low behaviour to high intention/high behaviour, the protocol should be adaptive and modular, offering tailored interventions for each cluster. SMEs in Cluster 1 may need

intensive support, whereas Cluster 3 SMEs can benefit from peer-sharing networks and recognition mechanisms. This finding aligns with Bandura (1986), Kabanda, Tanner & Kent (2018), Pala & Zhuang (2019), Collier et al. (2023), Moore (2022), and Shojaifar & Fricker (2020) in showing that CIS adoption is shaped by resource, cultural, and peer-network factors, but diverges from ISO 27032 (2012), Koepke (2017), and Chidukwani, Zander & Koutsakis (2022), which imply more uniform adoption pathways and underplay intention–behaviour gaps. This nuanced perspective highlights the flexibility of human-centric protocols, ensuring that interventions respond to situational and resource-based differences across SMEs.

This discussion highlights the complex interplay of human, social, and contextual factors that shape SME participation in CIS. Drawing on SCT, the insights emphasise how mastery experiences, social modelling, and outcome expectations can be leveraged to design interventions that are both practical and contextually relevant. Importantly, the study identified patterns and relationships between factors influencing SME cybersecurity sharing, but these should be understood as associations rather than proven causes. By designing interventions that fit the specific realities of South African SMEs, which include limited resources, trust issues, and informal processes, the protocol remains practical and relevant while acknowledging that other unmeasured factors could affect these patterns. Section 5.3 builds directly on this understanding, translating these nuanced, evidence-based insights into a human-centric CIS protocol that operationalises SCT components to enhance engagement, build trust, and standardise cybersecurity practices across diverse SME contexts in South Africa.

5.3 Human-centric CIS protocol

This study set out to achieve four objectives. The first two objectives were achieved: 1) to determine the human factors associated with effective CIS, and 2) to examine the influence of policy and technology on human factors. The first objective was addressed by identifying human factors influencing CIS through quantitative and qualitative analyses, interpreted through SCT. Spearman's Rank Correlation revealed strong associations between outcome expectations (such as, belief in resilience and CIS intention, $R_s = 0.73$) and peer norms ($R_s = 0.65$), showing that perceived benefits, social persuasion, and self-efficacy are key behavioural enablers. Thematic analysis confirmed that trust, prior incident experience, and confidence shape reporting behaviour. Cluster 3 SMEs were characterised by having high intention and structured participation.

The second objective highlighted policy and technology as critical moderators of human behaviour in CIS. Thematic data revealed constraints such as the lack of standardised reporting tools, difficulty

accessing platforms, and uncertainty in compliance (Table 4.14, Figures 4.5–4.6). Quantitative findings confirmed that SMEs with unclear policies (Governance Preparedness, Cronbach alpha = 0.85) had lower engagement. Literature supports these findings, indicating that insufficient governance and fragmented technological tools hinder SME CIS capacity (Sauerwein et al., 2017; Chidukwani, Zander & Koutsakis, 2022). Thematic codes such as *"technical* challenges," *"no* trust," and *"absence of feedback* loops" reinforced this insight. These results demonstrate that policy clarity and technological usability directly impact trust formation, self-efficacy, and behavioural consistency in CIS.

This section presents a refinement of the literature-informed protocol introduced in Chapter 2 (Figure 2.1). The earlier protocol proposed five interacting components: trust-building, simplification and incentives, collaborative culture, legal and ethical guidance, and ongoing support. These components were framed as a dynamic cycle. Although derived from the literature, these components had not yet been tested or contextualised within the realities of South African SMEs. The empirical findings presented in Section 5.2 now provide that contextual grounding. Using SCT as a lens, five domains emerged as critical to understanding SME participation in CIS: behavioural, socio-cultural, psychological, technological, and policy/governance. Each domain reflects a set of human factors that either enable or constrain information sharing, and together they provide a scaffold through which the original protocol components can be refined.

The refined protocol, therefore, integrates the domains (which capture the human-centric conditions for change) with the components (which provide the structural cycle of the protocol). In practice, this means that each component from Chapter 2 is now enriched with empirical evidence, SCT constructs, and domain-specific actions drawn from this study. Table 5.1 illustrates how the refined protocol draws together the SCT-informed domains, the original protocol cycle, and empirical findings:

Table 5-1: Refinement of the literature-informed protocol with SCT constructs and evidence strength

Domain (SCT lens)	Original Protocol Component (Chapter 2)	Refined Evidence-Informed Actions (from Findings)	Linked SCT Construct	Strength of Refinement
Behavioural	Trust-building	Role-based training, standardised incident templates, simulation-based drills, CIS champions	**Mastery Experiences** – confidence through repeated, structured practice	**Strong** – Quantitative + qualitative convergence (e.g., only 40.9% able to report formally)
Socio-Cultural	Simplification & incentives	Peer networks, recognition programmes, collaborative playbook exercises	**Social Persuasion** – influence of peer norms, recognition, and reinforcement	**Moderate–Strong** – Supported by correlation (R_s = 0.65) and thematic trust insights

Psychological	Collaborative culture & psychological safety	Anonymous reporting, feedback loops, visual heuristics, mentorship links	**Self-Efficacy** – aligning confidence with actual capability through supportive structures	**Strong** – Negative correlation (R_s = -0.69) and qualitative data on overconfidence vs. practice gaps
Technological	Legal & ethical guidance	Free-to-access CIS form builder, kiosk support, interoperable data exchange, pre-populated templates	**Reinforcement & Outcome Expectations** – clarity of tools stabilises belief in benefits and compliance	**Moderate** – Findings show 63.6% lack formats; Governance Preparedness α = 0.85
Policy and Governance	Ongoing support & feedback	Compliance starter kits, subcontractor mandates, sector-specific templates, feedback dashboards	**Outcome Expectations & Social Persuasion** – visible benefits and accountability reinforce engagement	**Strong** – Reliability of Governance Preparedness (α = 0.85) and cluster profiles show iterative reinforcement needed

Each row in Table 5.1 demonstrates how an SCT-informed domain contextualises one of the original protocol components from Chapter 2 by incorporating evidence from the empirical study. The first column identifies the five domains derived from SCT (behavioural, socio-cultural, psychological, technological, and policy and governance). The second column links each domain to its corresponding component of the literature-informed protocol cycle (trust-building, simplification and incentives, collaborative culture, legal and ethical guidance, and ongoing support). The third column lists the refined, evidence-informed actions that emerged from the findings, illustrating how empirical data operationalises protocol design. The fourth column explicitly indicates which SCT construct (mastery experiences, social persuasion, self-efficacy, or outcome expectations) is being enacted through that domain–component interaction. Finally, the fifth column indicates the strength of refinement, based on the degree of triangulation across quantitative (such as, correlations, reliability tests) and qualitative (such as, thematic codes, interview insights) evidence. The evidence from this study enriches and contextualises each component of the literature-informed protocol, yielding a human-centric CIS protocol for SMEs, as illustrated in Figure 5.1 below:

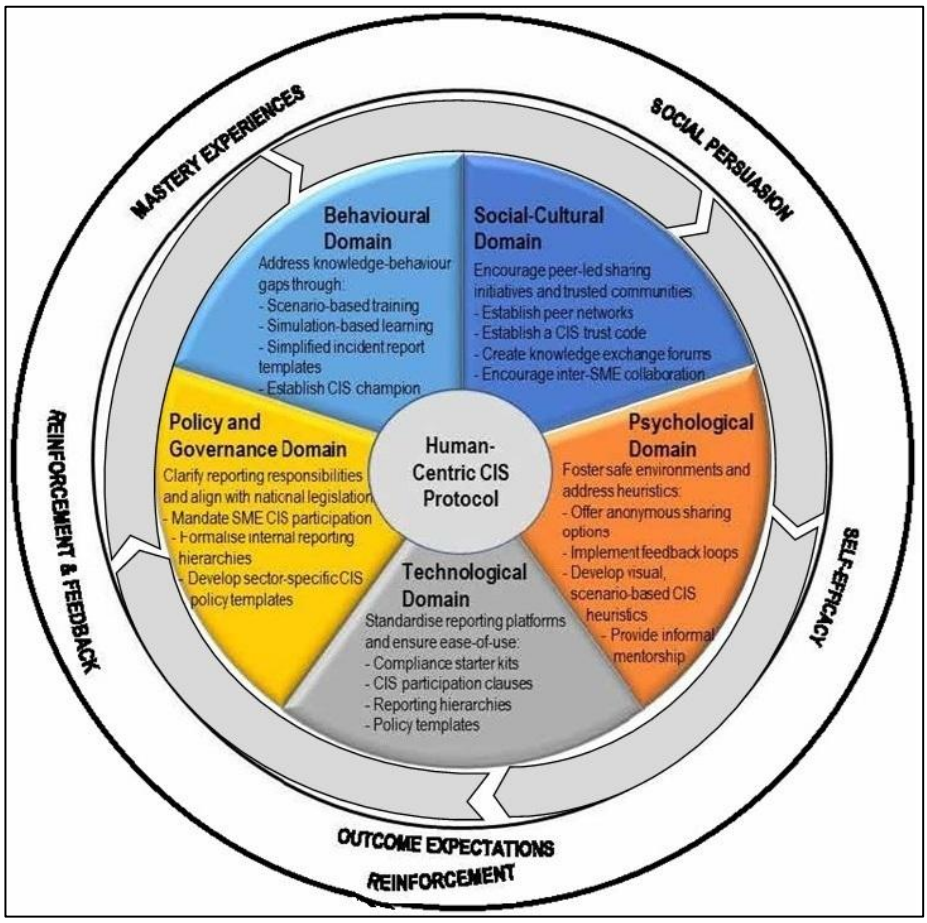


Figure 5-1: Refined human-centric CIS protocol

The central circle represents the Human-Centric CIS Protocol as the refined artefact. The first inner ring illustrates five domains and their domain-specific actions, while the outer ring maps each domain to its corresponding SCT construct. Curved arrows between the domains highlight their interdependence: behavioural practices are reinforced by socio-cultural norms, which in turn shape psychological safety; technological usability supports behavioural mastery, while policy and governance provide reinforcement and ongoing feedback. Together, these dynamic interactions operationalise SCT constructs into a practical, evidence-informed CIS protocol for SMEs.

1. Behavioural Domain → Establish trust-building mechanisms → Mastery experiences: Address knowledge-behaviour gaps through scenario-based training and simplified incident report templates (Kabanda, Tanner & Kent, 2018; Triplett, 2022). As per the findings, SMEs had conceptual awareness but lacked procedural mastery, where only 40.9% of respondents confirmed they can create cyber incident reports (Table 4.13). Qualitative responses revealed fragmented or informal reporting methods. To build SME staff capacity

that can identify, report, and communicate cyber incidents effectively, the following domain actions for this human factor are identified:

- Develop role-based training modules on cyber threat identification and response to gain mastery experiences.
- Distribute standardised cyber incident report templates tailored to SME operational contexts.
- Introduce simulation-based learning (such as, phishing email simulations, incident response drills) to provide mastery experiences.
- Establish internal CIS champions responsible for coordinating reporting.

The identified domain actions for this human factor map to establish trust-building mechanisms by embedding role-based training, scenario-driven exercises, and the establishment of CIS champions who model good practice. Resulting in the interacting behavioural and socio-cultural domains:

- Role in the Cycle: Trust acts as the entry point of the cycle, enabling SMEs to feel confident in sharing cybersecurity information. Without trust, all other interventions lose effectiveness.
- SCT Construct: Social Persuasion & Observational Learning – SCT posits that people are influenced by cues from trusted peers and authority figures, and by observing others' behaviours.
- Protocol Actions: Implement peer-led networks, recognition schemes, and safe sharing platforms. By establishing credibility and reinforcing trustworthiness, SMEs are more likely to participate in CIS actively.
- Evidence from Findings: Correlation (R_s = 0.65) between peer expectations and sharing behaviour shows the significance of trust and social reinforcement in real-world SME contexts.

2. Socio-Cultural Domain → Simplify and incentivize information sharing → Social persuasion: Encourage peer-led sharing initiatives and trusted communities (Lewis et al.,

2014; Collier et al., 2023). Collier et al. (2023) bring in cultural dimensions, revealing how norms and risk perceptions shape CIS participation. From the findings, trust issues were a major barrier (Figure 4.11), peer expectations were strongly correlated with sharing advocacy (R_s = 0.65), demonstrating the influence of social persuasion. To strengthen interpersonal and organisational trust and establish norms that promote regular and reciprocal sharing, the following domain actions for this human factor are identified:

- Establish or join regional CIS peer networks via industry or Chamber of Commerce affiliations.
- Launch a CIS trust code and recognition programme that publicly acknowledges collie consistent contributors.
- Create knowledge exchange forums (such as, quarterly sharing roundtables or webinars).
- Encourage inter-SME collaboration in joint cybersecurity playbook exercises.

The identified social-cultural domain actions map to the simplified processes and incentives from the literature-informed protocol to form the interacting behavioural & technological domains:

- Role in the Cycle: Reduces participation barriers and clarifies benefits. Simple reporting templates, accessible platforms, and incentives encourage engagement.
- SCT Construct: Self-Efficacy & Mastery Experiences – SMEs need to feel capable of performing CIS tasks efficiently. Hands-on practice, guided exercises, and reward structures enhance confidence.
- Protocol Actions: Standardised templates, online reporting tools, pre-filled forms, and training modules. The goal is to transform awareness into actionable behaviour.
- Evidence from Findings: Only 40.9% of SMEs could create incident reports; qualitative findings showed reliance on informal ad hoc methods, indicating a knowledge-behaviour gap.

3. Psychological Domain → Foster a collaborative culture and safety → Self-Efficacy: Foster safe environments and address heuristics through dialogue-based workshops and leadership support (Schinagl & Paans, 2017; Kobis, 2021; Triplett, 2022). Schinagl & Paans (2017) bring out communication challenges in decision-making processes, stressing how system language hampers CIS unless properly mediated. In the findings, it was presented that self-efficacy was inconsistently linked to best practices (R_s = -0.69). Confidence levels were often not matched with actionable structures. To create psychologically safe environments and boost SMEs' confidence in their ability to participate in CIS, the following domain actions for this human factor are identified:

    - Offer anonymous sharing options for SMEs concerned about reputation or exposure.
    - Implement feedback loops: provide SMEs with outcomes or insights gained from their submitted reports.
    - Develop visual, scenario-based CIS heuristics (such as, decision trees, flowcharts).
    - Provide informal mentorship or buddy systems linking lower-engagement SMEs to Cluster 3-type SMEs.

    The identified domain actions for fostering a collaborative culture and safety integrate anonymous reporting options, feedback loops, and mentorship systems to align outcome expectations with observable peer reinforcement. Thereby forming the interacting psychological and socio-cultural domains:

    - Role in the Cycle: Establishing a supportive environment where SMEs view sharing as low-risk and mutually beneficial. Psychological safety reduces fear of negative consequences from participation.
    - SCT Construct: Outcome Expectations & Social Persuasion – Anticipated positive outcomes and reinforcement from peers drive engagement. Social modelling demonstrates how sharing is a safe, normative practice.
    - Protocol Actions: Anonymous sharing options, mentoring or buddy systems, knowledge exchange forums, and workshops.

Evidence from Findings: Negative correlation (R_s = -0.69) shows that confidence without proper scaffolding may not translate into effective CIS behaviour, emphasising the need for a safe, supportive environment.

4. Technological Domain → Ensure legal and ethical guidelines → Reinforcement (linked to Outcome Expectations): Standardise reporting platforms and ensure ease of use, particularly for micro-enterprises (Sauerwein et al., 2017; Alaeifar et al., 2024). Alaeifar et al. (2024) synthesise current and future CIS approaches, advocating for incentive-aligned, user-friendly sharing ecosystems to foster SME participation. According to the findings, 63.6% of SMEs reported no access to standardised reporting formats (Table 4.14), while 59.1% called for improvements in CIS practices (Table 4.15). Clear, usable technologies act as reinforcement mechanisms, stabilising outcome expectations by demonstrating to SMEs that their reporting efforts will be recognised, compliant, and beneficial. To ensure that SMEs, regardless of size or resource base, can engage with user-friendly, secure, and functional CIS technologies, the following domain actions for this human factor are identified:

    - Create a free-to-access online CIS form builder for SMEs.
    - Partner with local ICT hubs to provide guided CIS reporting kiosks.
    - Promote interoperable data exchange formats (aligned with NIST 800-150 or MISP standards).
    - Pre-populate form templates with drop-downs, threat categories, and impact scales to reduce reporting friction.

    The identified domain actions enrich the ensure legal and ethical guidelines component of the literature-informed protocol by emphasising usability: free-to-access form builders, interoperable data standards, and kiosk-supported reporting. This informs the interacting technological, policy, and governance domains:

    - Role in the Cycle: Provides clarity, accountability, and alignment with national and sectoral regulations. Legal and ethical frameworks reduce uncertainty and standardise behaviour across SMEs.

- SCT Construct: Reinforcement & Observational Learning – Clear rules and expectations reinforce behaviour and provide observable norms for others to follow.
- Protocol Actions: Regulatory compliance starter kits, sector-specific policy templates, and formalised internal reporting hierarchies.
- Evidence from Findings: SMEs showed inconsistent understanding of reporting responsibilities; Governance Preparedness Cronbach Alpha = 0.85, highlighting policy clarity as a crucial enabler.

5. Policy and Governance Domain → Ongoing support and feedback → Reinforcement & Feedback (linked to Outcome Expectations): Clarify reporting responsibilities and align with national legislation (Chidukwani, Zander & Koutsakis, 2022; Moore, 2022). Social persuasion is reinforced through visible accountability and peer feedback. Based on the presented findings, SMEs showed an inconsistent understanding of who to report to (Figures 4.3 & 4.4). Governance Preparedness had acceptable reliability (Cronbach's Alpha = 0.85). To align internal policy and national regulations with clear, enforceable CIS procedures, the following domain actions for this human factor are identified:

    - Provide SMEs with a regulatory compliance starter kit (POPIA, Cybercrimes Act, etc.).
    - Encourage large enterprises and government suppliers to mandate CIS participation clauses for SME subcontractors.
    - Formalise internal reporting hierarchies (e.g., specify who receives reports internally and externally).
    - Develop sector-specific CIS policy templates that SMEs can customise.

    The identified domain actions expand the ongoing support and feedback component of the literature-informed protocol by embedding compliance starter kits, subcontractor mandates, and sector-specific templates, reinforced by dashboards and feedback mechanisms to sustain participation. This forms the interacting psychological and behavioural domains:

- Role in the Cycle: Ensures SMEs can continuously adapt, learn, and refine CIS participation. Feedback loops reinforce good practice and provide guidance for improvement.

- SCT Construct: Self-Efficacy, Outcome Expectations & Reinforcement – Regular feedback enhances confidence, highlights benefits, and encourages repetition of desired behaviours.

- Protocol Actions: Continuous monitoring, feedback dashboards, peer recognition, and iterative training. Insights from reporting activities inform SMEs of the value of their participation.

- Evidence from Findings: Cluster profiles (such as, intention-behaviour gaps) demonstrate the need for iterative feedback to convert high intention into consistent action.

This refined protocol explicitly integrates the empirical findings (Section 5.2) with the literature-informed model (Chapter 2). It includes a five-domain cycle with SCT constructs and shows how mastery experiences, social persuasion, self-efficacy, and outcome expectations now guide actionable steps across domains. Together, they produce a protocol that is evidence-informed, cluster-sensitive, and operationally actionable. It supports adaptive, cluster-specific interventions, bridging knowledge, confidence, and behaviour gaps while embedding trust, technological usability, and governance clarity. In doing so, it operationalises the objective 3 artefact of a human-centric CIS protocol for SMEs in South Africa, providing practical, measurable pathways to enhance engagement, standardise reporting, and sustain cybersecurity information sharing. This refinement therefore delivers on Objective 3 by producing an artefact: a practical and measurable human-centric CIS protocol for SMEs in South Africa.

5.4 Evaluation of protocol efficacy

To ensure thoroughness and rigour, the resulting protocol presented in Section 5.3 was evaluated by experts in the field. This section details the insights gained from the evaluation and identifies whether the protocol demonstrates theoretical alignment, empirical relevance, implementation feasibility, and validation readiness. The structure of this section begins with descriptive statistics of the profiles of the experts involved in the evaluation, followed by a reliability test to assess the internal consistency of the dataset. It then presents key variable groupings, which include the clarity of protocol components, the

relevance of the protocol to SMEs, the feasibility and impact of the protocol on SMEs, and the overall evaluation. Based on the findings from the expert evaluation, a final revised protocol is presented; it represents a validated, actionable framework for promoting the adoption of CIS participation through a human-centric process.

5.4.1 Experts profile

Table 5.2 presents the distribution of job roles across the subject matter expert respondents.

Table 5-2: Professional role

Item		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Educator	3	50,0	50,0	50,0
	Director	2	33,3	33,3	83,3
	Other	1	16,7	16,7	100,0
	Total	6	100,0	100,0	

The educator (50.0%) provided a more pedagogical or research-oriented evaluation, while the director (33.3%) offered an assessment from a decision-maker's perspective, applying a strategic or operational implementation lens. The remaining role (16.7%) contributed a domain-specific viewpoint. This distribution showcases a diversity of perspectives in the evaluation of the CIS protocol.

In Table 5.3, the expertise area/domain of the subject matter experts is presented.

Table 5-3: Areas of expertise

Item		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Cybersecurity	2	33,3	33,3	33,3
	SME Development	2	33,3	33,3	66,7
	Other	2	33,3	33,3	100,0
	Total	6	100,0	100,0	

The results show that 33.3% of respondents are experts in cybersecurity, covering the technical aspects of the CIS protocol. Another 33.3% are SME development experts, addressing the nuanced aspects of protocol feasibility for SMEs. The remaining 33.3% of respondents represent multi-disciplinary expertise, providing a balanced view of both technical and non-technical aspects of the CIS protocol.

Table 5.4 displays the years of experience that the subject matter experts have. 33.3% of respondents possess more than 15 years of experience, indicating that they are senior domain experts. 50.0% of respondents have between 6 and 10 years of experience, suggesting that they are middle-career experts, while the remaining 33.3% are early-career experts.

Table 5-4: Years of experience

Item		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-5	1	16,7	16,7	16,7
	6-10	3	50,0	50,0	66,7
	15+	2	33,3	33,3	100,0
	Total	6	100,0	100,0	

This distribution of expertise strengthens the credibility of the evaluation process. The balanced expertise profile of respondents ensures that the outcomes of the evaluation will further enhance the usefulness of the CIS protocol through recommended refinements.

5.4.2 Reliability of the evaluation dataset

In this section, the variables with the same Likert scales are tested for internal consistency. Table 5.5 presents Cronbach's Alpha values for the variables.

Table 5-5: Reliability statistics

Cronbach's Alpha	N of Items
,911	12

As per the interpretation of Cronbach's Alpha values held in Table 4.16, the internal consistency of this evaluation dataset is considered to be excellent reliability (very strong internal consistency) with a value of 0.911.

5.4.3 Clarity of protocol components

This section presents the first evaluation item, which relates to the clarity of CIS protocol components. Table 5.6 displays five variables associated with this evaluation variable group:

Table 5-6: Evaluation variable group: clarity of protocol components

Item	N	Minimum	Maximum	Mean	Std. Deviation
BehaviourClearlydefined	6	1	5	3,67	1,506
Socioculturalunderstandable_applicable	6	3	5	4,00	,632
PsychologicalArticulatedclearly	6	3	5	4,00	,894
TechnologicalEasytointerpret	6	2	5	3,67	1,033
PolicyLogicallystructured	6	3	5	4,00	,894
Valid N (listwise)	6				

Referring to Table 5.6 above, there are five variables associated with this group:

- BehaviourClearlydefined – Are behavioural interventions clearly defined?
- Socioculturalunderstandable_applicable – Are socio-cultural interventions understandable and applicable?
- PsychologicalArticulatedclearly – Are psychological strategies clearly articulated?
- TechnologicalEasytointerpret – Are technological interventions easy to interpret?
- PolicyLogicallystructured – Are policy recommendations logically structured?

The results for this variable group, as shown in Table 5.6, indicate a mean score of 3.87 for overall clarity. This suggests a general agreement that the core components of the protocol are clear, interpretable, and well-defined. However, there is an anomaly in the variable for behavioural interventions, where one respondent scored a 1 (strongly disagree), as well as in the variable for technology interventions, where another respondent scored a 2 (disagree). These two variables require some minor refinements, which may include improving guidance on implementation.

5.4.4 Relevance to SME CIS challenges

In Table 5.7, the evaluation item relates to the relevance of the CIS protocol to mitigate SME CIS challenges.

Table 5-7: Evaluation variable group: relevance to SME CIS challenges

Item	N	Minimum	Maximum	Mean	Std. Deviation
ProtocolBarriers	6	1	5	3,33	1,366
ProposedSMEconstraints	6	3	5	3,83	,753
HumanfactorRelevanttoSMEcontexts	6	3	5	4,33	,816
Valid N (listwise)	6				

According to Table 5.7 shown above, there are three variables associated with this group:

- ProtocolBarriers – Does the protocol meaningfully address the barriers SMEs face in participating in CIS?
- ProposedSMEconstraints – Are the proposed solutions aligned with the typical operational, technological, or financial constraints of SMEs?
- HumanfactorRelevanttoSMEcontexts – Are the human factor considerations (such as, trust, experience, confidence) applicable and realistic for SMEs?

The result presented for this variable group is an overall mean score of 3.83, indicating that experts generally agree the protocol is relevant to real SME challenges in engaging with CIS. However, there is an anomaly within this variable group concerning the protocol's ability to address the barriers SMEs face in participating in CIS, as one expert scored a 1 (strongly disagree). This suggests that some improvement is needed in this area. Potential improvements could include ensuring the availability of formal policies to support adoption.

5.4.5 Feasibility and impact

The Table 5.8 provides insight on whether this CIS protocol is practically implementable among SMEs.

Table 5-8: Evaluation variable group: feasibility and impact

Item	N	Minimum	Maximum	Mean	Std. Deviation
InterventionsfeasibleforSMEswithlimitedexpertise	6	3	4	3,33	,516
ProtocolEnhancetrust_collaborationwithinSME	6	3	5	4,00	,632
ProtocolAdaptableacrosssectors	6	2	4	3,67	,816
Valid N (listwise)	6				

The evaluation item displayed in Table 5.7 has three variables associated with it:

- InterventionsfeasibleforSMEswithlimitedexpertise – Are the interventions practical and manageable for SMEs with minimal cybersecurity capacity?
- ProtocolEnhancetrust_collaborationwithinSME – Will the protocol improve trust and collaborative practices among SMEs?
- ProtocolAdaptableacrosssectors – Is the protocol flexible and adaptable across various SME sectors?

The overall mean score for this variable group is 3.67, indicating that experts generally agree that the protocol is relevant to real SME challenges in engaging with CIS. However, there is an anomaly within this variable group concerning the indicator that assesses whether the protocol is flexible and adaptable across various SME sectors. One respondent scored this indicator a 2 (disagree), suggesting that there is room for further refinement, such as providing sector-specific case studies that outline different implementation strategies for varying contexts.

5.4.6 Overall evaluation

In this section, Table 5.9 presents the overall evaluation group that has two variables.

Table 5-9: Evaluation variable group: overall evaluation

Item	N	Minimum	Maximum	Mean	Std. Deviation
ProtocolUseful_practicaltoolforimprovingCIS	6	4	5	4,50	,548
Valid N (listwise)	6				

The one ordinal (scale) variable ProtocolUseful_practicaltoolforimprovingCIS and one nominal variable AdditionalFeedbackconcernssuggestions shown in Table 5.9 are defined as follows:

- ProtocolUseful_practicaltoolforimprovingCIS – This protocol is a useful and practical tool for improving SME participation in CIS.
- AdditionalFeedbackconcernssuggestions – Open-ended feedback from subject matter experts.

The mean score for this variable group is 4.50, indicating that experts strongly agree the protocol is a useful and practical tool. This confirms that experts believe the CIS protocol meets the expectations of clarity, practicality, and relevance to SME CIS needs. Therefore, this score validates the effectiveness of the design and affirms its readiness for real-world application.

The qualitative aspect of this evaluation offers deeper insights and corroborates the quantitative results. Table 5.10 presents feedback from subject matter experts regarding their perceptions of the CIS protocol.

Table 5-10: Feedback from subject matter experts on their perception of the refined protocol

Respondent #	Feedback
RESPONDENT001	Nothing
RESPONDENT002	Factors necessary to design a protocol to empower SMEs to actively participate in cybersecurity information sharing (CIS) for purposes of improving cybersecurity seem to have been well-considered
RESPONDENT003	Coming from a computer science background, I think there is little technical issues that are key that have been omitted
RESPONDENT004	Strengths: 1. The protocol demonstrates a clear knowledge of difficulties faced by SMEs in sharing threat information. 2. The protocol is adaptive across different sectors. 3. The proposed solutions are well-structured and take into account the human factor considerations. Concerns: 1. Some statements received an "Agree" rating instead of "Strongly Agree", indicating that there might be room for improvement in those areas. 2. The protocol's effectiveness in enhancing trust and collaboration within SME communities is crucial; it would be beneficial to provide more details on how this will be achieved. Suggestions: 1. Consider providing more concrete examples or case studies to illustrate the protocol's application in different sectors. 2. Include a clear implementation plan, outlining the steps and resources required for SMEs to adopt the protocol. 3. Provide guidance on how to monitor and evaluate the protocol's effectiveness in improving SME participation in CIS. By addressing these concerns and incorporating these suggestions, the final protocol design can be even more effective in supporting SMEs in sharing threat information and enhancing their cybersecurity posture.
RESPONDENT005	SMEs struggle basically because in most cases they do not have any policy document regarding issues such as cyber security, etc.
RESPONDENT006	Many SMEs have limited cybersecurity maturity and the proposed interventions may not be feasible or relevant.

The feedback provides an agreement on the usefulness and practicality of the protocol. Respondent004 provides elaborate feedback that highlights some key considerations when refining the protocol:

> "*...it would be beneficial to provide more details on how this will be achieved*"
>
> "*more concrete examples or case studies to illustrate the protocol's application in different sectors*"

"...clear implementation plan, outlining the steps and resources required for SMEs to adopt the protocol"

"*...guidance on how to monitor and evaluate the protocol's effectiveness*"

Respondent005 provides an additional refinement suggesting:

"*SMEs struggle basically because in most cases they do not have any policy document regarding issues such as cyber security, etc*"

Respondent006 indicates that:

"*Many SMEs have limited cybersecurity maturity and the proposed interventions may not be feasible or relevant*"

Based on this feedback and the identified anomalies in the variable groups, Table 5.11 represents a refined CIS protocol.

Table 5-11: Final CIS protocol

To empower SMEs to actively participate in CIS, this human-centric protocol addresses five interrelated domains:

1. Behavioural – skills and actions necessary for CIS;
2. Socio-Cultural – norms, peer influence, and organisational culture;
3. Psychological – trust, confidence, and perception of risk;
4. Technological – platform usability and tool accessibility;
5. Policy and Governance – internal and external structures that reinforce CIS.

Each domain includes actionable components to address key enablers and barriers identified in the study. Implementation considerations include:

- Tailoring by cluster profile: Cluster 1 SMEs should begin with behavioural and psychological interventions; Cluster 2 should focus on governance and technical enablement; Cluster 3 can serve as CIS role models.
- Low-cost rollout: Use local chambers and trade networks for protocol dissemination.
- Scalability: Begin with sectors exhibiting high threat exposure and low CIS maturity.

Cluster	Profile Description
Cluster 1	SMEs in cluster 1 exhibited high levels of intention across all CIS-related items but reported very low internal and external CIS activity.
Cluster 2	SMEs in cluster 2 showed medium intention with a mixed behavioural engagement where CIS participation is episodic or reactive.
Cluster 3	SMEs in cluster 3 exhibited high levels of intention across all CIS-related items with strong internal and external CIS activity.

The Protocol:

1. Behavioural Domain:

Enhancing Cybersecurity Competency and Reporting Capability

Objective:

Build SME staff capacity to identify, report, and communicate cyber incidents effectively.

Actions:

- Conduct readiness self-assessment.
- Develop role-based training modules on cyber threat identification and response.
- Distribute standardised cyber incident report templates tailored to SME operational contexts.
- Introduce simulation-based learning that is peer-led (such as, phishing email simulations, incident response drills).
- Establish internal CIS champions responsible for coordinating reporting.
- Conduct periodic cyber-awareness check-ins.
- Gamify managerial reinforcement strategies using verbal acknowledgements and digital leader boards.

2. Socio-Cultural Domain:

Building Trust and Shared Norms

Objective:

Strengthen interpersonal and organisational trust and establish norms that promote regular and reciprocal sharing.

Actions:

- Establish or join regional CIS peer networks via industry or Chamber of Commerce affiliations.
- Launch a CIS trust code and recognition programme that publicly acknowledges consistent contributors.
- Create knowledge exchange forums (such as, quarterly sharing roundtables or webinars).
- Encourage inter-SME collaboration in joint tabletop exercises.
- Encourage peer benchmarking and informal learning within sector-aligned business networks.
- Facilitate participation in trusted sharing forums, including regional SME cybersecurity task forces.

3. Psychological Domain:

Addressing Confidence, Risk Perception, and Heuristics

Objective:

Create psychologically safe environments and boost SMEs' confidence in their ability to participate in CIS.

Actions:

- Identify champions within the SME.
- Offer anonymous sharing options for SMEs concerned about reputation or exposure.
- Provide templates for anonymous sharing.
- Pre-written scripts for incident notifications.
- Implement feedback loops: provide SMEs with outcomes or insights gained from their submitted reports.
- Develop visual, scenario-based CIS heuristics (such as, decision trees).

- Provide informal mentorship or buddy systems linking lower-engagement SMEs to Cluster 3-type SMEs.
- Conduct monthly monitoring and evaluation of CIS events internally and externally
- Display cyber "success stories" on notice boards to reinforce positive outcomes.

4. Technological Domain:

Enabling Accessible and Standardised Platforms

Objective:

Ensure that SMEs, regardless of size or resource base, can engage with user-friendly, secure, and functional CIS technologies.

Actions:

- Determine SME CIS readiness using a checklist.
- Identify appropriate tools and platforms for CIS (open source or vendor-supported).
- Create a free-to-access online CIS form builder for SMEs.
- Use platform integration templates and vendor assessment checklists.
- Partner with local ICT hubs to provide guided CIS reporting kiosks.
- Promote interoperable data exchange formats (aligned with NIST 800-150 or MISP standards).
- Pre-populate form templates with drop-downs, threat categories, and impact scales to reduce reporting friction.

5. Policy and Governance Domain:

Embedding Structure and Compliance

Objective:

Align internal policy and national regulations with clear, enforceable CIS procedures.

Actions:

- Provide SMEs with a regulatory compliance starter kit (POPIA, Cybercrimes Act, etc.).
- Cyber incident response policies.
- Introduce SME-level confidentiality and trust agreements.
- Encourage large enterprises and government suppliers to mandate CIS participation clauses for SME sub-contractors.
- Internal and external sharing procedures (Standard Operating Procedures).
- Formalise internal reporting hierarchies (such as, specify who receives reports internally and externally).
- Develop sector-specific CIS policy templates that SMEs can customise.

Table 5.11 presents a comprehensive, validated human-centric CIS protocol. It provides an evidence-based and actionable roadmap for SMEs to adopt CIS practices. This protocol reflects a flexible, cluster-adapted approach that combines behavioural, social, psychological, technological, and policy

interventions. It serves as a research-to-practice translation, ensuring that SCT-informed findings are implemented in real-world SME contexts.

5.5 Summary

Chapter 5 integrated the literature-informed protocol with empirical findings to develop a human-centric CIS protocol for SMEs. Using SCT as the guiding framework, the chapter demonstrated how behavioural, socio-cultural, psychological, technological, and policy/governance domains collectively influence SME participation. Trust, self-efficacy, and perceived benefits emerged as key enablers, while policy clarity and technology usability moderated engagement. Cluster-based insights highlighted tailored interventions for SMEs with differing readiness and activity levels, and actionable domain-specific strategies were proposed, including role-based training, peer-led knowledge exchange, scenario-based heuristics, standardised platforms, and regulatory alignment. This resulted in a five-domain cycle, representing a dynamic interplay of SCT constructs across the protocol. Future directions were proposed, addressing scalability, adaptation beyond South Africa, integration of emerging technologies, and the need for pilot and longitudinal validation. The next chapter will conclude the study, outline its contributions, and suggest future research directions to further support SMEs in building cyber resilience through collaborative intelligence sharing.

6 CHAPTER SIX: CONCLUSION AND FUTURE WORK

6.1 Introduction

This chapter concludes the study by revisiting the purpose, objectives, and promises outlined in Chapter 1. While the introduction detailed what the research aimed to achieve, this chapter demonstrates how those aims were fulfilled. It synthesises the overall research journey, highlighting contributions, limitations, and directions for future work. The discussion extends beyond Chapter 5 to encompass the entire study, from the motivation and theoretical framing to the mixed-methods design, findings, and development of the human-centric CIS protocol for SMEs. Section 6.2 provides an overview of how the research objectives and questions were addressed. Section 6.3 outlines the contributions of the study, while Section 6.4 reflects on its limitations. Section 6.5 considers future directions, including scalability and technology integration, and Section 6.6 offers a closing summary. In this way, the chapter closes the loop with the introduction, demonstrating how the study's aims were achieved and situating its contributions within the broader discourse on SME cybersecurity in South Africa.

6.2 Overview of the research

This study was motivated by the persistent under-participation of South African SMEs in CIS, despite the existence of policies, frameworks, and technical platforms designed to encourage collaboration. Chapter 1 outlined four objectives along with their corresponding research questions. This section revisits those questions and demonstrates how each was addressed through the methodological design, data collection, and analysis processes. By linking findings across Chapters 4 and 5, it illustrates how the study achieved the aims set out in the introduction.

To strengthen the connection between the research questions, findings, and resulting recommendations, Table 6.1 provides a consolidated mapping that highlights how each component of the study aligns.

Table 6-1: Mapping of research questions to key findings and recommendations

Research Question	Key Findings (Chapters 4 and 5)	Resulting Recommendations (Chapter 6)
RQ1: What human factors are associated with effective CIS?	• Outcome expectations, self-efficacy, and subjective norms emerged as significant predictors of CIS engagement. • Qualitative insights highlighted trust-building, prior incident experience, and reporting confidence as central behavioural drivers.	• Strengthen SME self-efficacy through training and simplified reporting tools. • Introduce trust-building initiatives such as anonymised sharing and peer-supported learning forums.

RQ2: How do policies and technologies influence human factors associated with CIS?	• SMEs with unclear or absent policies showed lower engagement. • Technological constraints included lack of standardised reporting tools and limited interoperability. • Compliance difficulties weakened CIS participation.	• Develop simplified, SME-aligned CIS policies. • Promote adoption of standardised, low-complexity reporting platforms. • Strengthen regulatory awareness campaigns.
RQ3: What protocol can be implemented to achieve reciprocal CIS among SMEs?	• Five-domain human-centric CIS protocol developed: behavioural, socio-cultural, psychological, technological, and policy/governance. • Protocol grounded in SCT and reflects SME cluster diversity (such as, high-intention/low-behaviour profiles).	• Implement modular CIS protocol adaptable to SMEs of varying maturity levels. • Integrate peer collaboration, incentives, and simplified workflows to improve usability and uptake.
RQ4: What is the efficacy of the protocol in achieving reciprocal CIS?	• Expert validation showed high relevance and feasibility (mean scores >3.8). • One expert highlighted need for clearer policy scaffolding to ensure SME uptake.	• Refine protocol to strengthen policy alignment and clarify implementation steps. • Provide guidance for SMEs, policymakers, and industry bodies on scalable deployment.

The mapping presented in Table 6.1 demonstrates how each research question was fully addressed through aligned empirical evidence and actionable insights. The alignment clarifies how the study progressed from diagnosing behavioural and organisational barriers to developing and validating a practical, SCT-driven protocol for SMEs. It also shows how recommendations logically arise from the findings, reinforcing the study's contribution to both cybersecurity scholarship and SME practice.

- ***Objective 1: To determine the human factors associated with effective CIS among SMEs.*** This objective was addressed through a sequential explanatory mixed-methods design. Quantitatively, survey data (N=22) were analysed using descriptive statistics, Cronbach's alpha reliability tests, Spearman's Rank Correlation, and HCA (see Tables 4.1-4.24 and Figures 4.1-4.7). These analyses identified outcome expectations, self-efficacy, and subjective norms as significant predictors of CIS participation. Qualitatively, interviews with 10 SME participants (Chapter 5, Section 5.2) provided insights into trust-building, prior incident experience, and reporting practices. Together, these results confirmed that human factors are decisive in shaping CIS behaviour, fulfilling the first objective.
- ***Objective 2: To examine how policy and technology influence SME engagement in CIS.*** The second objective was addressed by integrating governance and technological dimensions into the analysis. Quantitative findings on governance preparedness (Cronbach's alpha = 0.85; see Table 4.18) revealed that SMEs with unclear or absent policies demonstrated lower levels of engagement. Thematic analysis (Chapter 4) highlighted constraints such as the lack of standardised reporting tools, interoperability challenges, and difficulties in complying with

legislative requirements. These findings show that policy clarity and technological usability act as moderators of human factors, either reinforcing or constraining SME participation in CIS.

- ***Objective 3: To develop a human-centric CIS protocol tailored to the South African SME context.***

  The integration of quantitative and qualitative findings facilitated the design of a refined human-centric CIS protocol (Chapter 5, Section 5.3). Building on the literature-informed protocol from Chapter 2, this new protocol incorporates five interrelated domains: behavioural, socio-cultural, psychological, technological, and policy and governance. Each domain operationalises SCT constructs, including mastery experiences, self-efficacy, social persuasion, and outcome expectations, into practical actions for SMEs. The protocol is modular and adaptive, addressing the diversity revealed in cluster profiles (Section 5.2.6), which ranged from high-intention/low-behaviour SMEs to those demonstrating consistent alignment between intention and practice. This outcome represents the central artefact of the study.

- ***Objective 4: To validate the relevance and feasibility of the proposed protocol.***

  Validation was achieved through an expert review exercise (see Tables 5.6-5.10). Experts confirmed the protocol's relevance to SME realities, with mean scores above 3.8 across key variables, including the protocol's capacity to reflect human-factor challenges and SME constraints. Divergent opinions, such as one expert's concern about the ability to address participation barriers, highlighted the need for refinement through clearer policy scaffolding. Overall, validation confirmed the protocol's theoretical soundness, practical applicability, and potential for scalability, thereby fulfilling the fourth objective.

In summary, this study employed a rigorous sequential explanatory design to identify human, policy, and technological factors, followed by analysis and synthesis leading to the development and validation of a novel protocol. The research questions were systematically answered through the triangulation of quantitative and qualitative evidence, and the objectives outlined in Chapter 1 were fully achieved. The resulting human-centric CIS protocol offers both an academic contribution to SCT-based cybersecurity research and a practical intervention for SMEs in South Africa.

6.3 Research contribution

The main contribution of this study is the development of the Human-Centric CIS Protocol, a five-domain framework operationalised through SCT constructs, designed to enhance SME participation in CIS. By embedding behavioural, socio-cultural, psychological, technological, and governance dimensions into a

modular protocol, the study presents a novel artefact that addresses the specific challenges faced by South African SMEs while remaining adaptable to broader contexts.

The theoretical contribution of this study extends SCT by demonstrating its applicability in modelling SME cybersecurity behaviour, a domain where behavioural theory remains underexplored. Chapter 4 revealed that SMEs' intention to share information does not always translate into practice (Cluster 1), illustrating an intention–behaviour gap that SCT helps explain through its construct of self-efficacy. Quantitative results, such as the strong positive correlation between outcome expectations and CIS intention (R_s = 0.73) and the negative correlation between self-efficacy and best practice (R_s = -0.69), highlight the complexity of behavioural engagement. These findings extend SCT by showing that confidence alone is insufficient without structural reinforcement. By integrating constructs such as mastery experiences, social persuasion, and outcome expectations into the protocol's design, this research advances theory by illustrating how behavioural and environmental factors co-determine cybersecurity practices in SMEs.

The methodological contribution of this study lies in the application of a sequential explanatory mixed-methods design to SME cybersecurity. Quantitative analysis (such as, Spearman's Rank Correlation, HCA) identified statistically significant relationships between SCT constructs and CIS behaviours, while qualitative analysis revealed organisational and psychological barriers, including a lack of procedural scaffolding, informal practices, and distrust of peers. These complementary insights were synthesised in the refinement of the protocol (Section 5.3). Furthermore, expert validation (Tables 5.6-5.10) added an evaluative layer that confirmed relevance (mean = 3.83) and alignment with SME contexts (mean = 4.33), while flagging areas needing policy reinforcement (mean = 3.33). This triangulation demonstrates a rigorous, multi-perspective approach rarely employed in SME cybersecurity studies, offering a replicable methodology for future research.

The practical contribution of this study is that it tested and refined a protocol that provides SMEs with actionable guidance for overcoming barriers to CIS. Unlike international frameworks such as ISO/IEC 27032 and NIST 800-150, which are resource-intensive and misaligned with SME realities, this protocol simplifies adoption through concrete measures: scenario-based training and standardised templates (behavioural), peer networks and recognition schemes (socio-cultural), anonymous reporting and feedback loops (psychological), accessible reporting tools and kiosks (technological), and compliance starter kits with sector-specific templates (policy and governance). Findings, such as only 40.9% of SMEs being able to generate incident reports, underscore the urgency of such targeted interventions.

The protocol has practical implications for SME owners and managers, business chambers, sectoral associations, regulators, and policymakers, all of whom are stakeholders in building collective cyber resilience. Its modular design also ensures adaptability to other SME-dominated sectors such as financial services, healthcare, and manufacturing, and scalability to neighbouring regions facing similar resource and trust constraints.

In summary, this study contributes to the body of knowledge by (1) theoretically extending SCT into the SME cybersecurity domain, (2) methodologically demonstrating the value of mixed-methods triangulation and expert validation, and (3) practically producing a novel Human-Centric CIS Protocol that translates behavioural theory into actionable, context-sensitive interventions. This collection of contributions enriches academic discourse while offering a practical tool for strengthening SME participation in CIS, thereby promoting improved cyber resilience amongst SMEs.

6.4 Study limitations

While this research contributes to understanding and enhancing SME CIS participation, several limitations must be acknowledged:

Sample size and representativeness: The quantitative sample (N = 22) and qualitative interviews (n = 10) were small and drawn through purposive and snowball sampling. While sufficient for exploratory research, the limited scale reduces statistical power, increases susceptibility to bias, and constrains generalisability. Snowball sampling may have introduced selection bias, potentially over-representing SMEs with a pre-existing interest in cybersecurity. Consequently, findings must be interpreted with caution when extrapolating to broader SME populations. Future studies should employ larger, stratified samples across sectors and regions to enhance representativeness and improve protocol validation.

Geographic and sectoral scope: The study focused exclusively on the Eastern Cape province and primarily the retail sector. This geographic and sectoral concentration limits the protocol's immediate applicability to rural or highly regulated SMEs. Contextual factors such as infrastructure availability, sector-specific compliance requirements, and local organisational culture may differ substantially, potentially affecting the protocol's relevance. Cross-sectoral and regional comparisons are recommended for future research to capture these variations.

Cross-sectional design: A cross-sectional approach captures behaviour and attitudes at a single point in time, limiting the ability to evaluate behavioural evolution or sustained adoption of the protocol.

Longitudinal studies could assess how SMEs' engagement with CIS changes over time and measure the impact and sustainability of the protocol.

Non-technical and legal constraints: Access to SME registers was restricted by the Protection of Personal Information Act (POPIA), which prevented business chambers in the Eastern Cape from sharing contact details. This limited outreach and reduced the ability to recruit a broader sample. Furthermore, some SMEs were reluctant to disclose cybersecurity practices or participate in the study due to concerns about reputational harm, exposure of sensitive information, or a lack of perceived benefit. These barriers reflect the broader challenges of trust and confidentiality that influence CIS participation itself and should be considered in designing recruitment strategies for future studies.

Technological scope: Although the study developed a protocol, it did not empirically test open-source or automated platforms for CIS. Integrating platforms with advanced capabilities, such as AI-assisted reporting or IoT-enabled threat monitoring, could further enhance adoption and usability. Future work should examine technical feasibility, platform usability, and automation to ensure technology aligns with SMEs' operational realities.

SCT limitations: SCT effectively captured individual- and organisational-level behaviour but is limited in addressing broader technological, organisational, and environmental factors. Integrating frameworks like Technology-Organisation-Environment (TOE) could provide macro-level insight, particularly for sector-specific adaptations and readiness assessments.

Diversity considerations: The study did not explicitly consider cultural, linguistic, and socio-economic diversity among SMEs. These factors could influence trust, communication, and willingness to share cybersecurity information. Incorporating frameworks such as Hofstede's cultural dimensions would help future studies better contextualise behaviour and refine interventions.

6.5 Future directions, scalability, and technology integration

The human-centric CIS protocol developed in Chapter 5, while tailored to South African SMEs, has been designed with modularity and adaptability in mind. Its five-domain structure, comprising behavioural, socio-cultural, psychological, technological, and policy and governance aspects, allows it to be applied not only within South Africa but also across other SME sectors such as financial services, healthcare, and manufacturing. Beyond national boundaries, the protocol holds potential for adoption in other emerging economies, particularly within the Southern African Development Community (SADC) and

broader sub-Saharan Africa, where SMEs face similar challenges of limited expertise, fragmented governance, and high exposure to cybercrime. Its layered design enables organisations to expand role-specific training, implement tiered governance, and foster peer mentorship, thereby embedding trust and engagement across multiple organisational levels.

Technology integration presents significant opportunities for further enhancement. Artificial intelligence (AI) can be leveraged to deliver personalised, scenario-based training, monitor SME participation, and generate actionable insights on compliance and behavioural trends. The Internet of Things (IoT) offers the potential for automated incident detection and real-time reporting, reducing operational burdens while improving responsiveness. Technology-assisted dashboards and open-source platforms can strengthen governance by tracking adherence to internal policies and national regulations, reinforcing accountability and transparency in CIS practices.

Future empirical validation is essential to confirm the scalability and effectiveness of the protocol. Pilot implementation in diverse contexts, which should include rural and resource-constrained SMEs, will identify practical barriers such as financial limitations, organisational resistance, and infrastructure variability. Cluster-specific strategies developed in Chapter 5 should guide these rollouts, ensuring that interventions are tailored to SMEs' readiness and engagement profiles. Lessons from these pilots can inform sectoral and national scaling, supported by cross-sectoral studies that assess adaptation in regulated industries (such as, finance, healthcare) and under-researched communities.

Longitudinal studies are recommended to monitor the sustainability of CIS behaviours and to measure long-term outcomes across the behavioural, socio-cultural, psychological, technological, and policy domains. Repeated observations over time will provide insight into the durability of trust, confidence, and reporting practices.

Cultural and socio-economic considerations represent another critical avenue. Qualitative research should explore how linguistic diversity, cultural norms, and socio-economic realities affect trust, communication, and CIS engagement. Frameworks such as Hofstede's cultural dimensions could provide nuance, ensuring that interventions remain human-centric and contextually grounded.

Policy alignment and stakeholder engagement are also necessary for sustainable adoption. The validation of the protocol should extend to government agencies, regulators, and large enterprise stakeholders, ensuring compatibility with national cybersecurity strategies and sector-specific

requirements. Policy-focused studies could evaluate incentives or mandates that encourage SME participation in CIS, particularly in compliance-heavy environments.

Finally, theoretical integration offers fertile ground for advancing scholarship. While the protocol has been anchored in SCT, combining SCT with the Technology–Organisation–Environment (TOE) framework could provide a multi-level perspective that integrates behavioural insights with organisational capacity and environmental influences. This extension would refine the protocol for SMEs operating in complex regulatory and technical ecosystems.

By aligning scalability, technological advancements, cultural sensitivity, and iterative validation, the human-centric CIS protocol is positioned as a dynamic and evolving tool. It not only addresses the immediate challenges of SME participation in South Africa but also contributes to the broader global discourse on collective cyber resilience.

6.6 Summary

This study has successfully developed and validated a human-centric CIS protocol tailored to South African SMEs, integrating behavioural, socio-cultural, psychological, technological, and policy domains underpinned by SCT. In doing so, it addressed all four research objectives outlined in Chapter 1: identifying human factors, examining policy and technology influences, designing an adaptive protocol, and validating its relevance. Theoretically, the study extends SCT by demonstrating its applicability to SME cybersecurity behaviour; methodologically, it illustrates the value of a sequential explanatory mixed-methods approach with expert validation; and practically, it delivers an artefact that SMEs, regulators, and policymakers can apply to strengthen cyber resilience.

While limitations in sample size, geographic scope, cross-sectional design, and technological scope are acknowledged, these do not diminish the value of the insights generated. Instead, they highlight opportunities for future research, particularly in pilot implementations, longitudinal studies, technology integration, and culturally sensitive interventions. The findings provide a roadmap for enhancing SME cybersecurity resilience by embedding human-centric principles into CIS strategies. By fostering trust, engagement, and sustainable participation, the study contributes not only to the academic literature but also to national and regional cybersecurity capacity.

REFERENCES

Abor, J. & Quartey, P. 2010. Issues in SME development in Ghana and South Africa. *International Research Journal of Finance and Economics*. 39.

Abzakh, A. & Althunibat, A. 2023. A Review: Human Factor and Cybersecurity. In *2023 International Conference on Information Technology (ICIT)*. IEEE. 589–592. DOI: 10.1109/ICIT58056.2023.10225828.

Adam, I.O. 2014. The Ontological, Epistemological and Methodological Debates in Information Systems Research: A Partial Review. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2411620.

Aferudin, F. & Ramli, K. 2022. The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia. *Budapest International Research and Critics Institute (BIRCI-Journal)*. DOI: 10.33258/birci.v5i3.6297.

Ajzen, I. 1985. From Intentions to Actions: A Theory of Planned Behavior. In *Action Control*. DOI: 10.1007/978-3-642-69746-3_2.

Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M. & Foo, E. 2024. Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. *Journal of Information Security and Applications*. 83:103786. DOI: 10.1016/j.jisa.2024.103786.

Al-Alawi, A.I., Alsaad, A.J., AlAlawi, E.I. & Naser Al-Hadad, A.A. 2021. The Analysis of Human Attitude toward Cybersecurity Information Sharing. In *2021 International Conference on Decision Aid Sciences and Application (DASA)*. IEEE. 947–956. DOI: 10.1109/DASA53625.2021.9682381.

AL-Dosari, K. & Fetais, N. 2023. Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics*. 12(17):3629. DOI: 10.3390/electronics12173629.

Allianz. 2023. *Stalked by the specter of cyber*. Available: https://commercial.allianz.com/news-and-insights/expert-risk-articles/SME-risks.html#:~:text=An%20increasing%20sweet%20spot%20for%20hackers&text=As%20larger%20companies%20have%20ramped,smaller%20companies%20with%20this%20process. [2025, August 17].

Ang, M.C.H., Ramayah, T. & Amin, H. 2015. DOI: 10.1108/EDI-02-2014-0012.

Aramo-Immonen, H. 2013. Mixed Methods Research Design. 32–43. DOI: 10.1007/978-3-642-35879-1_5.

Arenas, E., Palomino, J. & Mansilla, J.-P. 2023. Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications Based on ISO 27032 and NIST. In *2023 IEEE XXX International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*. IEEE. 1–8. DOI: 10.1109/INTERCON59652.2023.10326028.

Armenia, S., Angelini, M., Nonino, F., Palombi, G. & Schlitzer, M.F. 2021. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*. 147:113580. DOI: 10.1016/j.dss.2021.113580.

Astalin, P.K. 2013. Qualitative Research Designs: a Conceptual Framework. *International Journal of Social Science & Interdisciplinary Research*. 2(1).

Ayandibu, A.O. & Houghton, J. 2017. The role of Small and Medium Scale Enterprise in local economic development (LED). *Banach Journal of Mathematical Analysis*. 11(2).

Bahar, M., Muqeem, M. & Pattnaik, O. 2024. Cybersecurity Collaboration: Building Trust and Resilience through Information Sharing. *International Journal of Advanced Research in Science, Communication and Technology*. (May, 13):165–169. DOI: 10.48175/IJARSCT-18229.

Bandura, A. 1982. Self-efficacy mechanism in human agency. *American Psychologist*. 37(2). DOI: 10.1037/0003-066X.37.2.122.

Bandura, A. 1986. Social foundations of thought and action : a social cognitive theory / Albert Bandura. *New Jersey: Prentice-Hall, 1986*. 16(1).

Bearman, M. 2019. Focus on Methodology: Eliciting rich data: A practical approach to writing semi-structured interview schedules. *Focus on Health Professional Education: A Multi-Professional Journal*. 20(3). DOI: 10.11157/fohpe.v20i3.387.

Benz, M. & Chatterjee, D. 2020. Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*. 63(4):531–540. DOI: 10.1016/j.bushor.2020.03.010.

Bishop, L.M., Asquith, P.M. & Morgan, P.L. 2025. The Employee Cybersecurity Awareness Framework. *Human Behavior and Emerging Technologies*. 2025(1). DOI: 10.1155/hbe2/1025045.

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

Braun, V. & Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*. 3(2). DOI: 10.1191/1478088706qp063oa.

Bree, R. & Gallagher, G. 2016. Using Microsoft Excel to code and thematically analyse qualitative data: a simple, cost-effective approach. *All Ireland Journal of Teaching and Learning in Higher Education (AISHE-J)*. 8(2).

Bryman, Alan. 2016. *Social research methods 5th ed*.

Cano, J. 2019. The Human Factor in Information Security. *ISACA*. 5.

Cant, M.C. & Wiid, J.A. 2016. Internet-Based ICT Usage By South African SMEs: The Barriers Faced By SMEs. *Journal of Applied Business Research (JABR)*. 32(6):1877–1888. DOI: 10.19030/jabr.v32i6.9889.

Cashin, J. & Ifinedo, P. 2014. Using social cognitive theory to understand employees ' counterproductive computer security behaviors (CCSB): A pilot study. *27th. International Business Research Conference (IBRC)*. (June 2014).

Cele, N.N. & Kwenda, S. 2024. Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*. (April, 16). DOI: 10.1108/JFC-10-2023-0263.

Charmaz, K. 2006. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis (Introducing Qualitative Methods series)*. V. 1.

Chidukwani, A., Zander, S. & Koutsakis, P. 2022. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*. 10:85701–85719. DOI: 10.1109/ACCESS.2022.3197899.

Chidukwani, A., Zander, S. & Koutsakis, P. 2024. Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Computers & Security*. 145:104026. DOI: 10.1016/j.cose.2024.104026.

Cichonski, P., Millar, T., Grance, T. & Scarfone, K. 2012. *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD. DOI: 10.6028/NIST.SP.800-61r2.

Clark, A. & Mujeye, S. 2025. A Critical Analysis of SME Cybersecurity Policies and Practices. In *Proceedings of the 2025 8th International Conference on Software Engineering and Information Management*. New York, NY, USA: ACM. 178–183. DOI: 10.1145/3725899.3725926.

Cline, T. 2025. *Small business, big target*. Available: https://www.itweb.co.za/article/small-business-big-target/8OKdWMDXb89MbznQ [2025, September 12].

Cohen, J. 2013. *Statistical Power Analysis for the Behavioral Sciences*. DOI: 10.4324/9780203771587.

Colabianchi, S., Costantino, F., Nonino, F. & Palombi, G. 2025. Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation & Knowledge*. 10(3):100695. DOI: 10.1016/j.jik.2025.100695.

Collier, H., Morton, C., Alharthi, D. & Kleiner, J. 2023. Cultural Influences on Information Security. *European Conference on Cyber Warfare and Security*. 22(1):143–150. DOI: 10.34190/eccws.22.1.1127.

Collins, K.M.T., Onwuegbuzie, A.J. & Jiao, Q.G. 2007. A Mixed Methods Investigation of Mixed Methods Sampling Designs in Social and Health Science Research. *Journal of Mixed Methods Research*. 1(3). DOI: 10.1177/1558689807299526.

Comizio, V.G., Corn, G., Deckelman, W., Hopkins, K., Hughes, M., McCarty, P., Raman, S., Sanger, K., et al. 2023. Combating Ransomware: One Year On. *Joint PIJIP/TLS Research Paper Series*. (83).

Corbin, J. & Strauss, A. 2012. *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory*. DOI: 10.4135/9781452230153.

Creswell, J.W. & Creswell, J.D. 2018. *Research Design 5th Ed.* 5th ed. SAGE Publications Inc.

Creswell, J.W. & Plano Clark, V.L. 2018. *Designing and Conducting Mixed Methods Research: Third Edition*. V. 12.

Crotty, J. & Daniel, E. 2022. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics*. DOI: 10.1108/ACI-07-2022-0178.

Dannels, S.A. 2018. Research Design. In *The Reviewer's Guide to Quantitative Methods in the Social Sciences*. Second Edition. | New York : Routledge, 2019. | Revised edition of The reviewer's guide to quantitative methods in the social sciences, 2010.: Routledge. 402–416. DOI: 10.4324/9781315755649-30.

Data Protection Act 2018. 2018. Data Protection Act 2018. *Gov*. (4). Available: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [2023, September 20].

Davis, F.D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems*. 13(3). DOI: 10.2307/249008.

Denzin, N.K. 2012. Triangulation 2.0. *Journal of Mixed Methods Research*. 6(2):80–88. DOI: 10.1177/1558689812437186.

DeVellis, R.F. 2017. Scale Development Theory and Applications (Fourth Edition). *SAGE Publication*. 4.

Elder-Vass, D. 2021. Critical realism. In *Routledge International Handbook of Contemporary Social and Political Theory*. London: Routledge. 241–249. DOI: 10.4324/9781003111399-19.

El-Hajj, M. & Mirza, Z.A. 2024. ProtectingSmall and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool. *Electronics*. 13(19):3910. DOI: 10.3390/electronics13193910.

Enaifoghe, A. & Vezi-Magigaba, M.F. 2023. Conceptualizing the role of entrepreneurship and SME in fostering South Africa's local economic development. *International Journal of Research in Business and Social Science (2147- 4478)*. 12(4):96–105. DOI: 10.20525/ijrbs.v12i4.2444.

Etikan, I. 2016. Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*. 5(1). DOI: 10.11648/j.ajtas.20160501.11.

European Union Agency for Cybersecurity [ENISA]. 2022. *ENISA threat landscape 2022*.

Evans, C. & Lewis, J. 2018. *Analysing Semi-Structured Interviews Using Thematic Analysis: Exploring Voluntary Civic Participation Among Adults*. 1 Oliver's Yard, 55 City Road London EC1Y 1SP United Kingdom : SAGE Publications, Ltd. DOI: 10.4135/9781526439284.

Everitt, B.S., Landau, S., Leese, M. & Stahl, D. 2011. *Cluster Analysis*. Wiley. DOI: 10.1002/9780470977811.

Fard Bahreini, A., Cenfetelli, R. & Cavusoglu, H. 2022. The Role of Heuristics in Information Security Decision Making. DOI: 10.24251/HICSS.2022.587.

Fetters, M.D., Curry, L.A. & Creswell, J.W. 2013. Achieving Integration in Mixed Methods Designs—Principles and Practices. *Health Services Research*. 48(6pt2):2134–2156. DOI: 10.1111/1475-6773.12117.

Field, A.P. 2018. *Discovering statistics using IBM SPSS statistics: 5th edition*. V. 4.

Fowler, F.J. 2014. *Survey research methods (5th edition)*.

Gerzso, T. & Riedl, R.B. 2024. The Potential of Mixed Methods for Qualitative Research. In *Doing Good Qualitative Research*. Oxford University PressNew York. 72–84. DOI: 10.1093/oso/9780197633137.003.0007.

Ghafar, Z.N. 2023. Evaluation Research: A Comparative Analysis of Qualitative and Quantitative Research Methods. *Middle East Research Journal of Linguistics and Literature*. 3(02):25–32. DOI: 10.36348/merjll.2023.v03i02.003.

Glaspie, H.W. & Karwowski, W. 2018. Human Factors in Information Security Culture: A Literature Review. 269–280. DOI: 10.1007/978-3-319-60585-2_25.

Grace, H., Banson, K. & Saraf, A. 2023. Mixed-methods research. In *Translational Radiation Oncology*. Elsevier. 531–536. DOI: 10.1016/B978-0-323-88423-5.00029-7.

Grant, C. & Osanloo, A. 2014. Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your "House". *Administrative Issues Journal Education Practice and Research*. 4(2). DOI: 10.5929/2014.4.2.9.

Guest, G., Bunce, A. & Johnson, L. 2006. How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*. 18(1). DOI: 10.1177/1525822X05279903.

van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcătăian, A., Baumgartner, L., et al. 2021. A Shared Cyber Threat Intelligence Solution for SMEs. *Electronics*. 10(23):2913. DOI: 10.3390/electronics10232913.

Hair, J.F., Anderson, R.E., Tatham, R.L. & Black, W.C. 2019. *Multivariate Data Analysis, Multivariate Data Analysis*. V. 87.

Haque, Md.F. & Krishnan, R. 2021. Toward Automated Cyber Defense with Secure Sharing of Structured Cyber Threat Intelligence. *Information Systems Frontiers*. 23(4):883–896. DOI: 10.1007/s10796-020-10103-7.

Harrison, N.J. 2024. Mixed methods research in implementation science. In *Translational Orthopedics*. Elsevier. 455–459. DOI: 10.1016/B978-0-323-85663-8.00065-9.

Herath, T.B.G., Khanna, P. & Ahmed, M. 2022. DOI: 10.3390/jcp2010001.

Hoong, Y., Rezania, D. & Baker, R. 2024. When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands. *Technology in Society*. 78:102650. DOI: 10.1016/j.techsoc.2024.102650.

Ifinedo, P. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*. 31(1):83–95. DOI: 10.1016/j.cose.2011.10.007.

Ika Tamrin, S., Norman, A.A. & Hamid, S. 2021. Intention to share: the relationship between cybersecurity behaviour and sharing specific content in Facebook. *Information Research: an international electronic journal*. 26(1). DOI: 10.47989/irpaper894.

INTERPOL. 2024. *INTERPOL AFRICAN CYBERTHREAT ASSESSMENT REPORT 2024*. Available: https://www.interpol.int/en/content/download/19174/file/African%20Cyberthreat%20Assessment%20Report%202022.pdf [2024, September 01].

ISO 27032. 2012. ISO/IEC FDIS 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity. *International Organization for Standardization*. (50).

Ivankova, N. V., Creswell, J.W. & Stick, S.L. 2006. Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice. *Field Methods*. 18(1):3–20. DOI: 10.1177/1525822X05282260.

Jackson-Gordon, R. & Plano Clark, V.L. 2024. Using a Joint Display for Building Integration in a Sequential Study: Informing Data Collection for a Participatory Second Phase. *Journal of Mixed Methods Research*. 18(2):137–146. DOI: 10.1177/15586898231179848.

Jideani, P., Leenen, L., Alexander, B. & Barnes, J. 2018. Towards an Electronic Retail Cybersecurity Framework. In *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, icABCD 2018*. DOI: 10.1109/ICABCD.2018.8465428.

Johnson, C.S., Badger, M.L., Waltermire, D.A., Snyder, J. & Skorupka, C. 2016. *Guide to Cyber Threat Information Sharing*. Gaithersburg, MD. DOI: 10.6028/NIST.SP.800-150.

Johnston, A.C. & Warkentin, M. 2010. Fear Appeals and Information Security Behaviors: An Empirical Study Fear Appeals and Information Security Behaviors: An Empirical Study1. *Source: MIS Quarterly*. 34(3).

Johnston, A.C., Wech, B. & Jack, E. 2000. Engaging Remote Employees. *Journal of Organizational and End User Computing*. 25(1):1–23. DOI: 10.4018/joeuc.2013010101.

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

Karupiah, P. 2022. Positivism. In *Principles of Social Research Methodology*. Singapore: Springer Nature Singapore. 73–82. DOI: 10.1007/978-981-19-5441-2_6.

Kelly, L.M. & Cordeiro, M. 2020. Three principles of pragmatism for research on organizational processes. *Methodological Innovations*. 13(2). DOI: 10.1177/2059799120937242.

Kent, C., Tanner, M. & Kabanda, S. 2016. How South African SMEs address cyber security: The case of web server logs and intrusion detection. In *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*. IEEE. 100–105. DOI: 10.1109/EmergiTech.2016.7737319.

Kianpour, M., Øverby, H., Kowalski, S.J. & Frantz, C. 2019. Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties. 149–163. DOI: 10.1007/978-3-030-22351-9_10.

Kobis, P. 2021. Human factor aspects in information security management in the traditional IT and cloud computing models. *Operations Research and Decisions*. 31(1). DOI: 10.37190/ord210104.

Koepke, P. 2017. Cybersecurity Information Sharing Incentives and Barriers. *Working Paper*.

Kuo, B.C.H., Roldan-Bau, A. & Lowinger, R. 2015. Psychological Help-Seeking among Latin American Immigrants in Canada: Testing a Culturally-Expanded Model of the Theory of Reasoned Action Using Path Analysis. *International Journal for the Advancement of Counselling*. 37(2). DOI: 10.1007/s10447-015-9236-5.

Lee, Y.S. 2024. Qualitative and mixed methods. In *Translational Orthopedics*. Elsevier. 229–232. DOI: 10.1016/B978-0-323-85663-8.00010-6.

Leszczyna, R. & Wróbel, M.R. 2019. Threat intelligence platform for the energy sector. *Software: Practice and Experience*. 49(8):1225–1254. DOI: 10.1002/spe.2705.

Lewis, R., Louvieris, P., Abbott, P., Clewley, N. & Jones, K. 2014. Cybersecurity Information Sharing: A framework for sustainable information security management in UK SME supply chains. In *European Conference on Information Systems (ECIS)*. Brunel University of London. Available: https://aisel.aisnet.org/ecis2014/proceedings/track14/4/ [2024, August 01].

Malagon-Maldonado, G. 2014. Qualitative Research in Health Design. *HERD: Health Environments Research & Design Journal*. 7(4):120–134. DOI: 10.1177/193758671400700411.

Mcanyana, W., Brindley, C. & Seedat, Y. 2020. *Insight into the cyberthreat landscape in South Africa*.

Medoh, C. & Telukdarie, A. 2022. The Future of Cybersecurity: A System Dynamics Approach. *Procedia Computer Science*. 200:318–326. DOI: 10.1016/j.procs.2022.01.230.

Middleton, L., Hall, H. & Raeside, R. 2019. Applications and applicability of Social Cognitive Theory in information science research. *Journal of Librarianship and Information Science*. 51(4). DOI: 10.1177/0961000618769985.

MISP. 2025. *MISP as supporting platform for sharing information, following ISO/IEC 27010:2015*. Available: https://www.misp-project.org/compliance/ISO-IEC-27010/#:~:text=Is%20MISP%20a%20tool%20suitable,about%20existing%20malware%20or%20threats. [2025, August 17].

Mizrak, F. 2023. Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Pressacademia*. (September, 30). DOI: 10.17261/Pressacademia.2023.1807.

Mmango, N. & Gundu, T. 2023. Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs. In *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*. IEEE. 1–6. DOI: 10.1109/ICECET58911.2023.10389226.

Moeti, M.N., Langa, M.R. & Sigama, K. 2023. Information Security Framework Adoption for South African Small and Medium Enterprise. 218–233. DOI: 10.1007/978-3-031-28472-4_14.

Mohammed, A.-M., Benson, V. & Saridakis, G. 2020. Understanding the Relationship Between Cybercrime and Human Behavior Through Criminological Theories and Social Networking Sites. In *Encyclopedia of Criminal Activities and the Deep Web*. DOI: 10.4018/978-1-5225-9715-5.ch066.

Möller, D.P.F. 2023. Threats and Threat Intelligence. 71–129. DOI: 10.1007/978-3-031-26845-8_2.

Montasari, R., Hosseinian-Far, A. & Hill, R. 2018. Policies, Innovative Self-Adaptive Techniques and Understanding Psychology of Cybersecurity to Counter Adversarial Attacks in Network and Cyber Environments. 71–93. DOI: 10.1007/978-3-319-97181-0_4.

Moore, M.Ph.D. 2022. Your Guide to the NIST Cybersecurity Framework. *Tripwire*.

Mugwagwa, A., Bhero, E. & Chibaya, C. 2024. Cybersecurity strategy: future proof cybersecurity for small to medium enterprises in South Africa. *International Journal of Research in Business and Social Science (2147- 4478)*. 13(4):15–24. DOI: 10.20525/ijrbs.v13i4.3308.

Mwita, K. 2022. Strengths and weaknesses of qualitative research in social science studies. *International Journal of Research in Business and Social Science (2147- 4478)*. 11(6):618–625. DOI: 10.20525/ijrbs.v11i6.1920.

Mzekandaba, S. 2023. *Cyber crime's annual impact on SA estimated at R2.2bn*. Available: https://www.itweb.co.za/article/cyber-crimes-annual-impact-on-sa-estimated-at-r22bn/JN1gPvOAxY3MjL6m [2025, August 17].

Nabavi, R.T. 2012. Bandura's social learning theory & social cognitive learning theory. *Theory of Developmental Psychology*. 1(1).

Neuman, W.L. 2011. *Social Research Methods: Qualitative and Quantitative Approaches*.

Nunnally, J. & Bernstein, I. 1994. Psychometric Theory, 3rd edn, 1994. *McGraw-Hill, New York*. 3.

Nyimbili, F. & Nyimbili, L. 2024. Types of Purposive Sampling Techniques with Their Examples and Application in Qualitative Research Studies. *British Journal of Multidisciplinary and Advanced Studies*. 5(1):90–99. DOI: 10.37745/bjmas.2022.0419.

Paggio, V., Bafoutsou, G. & Sarri, A. 2021. *Cybersecurity for SMEs – Challenges and recommendations*. Athens.

Pala, A. & Zhuang, J. 2019. Information Sharing in Cybersecurity: A Review. *Decision Analysis*. 16(3):172–196. DOI: 10.1287/deca.2018.0387.

Panke, D. 2024. *Research Design & Method Selection: Making Good Choices in the Social Sciences*. DOI: 10.4135/9781529682700.

Parsons, K., Mccormac, A., Butavicius, M. & Ferguson, L. 2010. Human Factors and Information Security : Individual , Culture and Security Environment. *Science And Technology*. (DSTO-TR-2484).

Patton, M.Q. 2015. *Qualitative Research & Evaluation Methods (4th ed.)*. V. 3.

Pawar, S. & Palivela, Dr.H. 2022. LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*. 2(1):100080. DOI: 10.1016/j.jjimei.2022.100080.

Pawar, S., Khandagale, Y., Gopnarayan, A. & Pokharkar, M. 2024. Cyber Threat Intelligence: A Comprehensive Overview and Practical Implementation. *International Journal of Advanced Research in Science, Communication and Technology*. (May, 11):529–534. DOI: 10.48175/IJARSCT-18179.

Pienta, D., Tams, S. & Thatcher, J.B. 2020. Can trust be trusted in cybersecurity? In *Proceedings of the Annual Hawaii International Conference on System Sciences*. V. 2020-January. DOI: 10.24251/hicss.2020.522.

Pieterse, H. 2021. The Cyber Threat Landscape in South Africa: A 10-Year Review The African Journal of Information and Communication (AJIC) 2 Pieterse. *The African Journal of Information and Communication (AJIC)*. 28.

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. & Guerri, D. 2022. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*. 24(2):371–390. DOI: 10.1007/s10111-021-00683-y.

Purohit, S., Calyam, P., Wang, S., Yempalla, R.K. & Varghese, J. 2020. DefenseChain: Consortium Blockchain for Cyber Threat Intelligence Sharing and Defense. In *2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020*. DOI: 10.1109/BRAINS49436.2020.9223313.

Rahman, S. 2016. The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment" Research: A Literature Review. *Journal of Education and Learning*. 6(1):102. DOI: 10.5539/jel.v6n1p102.

Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C. & Katos, V. 2020. Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. *Computers*. 9(1):18. DOI: 10.3390/computers9010018.

Religia, Y., Ekhsan, M., Huda, M. & Fitriyanto, A.D. 2023. TOE Framework for E-Commerce Adoption by MSMEs during The COVID-19 Pandemic: Can Trust Moderate? *Applied Information System and Management (AISM)*. 6(1):47–54. DOI: 10.15408/aism.v6i1.30954.

Renaud, K. & Ophoff, J. 2021. A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*. 1(1):24–46. DOI: 10.1108/OCJ-03-2021-0004.

Riesco, R., Larriva-Novo, X. & Villagra, V.A. 2020. Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of information. *Telecommunication Systems*. 73(2). DOI: 10.1007/s11235-019-00613-4.

Ring, T. 2014. Threat intelligence: why people don't share. *Computer Fraud & Security*. 2014(3):5–9. DOI: 10.1016/S1361-3723(14)70469-5.

Rogers, E.M. 2003. *Diffusion of Innovations, 5th Edition Everett M. Rogers*.

Ryan, G. 2018. Introduction to positivism, interpretivism and critical theory. *Nurse Researcher*. 25(4):14–20. DOI: 10.7748/nr.2018.e1466.

Ryan, R.M. & Deci, E.L. 2000. Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology*. 25(1). DOI: 10.1006/ceps.1999.1020.

Safa, N.S. & Von Solms, R. 2016. An information security knowledge sharing model in organizations. *Computers in Human Behavior*. 57:442–451. DOI: 10.1016/j.chb.2015.12.037.

Salawu, R.O., Obe, A., Shamsuddin, B., Obe, A.-, Bolatitio, S. & Masibo, S. 2023. Theorical and Conceptual Frameworks in Research Conceptual Clarification. *Eur. Chem. Bull*. 2023(12).

Sangari, S., Dallal, E. & Whitman, M. 2022. Modeling Under-Reporting in Cyber Incidents. *Risks*. 10(11):200. DOI: 10.3390/risks10110200.

Sauerwein, C., Sillaber, C., Mussmann, A. & Breu, R. 2017. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. *The 13th International Conference on Wirtschaftsinformatik*.

Saunders, M.N.K., Lewis, P. & Thornhill, A. 2016. *Understanding Research Philosophy and Approaches to Theory Development. Research Methods for Business Students*.

Scauso, M.S. 2020. Interpretivism: Definitions, Trends, and Emerging Paths. In *Oxford Research Encyclopedia of International Studies*. Oxford University Press. DOI: 10.1093/acrefore/9780190846626.013.522.

Schinagl, S. & Paans, R. 2017. Communication Barriers in the Decision-making Process: System Language and System Thinking. DOI: 10.24251/HICSS.2017.738.

Schunk, D.H. & DiBenedetto, M.K. 2023. Learning from a social cognitive theory perspective. In *International Encyclopedia of Education(Fourth Edition)*. Elsevier. 22–35. DOI: 10.1016/B978-0-12-818630-5.14004-7.

Serini, F. 2024. Collective cyber situational awareness in EU. A political project of difficult legal realisation? *Computer Law & Security Review*. 55:106055. DOI: 10.1016/j.clsr.2024.106055.

Sharma, L.R., Bidari, S., Bidari, D., Neupane, S. & Sapkota, R. 2023. Exploring the Mixed Methods Research Design: Types, Purposes, Strengths, Challenges, and Criticisms. *Global Academic Journal of Linguistics and Literature*. 5(1):3–12. DOI: 10.36348/gajll.2023.v05i01.002.

Shojaifar, A. & Fricker, S.A. 2020. SMEs' Confidentiality Concerns for Security Information Sharing. 289–299. DOI: 10.1007/978-3-030-57404-8_22.

Shojaifar, A. & Fricker, S.A. 2023. Design and evaluation of a self-paced cybersecurity tool. *Information & Computer Security*. 31(2):244–262. DOI: 10.1108/ICS-09-2021-0145.

Siponen, M., Adam Mahmood, M. & Pahnila, S. 2014. Employees' adherence to information security policies: An exploratory field study. *Information and Management*. 51(2). DOI: 10.1016/j.im.2013.08.006.

Skopik, F., Settanni, G. & Fiedler, R. 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*. 60. DOI: 10.1016/j.cose.2016.04.003.

Smith, C.S. 2023. Critical Realism. In *Foundations of Interprofessional Health Education*. Cham: Springer Nature Switzerland. 19–23. DOI: 10.1007/978-3-031-33414-6_4.

Smolnik, S., Croasdell, D. & Jennex, M. 2024. Introduction to the Minitrack on Value, Success, and Performance Measurements of Knowledge, Innovation and Entrepreneurial Systems. DOI: 10.24251/HICSS.2023.672.

Solansky, S.T. & Beck, T. 2021. Interorganizational Information Sharing: Collaboration during Cybersecurity Threats. *Public Administration Quarterly*. 45(1):105–122. DOI: 10.37808/paq.45.1.5.

Sonwani, H., Divya, M., Dhawan, A., Mantri, A., G, Deepak. & Kumar, H. 2022. A Comprehensive Study on Threat Intelligence Platform. In *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*. IEEE. 1–5. DOI: 10.1109/IC3IOT53935.2022.9767985.

South African Government. 2020. *Cybercrimes Act 19 of 2020* . Pretoria: South African Government.

Staneiu, R.-M. 2022. Psychological Safety as a catalyst for Knowledge Sharing. *Proceedings of the International Conference on Business Excellence*. 16(1):98–108. DOI: 10.2478/picbe-2022-0010.

Sukumar, A., Mahdiraji, H.A. & Jafari-Sadeghi, V. 2023. Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*. 43(10):2082–2098. DOI: 10.1111/risa.14092.

Swaleh, M. & Wabwoba, F. 2025. IT Philosophy: Philosophical Paradigms in Information Technology Research. *International Journal of Research and Innovation in Applied Science*. X(I):259–268. DOI: 10.51584/IJRIAS.2025.1001021.

Taber, K.S. 2018. The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education*. 48(6):1273–1296. DOI: 10.1007/s11165-016-9602-2.

Taherdoost, H. 2018. A review of technology acceptance and adoption models and theories. In *Procedia Manufacturing*. V. 22. DOI: 10.1016/j.promfg.2018.03.137.

Taşkın, G. & Sandıkkaya, M.T. 2023. Comparison of Security Frameworks for SMEs. In *2023 14th International Conference on Electrical and Electronics Engineering (ELECO)*. IEEE. 1–5. DOI: 10.1109/ELECO60389.2023.10416030.

Tavakol, M. & Dennick, R. 2011. Making sense of Cronbach's alpha. *International Journal of Medical Education*. 2:53–55. DOI: 10.5116/ijme.4dfb.8dfd.

Teddlie, C. & Yu, F. 2007. Mixed Methods Sampling. *Journal of Mixed Methods Research*. 1(1):77–100. DOI: 10.1177/1558689806292430.

Tosh, D., Sengupta, S., Kamhoua, C., Kwiat, K. & Martin, A. 2015. An evolutionary game-theoretic framework for cyber-threat information sharing. In *2015 IEEE International Conference on Communications (ICC)*. IEEE. 7341–7346. DOI: 10.1109/ICC.2015.7249499.

Tounsi, W. 2019. What is Cyber Threat Intelligence and How is it Evolving? In *Cyber-Vigilance and Digital Trust*. Wiley. 1–49. DOI: 10.1002/9781119618393.ch1.

Triplett, W.J. 2022. Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*. 2(3). DOI: 10.3390/jcp2030029.

Venkatesh, Morris, Davis & Davis. 2003. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*. 27(3):425. DOI: 10.2307/30036540.

Wagner, T.D., Mahbub, K., Palomar, E. & Abdallah, A.E. 2019. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*. 87:101589. DOI: 10.1016/j.cose.2019.101589.

Ward, J.H. 1963. Hierarchical Grouping to Optimize an Objective Function. *Journal of the American Statistical Association*. 58(301). DOI: 10.1080/01621459.1963.10500845.

Watney, M. 2024. Exploring South Africa's Cybersecurity Legal Framework regulating Information Confidentiality, Integrity, and Availability. *International Conference on Cyber Warfare and Security*. 19(1):430–437. DOI: 10.34190/iccws.19.1.1999.

Wei, W., Kong, Z. & Zhao, Y. 2017. Overview of cyber threat intelligence. In *2017 7th International Workshop on Computer Science and Engineering, WCSE 2017*. DOI: 10.18178/wcse.2017.06.106.

Williams-Mcbean, C.T. 2019. The value of a qualitative pilot study in a multi-phase mixed methods research. *Qualitative Report*. 24(5). DOI: 10.46743/2160-3715/2019.3833.

World Economic Forum. 2025. *Global Cybersecurity Outlook 2025*.

Xie, W., Yu, X., Zhang, Y. & Wang, H. 2020. An improved shapley value benefit distribution mechanism in cooperative game of cyber threat intelligence sharing. In *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2020*. DOI: 10.1109/INFOCOMWKSHPS50562.2020.9162739.

Yang, A., Kwon, Y.J. & Lee, S.-Y.T. 2020. The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*. 120(9):1777–1794. DOI: 10.1108/IMDS-10-2019-0536.

Zhang, J.Z., Goel, L. & Williamson, S. 2024. Understanding enterprise cybersecurity information sharing: a theoretical model and empirical analysis. *Enterprise Information Systems*. 18(3). DOI: 10.1080/17517575.2024.2310844.

Zhang, X., Guduguntla, V., Emani, K., Kulkarni, G. & Kaparthi, P. 2018. Get Smart on Information-Sharing in Social Networks. In *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE. 1254–1259. DOI: 10.1109/CSCI46756.2018.00242.

Zhao, W. & White, G. 2012. A collaborative information sharing framework for Community Cyber Security. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*. IEEE. 457–462. DOI: 10.1109/THS.2012.6459892.

Zohrabi, M. 2013. Mixed method research: Instruments, validity, reliability and reporting findings. *Theory and Practice in Language Studies*. 3(2). DOI: 10.4304/tpls.3.2.254-262.

APPENDICIES

APPENDIX A: Glossary of key terms

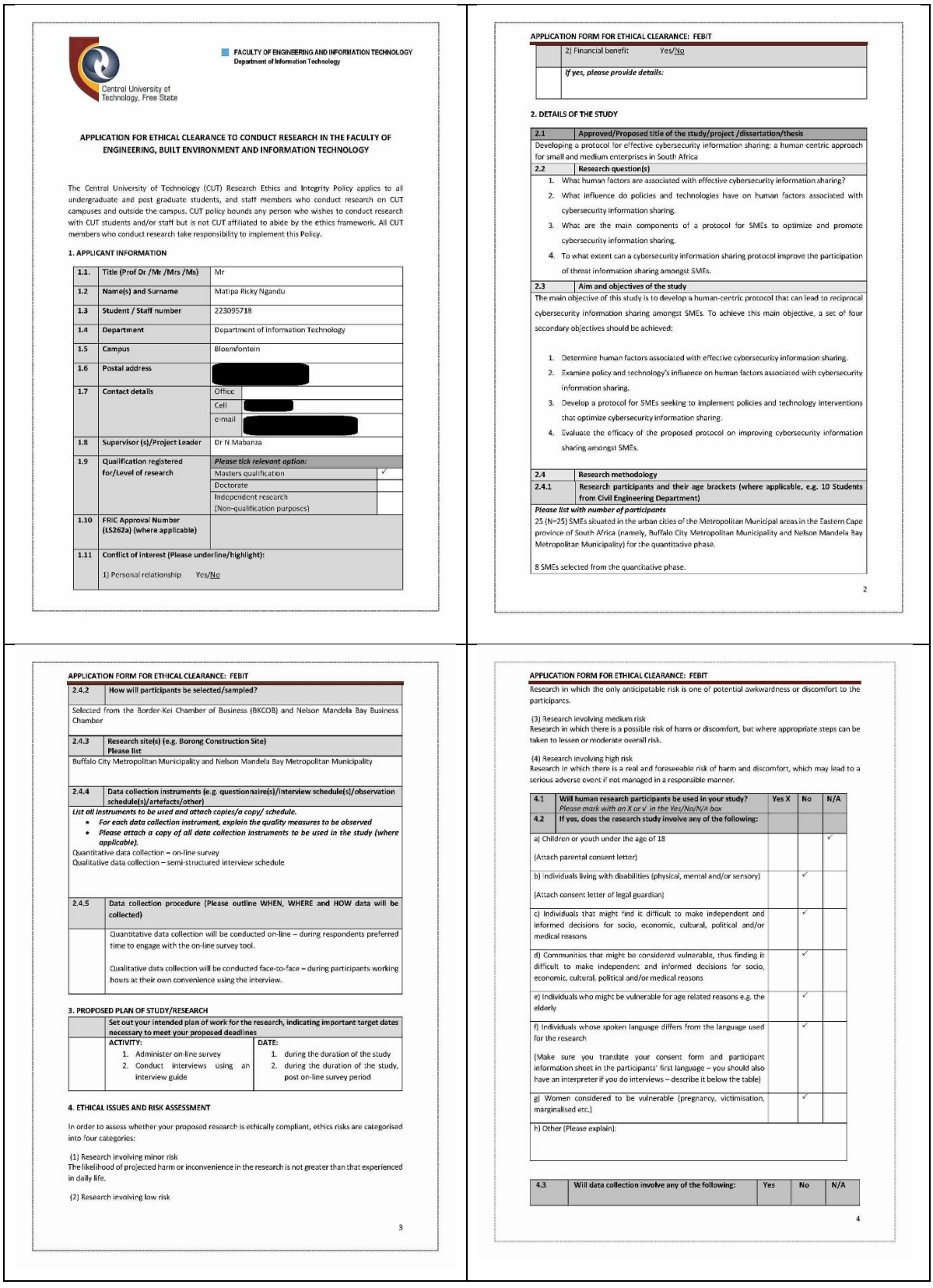
To support conceptual clarity and ensure consistent interpretation throughout this study, the following key terms are defined as they are used within the context of this research.

Key Term	Definition
Business Email Compromise (BEC)	A social engineering attack in which cybercriminals deceive organisations into transferring funds or revealing sensitive information by impersonating trusted individuals such as executives, suppliers, or clients. BEC exploits human trust rather than technical vulnerabilities.
Cyber Resilience	An organisation's ability to prepare for, withstand, respond to, and recover from cyber incidents while maintaining critical operations. For SMEs, resilience depends on technical controls and human-centric practices such as CIS.
Cybercrime-as-a-Service	A criminal business model in which cyber tools, infrastructure, or services are rented or sold to other threat actors, enabling scalable and sophisticated cyberattacks. This trend increases SME exposure due to the lowered barrier to entry for cybercriminals.
Cybersecurity Behaviour	The observable practices and actions individuals or organisations take to protect information assets, including identifying threats, reporting incidents, and sharing cybersecurity information. In this study, cybersecurity behaviour reflects SMEs' operational responses to cyber risks.
Cybersecurity Information Sharing (CIS)	The reciprocal exchange of cyber threat intelligence, including indicators of compromise, vulnerabilities, behavioural patterns, or incident reports, between organisations, sectors, or communities to improve collective defence.
Cyber Threat Information Sharing (CTIS)	Any information that can assist an organisation to identify, assess, monitor, and respond to cyber threats. It forms the core content shared within CIS processes.
Cyber Threat Intelligence (CTI)	Actionable cybersecurity information derived from observed events, cyberattacks, or emerging threats. CTI supports informed decision-making and forms the basis of CIS practices examined in this research.
Cyberthreat Landscape	The environment of threat actors, attack methods, vulnerabilities, technologies, and contextual factors that shape cyber risks in a given region or sector. In South Africa, this includes phishing, ransomware, BEC, mobile malware, and cybercrime-as-a-service.
Human-Centric Approach	An approach that prioritises human behaviour, socio-cultural influences, psychological factors, and organisational practices in

	the design of cybersecurity processes. In this study, human-centricity is essential for understanding SME participation in CIS.
Information Sharing Self-Efficacy	An individual's confidence in their ability to create, report, and share cybersecurity information effectively, derived from SCT.
Intention to Conduct CIS	The degree of willingness and commitment an organisation shows towards engaging in cybersecurity information sharing. This represents the final stage of the SCT-informed behavioural pathway.
Performance Accomplishments	A key SCT construct referring to past successes or failures in identifying threats, producing incident reports, or sharing cybersecurity information. These experiences influence self-efficacy and future behaviour.
Personal Outcome Expectations	Beliefs about the likely consequences of performing a behaviour (Bandura, 1986). In this study, outcome expectations shape whether SMEs view CIS as beneficial, risky, or worthwhile.
Phishing	A social engineering technique where attackers use deceptive emails, SMS messages, or websites to obtain sensitive information such as passwords or financial details.
Protocol (CIS Protocol)	A structured set of guidelines, steps, and enabling mechanisms that support SMEs in participating in CIS. The protocol developed in this study integrates behavioural, socio-cultural, psychological, technological, and regulatory components, with trust as the anchor.
Ransomware	Malicious software that encrypts data or systems and demands payment for their release. Ransomware disproportionately impacts SMEs due to weaker preventive controls.
Regulatory Compliance	The processes through which organisations adhere to legal and policy requirements such as POPIA and the Cybercrimes Act. In the context of this study, compliance influences SMEs' willingness to report incidents and share cybersecurity information.
Situational Awareness	The capacity to perceive, understand, and take action regarding the cybersecurity environment, including awareness of threats, vulnerabilities, and organisational risk posture.
Small and Medium Enterprises (SMEs)	Businesses defined under the South African National Small Enterprise Act according to sector-specific thresholds of turnover, employee numbers, and asset value. SMEs are central economic actors but typically lack advanced cybersecurity capacity.
Social Cognitive Theory (SCT)	A behavioural theory that explains human action as the result of interactions between personal factors, environment, and behaviour. SCT is the theoretical framework underpinning this study.

Social Persuasion	An SCT construct describing external influences such as organisational norms, peer expectations, or policy pressures that encourage or discourage behaviour, including CIS participation.
Subjective Norms	Perceived expectations from peers, industry groups, or regulatory bodies that influence an organisation's decision to share cybersecurity information.
Threat Intelligence	Actionable information describing threats, including indicators of compromise, adversary tactics, vulnerabilities, or contextual details that support detection and response.
Trust (in CIS Contexts):	Confidence that shared information will be handled securely, ethically, and without causing harm to the organisation. Trust encompasses faith in technology, people, processes, and networks and is a key determinant of SME CIS participation.

APPENDIX B: Ethical clearance certificate



Central University of Technology, Free State

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY
Department of Information Technology

APPLICATION FOR ETHICAL CLEARANCE TO CONDUCT RESEARCH IN THE FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

The Central University of Technology (CUT) Research Ethics and Integrity Policy applies to all undergraduate and post graduate students, and staff members who conduct research on CUT campuses and outside the campus. CUT policy bounds any person who wishes to conduct research with CUT students and/or staff but is not CUT affiliated to abide by the ethics framework. All CUT members who conduct research take responsibility to implement this Policy.

1. APPLICANT INFORMATION

1.1.	Title (Prof Dr /Mr /Mrs /Ms)	Mr	
1.2	Name(s) and Surname	Matipa Ricky Ngandu	
1.3	Student / Staff number	223095718	
1.4	Department	Department of Information Technology	
1.5	Campus	Bloemfontein	
1.6	Postal address	[redacted]	
1.7	Contact details	Office	
		Cell [redacted]	
		e-mail [redacted]	
1.8	Supervisor (s)/Project Leader	Dr N Mabanza	
1.9	Qualification registered for/Level of research	*Please tick relevant option:*	
		Masters qualification	✓
		Doctorate	
		Independent research (Non-qualification purposes)	
1.10	FRIC Approval Number (LS262a) (where applicable)		
1.11	Conflict of interest (Please underline/highlight): 1) Personal relationship Yes/No		

APPLICATION FORM FOR ETHICAL CLEARANCE: FEBIT

2) Financial benefit	Yes/No
If yes, please provide details:	

2. DETAILS OF THE STUDY

2.1	**Approved/Proposed title of the study/project /dissertation/thesis**
Developing a protocol for effective cybersecurity information sharing: a human-centric approach for small and medium enterprises in South Africa	
2.2	**Research question(s)**
1. What human factors are associated with effective cybersecurity information sharing? 2. What influence do policies and technologies have on human factors associated with cybersecurity information sharing. 3. What are the main components of a protocol for SMEs to optimize and promote cybersecurity information sharing. 4. To what extent can a cybersecurity information sharing protocol improve the participation of threat information sharing amongst SMEs.	
2.3	**Aim and objectives of the study**
The main objective of this study is to develop a human-centric protocol that can lead to reciprocal cybersecurity information sharing amongst SMEs. To achieve this main objective, a set of four secondary objectives should be achieved: 1. Determine human factors associated with effective cybersecurity information sharing. 2. Examine policy and technology's influence on human factors associated with cybersecurity information sharing. 3. Develop a protocol for SMEs seeking to implement policies and technology interventions that optimize cybersecurity information sharing. 4. Evaluate the efficacy of the proposed protocol on improving cybersecurity information sharing amongst SMEs.	
2.4	**Research methodology**
2.4.1	**Research participants and their age brackets (where applicable, e.g. 10 Students from Civil Engineering Department)**
Please list with number of participants 25 (N=25) SMEs situated in the urban cities of the Metropolitan Municipal areas in the Eastern Cape province of South Africa (namely, Buffalo City Metropolitan Municipality and Nelson Mandela Bay Metropolitan Municipality) for the quantitative phase. 8 SMEs selected from the quantitative phase.	

2

APPLICATION FORM FOR ETHICAL CLEARANCE: FEBIT

2.4.2	**How will participants be selected/sampled?**
Selected from the Border-Kei Chamber of Business (BKCOB) and Nelson Mandela Bay Business Chamber	
2.4.3	**Research site(s) (e.g. Borong Construction Site) Please list**
Buffalo City Metropolitan Municipality and Nelson Mandela Bay Metropolitan Municipality	
2.4.4	**Data collection instruments (e.g. questionnaire(s)/interview schedule(s)/observation schedule(s)/artefacts/other)**
List all instruments to be used and attach copies/a copy/ schedule. • ***For each data collection instrument, explain the quality measures to be observed*** • ***Please attach a copy of all data collection instruments to be used in the study (where applicable).*** Quantitative data collection – on-line survey Qualitative data collection – semi-structured interview schedule	
2.4.5	**Data collection procedure (Please outline WHEN, WHERE and HOW data will be collected)**
	Quantitative data collection will be conducted on-line – during respondents preferred time to engage with the on-line survey tool. Qualitative data collection will be conducted face-to-face – during participants working hours at their own convenience using the interview.

3. PROPOSED PLAN OF STUDY/RESEARCH

	Set out your intended plan of work for the research, indicating important target dates necessary to meet your proposed deadlines	
	ACTIVITY:	**DATE:**
	1. Administer on-line survey 2. Conduct interviews using an interview guide	1. during the duration of the study 2. during the duration of the study, post on-line survey period

4. ETHICAL ISSUES AND RISK ASSESSMENT

In order to assess whether your proposed research is ethically compliant, ethics risks are categorised into four categories:

(1) Research involving minor risk
The likelihood of projected harm or inconvenience in the research is not greater than that experienced in daily life.

(2) Research involving low risk

3

APPLICATION FORM FOR ETHICAL CLEARANCE: FEBIT

Research in which the only anticipatable risk is one of potential awkwardness or discomfort to the participants.

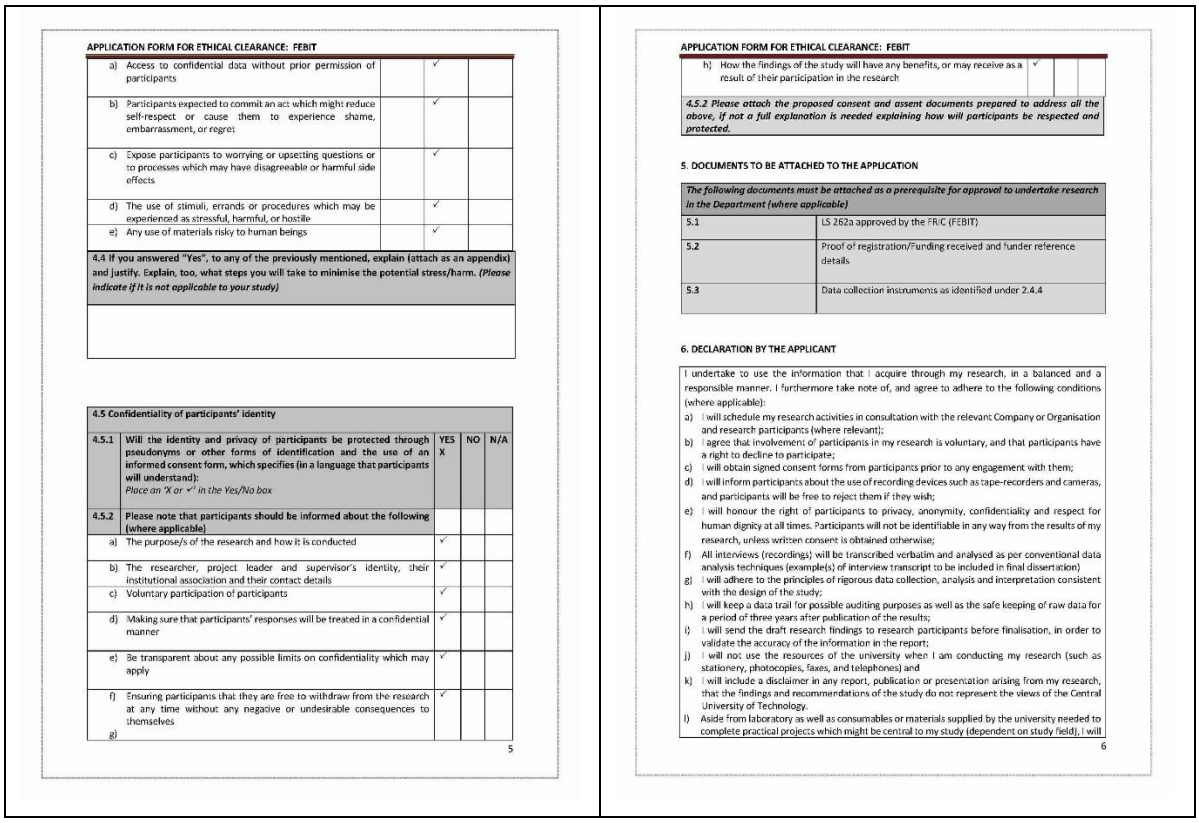
(3) Research involving medium risk
Research in which there is a possible risk of harm or discomfort, but where appropriate steps can be taken to lessen or moderate overall risk.

(4) Research involving high risk
Research in which there is a real and foreseeable risk of harm and discomfort, which may lead to a serious adverse event if not managed in a responsible manner.

		Yes X	No	N/A
4.1	**Will human research participants be used in your study?** *Please mark with an X or √ in the Yes/No/N/A box*			
4.2	**If yes, does the research study involve any of the following:**			
a) Children or youth under the age of 18 (Attach parental consent letter)				✓
b) Individuals living with disabilities (physical, mental and/or sensory) (Attach consent letter of legal guardian)			✓	
c) Individuals that might find it difficult to make independent and informed decisions for socio, economic, cultural, political and/or medical reasons			✓	
d) Communities that might be considered vulnerable, thus finding it difficult to make independent and informed decisions for socio, economic, cultural, political and/or medical reasons			✓	
e) Individuals who might be vulnerable for age related reasons e.g. the elderly			✓	
f) Individuals whose spoken language differs from the language used for the research (Make sure you translate your consent form and participant information sheet in the participants' first language – you should also have an interpreter if you do interviews – describe it below the table)			✓	
g) Women considered to be vulnerable (pregnancy, victimisation, marginalised etc.)			✓	
h) Other (Please explain):				

		Yes	No	N/A
4.3	**Will data collection involve any of the following:**			

4



APPLICATION FORM FOR ETHICAL CLEARANCE: FEBIT

a) Access to confidential data without prior permission of participants		✓	
b) Participants expected to commit an act which might reduce self-respect or cause them to experience shame, embarrassment, or regret		✓	
c) Expose participants to worrying or upsetting questions or to processes which may have disagreeable or harmful side effects		✓	
d) The use of stimuli, errands or procedures which may be experienced as stressful, harmful, or hostile		✓	
e) Any use of materials risky to human beings		✓	

4.4 If you answered "Yes", to any of the previously mentioned, explain (attach as an appendix) and justify. Explain, too, what steps you will take to minimise the potential stress/harm. ***(Please indicate if it is not applicable to your study)***

4.5 Confidentiality of participants' identity				
4.5.1	**Will the identity and privacy of participants be protected through pseudonyms or other forms of identification and the use of an informed consent form, which specifies (in a language that participants will understand):** *Place an 'X or ✓' in the Yes/No box*	**YES X**	**NO**	**N/A**
4.5.2	**Please note that participants should be informed about the following (where applicable)**			
a)	The purpose/s of the research and how it is conducted	✓		
b)	The researcher, project leader and supervisor's identity, their institutional association and their contact details	✓		
c)	Voluntary participation of participants	✓		
d)	Making sure that participants' responses will be treated in a confidential manner	✓		
e)	Be transparent about any possible limits on confidentiality which may apply	✓		
f)	Ensuring participants that they are free to withdraw from the research at any time without any negative or undesirable consequences to themselves	✓		
g)				

5

APPLICATION FORM FOR ETHICAL CLEARANCE: FEBIT

h) How the findings of the study will have any benefits, or may receive as a result of their participation in the research	✓		

4.5.2 Please attach the proposed consent and assent documents prepared to address all the above, if not a full explanation is needed explaining how will participants be respected and protected.

5. DOCUMENTS TO BE ATTACHED TO THE APPLICATION

The following documents must be attached as a prerequisite for approval to undertake research in the Department (where applicable)	
5.1	LS 262a approved by the FRIC (FEBIT)
5.2	Proof of registration/Funding received and funder reference details
5.3	Data collection instruments as identified under 2.4.4

6. DECLARATION BY THE APPLICANT

I undertake to use the information that I acquire through my research, in a balanced and a responsible manner. I furthermore take note of, and agree to adhere to the following conditions (where applicable):

a) I will schedule my research activities in consultation with the relevant Company or Organisation and research participants (where relevant);
b) I agree that involvement of participants in my research is voluntary, and that participants have a right to decline to participate;
c) I will obtain signed consent forms from participants prior to any engagement with them;
d) I will inform participants about the use of recording devices such as tape-recorders and cameras, and participants will be free to reject them if they wish;
e) I will honour the right of participants to privacy, anonymity, confidentiality and respect for human dignity at all times. Participants will not be identifiable in any way from the results of my research, unless written consent is obtained otherwise;
f) All interviews (recordings) will be transcribed verbatim and analysed as per conventional data analysis techniques (example(s) of interview transcript to be included in final dissertation)
g) I will adhere to the principles of rigorous data collection, analysis and interpretation consistent with the design of the study;
h) I will keep a data trail for possible auditing purposes as well as the safe keeping of raw data for a period of three years after publication of the results;
i) I will send the draft research findings to research participants before finalisation, in order to validate the accuracy of the information in the report;
j) I will not use the resources of the university when I am conducting my research (such as stationery, photocopies, faxes, and telephones) and
k) I will include a disclaimer in any report, publication or presentation arising from my research, that the findings and recommendations of the study do not represent the views of the Central University of Technology.
l) Aside from laboratory as well as consumables or materials supplied by the university needed to complete practical projects which might be central to my study (dependent on study field), I will

6

APPENDIX C: Consent form

Central University of Technology, Free State

Department of Information Technology

Faculty of Engineering, Built Environment and Information Technology

www.cut.ac.za

Research study information and consent form

Date: 20 MAY 2024

Title of the research project: Developing a protocol for effective cybersecurity information sharing: a human-centric approach for small and medium enterprises in South Africa

Student name and surname: Matipa Ricky Ngandu
Student number: 223095718
Student contact number: 078 321 8380

Supervisor(s): Dr N Mabanza
Co-supervisor(s): Dr G Mwansa

Introduction to the study

The purpose of this research study is to develop a human-centric protocol that can enhance cyber resilience through increased Cybersecurity Information Sharing (CIS) participation among Small and Medium Enterprises (SMEs). SMEs play a significant role in the economy in terms of employment and production. If SMEs are negatively affected by the rise of cybersecurity attacks it has a direct impact on the country's Gross domestic product (GDP) and employment rates. It is therefore important that SMEs become more cybersecurity resilient so that they ensure that their operational continuity is not compromised by cybersecurity incidents. CIS contributes towards improved cybersecurity resilience by providing participants with a cooperative cyberdefense mechanisms whereby timely actionable cybersecurity information is shared. Unfortunately, there is limited CIS participation amongst SMEs despite 1) efforts made by governments to enforce CIS participation through the enactment of laws; 2) research in this field exists but focuses on large enterprise contexts; 3) existing policies and technologies have not been able to improve the trajectory of CIS participation amongst SMEs. This study proposes a human-centric approach that will work in tandem with technology, policy and

20 Pres. Brand Street, Bloemfontein, South Africa, • **www.cut.ac.za** • Private Bag X20539, Bloemfontein, S.A, 9300

Central University of Technology, Free State

Department of Information Technology

Faculty of Engineering, Built Environment and Information Technology

www.cut.ac.za

Research study information and consent form

procedure thereby address the human behaviour aspect that is currently lacking in research on CIS participation amongst SMEs.

Consent to participate in the research project

I, ..., confirm my participation in this research project and that, the person asking my consent to take part in this research has introduced the study to me and highlighted its purpose.

I have read (or had explained to me) and understood the study as explained in the research study information and consent form. I have had an opportunity to ask questions and am prepared to participate in the study. I understand that my participation is voluntary and that I am free to withdraw at any time without penalty. I am aware that the findings of this study will be processed into a research report, journal publications, and/or conference proceedings. I am fluent in English and understand these documents or I have had the information explained to me in a language I understand well.

Full Name of Participant:

Signature of Participant: Date:

20 Pres. Brand Street, Bloemfontein, South Africa, • **www.cut.ac.za** • Private Bag X20539, Bloemfontein, S.A, 9300

APPENDIX D: Certificate of language editing

CERTIFICATE

OF LANGUAGE EDITING

ERRCDF

Rethinking Education 4 Inclusive Development

The certificate is awarded to

Matipa Ricky Ngandu

This certificate confirms that Matipa Ricky Ngandu's article titled "Developing A Protocol for Effective Cybersecurity Information Sharing: A Human-Centric Approach for Small and Medium Enterprises in South Africa" was edited by a professional English-language editing staff at the ERRCD Forum.

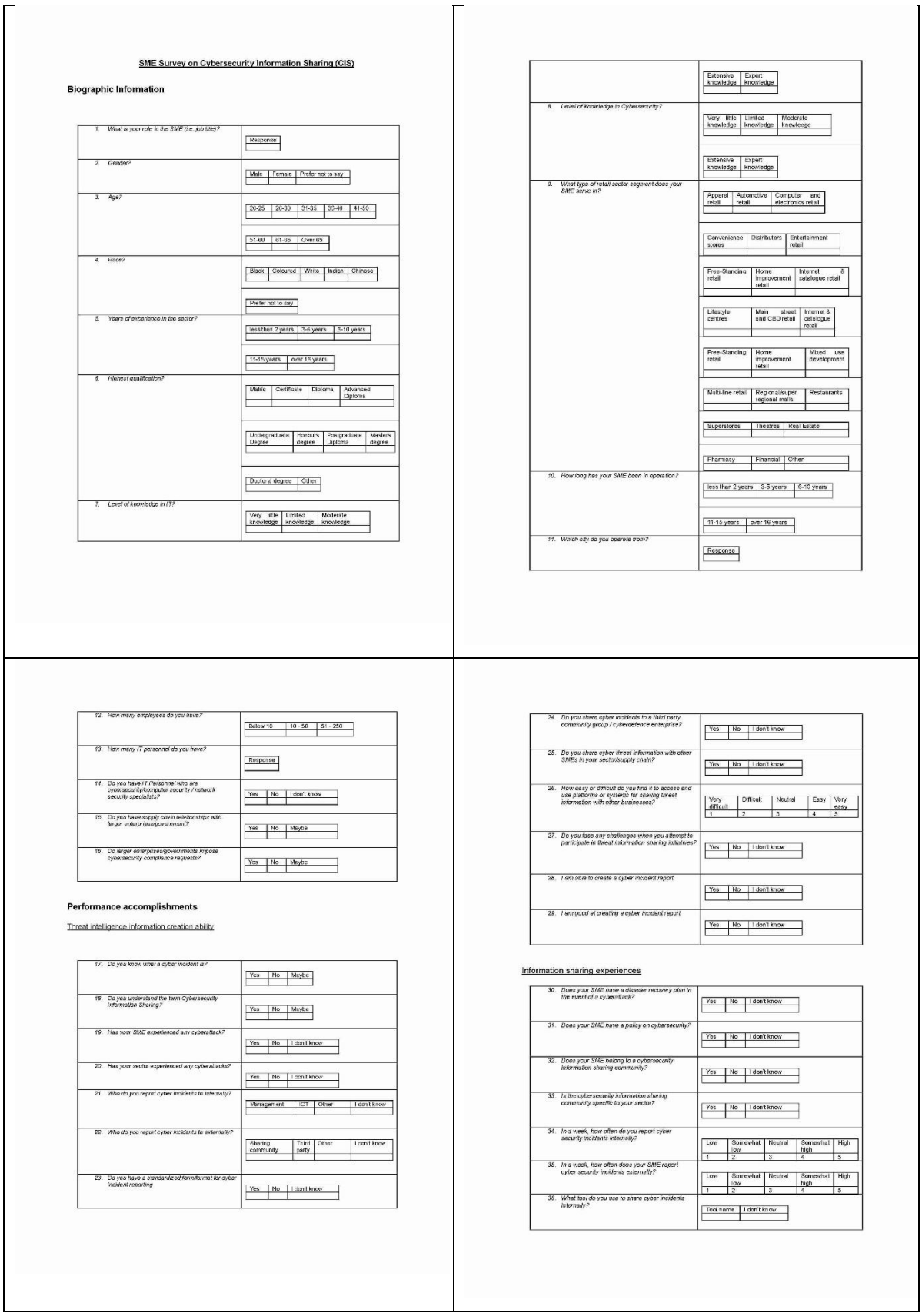
2025 AWARD

ERRCDF

21/09/2025

Bunmi Omodan (PhD)
Chief-Editor
ERRCDF Language Editing Service
LangEditor@errcd.com
www.errcd.com

APPENDIX E: Quantitative data collection instrument (survey)



SME Survey on Cybersecurity Information Sharing (CIS)

Biographic Information

1. What is your role in the SME (i.e. job title)? — Response
2. Gender? — Male | Female | Prefer not to say
3. Age? — 20-25 | 26-30 | 31-35 | 36-40 | 41-50 | 51-60 | 61-65 | Over 65
4. Race? — Black | Coloured | White | Indian | Chinese | Prefer not to say
5. Years of experience in the sector? — less that 2 years | 3-5 years | 6-10 years | 11-15 years | over 15 years
6. Highest qualification? — Matric | Certificate | Diploma | Advanced Diploma | Undergraduate Degree | Honours degree | Postgraduate Diploma | Masters degree | Doctoral degree | Other
7. Level of knowledge in IT? — Very little knowledge | Limited knowledge | Moderate knowledge | Extensive knowledge | Expert knowledge
8. Level of knowledge in Cybersecurity? — Very little knowledge | Limited knowledge | Moderate knowledge | Extensive knowledge | Expert knowledge
9. What type of retail sector segment does your SME serve in? — Apparel retail | Automotive retail | Computer and electronics retail | Convenience stores | Distributors | Entertainment retail | Free-Standing retail | Home improvement retail | Internet & catalogue retail | Lifestyle centres | Main street and CBD retail | Internet & catalogue retail | Free-Standing retail | Home improvement retail | Mixed use development | Multi-line retail | Regional/super regional malls | Restaurants | Superstores | Theatres | Real Estate | Pharmacy | Financial | Other
10. How long has your SME been in operation? — less than 2 years | 3-5 years | 6-10 years | 11-15 years | over 15 years
11. Which city do you operate from? — Response
12. How many employees do you have? — Below 10 | 10 - 50 | 51 - 250
13. How many IT personnel do you have? — Response
14. Do you have IT Personnel who are cybersecurity/computer security / network security specialists? — Yes | No | I don't know
15. Do you have supply chain relationships with larger enterprises/government? — Yes | No | Maybe
16. Do larger enterprises/governments impose cybersecurity compliance requests? — Yes | No | Maybe

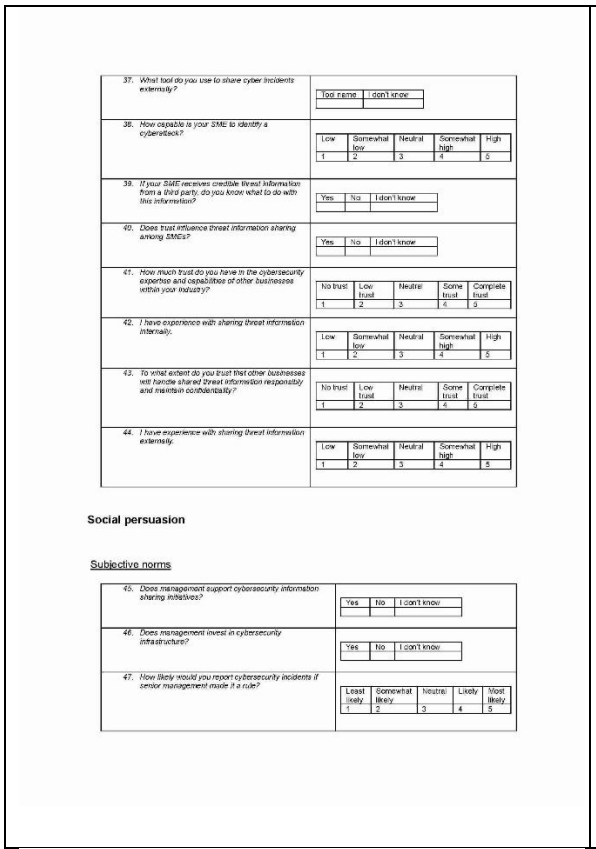
Performance accomplishments

Threat intelligence information creation ability

17. Do you know what a cyber incident is? — Yes | No | Maybe
18. Do you understand the term Cybersecurity Information Sharing? — Yes | No | Maybe
19. Has your SME experienced any cyberattack? — Yes | No | I don't know
20. Has your sector experienced any cyberattacks? — Yes | No | I don't know
21. Who do you report cyber incidents to internally? — Management | ICT | Other | I don't know
22. Who do you report cyber incidents to externally? — Sharing community | Third party | Other | I don't know
23. Do you have a standardized form/format for cyber incident reporting — Yes | No | I don't know
24. Do you share cyber incidents to a third party community group / cyberdefence enterprise? — Yes | No | I don't know
25. Do you share cyber threat information with other SMEs in your sector/supply chain? — Yes | No | I don't know
26. How easy or difficult do you find it to access and use platforms or systems for sharing threat information with other businesses? — Very difficult 1 | Difficult 2 | Neutral 3 | Easy 4 | Very easy 5
27. Do you face any challenges when you attempt to participate in threat information sharing initiatives? — Yes | No | I don't know
28. I am able to create a cyber incident report — Yes | No | I don't know
29. I am good at creating a cyber incident report — Yes | No | I don't know

Information sharing experiences

30. Does your SME have a disaster recovery plan in the event of a cyberattack? — Yes | No | I don't know
31. Does your SME have a policy on cybersecurity? — Yes | No | I don't know
32. Does your SME belong to a cybersecurity information sharing community? — Yes | No | I don't know
33. Is the cybersecurity information sharing community specific to your sector? — Yes | No | I don't know
34. In a week, how often do you report cyber security incidents internally? — Low 1 | Somewhat low 2 | Neutral 3 | Somewhat high 4 | High 5
35. In a week, how often does your SME report cyber security incidents externally? — Low 1 | Somewhat low 2 | Neutral 3 | Somewhat high 4 | High 5
36. What tool do you use to share cyber incidents internally? — Tool name | I don't know



37. What tool do you use to share cyber incidents externally?	Tool name | I don't know
38. How capable is your SME to identify a cyberattack?	Low | Somewhat low | Neutral | Somewhat high | High 1 | 2 | 3 | 4 | 5
39. If your SME receives credible threat information from a third party, do you know what to do with this information?	Yes | No | I don't know
40. Does trust influence threat information sharing among SMEs?	Yes | No | I don't know
41. How much trust do you have in the cybersecurity expertise and capabilities of other businesses within your industry?	No trust | Low trust | Neutral | Some trust | Complete trust 1 | 2 | 3 | 4 | 5
42. I have experience with sharing threat information internally.	Low | Somewhat low | Neutral | Somewhat high | High 1 | 2 | 3 | 4 | 5
43. To what extent do you trust that other businesses will handle shared threat information responsibly and maintain confidentiality?	No trust | Low trust | Neutral | Some trust | Complete trust 1 | 2 | 3 | 4 | 5
44. I have experience with sharing threat information externally.	Low | Somewhat low | Neutral | Somewhat high | High 1 | 2 | 3 | 4 | 5

Social persuasion

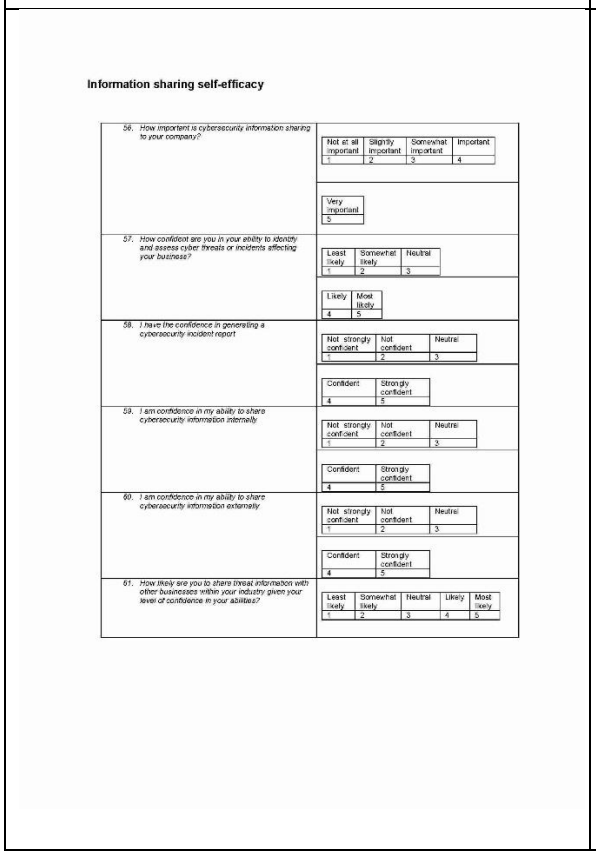
Subjective norms

45. Does management support cybersecurity information sharing initiatives?	Yes | No | I don't know
46. Does management invest in cybersecurity infrastructure?	Yes | No | I don't know
47. How likely would you report cybersecurity incidents if senior management made it a rule?	Least likely | Somewhat likely | Neutral | Likely | Most likely 1 | 2 | 3 | 4 | 5

48. How likely would you share threat information with other SMEs if you were made aware that your sector competitors are pro-actively sharing threat information in a threat sharing community?	Least likely | Somewhat likely | Neutral | Likely | Most likely 1 | 2 | 3 | 4 | 5
49. My peers expect me to share threat information	Least likely | Somewhat likely | Neutral | Likely | Most likely 1 | 2 | 3 | 4 | 5
50. My superiors expect me to share threat information	Least likely | Somewhat likely | Neutral | Likely | Most likely 1 | 2 | 3 | 4 | 5
51. My organization complies with laws governing threat information sharing	Yes | No | I don't know

Feedback

52. Does management provide a status report on cyber incidents that affect the SME?	Yes | No | I don't know
53. Does management provide incentives/rewards (verbal, physical or material) for sharing of threat information?	Yes | No | I don't know
54. I receive feedback (criticism and/or advice) about incident reports I have shared internally	Yes | No | I don't know
55. My company receives feedback (criticism and/or advice) about incident reports shared within the community	Yes | No | I don't know



Information sharing self-efficacy

56. How important is cybersecurity information sharing to your company?	Not at all important | Slightly important | Somewhat important | Important 1 | 2 | 3 | 4 Very important 5
57. How confident are you in your ability to identify and assess cyber threats or incidents affecting your business?	Least likely | Somewhat likely | Neutral 1 | 2 | 3 Likely | Most likely 4 | 5
58. I have the confidence in generating a cybersecurity incident report	Not strongly confident | Not confident | Neutral 1 | 2 | 3 Confident | Strongly confident 4 | 5
59. I am confidence in my ability to share cybersecurity information internally	Not strongly confident | Not confident | Neutral 1 | 2 | 3 Confident | Strongly confident 4 | 5
60. I am confidence in my ability to share cybersecurity information externally	Not strongly confident | Not confident | Neutral 1 | 2 | 3 Confident | Strongly confident 4 | 5
61. How likely are you to share threat information with other businesses within your industry given your level of confidence in your abilities?	Least likely | Somewhat likely | Neutral | Likely | Most likely 1 | 2 | 3 | 4 | 5

Personal outcome expectations

62. How strongly do you believe that sharing threat information within your business will improve your organization's cybersecurity resilience?	Not strongly believe | Not believe | Neutral 1 | 2 | 3 Believe | Strongly believe 4 | 5
63. I am confident that the information I share makes a positive contribution towards improving the state of cyber resilience in my company	Not strongly confident | Not confident | Neutral 1 | 2 | 3 Confident | Strongly confident 4 | 5
64. I am confident that the threat information my company shares with SMEs in a sharing community contributes towards improved cyber resilience	Not strongly confident | Not confident | Neutral 1 | 2 | 3 Confident | Strongly confident 4 | 5
65. How strongly do you believe that sharing threat information with other businesses will improve your organization's cybersecurity resilience?	Not strongly believe | Not believe | Neutral 1 | 2 | 3 Believe | Strongly believe 4 | 5
66. If I share threat information internally I will be given recognition from others	Least likely | Somewhat likely | Neutral | Likely | Most likely 1 | 2 | 3 | 4 | 5
67. If my company shares threat information externally within threat sharing communities we will receive a positive image/praise/recognition	Least likely | Somewhat likely | Neutral | Likely | Most likely 1 | 2 | 3 | 4 | 5
68. How confident are you that sharing threat information will lead to positive outcomes for your business?	Not strongly confident | Not confident | Neutral 1 | 2 | 3 Confident | Strongly confident 4 | 5

Cybersecurity behaviour

69. Does your company comply with laws governing cybersecurity information sharing?	Yes / No / I don't know
70. I have read the company cybersecurity related policy	Yes / No
71. I pay attention to incidents that might bring about cybersecurity issues	Never / Rarely / Sometimes / Often / Always (1 2 3 4 5)
72. I apply cybersecurity best practice	Never / Rarely / Sometimes / Often / Always (1 2 3 4 5)
73. To what extent do you observe other businesses within your industry sharing threat information with their peers?	Never / Rarely / Sometimes / Often / Always (1 2 3 4 5)
74. I am concerned about the security of key cyber and digital assets of the company	Not at all concerned / Slightly concerned / Somewhat concerned / Moderately concerned / Extremely concerned (1 2 3 4 5)
75. In the past I have on occasion conducted myself in a cyber unsafe way (i.e. browsed non-work related site on work network; shared passwords; ignored phishing emails without reporting them; shared sensitive company information without authorization)	Yes / No / I don't know
76. How much influence do these observations have on your own willingness to engage in threat information sharing?	Low / Somewhat low / Neutral / Somewhat high / High (1 2 3 4 5)
77. I share threat information in reasonable amount of time	Never / Rarely / Sometimes / Often / Always (1 2 3 4 5)

Intention to conduct Cybersecurity Information Sharing

78. I intend to share threat information internally	Never / Rarely / Sometimes / Often / Always (1 2 3 4 5)
79. My company intends to share threat information externally in a sharing community	Never / Rarely / Sometimes / Often / Always (1 2 3 4 5)
80. I will recommend other employees to share threat information	Never / Rarely / Sometimes / Often / Always (1 2 3 4 5)
81. My company will proactively and reciprocally promote the sharing of threat information within our sector segment	Never / Rarely / Sometimes / Often / Always (1 2 3 4 5)
82. Are there any improvements or changes you think are needed to see threat information sharing actioned?	Yes / No / May be

THANK YOU

--- End of questionnaire ---

APPENDIX F: Qualitative data collection instrument (interview)

SME Interview Guide on Cybersecurity Information Sharing (CIS)

Performance accomplishments

Threat intelligence information creation ability

1. Describe a cyber threat incident that has affected your company?
2. How do you identify a cyber threat incident?
3. How do you create an incident report?
4. How do you or your company stay informed about cybersecurity threats and trends that may affect your business?

Information sharing experiences

5. What do you consider to be the main barriers to sharing threat information with other businesses in your industry?
6. Describe any challenges you have encountered when attempting to participate in threat information sharing initiatives?
7. Why does your organization engage in threat information sharing with other businesses?
8. Describe any specific benefits or advantages that your organization has experienced as a result of sharing threat information?
9. What lessons have you learned from past experiences with threat information sharing, both positive and negative?

Social persuasion

Subjective norms

10. How do you assess the trustworthiness and credibility of other businesses within your industry when it comes to sharing threat information?
11. What factors influence your decision to trust or distrust other businesses with sensitive cybersecurity information?
12. How does management demonstrate their support for threat information sharing participation?

Feedback

13. How do you know that incident reports are shared internally or externally?
14. How do you know whether management values threat information sharing participation?
15. How can businesses motivate increased participation in threat information sharing?

Information sharing self-efficacy

16. Why is it important to participate in cybersecurity information sharing?
17. How confident are you in your ability to identify and assess cyber threats or incidents affecting your business?
18. How satisfied are you with the usability and effectiveness of existing platforms for threat information sharing?
19. Why will you share threat information with other businesses within your industry given your level of confidence in your abilities?

Personal outcome expectations

20. Can you identify any organizational factors that either facilitate or hinder the sharing of threat information among your peers?
21. How would you describe the culture within your company regarding cybersecurity and threat information sharing?
22. What improvements or changes would you like to see in the way threat information is shared among businesses in your industry?

Cybersecurity behaviour

23. How well does your company comply with laws governing cybersecurity information sharing?
24. Do you feel there is some improvement needed in your company on cybersecurity?
25. How do businesses in your industry show that they value the need for cybersecurity?

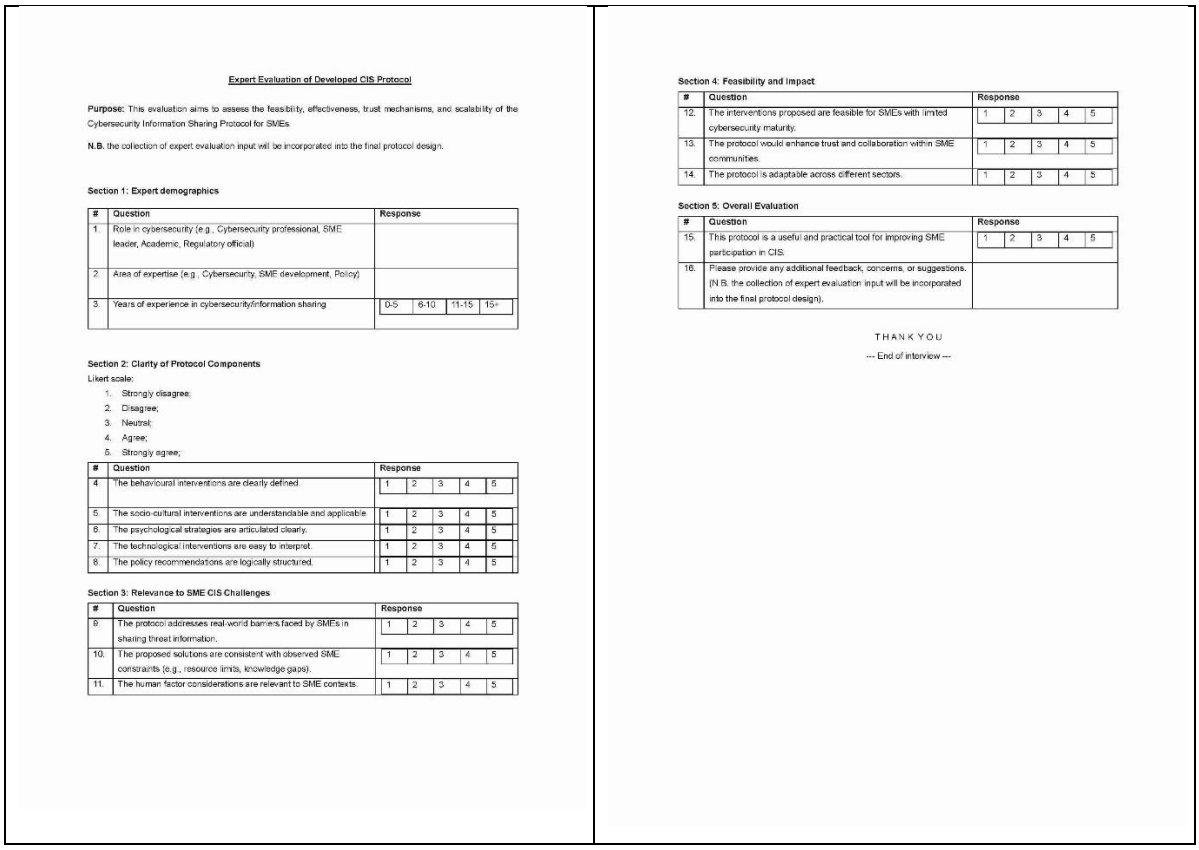
Intention to conduct Cybersecurity Information Sharing

26. How will you contribute towards improving the cyber posture of your company through threat information sharing?
27. Are there any improvements or changes you think are needed to see threat information sharing actioned?

THANK YOU

--- End of interview ---

APPENDIX G: Expert evaluation data collection instrument



Expert Evaluation of Developed CIS Protocol

Purpose: This evaluation aims to assess the feasibility, effectiveness, trust mechanisms, and scalability of the Cybersecurity Information Sharing Protocol for SMEs.

N.B. the collection of expert evaluation input will be incorporated into the final protocol design.

Section 1: Expert demographics

#	Question	Response
1.	Role in cybersecurity (e.g., Cybersecurity professional, SME leader, Academic, Regulatory official)	
2.	Area of expertise (e.g., Cybersecurity, SME development, Policy)	
3.	Years of experience in cybersecurity/information sharing	0-5 | 6-10 | 11-15 | 15+

Section 2: Clarity of Protocol Components

Likert scale:

1. Strongly disagree;
2. Disagree;
3. Neutral;
4. Agree;
5. Strongly agree;

#	Question	Response
4.	The behavioural interventions are clearly defined.	1 | 2 | 3 | 4 | 5
5.	The socio-cultural interventions are understandable and applicable	1 | 2 | 3 | 4 | 5
6.	The psychological strategies are articulated clearly.	1 | 2 | 3 | 4 | 5
7.	The technological interventions are easy to interpret.	1 | 2 | 3 | 4 | 5
8.	The policy recommendations are logically structured.	1 | 2 | 3 | 4 | 5

Section 3: Relevance to SME CIS Challenges

#	Question	Response
9.	The protocol addresses real-world barriers faced by SMEs in sharing threat information.	1 | 2 | 3 | 4 | 5
10.	The proposed solutions are consistent with observed SME constraints (e.g., resource limits, knowledge gaps).	1 | 2 | 3 | 4 | 5
11.	The human factor considerations are relevant to SME contexts.	1 | 2 | 3 | 4 | 5

Section 4: Feasibility and Impact

#	Question	Response
12.	The interventions proposed are feasible for SMEs with limited cybersecurity maturity.	1 | 2 | 3 | 4 | 5
13.	The protocol would enhance trust and collaboration within SME communities.	1 | 2 | 3 | 4 | 5
14.	The protocol is adaptable across different sectors.	1 | 2 | 3 | 4 | 5

Section 5: Overall Evaluation

#	Question	Response
15.	This protocol is a useful and practical tool for improving SME participation in CIS.	1 | 2 | 3 | 4 | 5
16.	Please provide any additional feedback, concerns, or suggestions. (N.B. the collection of expert evaluation input will be incorporated into the final protocol design).	

THANK YOU

--- End of interview ---