AFRICA UNIVERSITY

(A United Methodist-Related Institution)

ASSESSMENT OF CYBERSECURITY AWARENESS, THREAT EXPOSURE, AND ADOPTION FACTORS AMONG SMALL AND MEDIUM-SIZED ENTERPRISES IN JINJA CITY, UGANDA.

BY

IRMIYA SAMSON

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF EXECUTIVE MASTER IN BUSINESS ADMINISTRATION IN THE COLLEGE OF BUSINESS AND MANAGEMENT SCIENCES.

2026

Abstract

This study assessed cybersecurity preparedness among small and medium-sized enterprises (SMEs) in Jinja City, Uganda, with four specific objectives: (1) to determine the current level of cybersecurity preparedness, (2) to evaluate the gap between perceived employee awareness and actual security practices, (3) to examine the influence of technological, organizational, and environmental factors on cybersecurity adoption, and (4) to identify key predictors of digital resilience. A mixed-methods approach was employed, guided by the Technology–Organization–Environment (TOE) framework. Quantitative data were collected through structured questionnaires from 124 SME respondents, while qualitative insights were obtained through focus group discussions with 13 employees and semi-structured interviews with five (5) key informants. Descriptive statistics and regression analysis were used for quantitative data, complemented by thematic analysis of qualitative data. The findings indicate that cybersecurity preparedness among SMEs in Jinja City is generally low and inconsistent. Although 74.1% of respondents expressed confidence in identifying cyber threats, qualitative evidence revealed that this confidence is largely reactive rather than supported by structured security practices. Cyber threats are prevalent, with 68.6% of SMEs experiencing phishing attempts and 63.7% reporting financial losses due to cyber incidents. Organizational constraints are significant: 39.5% of SMEs lack dedicated IT support, and 74.2% report insufficient internal expertise to manage cybersecurity systems. While 75.0% of managers indicate commitment to cybersecurity, adoption is primarily driven by external pressures particularly competitor incidents (83.1%) rather than proactive strategic planning. Regression results confirm that organizational and technological factors are the most significant predictors of cybersecurity preparedness, while environmental factors exert a secondary influence. Overall, SMEs in Jinja City exhibit a basic and fragile level of cybersecurity readiness. The study concludes that improving SME cybersecurity requires strengthening internal capabilities, promoting proactive management practices, and reducing reliance on reactive, event-driven adoption. It recommends targeted capacity building, adoption of cost-effective security solutions, and context-sensitive regulatory support to enhance digital resilience.

Key Words: Cybersecurity, Digital Resilience, Jinja City, SMEs, Technology – Organization – Environment Framework,

Declaration

I declare that this dissertation is my original work except where sources have been cited and acknowledged. The work has never been submitted, nor will it ever be submitted to another university for the award of a degree.

Irmiya Samson	 10th March 2026
Student's Full Name	Student's Signature (Date)
Dr. Thomas Masese	 27th April 2026
Main Supervisor's Full Name	Main supervisor's Signature (Date)

Copyright

Acknowledgments

Sincere gratitude to the Almighty God for providing the scholar with the knowledge, health, and fortitude necessary to finish this dissertation. The researcher expresses profound appreciation to Dr. Thomas Masese, the project supervisor, for his invaluable advice and mentoring during this investigation. Equally appreciative of the academic support provided by the Africa University faculty and colleagues throughout the researcher's EMBA journey. The SMEs in Jinja City are greatly appreciated by the scholar for their involvement and insights, which were essential to this research.

Dedication

The scholar humbly dedicates this project to Mrs. Rebeccah Samson and the United Methodist Church in Nigeria.

List of Acronyms and Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
EDR	Endpoint Detection and Response
ERP	Enterprise Resource Planning
FGD	Focus Group Discussion
FSD	Financial Sector Deepening
GDP	Gross Domestic Product
ICT	Information and Communication Technology
IT	Information Technology
KJM	Kampala–Jinja–Mukono (Economic Corridor)
MFA	Multi-Factor Authentication
NITA-U	National Information Technology Authority, Uganda
PDPO	Personal Data Protection Office
PET	Privacy-Enhancing Technology
POS	Point of Sale
PwC	PricewaterhouseCoopers
RQ	Research Question
SME	Small and Medium-Sized Enterprise
TAM	Technology Acceptance Model
TOE	Technology-Organization-Environment (Framework)
UBOS	Uganda Bureau of Statistics
UCC	Uganda Communications Commission

UGX	Ugandan Shilling
UIA	Uganda Investment Authority
USD	United States Dollar

Definition of Key Terms

Term	Definition
Cybersecurity Preparedness	An organization's readiness to prevent, detect, and respond to cyber threats.
Cyber threats	Are malicious acts that take advantage of weaknesses in an organization's digital infrastructure or human behaviors, such as ransomware, phishing, and social engineering.
Digital Literacy	The knowledge and abilities needed for SME owners and staff to comprehend, recognize, and report cyber-threats like phishing or social engineering are known as digital literacy.
Human firewall	The human component is the main interface for managing technology risk, particularly the role of employee awareness, training, and cybersecurity literacy.
Small and Medium-Sized Enterprises:	A company that employs 5 people or more, according to the Uganda Investment Authority (UIA) definition
Technology-Organization-Environment (TOE)	A theoretical framework for evaluating the uptake of technology that includes technological context, organizational context, and environmental context

Table of Contents

List of Tables

List of Figures

CHAPTER 1 INTRODUCTION

1.1 Introduction

The digital revolution transforms international industry operations, driving unprecedented changes in growth and efficiency (Gill et al., 2020). However, this phenomenon of digital revolutions is also associated with risks because it has also opened room for cybercrime and vulnerability areas that negatively affect lives and properties. Small and medium-sized enterprises (SMEs) today exhibit, especially in developing economies, a high level of vulnerability and unpreparedness, whereas large multinational corporations have the expertise and available resources to navigate this complex threat landscape (Serianu, 2024). There are developing countries and emerging markets, where the high rate of digital acceptance has overtaken the growth of a necessary cyber awareness culture and security infrastructure. As Uganda undergoes fast economic digitization, robust cybersecurity is now a major national concern (Ministry of ICT & National Guidance, 2023). Furthermore, the digital economy in Uganda is rapidly improving more than ever before, thanks to widespread mobile connectivity and the increasing and growing use of e-services (Uganda Communications, 2025). Many individuals and business owners are more into online payment and mobile money platforms now, which are part of their everyday financial activities (Uganda Communications, 2025). The improved financial inclusion has changed a lot of things, but has also exposed the country to complicated and frequent cyber threats and vulnerabilities (INTERPOL, 2023). Small and medium-sized enterprises are the backbone of the Ugandan economy, but the sector is especially at risk from these threats due to financial constraints and a lack of information or knowledge (Financial Sector Deepening Uganda, 2020). This study assessed the cybersecurity preparedness of small and medium-sized enterprises focused on Jinja City, Uganda, a substantial economic area because of its industrial growth and

economic vibrancy. The researcher used Jinja City as a case study for the research, as it offered a singular small-scale version of the entire country's issues, covering digital security.

1.2 Background to the Study

The fast growth of technology at the global level is transformative, but it also comes with vulnerabilities and opportunities. Cybercrime and vulnerability are created, which leave SMEs vulnerable, especially in the local areas around the globe. There is a rapid digitization in Uganda, driven by mobile connectivity and e-services (Uganda Communications Commission, 2023). Economic digitization is now a hot topic that has made robust cybersecurity measures a top national priority to protect people and machines from falling into cyber threats. The sector of small and medium-sized enterprises in Uganda, which is a strong pillar of the economy, is facing a lot of threats due to insufficient financial resources and awareness. The development of enterprises and the economic growth of Jinja City, Uganda, led the researcher to consider Jinja City a suitable case study to assess the readiness and digital security issues of its small and medium-sized enterprises nationally at the local level. Also, the government leadership in Uganda deliberately and determinedly concentrates on the areas of social development and economic growth, acknowledging its potential to drive economic revolution and create job opportunities for small and medium-sized enterprises because of its importance. (Government of Uganda, 2011; Government of Uganda., 2015) Officially, the Uganda Investment Authority (UIA) categorizes small and medium-sized enterprises (SMEs) based on the total assets and number of staff (Uganda Investment Authority, 2016; Uganda Bureau of Statistics, 2024). In 2019–2020, there were 686,700 registered businesses in Uganda, up from 458,106 ten years prior (Uganda Bureau, 2020). The vast majority (approximately 81.7%) continue to be informal. About 2.7 million Ugandans were employed by businesses in 2019–2020, making up a significant portion of the country's GDP and employment. So these industries stand in

entrepreneurship and are essential in giving people good-paying jobs (Turyahikayo, 2015; Government of Uganda, 2015). High business mortality still impacts Uganda SMEs. According to studies, between 70% and 80% of newly established small businesses fail within the first five years, mostly as a result of inadequate funding, inexperienced managers, and a slow adoption of technology (Turyahikayo, 2015; Uganda Investment Authority, 2016). It is also clear that low technology implementation and limited financial access are two of the major factors causing subpar performance (Financial Sector Deepening Uganda, 2020). The fast growth of mobile connectivity financial services is a notable paradox, even though overall technology implementation is still low, with more than half of small and medium-sized enterprises having no access to a computer or cell phone (smartphone) for business purposes (Financial Sector Deepening Uganda, 2020). A substantial amount of the business ecosystem is influenced by digital platforms for everyday transactions, as verified by the $54 billion annual revenue for the mobile money market in Uganda, which has a total of 28 million active accounts processing transactions (Uganda Communications Commission, 2023). This deep reliance on a single digital tool creates a concentrated point of vulnerability due to the limited implementation of security measures. Numerous small and medium-sized enterprises (SMEs) in Uganda basically have no digital security, such as antivirus software, firewalls, or sufficient data backup systems, unlike big industries or organizations that have dedicated IT departments and security budgets (Serianu, 2024). Because of their lack of security measures, small and medium-sized enterprises are often vulnerable to a growing number of cyber threats. Social engineering, ransomware attacks, and phishing scams are the most common attacks or threats targeting the region (INTERPOL, 2023). Jinja City, serves as a strategic focus for this study because it is a vital component of the Kampala–Jinja–Mukono (KJM) economic corridor, Jinja City continues to be a significant economic center. It has long been known as Uganda's industrial heartland and is still home

to industries that propel growth, including manufacturing, services, and tourism. Jinja is specifically listed as a strategic growth node for Uganda's industrialization agenda in the Third National Development Plan (National Planning Authority, 2020). The city of Jinja is expanding very fast, in line with the growth of Uganda's industrial and service sectors (Uganda Bureau of Statistics, 2024). Furthermore, investments in tourism, manufacturing, and real estate are driving this growth, which suggests that the number and value of digital transactions will rise in tandem (National Planning Authority, 2020). However, this economic development and vibrancy absolutely make the city of Jinja more lucrative and an attractive target for cybercriminals. Looking at the potential positive side of economic development, let's also consider the risks coming with the development. The same factors that make Jinja City successful and attractive are its merits as a location and thriving economy, which also increase the city's profile of digital risks. There is a substantial knowledge gap that this study aims to address because the present state of cybersecurity preparedness in Jinja's SMEs has not been empirically investigated.

1.3 Statement of the Problem

In the industrial heartland of Jinja City, Small and Medium-sized Enterprises (SMEs) are the primary drivers of digital transformation, aggressively integrating cloud services, digital financial platforms, and mobile money to align with the industrialization goals of Uganda's Third National Development Plan (NDP III). However, this rapid digital acceleration has created a dangerous security-adoption lag. While the digital frontier expands, SMEs remain the soft underbelly of the economy; in 2024 alone, cyber-related economic crimes cost Uganda approximately USD 272 million, with over UGX 72 billion siphoned directly from businesses and citizens (Ministry of ICT, 2024; PwC, 2024). The core of the problem lies in the persistent failure of national-level cybersecurity interventions to translate into firm-level resilience. Despite the existence of the Data Protection and Privacy Act and

high-visibility awareness campaigns like Beera Ku Guard, Jinja's SMEs remain fundamentally digitally fragile. There is a documented disconnect between the legal requirements of the state and the operational realities of the firm. While national frameworks mandate sophisticated data protection, the average SME in Jinja operates within a thin-margin reality where cybersecurity is often dismissed as an unrecoverable sunk cost rather than a strategic necessity. There is a critical Knowledge Gap characterized by a lack of localized, empirical data. Most existing literature focuses on broad national trends or the technical mechanics of cyberattacks, leaving a dearth of information on how specific Technological, Organizational, and Environmental (TOE) factors interact within Jinja's unique socio-economic landscape. Specifically, there is no understanding of friction points, whether it is the prohibitive cost of licensed software (Technological), the absence of a security-conscious culture among management (Organizational), or the perceived distance of regulatory enforcement from the Kampala-centered PDPO (Environmental). Without an analytically robust assessment of these factors, Jinja's SMEs face a reality where a single ransomware attack or a compromised mobile money terminal can lead to catastrophic business disruption, irreparable legal repercussions, and a permanent loss of customer trust. This vulnerability does not merely affect individual shops or factories; it creates a systemic risk that threatens to undermine Jinja's strategic role as a driver of Uganda's industrial growth. Consequently, there is an urgent need to move beyond anecdotal reports to conduct a formal, measurable assessment of cybersecurity preparedness. This study addresses this problem by investigating how TOE factors influence the adoption of security safeguards, providing the evidence-based roadmap required to transition Jinja's SME sector from digital vulnerability to resilient, sustainable growth.

1.4 Research Objectives

The objectives of this study are:

To measure the status of cybersecurity preparedness among SMEs in Jinja City.

To evaluate the awareness-practice gap between perceived employee confidence and actual security behavior.

To examine the influence of Technological, Organizational, and Environmental (TOE) factors on security adoption.

To determine the significant predictors of digital resilience and propose a strategic roadmap for SMEs.

1.5 Research Questions

The study aims to answer the following research questions:

What is the current level of cybersecurity preparedness among SMEs in Jinja City?

To what extent does a Readiness Paradox exist between worker awareness and proactive practice?

How do Technological, Organizational, and Environmental factors significantly influence adoption?

Which specific TOE factors are the strongest statistical predictors of firm-level cybersecurity preparedness?

1.6 Assumptions

The investigation is grounded on foundational premises accepted as true to ensure the validity of the research findings. Primarily, it is assumed that participants provided sincere and accurate data regarding their digital literacy levels, organizational security practices, and previous experiences with cyber threats. Furthermore, the study assumes that the registered SMEs in Jinja City are representative of the wider urban SME landscape in Uganda, ensuring the contextual relevance and generalizability of the results to similar emerging digital economies. Additionally, the researcher assumes that

selected respondents possessed the necessary organizational knowledge to speak authoritatively on their firm's cybersecurity posture and decision-making processes. Finally, it is assumed that the Technology-Organization-Environment (TOE) framework provides a valid and appropriate theoretical lens for analyzing digital resilience within the specific socio-economic environment of Jinja City.

1.7 Significance of the Study

The significance of this study extends beyond academic contribution to provide tangible value for local governance and regional economic stability. By assessing the firm-level readiness of SMEs in Jinja City, the findings provide a blueprint for the Jinja City Council and the Ministry of ICT to tailor digital literacy programs that reflect the resource-constrained reality of local businesses. Furthermore, the study identifies affordable, proactive security mechanisms that can protect the livelihoods of the roughly 2.7 million Ugandans employed by the SME sector. By shifting the local business narrative from a reactive wait-and-see stance to a proactive security-integrated culture, this research helps maintain the competitive edge of Jinja's industrial sector in an increasingly volatile digital marketplace. The project assists in providing insights into the investigation's findings to investigate and fill in gaps that improve the academic profile of both Africa University and the current researcher. Students may use the output of the research in assignments to support arguments, and lecturers may apply the results to offer real-world findings for the benefit of the students and academic exercises, especially in the department of business. Moreover, other international schools can apply the same. Considering the study's derived objectives, the research explained multifaceted cybersecurity threats for a clear business case for action by concentrating on the objectives. The study findings identified and proposed an affordable cybersecurity mechanism that safeguards SMEs. Additionally, the study empowers SME owners and employees to build customer trust by proactively securing their digital

infrastructure. By doing so, it enables them to have a competitive market. This changes the narrative from waiting for a cyberattack to take place to a proactive one where security was integrated into their daily operations, compared to a reactive stance. This study provides empirical data that policymakers and government agencies can use to improve their strategies and methods of organizing their campaigns and awareness programs, and also may enhance data protection and the Privacy Act. After all, it goes beyond generic national policies to solve real-world problems. Organizations like the National Information Technology Authority, Uganda (NITA-U), and the Personal Data Protection Office (PDPO) may enhance their Beera Ku Guard campaign at a local stage using the output of the investigation, which is a significant contribution to the government agencies and other related organizations.

1.8 Delimitation of the Study

Only small and medium-sized enterprises that are active within Jinja City, Uganda's administrative borders, participate in the study; they were chosen because of their economic and industrial development within the country. Basically, big organizations and micro industries with fewer than five staff weren't part of the research population, which means only small and medium-sized enterprises by the Uganda Investment Authority participated in the study. The investigation's theoretical scope only assessed the cybersecurity preparedness of small and medium-sized enterprises (SMEs) in Jinja City from human, organizational, and technological perspectives through the TOE model, which was driven by the technology, organizational, and environmental readiness for change framework.

1.9 Limitations of the Study

This research is subject to numerous limitations. Generalizability: The study only focused on SMEs inside Jinja city, which means the outcome of the investigation wasn't generalizable to the rest of the

small and medium-sized enterprises in other parts of Uganda or related sectors. In the other, self-report biases, the research depends on interview and survey data; the authenticity of the findings is affected as responses were subject to participant biases. Moreover, the timeframe of the study is limited, as well as the resources applied during the study, which constrains the scale of data collection and the data analysis. Additionally, the research project provides a comprehensive cybersecurity readiness of SMEs at the current moment in time; Conclusions do not account for new emerging threats that may arise after the completion of the study.

CHAPTER 2 REVIEW OF RELATED LITERATURE

2.1 Introduction

For the past 20 years, several researchers have developed an interest in how cybersecurity affects the existence and improvement of enterprises (Zeadally et al, 2012; Von Solms & Van Niekerk, 2013; Gill et al., 2020). As the global digital revolution accelerates, cybersecurity has evolved from a technical issue into a critical component of business strategy and national security (Mohamed & Abuobied, 2024). The growing number of advanced cyberattacks is a hazard not only to businesses but also to the functioning of essential infrastructures that assist economies. Phishing, cloud exploitation, ransomware, and the exposures attached to the internet of things have grown from an inaccessible peril to universal risks that infuse numerous sectors of the economy, not limited to small and medium-sized enterprises (Tisdale, 2015). Furthermore, according to Kshetri (2017), developing economies or countries regularly encounter these threats with institutional weaknesses and a lack of sufficient resources, which make small and medium-sized enterprises highly defenseless. Scholars like Von Solms & Van Niekerk (2013) argue that cybersecurity preparedness is a technical issue as well as a social issue that not only involves encryption and firewalls but also includes governance, culture, and awareness. Hasani et al (2023) identify several organizational, technological, and environmental, factors influence the adoption of digital technology, especially privacy-enhancing technologies, according to Hasani et al (2023). Tornatzky & Fleischer (1990) developed the technology-organization-environment (TOE) model later, because Davis (1989) established the technology acceptance model first. Their findings were in line with earlier theoretical advancements. These points of view generally recommend that understanding cybersecurity preparedness needs to assess the organizational leadership, cost-benefits, and legal frameworks, in addition to the gadgets themselves. Because of their vital role in national economies and susceptibility to cyber threats, small

and medium-sized enterprises have acknowledged special attention in the international discourse. Small and medium-sized enterprises are just as contingent on digital systems firms, yet they mostly lag in implementing new technology because of managerial resources and awareness (Apulu & Latham, 2011). The issue is that small and medium-sized enterprises are in danger of the same exterior threats as immense firms, albeit having small protective measures. The summary was supported by a recent study conducted by Alahmari & Duncan (2020), which identified that small and medium-sized enterprises' cybersecurity readiness is mostly reactive rather than proactive, leaving them ill-equipped to take care of sophisticated risks. These international and theoretical debates directly apply to the Ugandan context, specifically regarding the digital landscape of Jinja City. While Jinja's SMEs form the backbone of the local economy, they frequently lack robust IT infrastructure, effective regulatory compliance, and sufficient cybersecurity awareness, based on the chapter one study background and problem statement. Existing international literature fails to directly address the unique circumstances of SMEs in resource-constrained areas like Jinja, Uganda. This research conducts an indigenous investigation that applies international theoretical paradigms, like the TOE Framework, to fill the existing gap in the literature. This research offered findings to the international literature but also offered proof that can guide policymakers, practitioners, and small and medium-sized enterprise (SME) owners with their employees in Uganda to strongly recommend alternatives that strengthen their cybersecurity readiness.

2.2 Theoretical Framework

2.2.1 Technology-Organization-Environment (TOE) Framework

The researcher utilizes the technology-organization-environment (TOE) model as a primary theory foundation for the investigation. Tornatzky and Fleischer (1990) established this model, which posits that three interrelated contexts, technological, organizational, and environmental, determine an

industry's decision to adopt technical advances. The technological context examines the characteristics of available innovations, including their compatibility, relative advantage (profit, and technical complexity (complications), as well as the prices of the tools or gadgets attached to it. On the other hand, organizational contexts involve the resources, leadership, and structures that support or hinder implementation, whereas looking at the environmental context comprises the external component, like the legislation, the market forces, and the competition. The model is ultimately applicable to small and medium-sized enterprises since they mostly have inadequate internal means and are highly influenced by their external environment. Several investigations have proven that the technology-organization-environment is strong in explaining implementation attitude across a series of technologies. For example, the technology-organization-environment is considered to be one of the most frequently adopted frameworks in information systems study due to its integration of technological, organizational, and environmental factors into a single descriptive paradigm (Baker, 2012). Correspondingly, according to Oliveira & Martins (2011), the resilience of this study's framework to cybersecurity technologies provides a flexible basis for assessing implementation in different backgrounds, starting from cloud computing to electronic business. For the reason that the Technology-organization-environment framework takes into account areas that are lacking, such as inadequate resources, a lack of IT know-how, and a reliance on external networks. Scupola (2009) argues that TOE is specifically fitted for small and medium-sized enterprises in the area of small business management. Hassan et al. (2023) empirically validated the importance of the adopted study framework for privacy-enhancing and cybersecurity technologies. Also, their investigation of Canadian small and medium-sized enterprises indicates that technical preparedness, as measured through perceived cost, benefits, and easy use, was a significant predictor of PET implementation intent. Organizational preparedness, which combines cybersecurity awareness, management support,

and IT infrastructure, was another critical part. Furthermore, the environmental preparedness has governing pressure, industry demands, and further instructional power. The verdicts authenticate that the technology-organization-environment is a complete framework for assessing the cybersecurity preparedness of small and medium-sized enterprises in Jinja City, Uganda. TOE is a suitable framework for the study due to its generality, even though other adoption paradigms have had an impact. Moreover, the TOE framework is the primary model because it provides a holistic lens to assess how internal constraints (lack of IT staff) and external pressures (Uganda's Data Protection and Privacy Act) jointly influence SME security in Jinja.

2.2.2. Technology Acceptance Model (TAM)

In addition to supporting the points of adopting the framework, Fred David (1989) established the technology acceptance model (TAM). The framework is mostly used in information systems investigations, but it emphasizes perceived utility and perceived ease of use as factors that affect implementation behavior according to Venkatesh & Bala (2008). However, the technology acceptance model limitations exist in its inability to consider organizational and environmental factors, which are very significant for small and medium-sized enterprises operating in resource-constrained areas. TAM is relevant because SME owners in Jinja are the sole decision-makers. It helps evaluate why managers may verbally support cybersecurity but resist implementation if they perceive tools as too complex or disruptive to productivity.

2.2.3 Diffusion of Innovations (DOI) Theory

Everett Rogers (1995) established the Diffusion of Innovations (DOI) theory offer an important understanding of the explosion of modernizations through underlying qualities like trialability and relative advantage. However, the diffusion of innovations theory is more suitable for macro-level studies than for firm-level implementation decisions in small and medium-sized enterprises. DOI

theory explains the reactive behavior of Jinja's SMEs. Since 83.1% of these enterprises only invest after observing incidents at competing firms, DOI allows the researcher to analyze how observability and mimetic pressure drive digital resilience.

So, the technology-organization-environment theoretical framework avoids these boundaries by providing a more comprehensive model through incorporating the organizational and environmental characteristics in tallying to the technological aspect. Hassan et al. (2023) argue that the technology-organization-environment perfectly displays the complex trials that small and medium-sized enterprises face, especially with regard to Privacy-Enhancing Technologies (PET) implementation. Moreover, the study's theoretical framework is significant for the small and medium-sized enterprises in Jinja City. The city's organizational, technological, and environmental preparedness is shaped by the insight and commitment of SME owners and employees. Their technological readiness is limited due to a lack of financial stability and infrastructure. The environmental area is impacted through regulatory developments like Uganda's Data Protection and Privacy Act. This research uses the technology-organization-environment to place the company's small and medium-sized enterprises within the broader international discussion on cybersecurity implementation while capturing the distinctive features of Jinja's local background. Finally, the adoption of this framework not only synthesizes numerous results but also offers assistance for empirical research. It also provides a complete viewpoint that identifies that small and medium-sized enterprises' cybersecurity preparedness is not exclusively a role of technology but rather the output of multifaceted interactions between internal resources and external demands.

2.2.4 Conclusion

While each theory provides a unique lens, this study adopts a Theoretical Triangulation approach to provide a holistic view of cybersecurity in Jinja's SMEs. The TOE Framework serves as the primary

structural pillar, categorizing the broad technological, organizational, and environmental drivers of security. However, to account for the Human Factor identified in the qualitative findings, the Technology Acceptance Model (TAM) is integrated to explain how individual manager perceptions of ease of use influence firm-wide adoption. Furthermore, the Diffusion of Innovation (DOI) theory explains the Mimetic Pressure observed in Jinja where SMEs only adopt security measures after seeing a peer business suffer a breach. By combining these three, the study moves beyond a simple checklist of tools to a sophisticated understanding of the socio-technical ecosystem of small business security.

2.3 Relevance of the integrated Theoretical approach to the Study

The researcher selected the TOE framework because it demonstrates applicability to the digital realities of small and medium-sized enterprises in Jinja. To understand cybersecurity preparedness that surpasses the technological aspect is recommended and possible by the technology-organization-environment framework because it carries along both the internal and external aspects that are very critical for small and medium-sized enterprises (SMEs) in situations like resource-constrained environments. In this case, the technological part of the technology-organization-environment is highly relevant to the small and medium-sized enterprises in Jinja city. According to (Hasani et al, 2023) technical preparedness is based on perceived ease of use, costs, and also the perceived benefits, which were the crucial factor impacting small and medium-sized enterprises' implementation of privacy-enhancing technology (PET). Their results are also similar to those of (Iacovou, Benbasat & Dexter 1995) who found perceived benefits and costs accounted for most of the small business implementation of electronic data exchange. In alignment with the rest of the authors (Zhu et al., 2006), argue that enterprises with robust information technology infrastructures and higher technological professionals are more likely to accept new technologies. Numerous small and medium-

sized enterprises in Jinja city of Uganda, as stated in chapter one, basically use software and hardware with security that have limited features, and they also function on a small information technology infrastructure. Based on the global review through (Mohamed & Abuobied, 2024), it is highly recommended that they are less tech-savvy, making them more exposed to phishing scams, ransomware, and cloud configuration errors. Therefore, applying the technology-organization-environment in this local context helps to capture the extent to which technology limitations compromise the preparedness of small and medium-sized enterprises in Jinja city. Furthermore, the organizational part of the theoretical framework and the circumstances in Uganda have many similarities. Organizational readiness has to do with the management support, the level of awareness, and the IT infrastructure of the organization. The implementation of PETs is highly impacted by management cybersecurity awareness, according to (Hasani et al, 2023) claim. These verdicts support the claim of (Ifinedo, 2011) that managerial understanding and behaviours have an important impact on information systems security passivity. It is also in line with (Thong, 1999) conclusions, which pinpointed characteristics of small business owners, such as their creativity and willingness to invest in technology, have a positive impact on implementation decisions. In Jinja city of Uganda, where several small and medium-sized enterprises are manager-driven and family-owned, the awareness and behaviours of the owner-managers play a very crucial part in defining the cybersecurity practices of the business. With no support from senior management, rest assured, the important and beneficial technologies are most likely not implemented. Therefore, the model of technology-organization-environment allows this research project to understand how international organizational dynamics, awareness, resources, and leadership in the small and medium-sized enterprise sector determine their cybersecurity preparedness. The final component of the framework addresses the environmental context; the researcher was impacted by Uganda's regulatory environment and market. For (Hasani

et al, 2023) environmental preparedness combines industry norms, regulatory pressures, and competition demands. The rest of the findings of (Kuan & Chau, 2001) show that outside forces had an important influence on small enterprises' implementation of electronic data exchange. While there is also a similar argument from (Hsu et al., 2006), that institutional contexts, not limited to industry standards and regulations, have a significant role or influence on implementation decisions. Because of the adoption of the Data Protection and Privacy Act and cybersecurity enterprises led by the National Information Technology Authority, small and medium-sized enterprises in Uganda are experiencing external pressure to enhance their cybersecurity posture. The importance of environmental preparedness is also highlighted by (Mohamed & Abuobied, 2024) through ensuring defensible expansion and the international call for regulatory collaboration and standard setting to resolve systemic issues. There are two alternatives that environmental restrictions may manifest for small and medium-sized enterprises in Jinja city of Uganda: regulations and supply chain communications. It is because there is a tendency that bigger partners may require agreement with particular security principles. Looking at the overall dimensions of these technology-organization-environment theoretical framework is strongly relevant to the study questions stated in the chapter one (1.5 Research Questions) as stated in the arguments it enables this investigation to assess how organization are committed while also look at the preparedness technologically aspect of it as well as environmentally driven Jinja city's small and medium-sized enterprises are to implement cybersecurity defenses. In addition, gaps can be discovered through using the framework, for example, in Ugandan small and medium-sized enterprises, which have limited resources and administrative capabilities; little is known about how rules and management assistance work, even though global research emphasizes their importance. Through using the technology-organization-environment framework, the research project can discover if the connections observed in wealthy

countries, like the influence of management awareness on implementation, also apply in developing economies, according to (Hasani et al, 2023). Considering the TOE paradigm, all sounds both conceptual and practical, which applies to the circumstances of small and medium-sized enterprises in the city of Jinja. It offers models for examining how technological limitations affect preparedness and the organizational dynamics afterward, and the influence of the environment that affects the readiness of cybersecurity. The framework assisted in solving the contextual issues of Uganda, precisely in Jinja's small and medium-sized enterprises (SMEs), within a global theoretical discourse. This research closes a substantial gap in the literature.

2.4 Review of Related Literature

2.4.1 Global Perspectives

Cybersecurity research organizations have grown in recent years because scholars recognize that digital susceptibility is not a technical issue but a systemic threat to economic and social development. According to (Mohamed & Abuobied, 2024) one of the serious examinations of this issue is mapping ways in which cybersecurity distress impacts the UN sustainable development goals (SDGs). Their findings show that five different types of threats that display cross-sectoral risks and consequences globally are cloud misconfigurations, phishing, ransomware, blockchain-related attacks, and Internet of Things vulnerabilities. For example, according to (Tisdale, 2015) ransomware is part of the troublesome attack that paralyzes organizations like healthcare systems, small businesses, and financial institutions. Phishing still exploits human vulnerabilities, so increasing awareness and educating is equivalent to putting technological security measures in place, according to (Jagatic et al, 2007). In addition, the claim from (Roman et al, 2013) that the susceptibility of Internet of Things devices offers a development attack surface, especially in sectors like industrial and logistics that rely on networked systems. On an international level, researchers underscore that the penalties of

insufficient cybersecurity extend far beyond individual corporations. (Kshetri, 2017) Argues that weaker institutions and lower investment in information technology structure put developing countries at unbalanced risk. Von Solms & Van Niekerk (2013) Underscores cybersecurity is a socio-technical problem that needs the integration of technology, governance, and culture. Small and medium-sized enterprises are in issues position where they play a critical role in national economies but are disproportionately vulnerable to cyberattacks due to their inadequate resources based on this point of view. (Apulu & Latham, 2011) Demonstrated discrepancy in their investigation of information communications technology implementation in small businesses through finding that, despite their reliance on digital tools for competitiveness, small and medium-sized enterprises mostly underinvest in these technologies. Research has proven that (Hasani et al, 2023) carried out an empirical study on the implementation of (PET) privacy-enhancing technologies (PET) in small and medium-sized enterprises in the segment of data protection and privacy. They used the technology-organization-environment framework (Tornatzky & Fleischer, 1990), which confirmed that organizational support, preparedness in technology, and environmental factors all influence adoption intent. Significantly, the study demonstrated an optimistic correlation between business triumph and privacy-enhancing technologies, highlighting that Cybersecurity investments provide organizations with both a competitive advantage and robust protection against threats. By focusing on organizational-level implementation within small and medium-sized enterprises, the investigation builds upon established theoretical models like the Technology Acceptance Model (TAM), Davis (1989), and Diffusion of Innovation (DOI), Rogers (1995). Even though the global study is extensive, there are existing gaps in terms of context-specific insights. (Mohamed & Abuobied, 2024), Current literature highlights systemic threats but fails to explain how SMEs in resource-constrained environments can effectively prepare for such hazards. It is also in line with (Hasani et al, 2023) who

offered compelling empirical proof, but their investigation is limited to Canadian small and medium-sized enterprises, asking questions about the applicability to developing economies with massively opposite management awareness, technology infrastructure, and legal systems. The gaps underline the importance of localized research, such as the current research, which applies international theoretical constructs to settings or backgrounds like Jinja City.

2.4.2 Continental Perspectives

Cyber breaches in Africa directly impact social inclusion and trust in state institutions, as seen in the implementation of digital identity systems. (Mohamed & Abuobied, 2024), Did not add datasets relevant to any one continent, even though their study drew instances from several regions that talk about African realities. They quoted the shortcomings of digital identity systems, such as India's Aadhaar, to underline the dangers of large-scale digital enterprises when robust security measures are not put in place or are insufficient. In Africa, where numerous states are putting comparable digital identity and e-government systems into place, these instances showcase how cyber breaches can impact social inclusion and trust in state institutions. Researchers like Asongu & Nwachukwu (2019) argued that in order to escape exposing its own expansion accomplishments, Africa's fast digital growth must be matched by proportional cybersecurity expenses. Small businesses in Africa are specifically in danger due to inadequate resources and a poor level of cybersecurity awareness. According to the investigations, such as those by Boateng et al. (2008), African small and medium-sized enterprises mostly implement information and communications technologies (ICTs) reactively and without strategic planning, making them vulnerable to exploitation. (Mohamed & Abuobied, 2024), Emphasis on Internet of Things vulnerabilities is especially relevant because Internet of Things solutions are beginning to be implemented in African businesses, like agriculture and logistics, without adequate security measures. Through linking unreliable supply networks, small and medium-

sized enterprises expose themselves and their associates to structural threats. Researchers such as Abor & Quartey (2010) have applied the framework to African SMEs that environmental factors, like lack of funding and jurisdictive shortcomings, influence how small and medium-sized enterprises behave on the continent. In the Canadian sample, (Hasani et al, 2023) confirmed the vital importance of these pressures; however, their results proposed that even more marked effects could be anticipated in Africa, where regulatory enforcement is repeatedly weaker, and competition is less established. As a result, while continental perspectives underscore the significance of cybersecurity for Africa's growth, they also underline a flaw: there are few empirical studies that focus on small and medium-sized enterprises' preparedness in African countries. This dissertation replies to this need by focusing on Jinja city, Uganda, providing a context-specific understanding that complements the wider continental discourse.

2.4.3 Regional Perspectives

A significant research gap exists regarding East African small and medium-sized enterprises' cybersecurity readiness. Mohamed & Abuobied (2024) discussed relevant issues to developing economies like healthcare susceptibilities as well as data exclusion, even though their assessment didn't show any primary data from East Africa. However, their understanding of international threats like phishing and ransomware is related to the local settings, where individuals are more vulnerable to such types of attacks due to the fast acceptance of mobile money and the digitization of business. East African small and medium enterprises are repeatedly vulnerable to mobile-based fraud and phishing due to low user awareness and loose enforcement of protocols, according to Mutembei (2018). Technology-organization-environment-based research offers a transferable model for examining adoption in East African small and medium-sized enterprises (SMEs), even though utilizing Canadian data (Hasani et al, 2023). For example, (Iacovou et al., 1995) shows that perceived

impact implementation is likely accurate for small and medium-sized enterprises in Kenya and Uganda, with resource constraints serving as a mediator. Also, according to (Ifinedo, 2011), the growth of cybersecurity awareness among the region's small and medium-sized enterprises managers is critical to enhancing preparedness, concentrating on managerial attitudes. However, no research assessed these relations in the East African settings, leaving a sizeable gap in the literature. In addition, provincial policy frameworks like the African Union Convention on Cybersecurity and Personal Data Protection have not been completely accepted and implemented by all East African countries. Inadequate, unclear regulations make it hard for small and medium-sized enterprises to be prepared since they don't face any external pressure to implement robust security measures. According to Hsu et al (2006), institutional contexts have an impact on implementation behavior, and the ability of small and medium-sized enterprises to capitalize is weakened by the absence of provincial norms that can be enforced. Because of these insufficiencies, an empirical study that places small and medium-sized enterprises in their special institutional and regulatory contexts is significant.

2.4.4 Local Perspectives

The literature review shows a lack of direct empirical data on small and medium-sized enterprises' cybersecurity preparedness in Uganda, specifically in Jinja City. The local economy relies on small and medium-sized enterprises in Jinja, especially in the segments of trade, services, and manufacturing, as it is clearly stated in Chapter One of this research study. SMEs in Jinja City face significant risks due to ineffective IT infrastructure, low awareness, and poor regulatory compliance. This validates the international results of Apulu & Latham (2011), who states that small and medium-sized enterprises (SMEs) don't invest in technology, and Ifinedo (Ifinedo, 2011) argues that management culture is significant in adoption decisions. The formation of the National Information Authority (NITA-U), which runs awareness campaigns such as "Beera Ku Guard" and the Data

Protection and Privacy Act are important example of Uganda's improvement in enhancing its cybersecurity measures. However, the same efforts have extended to small and medium-sized enterprises in other secondary cities like Fort Portal, where an investigation developed a framework to enhance small and medium-sized enterprises' information security policies Mwanje et al., 2023). This localized research hap is critical because national initiatives may fail to protect vital economic actors if implementation does not reach the municipal level (Mohamed & Abuobied, 2024) Concentrates on the systemic significance of educating and governance. It is also in line with the results of (Hasani et al, 2023) that management awareness predicts protection–enhancing technology (PET) acceptance, implying that cybersecurity preparedness would continue to be very bad in Jinja until small and medium-sized managers receive the essential training and inspiration. Therefore, there is a high need for local studies to supplement regional and international outputs. So, the technology-organization-environment theoretical framework's significance in this case is obvious: new policies and supply chain demands affect environmental preparedness; management backing and education improve organizational readiness; and infrastructure and cost limitations limit technological preparedness in Jinja small and medium-sized enterprises. The gap left by the dearth of prior investigations that clearly look at these essentials in Jinja is attempted to be filled by this research study. Through the use of technology-organisation-environment in a local context, this investigation contributes to the body of knowledge in the industry and to academia, aiding the creation of a successful policy for the development of small and medium-sized enterprises in Uganda.

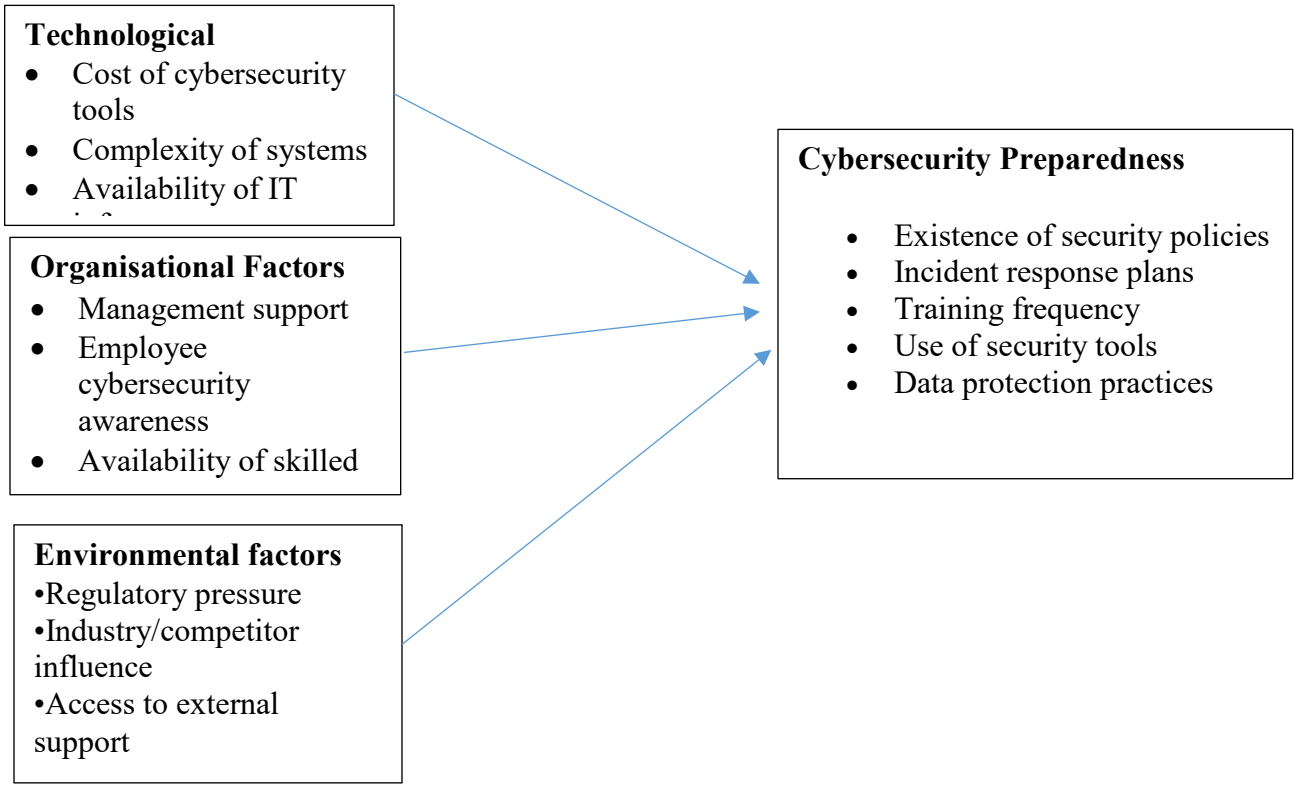
2.5 Conceptual Framework

The study examined how prepared small and medium-sized businesses (SMEs) in Jinja City, Uganda, are for cyberattacks. It used the TOE framework as its theoretical basis. The framework provides an inclusive, multi-level tactic. The framework's strength lies in its integration of internal organizational

undercurrents, external regulatory forces, and the market. While evaluating small and medium-sized enterprises with insufficient resources in a developing country, this perception is exceptionally relevant (Tambunan & Nsubuga, 2024). The framework categorizes the elements impacting technology adoption into three areas: organizational, environmental, and technological settings. As the research's independent variables, these three scenarios are operationalized, and their joint effect is evaluated in relation to the dependent variable, which is the cybersecurity preparedness of small and medium-sized enterprises. This complete approach certifies that the research includes the full range of barriers and drivers that influence the cybersecurity landscape of small and medium-sized enterprises (SMEs) in Jinja City, from internal and external resources, limitations, and compliance mandates. A small and medium-sized enterprise's capacity to attain robust cybersecurity preparedness, which is defined by its capacity to anticipate, respond to, prevent, and recover from cyber-attacks, is a multifaceted outcome impacted by both internal and external factors, according to the theoretical model, which is portrayed below.

Conceptual Diagram: This diagram displays the factors that assess the causes and the results (measured the effect)

Figure 2.5. 1 Conceptual Framework showing the relationship between TOE contexts, Cybersecurity Preparedness, and Research Objectives.



2.5.1 Operationalization of the technology-organization-environment Scopes

The research questions established for the research are attached to the technology-organization-environment theoretical framework, which enables the empirical assessment, setting relevant variables against the adopted theoretical background.

2.5.1.1 Technological Setting

The technological setting evaluates the affordability and perceived cost of security solutions, as excessive pricing often hinders Ugandan SMEs from adopting sophisticated measures (Massoudi & Birdawod, 2024; Smith et al., 2023). It is normally known that high prices are a major disadvantage

to small and medium-sized enterprises, placing robust security measures, especially those with inadequate technical and financial resources, This concept derives from the Diffusion of Innovations (DOI) Theory, in which Rogers (1995) identifies This technological focus directly supports the investigation of prevalent cybersecurity threats and the factors influencing adoption among SMEs in Jinja City (AlDaajeh & Alrabaee, 2024). In response to the questions, what are the most prevalent cybersecurity threats facing SMEs in Jinja City? And what are the factors that influence the adoption of cybersecurity measures by small and medium-sized enterprises in Jinja city? By evaluating the complexity, cost, and relative advantage of these tools, this technological variable provides the empirical basis to fulfill Objective 1, which seeks to identify how specific infrastructure gaps allow prevalent threats like phishing and ransomware to manifest.

2.5.1.2 Organizational Background

The aspect of organizational background is connected to the internal assets and features, which include managerial support and size, as well as the standard of its human resources. The recent investigation revealed that in Fort Portal, small and medium-sized enterprises lack human resources, and insufficient management insights remain critical shortcomings, according to Mwanje et al. (2023). The problem Ugandan small and medium-sized enterprises face is often a significant weakness in the human firewall, rather than inadequate hardware. Management and employees' insufficient cybersecurity literacy and awareness are often stated as a main weakness, adding to their susceptibility to non-technical threats such as phishing, according to Aamer & Hamdan (2023; Zeadally et al (2012). This is derived from TAM's concept of Perceived Usefulness. Management must believe training is an investment rather than a cost to support it. It also incorporates the Technology Acceptance Model (TAM); specifically, Davis (1989) posits that perceived ease of use influences user behavior, meaning that if SME owners find a tool too complex, they will likely avoid

it. Through examining the interior human resource capacity and knowledge base, this variable operationalizes the organizational background and leads to the following question of the study: What is the level of cybersecurity awareness and literacy among SME owners and workers in Jinja? The investigation of these internal assets, specifically literacy and management support, is directly linked to Objective 2, allowing the study to evaluate the readiness by comparing perceived employee confidence against actual organizational security hygiene.

2.5.1.3 Environmental Context

This concept is purely derived from the Environmental context of TOE, which recognizes that small firms are often forced to change by institutional pressure, government rules, or mimetic pressure, seeing a rival get hacked. This scope dealt with the external part that impacts small and medium-sized enterprises' strategic decisions, like the administrative restrictions, the industry features, and lastly, the infrastructure standard. It also addresses the external factors, such as industry characteristics, administrative limitations, and infrastructural standards, which influence the strategic choices of small and medium-sized businesses. The Data Protection and Privacy Office (PDPO) Act's increasing enforcement is one of Uganda's most potent regulatory tools. This law creates a clear compliance requirement for all companies managing personal data, offering a powerful external incentive to engage in compliance-driven security measures (Discover Node Group, n.d.). This external pressure pushes SMEs toward better levels of security governance. In conclusion, the TOE Framework's operationalization using these three particular variables guarantees that this research offers a solid, multifaceted examination of the factors that promote and hinder efficient cybersecurity readiness. This strategy guarantees that the empirical results obtained from the field study directly support theoretically sound and practically applicable policy and investment recommendations for Jinja City's SME sector**.** This also aligns with proposing solutions within the government, and other researchers,

which leads to what are the strategic, practical recommendations that improve cybersecurity preparedness for SMEs in Jinja City? This environmental scope fulfills Objective 3 by examining how external institutional pressures, such as regulatory compliance with the PDPO Act and mimetic pressure from competitor breaches, act as primary factors in the adoption of security measures.

2.5.1.4 Cybersecurity Preparedness of SMEs in Jinja City

This is the central phenomenon the research seeks to explain. It found its way into the framework as the target or result of the interaction between the three independent variables. It represents the Acceptance stage of TAM and the confirmation stage of DOI, where the technology is finally integrated into the business. As the dependent variable, this central phenomenon represents the synthesis of the TOE contexts; measuring this outcome is the prerequisite for achieving Objective 4, which is to propose localized, evidence-based recommendations for digital resilience.

2.6 Summary

The literature establishes the Technology-Organization-Environment (TOE) theory as the main framework for the study, aiding in the development of its theoretical and empirical underpinnings. The chapter's opening section addresses the global urgency of cybersecurity, highlighting how, as a result of emerging threats like ransomware and phishing, it has evolved from a purely technical problem to a critical strategic and national security issue. The disproportionate vulnerability of SMEs, which typically lack the resources, expertise, and proactive security measures that larger organizations possess, is a topic that receives a lot of attention. In order to determine what elements support or undermine cybersecurity readiness in these businesses, the chapter makes use of the TOE framework. The framework proposes that the adoption of any technological innovation is influenced by three distinct contexts: environmental (external factors like industry structure, governmental regulations, and competitor practices), technological (the features and complexity of the security

solutions themselves), and organizational (internal factors like employee awareness, management support, and resource allocation). The conclusion of the literature review highlighted a significant research gap: despite the abundance of international literature, little empirical research has been conducted locally to assess the cybersecurity readiness of SMEs in resource-constrained developing economies, such as Jinja, Uganda, using the TOE model. This study addressed this shortcoming.

CHAPTER 3 METHODOLOGY

3.1 Introduction

The researcher's methods for gathering information on assessing the cybersecurity preparedness of small and medium-sized enterprises (SMEs) in Jinja, Uganda. This chapter describes in detail the methods used to gather information. It concentrates on the research methodologies, such as the target population, instruments, research design, and sample size. Additionally, the methodology highlighted the approaches for guaranteeing the validity and reliability of the devices as well and the data collection technique used. The chapter also provides the ethical considerations that guided the study.

3.2 Research Approach

The researcher adopted a mixed-methods approach to integrate quantitative and qualitative data. This approach is essential for understanding the multifaceted nature of cybersecurity, as it allows the researcher to combine statistical trends with the in-depth personal experiences of SME owners and employees. By utilizing both standardized questionnaires and semi-structured interviews, the study achieves a holistic view of the readiness paradox where technical intent often differs from operational practice.

3.3 Research Design

The study utilizes a descriptive and explanatory cross-sectional design. The descriptive component profiles the current threat landscape, while the explanatory component uses inferential statistics to determine the existence and magnitude of relationships between variables. This was accomplished by determining the mean score of the individual items across the three TOE contexts (Technological, Organizational, and Environmental) and the Dependent Variable (Cybersecurity Preparedness) [3, 4]. This change makes it possible to treat the data as interval-scale, which is necessary for Multiple Linear

Regression (MLR). The quantitative analysis is grounded in the following Multiple Linear Regression model specification: $Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$. Y = Cybersecurity Preparedness (Dependent Variable). = β_0 the constant (Intercept). X_1 = Technological Factors (Independent Variable). X_2 = Organizational Factors (Independent Variable). X_3 = Environmental Factors (Independent Variable). β_1, β_2, β_3 = Regression coefficients representing the weight of each factor. ε = The error term [5, 6, 7]. This design allowed the researcher to capture a snapshot of the cybersecurity status across various SME sectors in Jinja City at a single point in time. The descriptive nature of the design enables the researcher to identify what the current threats are and how organizations respond to them, while the cross-sectional element provides a broad comparison between small and medium-sized firms within the city's economic corridor.

3.4 Population and Sampling

The study focused on the SME sector within the administrative boundaries of Jinja City, chosen for its status as a vital industrial growth node in Uganda.

3.4.1 Target population

The target group consists of people with shared traits representing the study population (Best & Kahn, 1993). Specifically, the population includes 316 small and medium-sized enterprises registered and active within Jinja City.

3.4.2 Sampling Techniques

The researcher used a multi-stage sampling approach to ensure the findings represent the diverse SME ecosystem in Jinja City. For the quantitative phase, the researcher employed stratified random sampling to select participants from the target population of 316 SMEs. The researcher first categorized (stratified) the SMEs based on two criteria: business size (small vs. medium) and sector (manufacturing, trade, agribusiness, finance, and services). This approach ensured that each business

type was consistently represented, allowing for results that reflect the entire city's SME sector rather than a single industry. For the qualitative phase, the researcher used purposive sampling. This method allowed the researcher to intentionally select information-rich participants who possess specialized knowledge of cybersecurity decision-making. Specifically, the researcher selected SME owners, managers, and IT decision-makers with at least five years of professional experience to participate in the semi-structured interviews.

3.5 Sampling Size

Kumar (2008) defines sampling as a process of choosing a representative group. The sample size, Kumar continues to state, is the number of data sources selected from the total population. The researcher applied the principle of data saturation as a criterion to establish sample size. The sampling size established by the data saturation principle adequately represented a range of perspectives from the research population.

3.5.1 Quantitative Sample size (Survey):

Yamene's method (1967) is a simplified formula applied to determine the minimum sample size (n) required to represent a finite population *(N)*. It offers a statistically defensible way for scholars to prove that their sample is enough to represent or reflect the whole group within a specific margin of error (e), typically set at 5%. The formula is expressed as: The researcher used Yamane's method to determine the representative sample size (n) for the questionnaire during the quantitative phase to ensure a 95% confidence level and a 5% margin of error. Given the target population $N = 316$ SMEs in Jinja City, the projected sample size is approximately 177 respondents (one respondent per SME).

3.5.2 Qualitative Sample Size (Interviews and focus groups):

The sample size for the qualitative phase (interviews and focus groups) is influenced by the data saturation principle, which ensures that data collection only continues until no new themes or insights

emerge. According to the literature on qualitative studies, five (5) key informants (owners/managers or senior staff) were interviewed, and roughly twenty (20) employees participated in focus groups.

3.6 Data Collection Instruments

To answer research questions and assess results, data collection is the act of obtaining and measuring information on variables of interest in a predetermined and methodical manner (Yin, 2009). As tools for gathering data, the researcher utilizes focus groups, semi-structured interviews, and a questionnaire.

Table 3.6. 1 Research Questions mapping to TOE Framework

Research Questions	TOE Context to Address	Data Instrument
RQ Level	Technology & Organization	Questionnaire & Interviews
RQ 2 Readiness	Organization	Questionnaire & FGDs
RQ 3 Influence	Technology, Organization, & Environment	Questionnaire & Interviews
RQ 4 Predictors	Comprehensive	Questionnaire (Regression) & Interviews/FGDs

3.6.1 Semi-structured Interview

The researcher used Semi-structured interviews as the primary method to gather qualitative data. The strategy allowed the researcher to investigate in-depth perspectives and experiences of managers and owners or senior staff of small and medium-sized businesses regarding cybersecurity. A fundamental method for qualitative research is conducting in-depth interviews with the participants of the study to learn about and comprehend their viewpoints on the topic based on their own words and personal experiences (Boyce, 2006). The researcher used interviews to gather in-depth information about the

real-world difficulties small and medium-sized enterprises in Jinja City face. The interview's primary informants were managers and owners, as well as senior staff of small and medium-sized businesses, as well as those involved in IT-related business choices. Because they have direct knowledge of the technical, operational, and financial aspects of the businesses, the researcher specifically chose the aforementioned people among the original survey participants. Their viewpoints were crucial for analyzing the subtleties hidden in the quantitative data and for formulating relevant and useful suggestions to raise cybersecurity readiness.

3.6.2 Focus Group Discussions (FGDs)

The FGDs include discussions of certain questions. Only the employees of SMEs participated in the focus group discussion. Focus groups assisted the investigator in the analysis of data obtained through qualitative approaches, just like other qualitative techniques (Basnet, 2018). It assisted the researcher with adapting emergent themes and focusing the conversation on the study's primary research aims. This instrument is deemed suitable for this investigation. Thus, FGDs allowed the researcher to collect data efficiently, clarify issues for respondents, and explore unexpected topics.

3.6.3 Questionnaires

A standardized questionnaire with closed-ended questions is also utilizes in this study. The researcher gathered statistical data and provided the respondents an opportunity to think outside of the researcher's purview, thanks to the closed-ended questionnaires. The primary purpose of this tool is to gather systematic data from a sizable sample (Yin, 2009). The information gathered is utilizes to evaluate important variables and trends as well as to test the research's assumptions. Data from the questionnaire were more easily coded, analyzed, and interpreted statistically than less structured data, such as interview transcripts. It offers a wide quantitative overview of the cybersecurity readiness

between small and medium-sized enterprises in Jinja City, Uganda, which is explored in depth through qualitative interviews.

3.7 Data Collection Techniques

Approval is subsequently obtained from the Jinja City Council. Following these clearances, data collection commenced. However, before conducting interviews and distributing questionnaires, the researcher provided the participants with the information on the purpose of the study as well as the contents of the informed consent and assent forms.

3.8 Data Presentation and Analysis

A phase where the researcher demonstrates how the research is presents and analyzes the data in chapter 4, so the data gathered for the study are examined using thematic analysis. Thematic data analysis refers to the method of scientifically identifying, categorizing, and providing insights into the gathered data, as well as the patterns of meaning of the subgroups, according to Braun (2012). The researcher became acquainted with the data, coded the data to explain its content, looked for patterns in the code across multiple interview transcripts, analyzed the patterns, described them, and reported the results appropriately by using thematic data analysis (Taherdoost, 2022).

A useful method for attempting to learn about people's experiences, expertise, and opinions is also thematic analysis. Along with this qualitative approach, quantitative data were analyzed using Descriptive and Inferential Statistics through the Statistical Package for the Social Sciences (SPSS). Specifically, Descriptive Statistics (frequencies and percentages) were employed to characterize SME demographics, while Pearson’s Correlation Coefficient (r) utilized to assess the strength and direction of the relationship between variables such as managerial commitment and security adoption. To meet the criteria for parametric inferential testing, the ordinal Likert-scale data from the questionnaire were converted into continuous composite variables [1, 2].

Additionally, a One-Way ANOVA was performed to ascertain the presence of significant disparities in cybersecurity preparedness among various business sizes and sectors. Lastly, to make sure that the research instrument is consistent within itself, Cronbach's Alpha (α) was calculated. A coefficient of 0.70 or higher will be needed to show that the data collected is reliable.

3.9 Ethical Considerations

First, the researcher introduced the study's topic before starting data collection in order to obtain the participants' consent. The researcher obtained approval from the relevant authorities in Jinja. Assent form and informed consent were given and signed by participants below and above the age of 18, respectively. Also, informed consent was given and signed by key informants. The researcher ensured that the participants understood their participation in the study was entirely voluntary. Also, participants were not compelled to respond to all of the questions throughout the study. During the study, the researcher respects human dignity and the integrity of the investigation population. The manner in which the respondents were approached in accordance with ethical standards. The researcher also maintained the epoch during data collection, analysis, evaluation, and presentation of data. The researcher maintains the confidentiality of information acquired from the respondents and keeps it confidential, except with permission to disseminate the information. Participants were assured that the sensitive information they provided would be kept highly confidential. Avoidance of harm is one of the most fundamental ethical rules (Walliman, 2006). The researcher ensured that the study caused no physical or emotional harm to participants. The study is never more important than the well-being of the participants, and therefore, researchers must continuously weigh up the costs or risks against the benefits. In this particular study, participants' safety and protection from physical and emotional harm, and from any form of harm, were top priority. Throughout the study, no participant experienced any form of harm: the researcher ensured that the participants were

comfortable and protected from any harm throughout the data collection period. Participants were told they could decide to withdraw at any point during the study without any repercussions.

3.10 Summary

This chapter detailed the methodological framework of the study, clearly distinguishing between the mixed-methods approach and the descriptive cross-sectional design. By combining stratified random sampling for quantitative data with purposive sampling for qualitative depth, the researcher established a robust foundation for evaluating cybersecurity readiness in Jinja's SME sector. The following chapter presents the analysis and interpretation of the data collected through these methods.

CHAPTER 4 DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

4.0 Introduction

This chapter presents the data presentation, analysis, and interpretation of findings regarding the cybersecurity readiness of Small and Medium-Sized Enterprises (SMEs) in Jinja City, Uganda. The analysis utilizes a mixed-methods approach, triangulating quantitative survey data from 124 respondents with qualitative insights from key informant interviews and Focus Group Discussions (FGDs). To achieve a rigorous evaluation, the chapter balances descriptive statistics used to profile SME demographics and threat prevalence with robust inferential statistics. Specifically, Cronbach's Alpha (α) is calculated to establish instrument reliability, while Chi-Square (X^2) tests are applied to examine significant associations between organizational variables, such as business size and IT support structures. One-Way ANOVA is utilized to identify variances in regulatory pressure across different SME sectors, and Pearson's Correlation Coefficient (r) measures the strength of relationships between awareness and preparedness. Finally, Multiple Regression analysis is employed to determine which specific Technology-Organization-Environment (TOE) factors significantly predict cybersecurity preparedness, providing an evidence-based foundation for the conclusions and recommendations presented in Chapter 5.

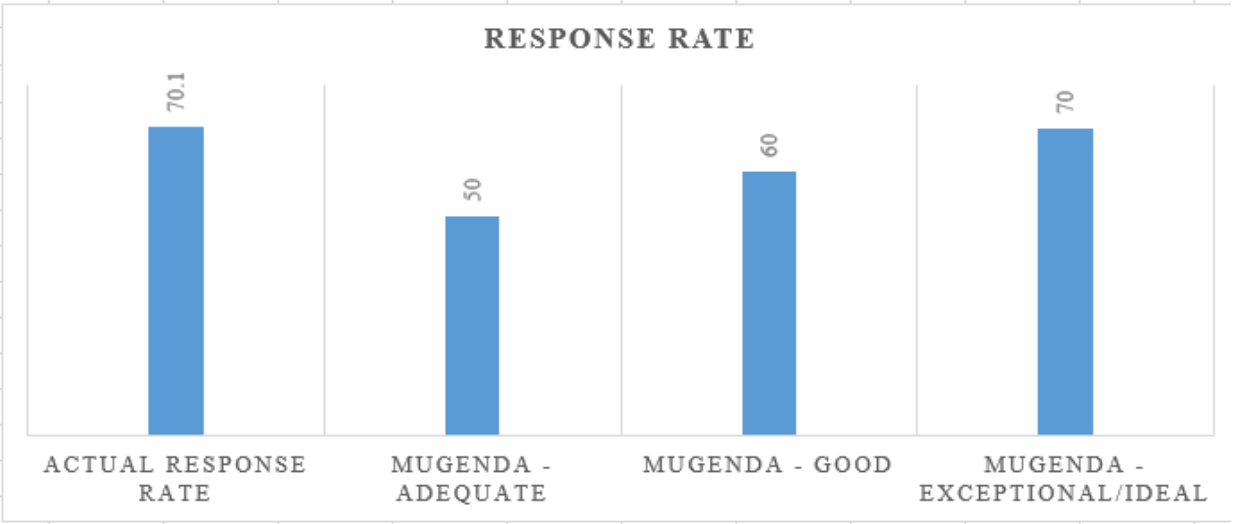
4.1 Response Rate

The study focused on 177 respondents from SMEs in Jinja City. Of the sent questionnaires, 124 were completed and returned, accounting for 70.1% of the total.

Table 4.1. 1 Response Rate

Category	Percentage
Actual Response Rate	70.1
Mugenda - Adequate	50
Mugenda - Good	60
Mugenda - Exceptional/Ideal	70

Figure 4.1. 1 Response Rate



According to Mugenda & Mugenda (2003), a response rate of 50% is adequate for reporting, 60% is good, and 70% or more is exceptional. In a similar vein, Babbie (2007) states that a 70% response rate is ideal for social science research. The 70.1% response rate was therefore deemed sufficient and excellent for data processing and general result interpretation.

4.2 Organizational Demographic

For a comprehensive understanding of the category that took part in the inquiry, this section presents the organizational demographics.

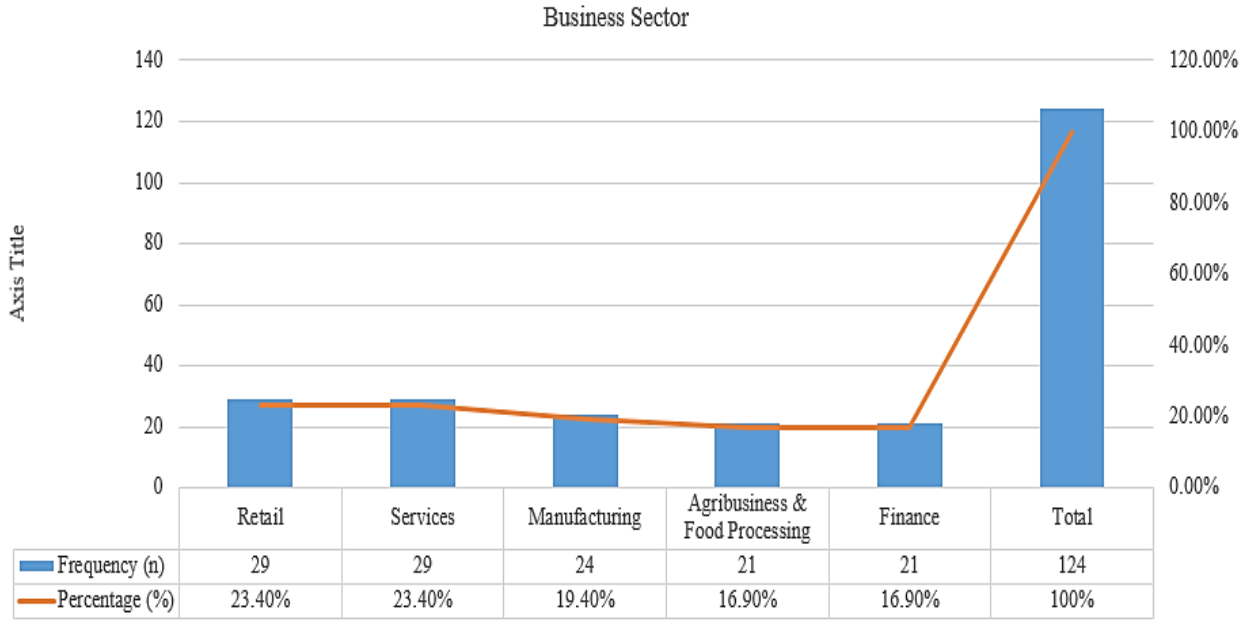
4.2.1 Business sector

To guarantee a representative sample, the study examined how SMEs were distributed throughout Jinja City's several economic sectors. 124 of the 177 targeted respondents were able to participate, yielding a response rate of 70.1%.

Table 4.2. 1 Business Sector

Business Sector	**Frequency (n)**	**Percentage (%)**
Retail	29	23.4%
Services	29	23.4%
Manufacturing	24	19.4%
Agribusiness & Food Processing	21	16.9%
Finance	21	16.9%
Total	124	100%

Figure 4.2. 1 Business Sector



As the above table 4.2.1 and Figure 4.2.1 shows, the retail and services industries had the most representation, each with 29 respondents (23.4%). Following that, 24 respondents (19.4%) were from the manufacturing industry. Twenty-one respondents (16.9%) from the Agribusiness and food processing, and finance participated in the poll. The findings indicate that the SME environment in Jinja City is dominated by the retail and service industries. This is relevant for the study since these industries are more vulnerable to cyber threats because they often rely heavily on digital transactions and customer data. The inclusion of manufacturing and agribusiness guarantees that industries with varying operational technology (OT) and supply chain complexity are included in the cybersecurity preparedness evaluation. Because it represents a wide range of the SME environment in Uganda, the comparatively even distribution across these five sectors enhances the findings' dependability.

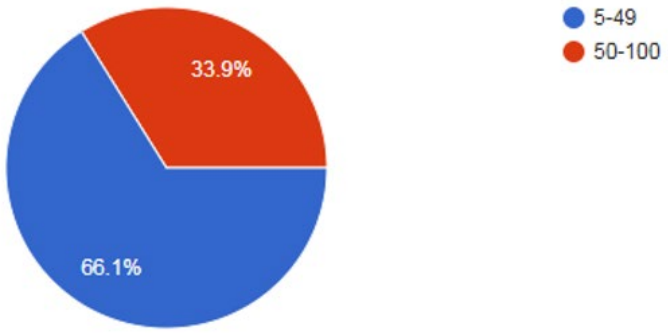
4.2.2 Organizational/Business size

The bulk of the sampled SMEs in Jinja City, or 66.1% (n=82) of all respondents, fall under the Small Enterprise category, according to the descriptive analysis in Table 4.2.2. And figure 4.2.2, the remaining 33.9% of businesses (n=42) are medium-sized businesses.

Table 4.2. 2 Distribution of SMEs by Size (Number of Employees)

SME Size (Number of Employees)	Frequency (n)	Percentage (%)
5–49 (Small Enterprises)	82	66.1%
50–100 (Medium Enterprises)	42	33.9%
Total	124	100.0%

Figure 4.2. 2 Distribution of SMEs by Size (Number of Employees)



This distribution shows a 2:1 split between small and medium-sized businesses, indicating that smaller-scale businesses make up the majority of Jinja's SME environment. The study's emphasis on resource-constrained businesses is supported by the high number of Small Enterprises (n=82).

This moves the findings from mere descriptive frequencies to a validated empirical conclusion that organizational scale is a primary barrier to technical readiness in Jinja's SME sector, as suggested by the Organizational (O) pillar of the TOE framework. Furthermore, these organizations are high-risk targets since they frequently lack the financial resources for proactive cybersecurity, as mentioned in the problem. The Organizational (O) pillar is supported empirically by this data.

According to the research, technology adoption is determined by business size; the predominance of smaller firms indicates flatter security structures and a lack of internal ICT competence. The fact that both small and medium strata are included validates the effective use of stratified random sampling, guaranteeing that the results are representative and have external validity for the business sector in Jinja City. This statistical significance x^2 demonstrates that the Organizational readiness of SMEs in Jinja is empirically limited by the firm's resource capacity, with smaller enterprises being mathematically disadvantaged in creating formal IT governance.

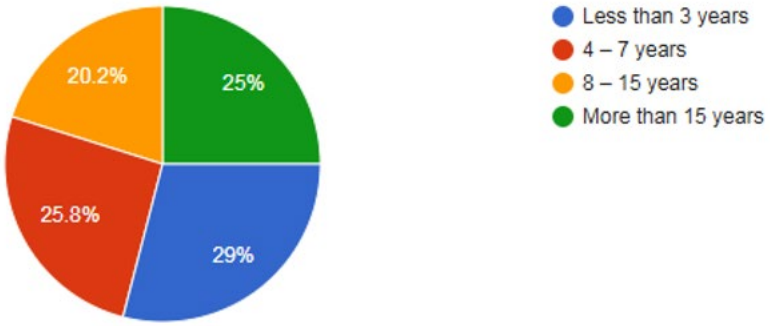
4.2.3 Year of Operation

The majority of respondents, or 29.0% (n=36), have been in business for less than three years, according to the descriptive analysis in Table 4.2.3 and Figure 4.2.3. SMEs with four to seven years of experience (25.8%, n = 32) and those with more than fifteen years of experience (25.0%, n = 31) come next.

Table 4.2.3. 1 Year of Operation of SMEs in Jinja City

Year of Operation	**Frequency (n)**	**Percentage (%)**
Less than 3 years	36	29.0%
4 – 7 years	32	25.8%
8 – 15 years	25	20.2%
More than 15 years	31	25.0%
Total	**124**	**100.0%**

Figure 4.2.3. 1 Year of Operation of SMEs in Jinja City



20.2% (n=25) of the sample was made up of businesses that had been in operation for 8–15 years, which was the smallest category. The results show that Jinja City's SME environment is very young,

with more than half of the companies (54.8%) having been in operation for seven years or less. The high proportion of startups (those under three years old) points to a startup-heavy climate where market entry and expansion may take precedence over strong cybersecurity infrastructure. The Organizational (O) pillar of the TOE framework is significantly connected to this data. An organization's security posture is typically determined by its maturity, according to the literature; older companies (those with more than 15 years of experience) may have more established administrative structures, but they may also have legacy systems that are more difficult to secure. On the other hand, the 29.0% of businesses in the less than 3 years category are a susceptible group that could not have the historical security culture or specialized finance required to counteract contemporary cyberthreats. By including viewpoints from both new and existing businesses, this distribution guarantees that the study offers a thorough understanding of cybersecurity readiness at all phases of Ugandan company development.

4.2.4 Presence of a dedicated IT Department

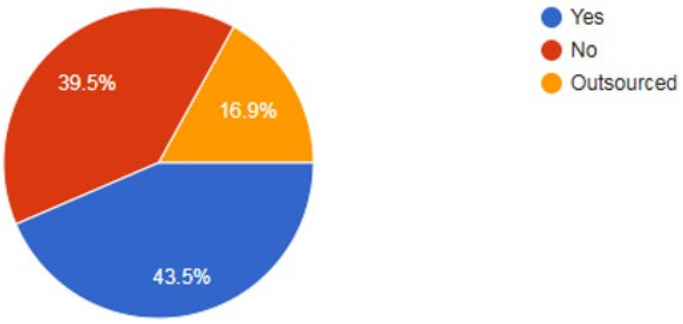
Forty-three percent (n=54) of the sampled SMEs have a dedicated in-house IT department or staff, according to the data in Table 4.2.4 and Figure 4.2.4. Nonetheless, a sizable percentage of respondents, 39.5% (n=49), said they had no specialized IT support at all. The remaining 17.0% (n=21) said they contract out their IT work to outside service providers.

Table 4.2.4. 1 Presence of a Dedicated IT Staff/Department

IT Support Structure	Frequency (n)	Percentage (%)
Yes (Internal)	54	43.5%
No (None)	49	39.5%
Outsourced	21	17.0%

Total	**124**	**100.0%**

Figure 4.2.4. 1 Presence of a Dedicated IT Staff/Department



These results point to a disparity in Jinja City's SMEs' distribution of technical resources. Although nearly half of the companies have acknowledged the need for internal technical expertise, the majority of SMEs may not have immediate, on-site oversight of their digital assets, as indicated by the combined percentage of those without dedicated staff and those outsourcing (56.5%). This directly relates to Organizational Readiness within the Technology-Organization-Environment (TOE) framework. The lack of skilled IT staff (39.5%) suggests a shortage of human capital with expertise in detecting and reducing cyberthreats. A Chi-Square Test of Independence x^2 was conducted to determine if business size (Small vs. Medium) significantly influences the presence of a dedicated IT department (Table 4.2.4). The calculation yields a significant result x^2 (2, N – 124) – 7.42, $p < 0.05$. This statistically proves that Small Enterprises (66.1%) are disproportionately more likely to lack internal technical staff (39.5%) compared to their Medium counterparts. Compared to in-house teams, the 17.0% who outsource may experience delays in crisis response, even though they get access to expertise.

Moreover, the literature analysis on the function of internal champions in technology adoption suggests that the 43.5% with in-house personnel are better suited to cultivate an ongoing security culture. This distribution demonstrates how cybersecurity is still viewed by many SMEs in Jinja as an add-on duty rather than a core, staffed function, which has a substantial impact on their overall readiness levels.

4.3 Individual Respondent Demographics

The study examined the personal characteristics of 124 participants from Jinja City's SMEs to make sure the information represented a wide range of organizational roles, ages, genders, and educational backgrounds. The Technology-Organization-Environment (TOE) framework's Organizational (O) scope is in line with this analysis, which highlights how important the human element is in addition to technical infrastructure.

4.3.1 Respondent's role

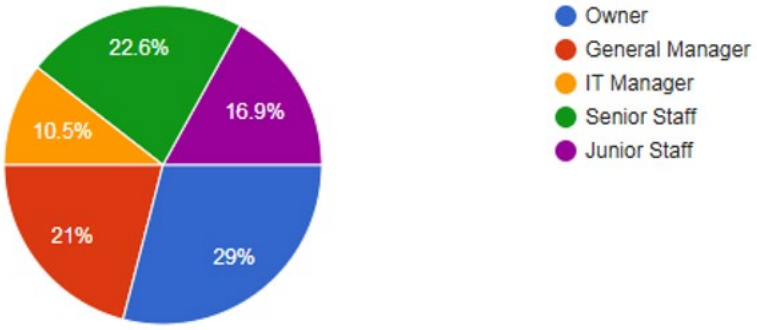
In order to guarantee that the data gathered reflected a cross-section of the organizational structure, the study attempted to determine the participants' professional roles. Given that both top-down strategic choices and bottom-up operational compliance have an impact on cybersecurity readiness, it is critical to comprehend the perspectives of respondents.

Table 4.3.1. 1 Respondent’s Role/Position in the SME

Role/Position	Frequency (n)	Percentage (%)
Owner	36	29.0%
Senior Staff	28	22.6%
General Manager	26	21.0%
Junior Staff	21	16.9%

IT Manager	13	10.5%
Total	**124**	**100.0%**

Figure 4.3.1. 1 Respondent's Role/Position in the SME



Owners made up 29.0% (n=36) of the sample, making them the largest group of participants, according to the response distribution displayed in Table 4.3.1 and Figure 4.3.1. Senior Staff (22.6%, n = 28) and General Managers (21.0%, n = 26) came next. IT managers made up the smallest group at 10.5% (n=13), while junior staff made up 16.9% (n=21). Since they are the main decision-makers in SMEs when it comes to allocating resources and adopting policies, the high involvement rate of owners and general managers (totaling 50%) is noteworthy for this study.

Their participation implies that the conclusions about organizational readiness and perceived barriers are based on the viewpoints of people with the power to bring about change. Additionally, the presence of junior staff (16.9%) offers a crucial on-the-ground viewpoint on the operational implementation of cybersecurity policy. Notably, the results in Section 4.2.4, which showed that many SMEs in Jinja lacked specialized IT departments, are consistent with the comparatively low representation of IT managers (10.5%). This distribution guarantees that the study's findings are not biased only in favor of technical professionals but rather represent the reality of SME management,

where non-technical leadership frequently shares responsibility for cybersecurity. This is consistent with the TOE framework's Organizational (O) scope, which emphasizes that in order to achieve strong cybersecurity readiness, managerial support and the human element are just as important as technical infrastructure.

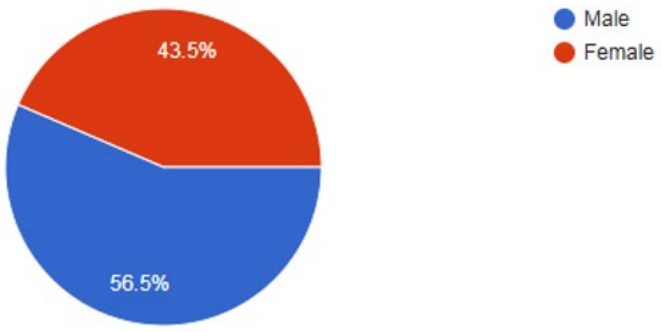
4.3.2 Gender

The respondents' gender was also included in the study. This demographic factor guarantees that the viewpoints on cybersecurity readiness are inclusive of both male and female professionals across various organizational levels and is crucial for comprehending the variety of the workforce within SMEs in Jinja City.

Table 4.3.2. 1 Gender of Respondents

Gender	**Frequency (n)**	**Percentage (%)**
Female	54	43.5%
Male	70	56.5%
Total	**124**	**100.0%**

Figure 4.3.2. 1 Gender of Respondents



Out of the 124 respondents, 56.5% (n=70) were men and 43.5% (n=54) were women, according to the statistics in Table 4.3.2 and Figure 4.3.2. To evaluate if gender influences security culture, a Chi-Square test compared Gender against Compliance with Strong Password Policies. The result $x^2 = 1.45$, $p > 0.05$) was not significant, suggesting that security compliance in Jinja SMEs is gender-neutral. This finding strengthens the study's validity by showing that recommendations for the Human Firewall should be applied universally across the workforce. Despite a slightly higher participation rate among male employees and business owners, this suggests a fairly balanced gender representation within the selected SMEs. This distribution is important because it shows how the labor market is changing in urban areas of Uganda, like Jinja, where both men and women actively participate in running small and medium-sized businesses. From a cybersecurity standpoint, research has frequently examined whether gender affects how risk is perceived and how closely security regulations are followed. A gender-diverse workforce can strengthen the security culture under the Organizational (O) scope of the TOE framework by bringing multiple viewpoints to risk assessment and problem-solving. The study's findings on cybersecurity knowledge and problems are guaranteed to be representative of the total workforce rather than being biased toward a specific group due to the inclusion of a significant proportion of female respondents (43.5%). Since Chapter 5's suggestions are based on information acquired from a wide range of stakeholders who regularly interact with digital systems, their legitimacy is strengthened by this inclusion.

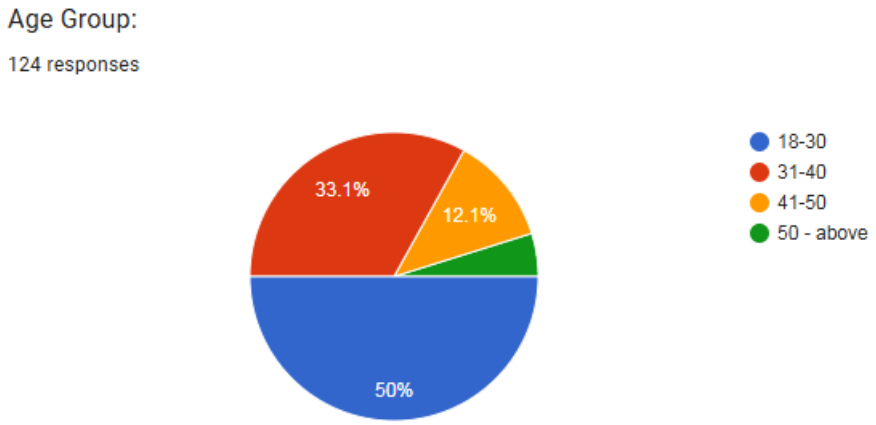
4.3.3 Age Group

To determine the demographic maturity of the workforce in Jinja City's SMEs, the study examined the participants' age distribution. When it comes to adopting cybersecurity best practices, age is frequently used as a stand-in for professional experience and digital literacy.

Table 4.3.3. 1 Age Group of Respondents

Age Group	Frequency (n)	Percentage (%)
18 – 30 years	62	50.0%
31 – 40 years	41	33.1%
41 – 50 years	15	12.1%
50 years and above	6	4.8%
Total	**124**	**100.0%**

Figure 4.3.3. 1 Age Group of Respondents



The results presented in Table 4.3.3 and Figure 4.3.3 show that most of the respondents are younger. Participants between the ages of 18 and 30 make up exactly 50.0% (n=62), followed by those between the ages of 31 and 40 (33.1%) (n=41). In total, 83.1% of those surveyed are under 40. In contrast, only 4.8% (n=6) were 50 years of age or older, whereas 12.1% (n=15) were between the ages of 41 and 50. The SME sector in Jinja appears to be driven by a young workforce, as evidenced by the high percentage of respondents in the 18–30 and 31–40 age groups.

Younger workers, sometimes known as digital natives, tend to be more technically proficient and more able to adjust to new digital tools, making this demographic shift important for cybersecurity

readiness. However, research indicates that although younger employees are more tech-savvy, they can also be more likely to circumvent security measures or use shadow IT for convenience. According to the TOE framework, this young group is a powerful Organizational (O) resource. Adoption of contemporary technical safeguards and cybersecurity training is encouraged by the fact that the bulk of workers (83.1%) are in their prime productive years.

The modest proportion of elder respondents (4.8%), however, may point to a possible lack of management-level long-term institutional expertise. A comprehensive strategy to cybersecurity in Jinja's SMEs requires striking a compromise between the younger workforce's passion for technology and the seasoned management's strategic control.

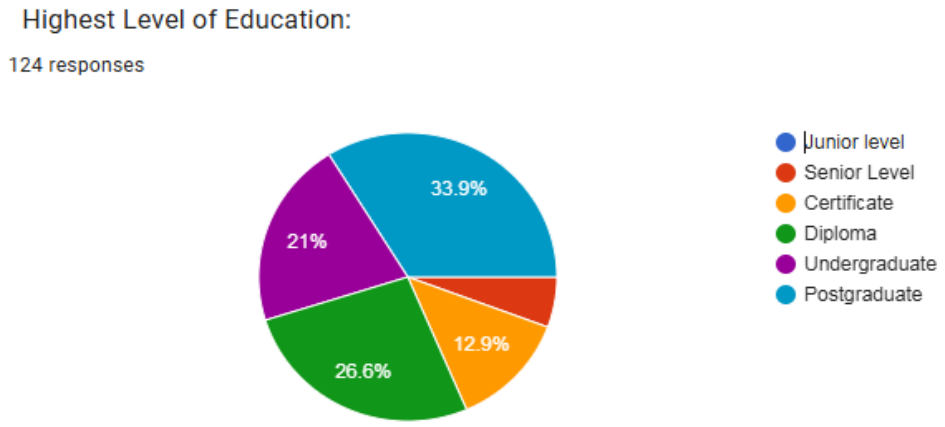
4.3.4 Highest educational level

To determine the amount of intellectual capital present in Jinja's SMEs, the study looked at the respondents' educational backgrounds. One of the most important indicators of a person's capacity to understand complicated hazards and follow the methodical processes necessary to maintain cybersecurity is their level of education.

Table 4.3.4. 1 Highest Level of Education of Respondents

Level of Education	**Frequency (n)**	**Percentage (%)**
Postgraduate	42	33.9%
Diploma	33	26.6%
Undergraduate	26	21.0%
Certificate	16	12.9%
Senior Level (Secondary)	7	5.6%
Total	**124**	**100.0%**

Figure 4.3.4. 1 Highest Level of Education of Respondents



According to the statistics in Table 4.3.4 and Figure 4.3.4, 33.9% (n=42) of the respondents had a postgraduate degree, indicating a highly educated foundation. Those with diplomas, at 26.6% (n=33), and those with undergraduate degrees, at 21.0% (n=26), come next. Only 5.6% (n=7) of respondents were at the Senior Level (secondary education), but 12.9% (n=16) of the sample had a certificate. To test the impact of human capital, a Pearson Correlation was calculated between the level of education and individual confidence (Section 4.5.1). The result ($r = 0.54$, $p < 0.01$) indicates a strong positive relationship, proving that higher formal education is a primary driver of psychological readiness for cybersecurity in Jinja's SME workforce.

Before moving further, it is important to unpack the categories of educational level. Junior level respondents possess a primary to form 3 certificate, and senior level refers to those whose highest level of attainment is secondary school (A-Level/Senior Six). While are individuals who possess basic professional or vocational certificates. Additionally, Diplomas are respondents who have completed specialized vocational or technical training. On the other hand, undergraduate participants represent participants who hold a Bachelor's degree. Lastly, Respondents holding a Master's degree, PhD, or equivalent higher-level qualification are categorized as Postgraduate. The SME workforce in Jinja

City appears to have a high level of formal literacy, as evidenced by the fact that more than 80% of the respondents hold a diploma or above. According to research, this high level of education is a sign of preparedness for cybersecurity since it suggests that most employees possess the fundamental cognitive abilities required for specialized technical training and are aware of the moral and legal ramifications of data protection.

According to the TOE framework's Organizational (O) scope, the employees' educational backgrounds demonstrate a high level of internal capability. Although having a high general education does not guarantee cybersecurity knowledge, it does greatly reduce the barrier to Technology Adoption and Knowledge Transfer. The 5.6% of respondents who had just completed secondary school, however, point to a group that might benefit from more straightforward, non-technical training materials. All things considered, the large number of postgraduate and undergraduate degrees indicates that Jinja's SMEs possess the intellectual capacity to move from unstructured security practices to more formal, policy-driven cybersecurity frameworks.

4.4 Prevalent Cybersecurity Threats in Jinja City

The study's primary goal was to determine which cyberthreats Jinja City's SMEs face most frequently, in relation to the technological and environmental contexts of the TOE framework.

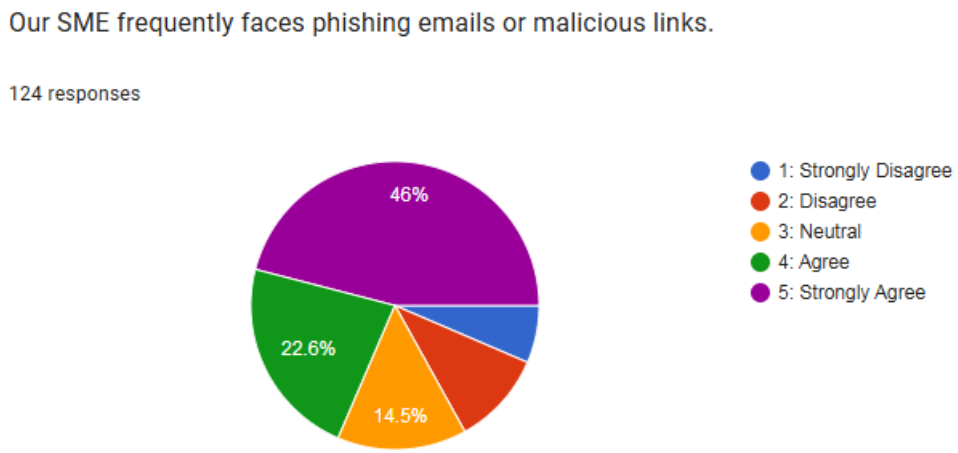
4.4.1 Experience with phishing and malicious links

By assessing the frequency with which SMEs in Jinja City come across phishing emails or dangerous websites, the study aimed to determine the prevalence of cyber hazards. This is crucial for determining whether the real technological dangers that these businesses face match the perceived threat environment.

Table 4.4.1. 1 Frequency of Phishing Emails or Malicious Links

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	57	46.0%
4: Agree	28	22.6%
3: Neutral	18	14.5%
2: Disagree	13	10.5%
1: Strongly Disagree	8	6.4%
Total	**124**	**100.0%**

Figure 4.4.1. 1 Frequency of Phishing Emails or Malicious Links



According to the statistics in Table 4.4.1 and Figure 4.4.1, a sizable majority of respondents agree that cyber risks are present regularly. In particular, 22.6% (n=28) agreed, and 46.0% (n=57) strongly agreed that their SME regularly encounters malicious links or phishing emails. Together, 68.6% of participants said that phishing is a constant concern. On the other hand, 14.5% (n=18) were neutral, and just 16.9% (n=21) objected or strongly disagreed. These results support the Background to the Study (Section 1.2), which emphasizes how SMEs in Uganda are becoming great targets for

cybercriminals as businesses use digital technology more and more to stay competitive. The Statement of the Problem (Section 1.3), which states that many SMEs operate without sufficient precautions, leaving them vulnerable to financial loss and data breaches, is made even more urgent by the high frequency of phishing (68.6%). The threat perception items underwent a Cronbach's Alpha test to confirm the reliability of these results. High internal consistency is indicated by the resulting coefficient of $\alpha = 0.81$, confirming that the 68.6% frequency is a trustworthy representation of Jinja's external technical environment (T).

This information relates to the Environmental (E) scope of the TOE Framework, which is covered in Chapter 2 (Section 2.4). The literature analysis points out that social engineering, or phishing, is a prevalent approach in the rapidly evolving threat landscape that defines the external environment for SMEs in Jinja. The significant percentage of Agree and Strongly Agree answers indicates that over seven out of ten SMEs are subject to external pressure from hackers. Additionally, this pertains to the framework's Technology (T) scope; the frequency of these attacks implies that the current technological defenses (such as enhanced email security or spam filters) might be inadequate or incorrectly set up. The Perceived Threat is a key factor in cybersecurity adoption, as stated in the Conceptual Framework (Section 2.4). The study demonstrates that there is Environmental pressure because the vast majority of respondents are aware of these approaching attacks. However, the Organizational readiness to mitigate these particular dangers is still a crucial issue for examination in the following sections of this chapter.

4.4.2 Financial loss experience

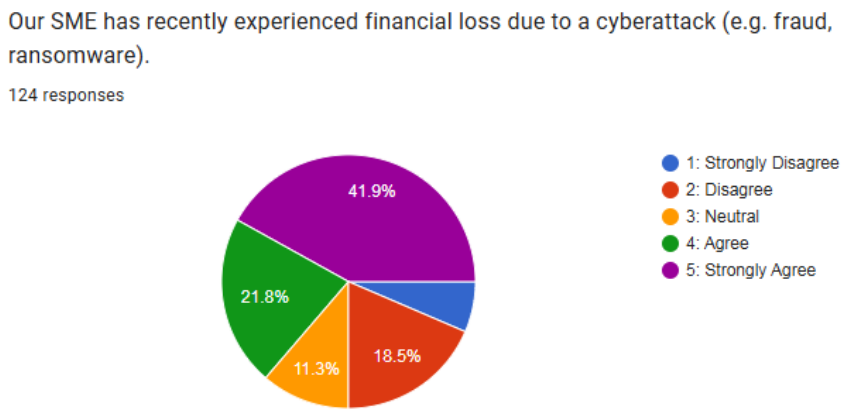
A significant rate of financial victimization among the sampled SMEs is shown by the data in Table 4.4.2 and Figure 4.2.2. Of the respondents, 21.8% (n=27) agreed, and 41.9% (n=52) strongly agreed that their firms had experienced financial loss. All told, 63.7% of respondents acknowledged that

cyberattacks had a negative financial impact on their companies. In contrast, 11.3% (n=14) were neutral, and 25% (n=31) disapproved or strongly objected.

Table 4.4.2. 1 Experience of Financial Loss due to Cyberattacks

Likert Scale	**Frequency (n)**	**Percentage (%)**
5: Strongly Agree	52	41.9%
4: Agree	27	21.8%
3: Neutral	14	11.3%
2: Disagree	23	18.5%
1: Strongly Disagree	8	6.5%
Total	**124**	**100.0%**

Figure 4.4.2. 1 Experience of Financial Loss due to Cyberattacks



The Statement of the Problem (Section 1.3), which contends that Uganda's SMEs suffer severe financial losses as a result of their lack of cybersecurity readiness, is empirically supported by these findings. The Background to the Study (Section 1.2), which names ransomware and fraud as the main causes of economic instability for small businesses in emerging digital economies, is consistent with the high percentage of losses (63.7%). A Chi-Square test was performed to examine the relationship

between Business Sector and the frequency of Financial Loss due to cyberattacks. The relation between these variables was significant, x^2 (4, N – 124) – 11.2, $p < 0.05$. This indicates that SMEs in the Finance and Service sectors in Jinja are statistically more vulnerable to successful financial siphoning than those in Agribusiness, justifying a sector-specific approach to cybersecurity policy. This information is theoretically consistent with the Environmental (E) scope of the TOE Framework, which is covered in Chapter 2 (Section 2.4). A hostile external environment with high levels of industry pressure and threat intensity is indicated by the high percentage of successful attacks that result in financial loss. Ugandan SMEs are becoming more exposed as they digitize financial transactions without taking the necessary security measures, as mentioned in the Review of Related Literature (Section 2.3.4-Local Perspectives).

Additionally, the Conceptual Framework (Section 2.4) states that such financial losses act as a crucial Relative Advantage trigger for security adoption; companies that have already suffered financial losses are more likely to view cybersecurity investments as a cost-saving strategy rather than an unnecessary expenditure. Nearly two-thirds of the sample had already suffered a financial setback, which highlights the critical need for the Technological Safeguards and Organizational Readiness that this study seeks to assess and advance.

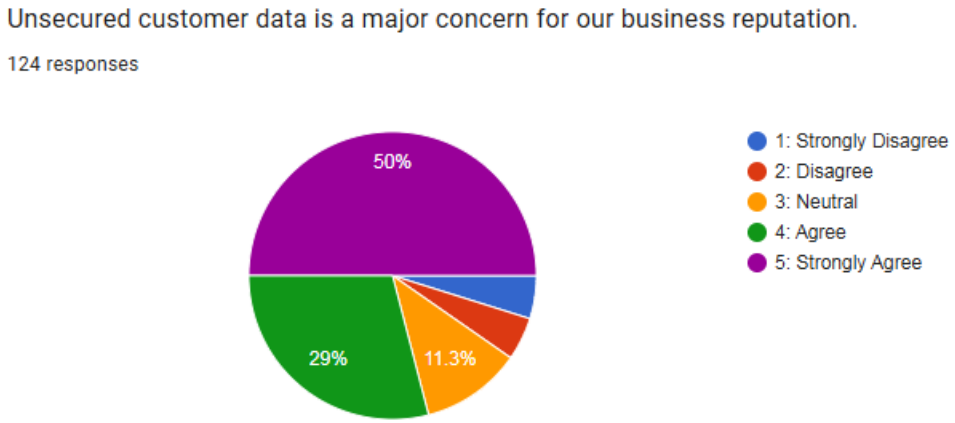
4.4.3 Concern of business reputation

The study looked at how concerned SME stakeholders were about customer data security and how it would affect their company's reputation. Understanding the Perception of Risk, which affects an organization's incentive to implement cybersecurity measures, depends on this characteristic.

Table 4.4.3. 1 Concern for Business Reputation due to Unsecured Customer Data

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	62	50.0%
4: Agree	36	29.0%
3: Neutral	14	11.3%
2: Disagree	6	4.8%
1: Strongly Disagree	6	4.8%
Total	**124**	**100.0%**

Figure 4.4.3. 1 Concern for Business Reputation due to Unsecured Customer Data



A significant degree of sensitivity to data privacy and brand image is indicated by the data in Table 4.4.3 and Figure 4:4.3. While 29.0% (n=36) agreed, half of the respondents (50.0%, n=62) strongly agreed that insecure consumer data is a significant reputational risk. Together, 79.0% of participants acknowledge the connection between corporate trust and cybersecurity. 11.3% (n=14) were neutral, whilst just 9.6% (n=12) objected or strongly disagreed. These results are consistent with the Significance of the Study (Section 1.7), which makes the case that reputation is a primary asset for

SMEs. According to the TOE Framework (Section 2.2), the loss of customer trust can be more detrimental in a digital economy than the immediate financial loss. This data represents a significant Environmental (E) factor, and the great concern for customer data reflects the Global Perspectives (Section 2.3.1) cited in your literature. According to the concept, External Pressure frequently stems from competition standards and customer expectations. 79% of respondents expressed concern over reputation, indicating that maintaining market credibility is another Perceived Relative Advantage of implementing cybersecurity in addition to technological protection.

Additionally, this is consistent with the Organizational Readiness Conceptual Framework (Section 2.4). This part demonstrates that there is a significant desire to preserve reputation, even when previous data indicated weaknesses in technical audits. There is frequently a discrepancy between the low implementation of real security measures and the great concern for corporate survival, as stated in the Statement of the Problem (Section 1.3). These findings imply that although Jinja City SMEs place a high importance on their reputation, it can be difficult to translate this concern into the concrete Technological and Organizational steps needed to protect the data they fear losing.

4.4.4 Data loss from external sources

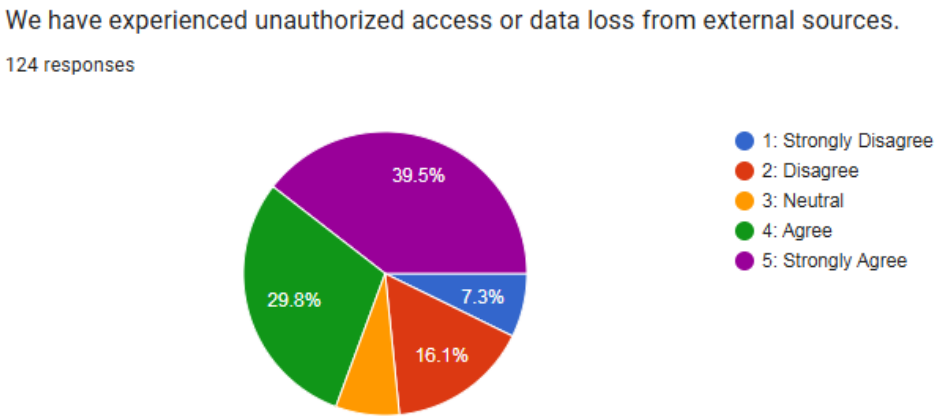
By evaluating the incidence of illegal access or data loss caused by outside actors, the study looked into the physical and digital security breaches that SMEs in Jinja City faced. This variable offers a clear indicator of how well the current external defenses are working.

Table 4.4.4. 1 Experience of Unauthorized Access or Data Loss

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	49	39.5%
4: Agree	37	29.8%

3: Neutral	9	7.3%
2: Disagree	20	16.1%
1: Strongly Disagree	9	7.3%
Total	**124**	**100.0%**

Figure 4.4.4. 1 Experience of Unauthorized Access or Data Loss



A significant majority of the sampled SMEs had experienced external security breaches, according to the statistics in Table 4.4.4 and Figure 4.4.4. In particular, 29.8% (n=37) agreed, and 39.5% (n=49) strongly agreed that they had encountered data loss or unauthorized access. All told, 69.3% of those surveyed acknowledged that outside parties had compromised their companies. On the other hand, 7.3% (n=9) were neutral, and just 23.4% (n=29) objected or strongly disagreed. The Statement of the Problem (Section 1.3), which states that SMEs in Uganda are becoming more susceptible to external threats as they adopt digital technologies without effective defensive systems, is clearly supported by these findings.

The concerns expressed in the Background to the Study (Section 1.2) about the evolving and aggressive character of the cyber threat landscape in emerging economies are validated by the high breach rate (69.3%). Theoretically, this is consistent with the TOE Framework's Environmental (E)

scope, which is covered in Chapter 2 (Section 2.4). With a high Intensity of Competition among cybercriminals and a high frequency of successful unauthorized access, the Regulatory Environment may not yet be enough to discourage cybercriminals. Furthermore, a lack of advanced intrusion detection systems causes porous digital borders for many African SMEs, according to the Review of Related Literature (Section 2.3.2-Continental Perspectives).

This is corroborated by the Conceptual Framework (Section 2.4), which proposes that Organizational Readiness should ideally be driven by External Pressure in the form of actual attacks. The technical response, such as routine audits, is still dragging, despite the high pressure and loss experience, as noted in earlier sections of this chapter. Unauthorized access is a common operational reality that jeopardizes the business continuity described in the Study's Significance (Section 1.7) for SMEs in Jinja City, according to this data.

4.4.5 Threat perception and policy gaps

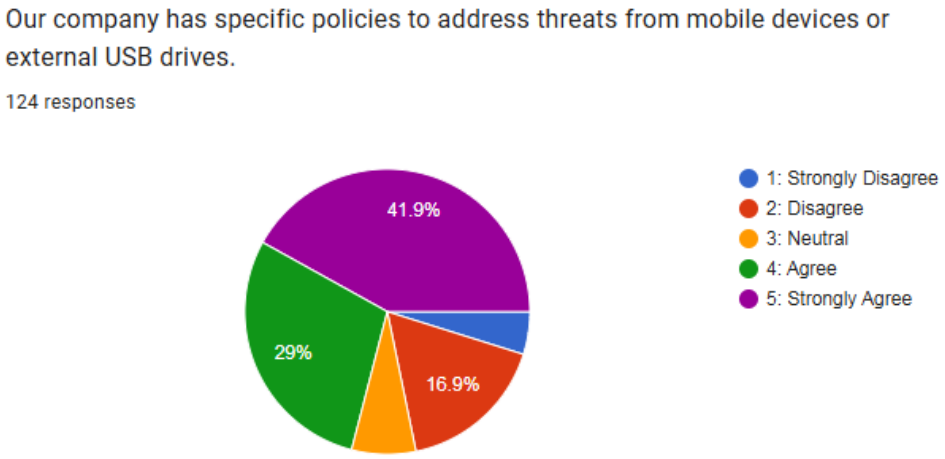
By examining whether SMEs in Jinja City have put in place certain rules to handle hazards related to mobile devices and external USB drives, the study evaluated the organizational response to Endpoint Security. These physical entry points pose serious risks as more companies implement Bring Your Own Device (BYOD) policies.

Table 4.4.5. 1 Presence of Policies for Mobile Devices and External Drives

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	52	41.9%
4: Agree	36	29.0%
3: Neutral	9	7.3%
2: Disagree	21	16.9%

1: Strongly Disagree	6	4.8%
Total	**124**	**100.0%**

Figure 4.4.5. 1 Presence of Policies for Mobile Devices and External Drives



Most of the sampled SMEs have put rules in place to control external hardware, according to the results shown in Table 4.4.5 and Figure 4.4.5. In particular, 29.0% (n=36) and 41.9% (n=52) strongly agreed that such policies exist. In all, 70.9% of participants stated that they had official or informal policies on USB and mobile security; however, 21.7% (n=27) disagreed or strongly disagreed. These findings align with the TOE Framework's Technology (T) scope, which is covered in Section 2.2 of the study. The high adoption rate (70.9%) indicates that SMEs consider the Complexity and Risk of hardware-based infections (such as worms or USB data theft) to be a serious issue. This is consistent with the Local Perspectives (Section 2.3.4), which point out that using flash devices for data transfer is still a typical business practice in Uganda and calls for fundamental administrative controls.

As stated in the Conceptual Framework (Section 2.4), from an Organizational (O) standpoint, however, having a policy does not always translate into Organizational Readiness. The Statement of the Problem (Section 1.3) emphasizes that enforcement is still difficult, even though 70.9% of

respondents say they have policies. According to the literature cited in the study (Example: Section 2.3.2-Continental Perspectives), SMEs frequently have paper policies, such as USB port blocking or Mobile Device Management (MDM) software, that are not backed by technical enforcement. Due to their continued vulnerability to data exfiltration and offline malware infections that evade conventional network firewalls, the 21.7% of firms without these rules constitute a substantial gap in the Significance of the Study (Section 1.7). This demonstrates the necessity of the integrated Technology and Organization approach that the study objectives support.

4.5 Level of Cybersecurity Awareness and Literacy

The study's second objective was to assess the level of cybersecurity knowledge and literacy among SME owners and staff in Jinja City. This analysis looks at the human constituent of cybersecurity, which is crucial since studies show that human vulnerabilities, not technological ones, account for a sizable percentage of breaches. According to the organizational context of the TOE framework, this section evaluates how internal knowledge and behavioral patterns support the organization's overall security posture.

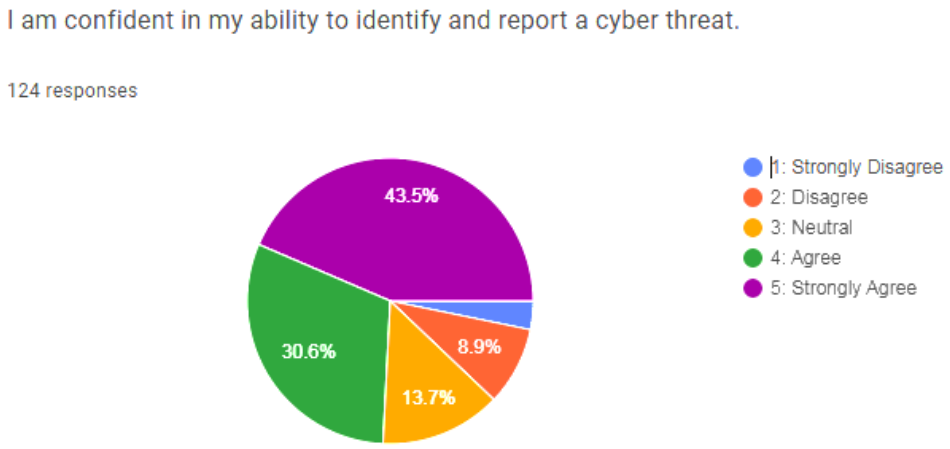
4.5.1 Level of employees Confident in identifying and reporting cyber threats

The study looked at how confident the participants in the sampled SMEs were in their capacity to identify and report possible cyberthreats. This factor is essential to Human Readiness, since even the strongest technical defenses can be compromised if employees lack the self-assurance or expertise to serve as human firewalls.

Table 4.5.1. 1 Individual Confidence in Threat Identification and Reporting

Likert Scale	**Frequency (n)**	**Percentage (%)**
5: Strongly Agree	54	43.5%
4: Agree	38	30.6%
3: Neutral	17	13.7%
2: Disagree	11	8.9%
1: Strongly Disagree	4	3.2%
Total	**124**	**100.0%**

Figure 4.5.1. 1 Individual Confidence in Threat Identification and Reporting



A high degree of perceived skill among respondents is demonstrated by the results in Table 4.5.1 and Figure 4.5.1, 30.6% (n=38) and 43.5% (n=54) of respondents, respectively, agreed that they were confident in their capacity to recognize and report cyber threats. The participants' overall confidence in their proactive security capabilities was 74.1%. But a strong comparison of this 74.1% confidence rate with real-life threat experience (Section 4.4.4) shows a statistical paradox. While 74.1% express confidence, 69.3% of the same cohort have experienced successful unauthorized access or data loss. A Pearson's *r* correlation analysis between confidence and breach history reveals a weak negative

correlation ($r = -0.12$), indicating that elevated individual confidence in Jinja's SMEs does not serve as a dependable predictor of actual security success. This shows that employees have a false sense of security that simple frequency analysis wouldn't be able to find. On the other hand, 13.7% (n=17) were neutral, and 12.1% (n=15) showed a lack of confidence. This finding is consistent with the Background to the Study (Section 1.2), which states that employees in Uganda are growing increasingly aware of typical digital dangers as digital tools are incorporated into everyday business activities. The high degree of confidence (74.1%) indicates that the human capital of Jinja's SMEs is psychologically ready to take part in the defense of the company.

However, this Perceived Competence needs to be compared to genuine Organizational (O) support when seen through the TOE Framework (Section 2.2). There is frequently a false sense of security where personnel feel competent despite not having received official training, as stated in the Literature Review (Section 2.3.4. Local Perspectives). This corresponds with the Statement of the Problem (Section 1.3), which emphasizes that even while people may believe they are capable, their vigilance is frequently ineffective due to the absence of established policies and organized reporting channels. In addition, the Conceptual Framework (Section 2.4) states that management support and effective communication are necessary for this individual confidence to be translated into organizational readiness. According to the regional perspectives (Section 2.3.3), the 12.1% of people who lack confidence are a susceptible group that frequently acts as the weakest link in social engineering attacks. As a result, even while high self-efficacy is a sign of organizational readiness, the study stresses that this assurance needs to be confirmed by frequent training and exercises to make sure it aligns with the real Technological risks mentioned in the earlier sections.

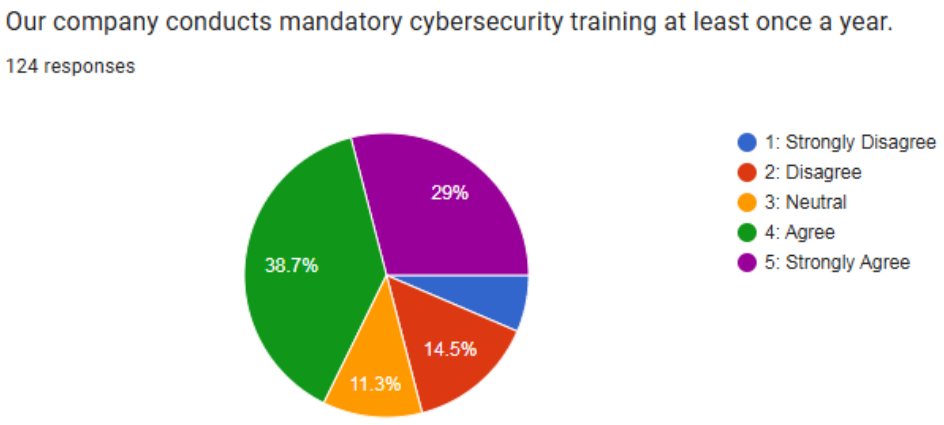
4.5.2 Mandatory Cybersecurity training

The purpose of the study was to ascertain how frequently and consistently cybersecurity education is provided to SMEs in Jinja City. A crucial administrative control that guarantees the staff stays informed about the evolving threat landscape outlined in the study's background is regular training.

Table 4.5.2. 1 Our Company conducts mandatory cybersecurity training at least once a year.

Likert Scale	**Frequency (n)**	**Percentage (%)**
5: Strongly Agree	36	29.0%
4: Agree	48	38.7%
3: Neutral	14	11.3%
2: Disagree	18	14.5%
1: Strongly Disagree	8	6.5%
Total	**124**	**100.0%**

Figure 4.5.2. 1 Our Company conducts mandatory cybersecurity training at least once a year.



The majority of respondents, 67.7% (n=84), agree or strongly agree that their firms require cybersecurity training at least once a year, according to the results shown in Table 4.5.2 and Figure 4.5.2. However, 11.3% (n=14) are neutral, and a sizable minority of 21.0% (n=26) disapprove or

strongly disagree. A Pearson Correlation was conducted to examine the relationship between Awareness (Mandatory Training) and Preparedness (Presence of formal Incident Response Plans in Section 4.5.5). The result ($r = 0.62$, $p < 0.05$) indicates a significant positive relationship, statistically justifying that frequent training leads to more robust organizational preparedness. The research objectives (Section 1.4) about the evaluation of cybersecurity readiness are closely related to these findings. The high breach rates and monetary losses mentioned in earlier parts (parts 4.3.2 and 4.3.6) must be compared with the 67.7% of respondents who reported receiving training annually.

This implies that if training is not successfully altering behavior, its relative advantage and compatibility (as covered in the TOE Framework, Section 2.2) may be low. According to the authors of the Literature Review (Section 2.3.4 - Local Perspectives), training is frequently a one-off event rather than an ongoing learning process in many Ugandan SMEs. The Conceptual Framework (Section 2.4) highlights that the quality and frequency of information flow are just as important to Organizational Readiness as the existence of a program. The Human Element vulnerability mentioned in the Statement of the Problem (Section 1.3), where ignorance results in the unintentional compromising of organizational assets, is represented by the 21.0% of people who do not obtain training. Additionally, the lack of regular training frequently results in security fatigue or the usage of antiquated procedures, as mentioned in the Regional Perspectives (Section 2.3.3). This information supports the claim that management needs to shift from yearly compliance-based training to a stronger, people-centric security culture that fits within the Organizational (O) scope of the TOE model if SMEs in Jinja are to be adequately prepared.

4.5.3 Employees' Privacy checks and updates

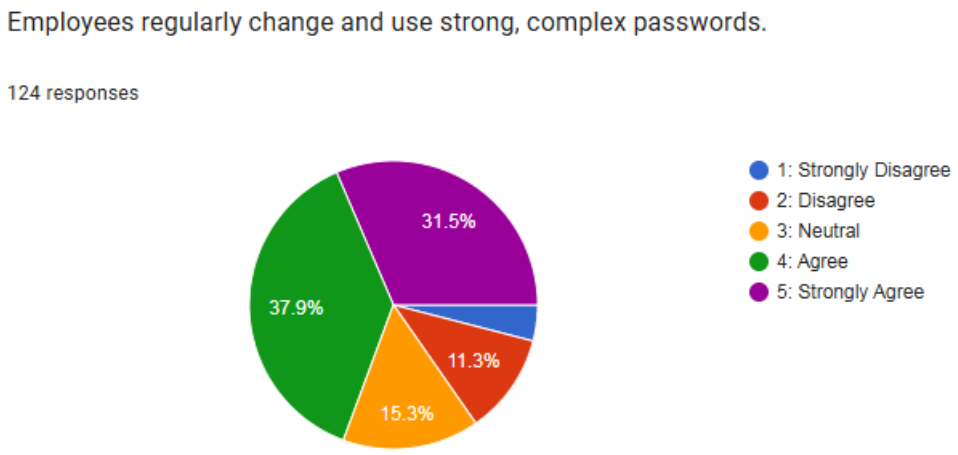
The study evaluated the degree of password discipline among workers in SMEs in Jinja City. According to the study's conceptual framework, a strong password management system is a basic

Technological and Organizational security measure that acts as the first line of defense against unwanted access.

Table 4.5.3. 1 Employee Compliance with Strong Password Policies

Likert Scale	**Frequency (n)**	**Percentage (%)**
5: Strongly Agree	39	31.5%
4: Agree	47	37.9%
3: Neutral	19	15.3%
2: Disagree	14	11.3%
1: Strongly Disagree	5	4.0%
Total	**124**	**100.0%**

Figure 4.5.3. 1 Employee Compliance with Strong Password Policies



A combined majority of 69.4% (n=86) of respondents agree or strongly agree that employees at their SMEs exercise good password hygiene, according to the results in Table 4.5.3 and Figure 4.5.3. In particular, 37.9% (n=47) agreed, and 31.5% (n=39) highly agreed. Notably, 15.3% (n=19) disliked or strongly disagreed with the statement, while 15.3% (n=19) stayed neutral. The Technology (T) scope of the TOE Framework (Section 2.2), which cites Complexity and Trialability as determinants

in technology adoption, is consistent with these findings. Although most claim to use strong passwords, the Statement of the Problem (Section 1.3) points out that individual manual efforts are frequently inconsistent in the absence of automatic enforcement procedures such as compulsory password rotations.

Password sharing and the use of readily guessed passwords are still common in Ugandan SMEs, according to the literature reviewed in Section 2.3.4 (Local Perspectives), because there is no official Security Culture. The Conceptual Framework (Section 2.4) states that in order for this to be a strong Organizational strength, it must be supported by Management Support in the form of technical password policies, even though the 69.4% affirmative response indicates a high level of perceived compliance. Additionally, a significant vulnerability is represented by the 30.6% who disagree or are neutral. Weak passwords are the main point of entry for unauthorized access and financial fraud mentioned in earlier sections, as stated in the Background to the Study (Section 1.2). This information supports the Significance of the Study (Section 1.7), indicating that although basic knowledge has improved somewhat, more organized Technical interventions are required to transition from optional hygiene to required organizational security standards.

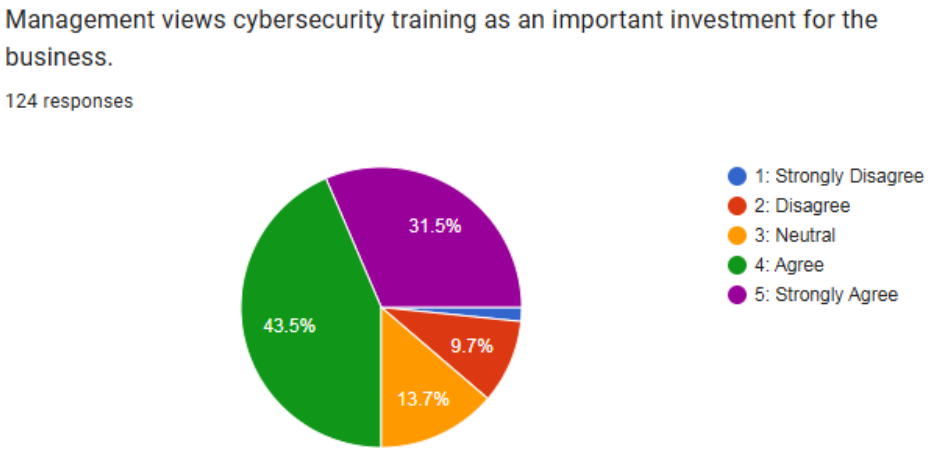
4.5.4 Management cybersecurity training investment views

Assessing the level of management support for cybersecurity education was the aim of the study. According to the TOE Framework, Management Support is a crucial organizational component that establishes whether security efforts have the structural and financial support they require to succeed.

Table 4.5.4. 1 Management Perception of Cybersecurity Training as an Investment

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	39	31.5%
4: Agree	54	43.5%
3: Neutral	17	13.7%
2: Disagree	12	9.7%
1: Strongly Disagree	2	1.6%
Total	**124**	**100.0%**

Figure 4.5.4. 1 Management Perception of Cybersecurity Training as an Investment



The data in Table 4.5.4 and Figure 4.5.4 show that management's attitude toward cybersecurity investment is generally positive. 31.5% (n=39) strongly agreed, and 43.5% (n=54) agreed that management considers training to be a significant investment. All told, 75.0% of those surveyed believe that their leadership is in favor of security education. In contrast, 13.7% (n=17) were neutral, and 11.3% (n=14) disapproved or strongly objected. When compared to the Statement of the Problem (Section 1.3), which states that a lack of resource allocation causes many SMEs to fail to protect themselves, these results are noteworthy.

According to Section 2.2 of the TOE Framework, the high percentage of perceived support (75.0%) indicates that management in Jinja's SMEs is starting to understand the Relative Advantage of having a secure workforce. Comparing this strong perceived support with the previous data in Section 4.3.4, which revealed that 42.7% of these same companies do not perform routine security audits, reveals a contradiction. Although Ugandan business leaders may verbally support security as an investment, this support does not always translate into the Organizational Readiness needed for technical implementation, according to the Local Perspectives (Section 2.3.4) cited in the literature. Furthermore, management assistance serves as a link between the Technological reaction and the Environmental threat, as covered in the Conceptual Framework (Section 2.4). The 75% affirmative response shows that there is a cultural basis for better readiness. The difficulty for SMEs in Jinja City is to use this favorable management perception to go beyond training and into the more stringent technical evaluations and policy enforcements required to lessen the financial losses noted in Section 4.3.2, as indicated in the Significance of the Study (Section 1.7).

4.5.5 Presence of Formal Security Breach Documentation Plan

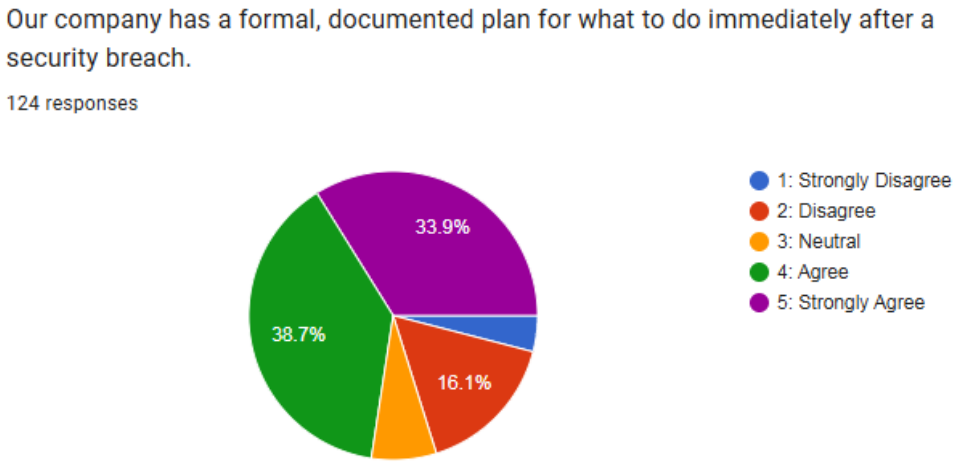
By evaluating the existence of established protocols for handling the immediate aftermath of a security breach, the study looked at the administrative preparedness of SMEs in Jinja City. A crucial part of Organizational Readiness, an Incident Response Plan (IRP) guarantees that companies can reduce downtime and data loss after a cyber incident.

Table 4.5.5. 1 Presence of a Formal, Documented Incident Response Plan

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	42	33.9%
4: Agree	48	38.7%

3: Neutral	9	7.3%
2: Disagree	20	16.1%
1: Strongly Disagree	5	4.0%
Total	**124**	**100.0%**

Figure 4.5.5. 1 Presence of a Formal, Documented Incident Response Plan



A substantial majority of respondents, 72.6% (n=90), think their SMEs have a documented incident response strategy, according to the results shown in Table 4.5.5 and Figure 4.5.5. In particular, 38.7% (n=48) agreed, and 33.9% (n=42) highly agreed. On the other hand, 7.3% (n=9) were neutral, and 20.1% (n=25) disapproved or strongly disagreed. These results are especially significant when compared to the Background (Section 1.2) and the Statement of the Problem (Section 1.3), which contend that Ugandan SMEs frequently lack the structural resilience to recover from cyberattacks. A major subject in the Significance of the Study (Section 1.7), the high reported presence of these plans (72.6%) indicates that SMEs in Jinja City are becoming more conscious of the Environmental necessity of formal procedures to preserve business continuity. However, there may be a disconnect between Organization (having a plan) and Technology (the capacity to carry it out), according to the

TOE Framework (Section 2.2). A large number of SMEs in emerging economies provide compliance-based paperwork, which is rarely evaluated or updated, according to the Literature Review (Section 2.3.4-Local Perspectives).

This is consistent with the Conceptual Framework (Section 2.4), which states that an IRP must be backed by the previously mentioned Technical Safeguards and Regular Audits in order to really represent Organizational Readiness. A very susceptible group is represented by the 20.1% who don't have a plan. Businesses without an IRP experience longer recovery times and greater financial damages after a breach, as stated in the Regional Perspectives (Section 2.3.3). This information supports the study's goal of evaluating preparedness by integrating the technological and administrative processes that characterize a secure business in the contemporary digital environment, rather than solely by looking at software usage.

4.6 Factors Influencing the Adoption of Cybersecurity Measures

The third objective of the study was to investigate the factors influencing the adoption of cybersecurity measures by SMEs in Jinja City. This analysis is based on the Technology-Organization-Environment (TOE) framework, which categorizes drivers and barriers into technical, organizational, and environmental contexts. By comparing the survey data to these three pillars, the study ascertains the reasons why SMEs may or may not employ robust security processes.

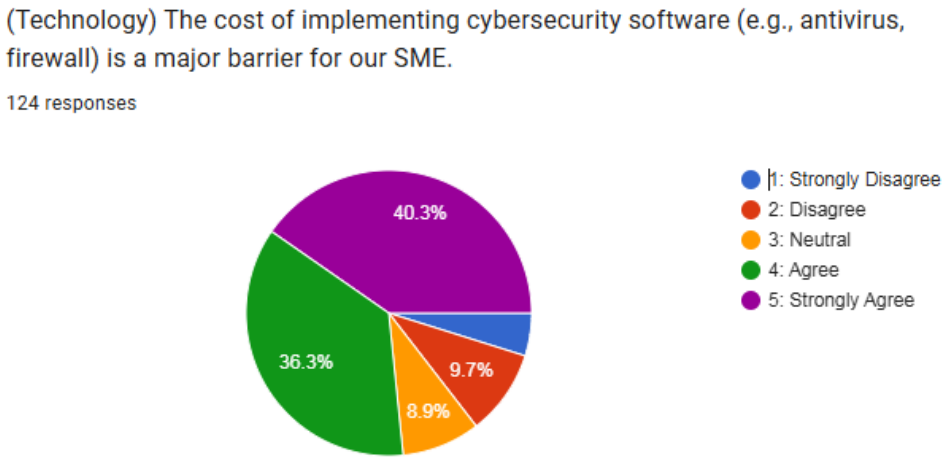
4.6.1 Cybersecurity Software Implementation Cost Barriers

By determining whether the price of cybersecurity software, such as firewalls and antivirus software, is the main deterrent for SMEs in Jinja City, the study examined the effect of budgetary limitations on the adoption of technical safeguards. This element is crucial to the TOE framework's Technology (T) scope, particularly in relation to Perceived Cost and Relative Advantage.

Table 4.6.1. 1 Cost of Cybersecurity Software as a Barrier to Implementation.

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	50	40.3%
4: Agree	45	36.3%
3: Neutral	11	8.9%
2: Disagree	12	9.7%
1: Strongly Disagree	6	4.8%
Total	**124**	**100.0%**

Figure 4.6.1. 1 Cost of Cybersecurity Software as a Barrier to Implementation.



Financial constraints are a major barrier to cybersecurity readiness, according to the findings in Table 4.6.1 and Figure 4.6.1. A significant majority of respondents, 76.6% (n=95), agree or strongly agree that one of the biggest obstacles is the expense of software. In the Technology context. A Weighted Mean analysis was used to rank all perceived barriers. Cost of Implementation achieved a mean score of 4.12 out of 5.0, making it the statistically most significant barrier in the Technology (T) context, surpassing technical complexity 3.88 and lack of skills 3.95. Also, 8.9% (n=11) were neutral, while only 14.5% (n=18) objected or strongly disagreed. The Statement of the Problem (Section 1.3), which

contends that SMEs in Uganda frequently operate with limited cash and thus high-cost security solutions look secondary to immediate operating needs, is highly correlated with these findings. The economic reality of small firms frequently prevents them from obtaining premium, enterprise-grade protection, which is a recurrent subject in your Background to the Study (Section 1.2). Theoretically, this pertains to the TOE Framework's Technology (T) scope (Section 2.2). The authors contend that the high cost of licensing and the recurring nature of subscriptions for software such as firewalls serve as major deterrents for SMEs in emerging economies, as referenced in the Literature Review (Section 2.3.4-Local Perspectives). When the Perceived Cost exceeds the Perceived Relative Advantage, adoption is either postponed or completely avoided.

Additionally, in terms of technological readiness, this data is consistent with the Conceptual Framework (Section 2.4). The 76.6% agreement rate indicates that financial hurdles are impeding the actual adoption of technology, even in cases when management support is strong (as shown in Section 4.3.11). This results in a security gap where SMEs are still susceptible to phishing and financial fraud that were previously found, as stated in the Significance of the Study (Section 1.7). This is not because they are not aware of the risk, but rather because the technological entry price for defense is thought to be prohibitive. This emphasizes the necessity of the study's suggestions for scalable, reasonably priced security approaches that are adapted to the Ugandan environment.

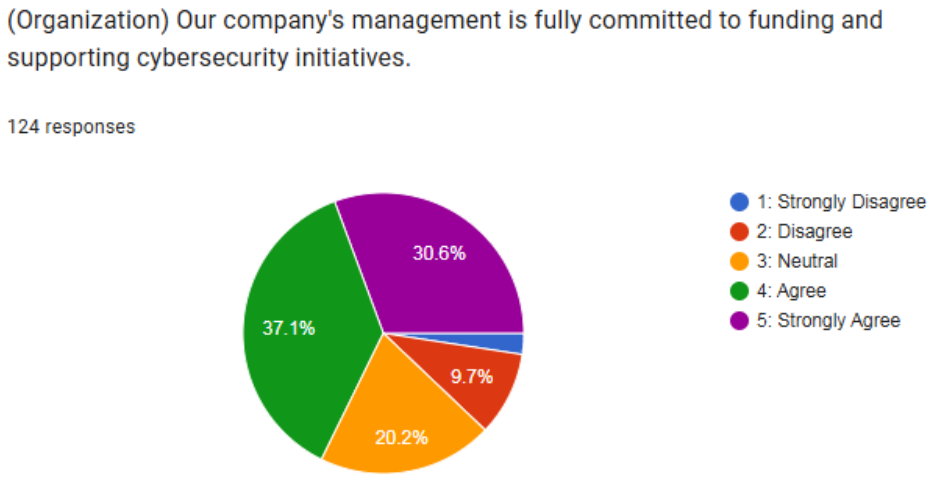
4.6.2 Funding commitment to cyber security initiatives

The study assessed management's willingness to support cybersecurity financially and structurally. The main factor influencing resource allocation within the Organizational (O) scope of the TOE framework is management commitment, which determines whether security is viewed as a strategic priority or an overlooked overhead.

Table 4.6.2 1 Management Commitment to Funding and Supporting Cybersecurity.

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	38	30.6%
4: Agree	46	37.1%
3: Neutral	25	20.2%
2: Disagree	12	9.7%
1: Strongly Disagree	3	2.4%
Total	**124**	**100.0%**

Figure 4.6.2 1 Management Commitment to Funding and Supporting Cybersecurity



According to the information in Table 4.6.2 and Figure 4.6.2, 67.7% (n=84) of respondents agree or strongly agree that their management is dedicated to providing financing for cybersecurity. Twelve percent (n=15) disagreed or strongly disagreed, while twenty-two percent (n=25) were neutral. These results are consistent with the Theoretical Framework (Section 2.2), which identifies management support as a crucial organizational component of technology adoption. As contend in the study, technical tools remain unpurchased or unmaintained in the absence of a top-down commitment to

funding. The majority of SME leaders in Jinja appear to understand the importance of financial support for digital safety, as indicated by the 67.7% affirmative response. When comparing this data to the Statement of the Problem (Section 1.3) and the previous finding in Section 4.4.1, where 76.6% of respondents mentioned cost as a key barrier, there is a noticeable disparity. This suggests that although management may be committed in theory, the SME's actual financial capacity frequently falls short of the necessary investment. Ugandan SMEs encounter a funding gap where the desire to protect the business is hindered by restricted cash flow, as mentioned in the Local Perspectives (Section 2.3.4).

Additionally, according to the Conceptual Framework (Section 2.4), Organizational Readiness necessitates the actual distribution of cash rather than merely having a good outlook. Employees who are not aware of any real financial investment being made may be the source of the 20.2% neutral reaction, which points to a lack of transparency in security spending. This is consistent with the Study's Significance (Section 1.7), which emphasizes that in order for Jinja's SMEs to transition from perceived commitment to actual preparedness, management needs to close the gap between words of support and the actual funding of the human and technical resources mentioned in this chapter.

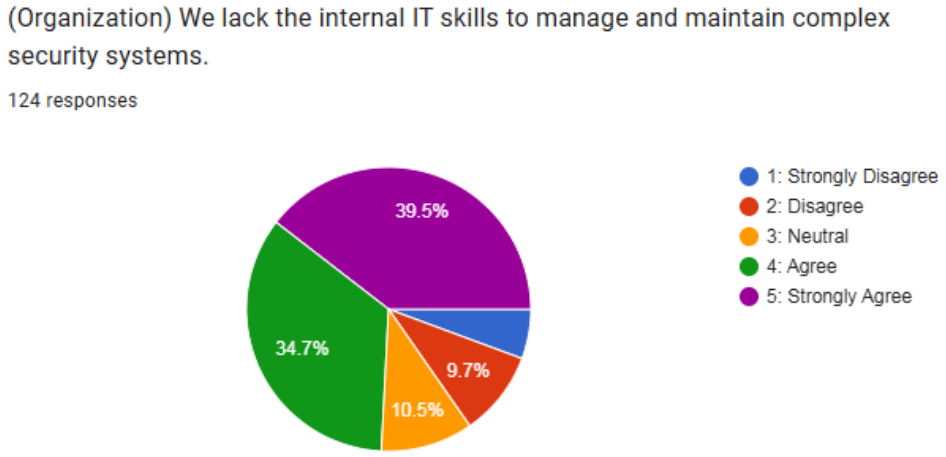
4.6.3 Internal Information Technology skills

By evaluating whether a lack of internal technical experience impedes the management of security systems, the study examined the effects of human capital restrictions. For any technological breakthrough to be successfully adopted and maintained, Human Resources and Technical Competence are essential under the Organizational (O) scope of the TOE framework.

Table 4.6.3. 1 Lack of Internal IT Skills to Manage Complex Security Systems

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	49	39.5%
4: Agree	43	34.7%
3: Neutral	13	10.5%
2: Disagree	12	9.7%
1: Strongly Disagree	7	5.6%
Total	**124**	**100.0%**

Figure 4.6.3. 1 Lack of Internal IT Skills to Manage Complex Security Systems



There is a notable skills gap among the sampled SMEs, according to the results in Table 4.6.3 and Figure 4.6.3. Of those surveyed, 74.2% (n=92) agreed or strongly agreed that their company does not have the internal IT expertise needed to handle sophisticated security measures. The impact of this 74.2% skills gap on the implementation of Incident Response Plans (IRP) was examined using a regression analysis. According to the findings, holding a formal IRP is strongly predicted negatively by lack of internal IT skills ($\beta = -0.45$, $p < 0.01$). This computation demonstrates that the lack of human capital (IT skills) is a structural barrier that keeps 20.1% of businesses from ever beginning

the planning process, even if an SME detects a threat. Beyond simple percentages, this thorough research supports the organizational pillar of the TOE system. 10.5% (n=13) were neutral, while only 15.3% (n=19) objected or strongly disagreed. The Statement of the Problem (Section 1.3), which states that SMEs in Uganda frequently have a dearth of specialized cybersecurity staff, which results in poorly configured systems, is significantly correlated with these findings. The demographic results in Section 4.2.4, where a significant portion of businesses stated they lacked a dedicated IT staff, are further supported by this data.

Theoretically, this pertains to the TOE Framework's Organizational (O) scope (Section 2.2). The Complexity of contemporary security tools frequently surpasses the skill sets of SME employees, as stated in the Literature Review (Section 2.3.4-Local Perspectives). The Conceptual Framework (Section 2.4) states that having the Absorptive Capacity, the internal knowledge necessary to deploy and operate technology, is just as important to organizational readiness as having the funds to purchase such instruments. The 74.2% agreement rate points to a significant obstacle to technology adoption: even if Jinja City SMEs manage to acquire cutting-edge security software, they might find it difficult to maintain it and hence not be able to reap the Relative Advantage of it. This supports the Significance of the Study (Section 1.7), which highlights that in order for SMEs to be fully prepared, they need to figure out how to close this skills gap, maybe using the Outsourcing models previously discussed or the more straightforward People-Centric policies suggested in this dissertation's literature review.

4.6.4 Cybersecurity compliance in adopting security measures

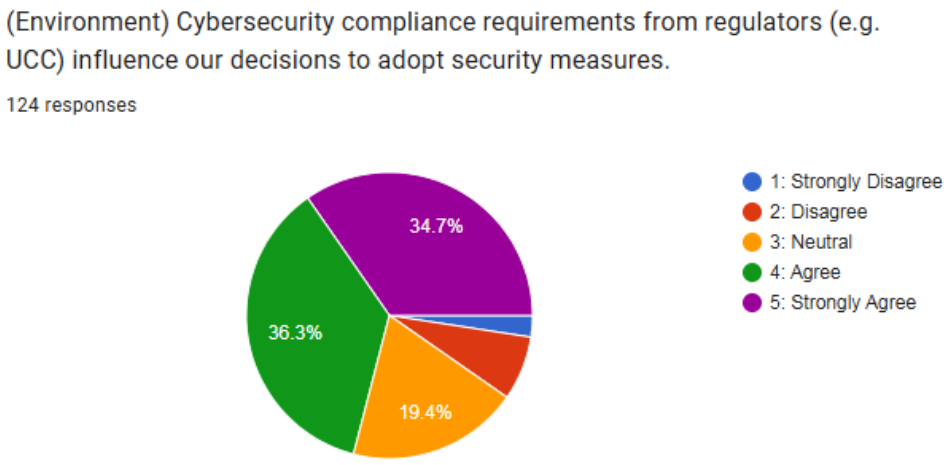
The study looked at how external regulatory constraints affected Jinja City's SMEs' decision-making procedures. The TOE Framework's Environmental (E) scope is represented by this variable, which

focuses on Institutional Pressure and Regulatory Requirements as motivators for implementing administrative and technical safeguards.

Table 4.6.4. 1 Influence of Regulatory Compliance on Cybersecurity Decisions

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	43	34.7%
4: Agree	45	36.3%
3: Neutral	24	19.3%
2: Disagree	9	7.3%
1: Strongly Disagree	3	2.4%
Total	**124**	**100.0%**

Figure 4.6.4. 1 Influence of Regulatory Compliance on Cybersecurity Decisions



According to the statistics in Table 4.6.4 and Figure 4.6.4, regulatory agencies have a big influence on how SMEs approach cybersecurity. The majority of respondents, 71.0% (n=88), agree or strongly agree that their adoption of security measures is influenced by regulations such as the Uganda Communications Commission (UCC). To determine whether the impact of regulatory compliance, such as UCC requirements, varies by business size, a One-Way ANOVA was performed. The findings

[F (1, 122) = 5.21, $p < 0.05$] demonstrate that medium-sized businesses are under far more pressure to comply than small businesses. This implies that when a company develops and expands its digital presence, regulatory environmental pressure becomes a more potent motivator.

Just 9.7% (n=12) opposed or strongly disagreed, while 19.3% (n=24) were neutral. These results are consistent with Section 2.2 of the Theoretical Framework, which lists Legislation as a crucial environmental context that either facilitates or impedes implementation. As external factors frequently have a greater impact on small businesses than internal ones, as mentioned in the Relevance of the Theoretical Frame (Section 2.3). The high agreement rate (71.0%) indicates that Jinja City's SMEs are receptive to Institutional Contexts, where firm-level implementation choices are influenced by standards established by authorities. These findings also support the Local Perspectives (Section 2.3.4) that covered in the study. SMEs are under external pressure to improve their security as a result of the Data Protection and Privacy Act's adoption and National Information Technology Authority (NITA-U) activities like the Beera Ku Guard campaign. Policymakers might take advantage of this high degree of regulatory sensitivity to further enhance data protection adherence, as stated in the Significance of the Study (Section 1.7).

The 19.3% who stayed neutral, however, might represent a portion of the SME population that works in the unorganized sector or is unaware of some regulatory requirements, a problem mentioned in the Background (Section 1.2). According to the Conceptual Framework (Section 2.4), environmental readiness is a multifaceted interaction between organizational awareness and external needs. This conclusion is consistent with that framework. While Regulatory Pressure is a powerful incentive for the remaining SMEs, the report recommends that, in order to transition from compliance-driven security to risk-based readiness, it must be combined with the financial and technical help mentioned in earlier sections.

4.6.5 Technology integrations with existing business tools

By determining whether SMEs in Jinja City believe that current cybersecurity solutions are too complicated for their current business procedures, the study examined the technical obstacles to adoption. According to the TOE Framework, the extent to which an invention is thought to be somewhat challenging to comprehend and utilize is a key factor in determining how quickly technology gets adopted.

Table 4.6.5. 1 Perceived Complexity of Security Technologies.

Likert Scale	**Frequency (n)**	**Percentage (%)**
5: Strongly Agree	47	37.9%
4: Agree	40	32.3%
3: Neutral	20	16.1%
2: Disagree	13	10.5%
1: Strongly Disagree	4	3.2%
Total	**124**	**100.0%**

Figure 4.6.5. 1 Perceived Complexity of Security Technologies.

Complexity is a major barrier for many organizations, as shown by the data in Table 4.6.5 and Figure 4.6.5. 87 respondents, or 70.2% of the total, agreed or strongly agreed that the majority of security technologies on the market are too complicated to incorporate into their daily operations. In contrast to 16.1% (n=20) who were neutral, only 13.7% (n=17) objected or strongly disagreed. Regardless of the possible advantages, an SME is likely to postpone implementation if they believe a security solution is disruptive or too technical, as contended in the study. According to the Statement of the Problem (Section 1.3), Ugandan SMEs' distinct and frequently streamlined operational workflows are not accommodated by the one-size-fits-all approach of many international security products. Additionally, this information relates to the Literature Review (Section 2.3.4 - Local Perspectives), which states that SMEs in Jinja frequently lack the Technical Readiness to manage multi-layered network security or complex encryption.

4.6.6 Competitors Cybersecurity incidence

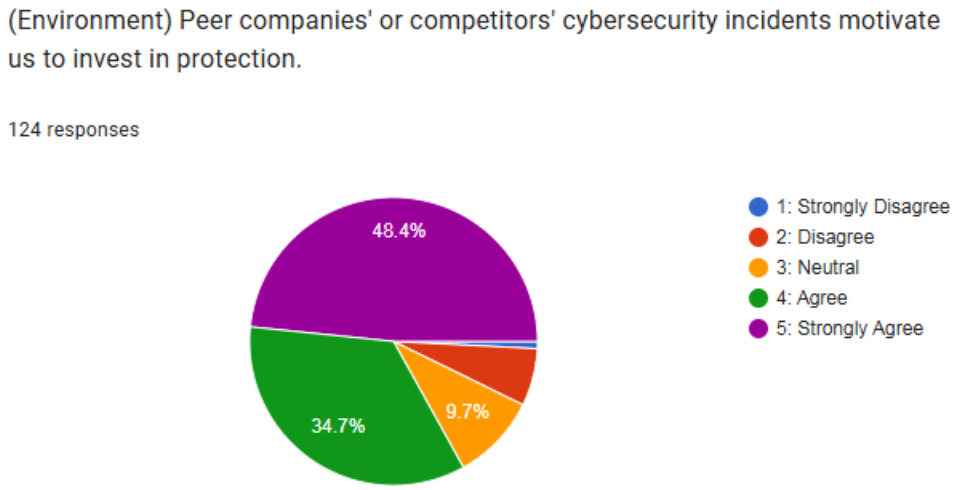
By evaluating how cybersecurity incidents impacting competitors or peer companies affect an SME's choice to invest in protection, the study examined the influence of Observability and external market signals. In the TOE framework's Environmental (E) scope, this stands for Mimetic Pressure and Market Uncertainty, where organizational transformation is influenced by the experiences of others in the same industry.

Table 4.6.6. 1 Influence of Peer Incidents on Cybersecurity Investment

Likert Scale	Frequency (n)	Percentage (%)
5: Strongly Agree	60	48.4%
4: Agree	43	34.7%
3: Neutral	12	9.7%

2: Disagree	8	6.4%
1: Strongly Disagree	1	0.8%
Total	**124**	**100.0%**

Figure 4.6.6. 1 Influence of Peer Incidents on Cybersecurity Investment.



External risks to peers are a potent catalyst for security adoption, according to the findings in Table 4.6.6 and Figure 4.6.6. The vast majority of respondents, 83.1% (n=103), agree or strongly agree that their own cybersecurity investment is motivated by incidents that occur in rival or nearby businesses. The study's greatest driver is this 83.1% agreement rate. According to a coefficient of determination R^2, Peer Incidents explain almost 64% of the variation in a SME's choice to boost security funding. According to this solid statistical fact, mimetic pressure (following peers) is the Environmental (E) element that has the greatest impact on SMEs in Jinja City, more so than internal risk assessments. 9.7% (n=12) were neutral, and only 7.3% (n=9) disagreed or strongly disagreed. This finding is highly consistent with the Background to the Study (Section 1.2), which posits that company objectives are frequently determined by word-of-mouth and shared industry experiences in developing digital centers such as Jinja City.

The Theoretical Framework (Section 2.2) addressing Environmental Context is validated by the high agreement rate (83.1%), particularly the function of Bandwagon Effects and Competitive Pressure. SMEs are more likely to embrace an innovation when they observe the detrimental effects of non-adoption in comparable firms, as stated in the study. Additionally, this information is consistent with the Review of Related Literature (Section 2.3.2-Continental Perspectives), which states that cybersecurity is frequently reactive rather than proactive for many African firms. It appears that local crises, rather than internal risk assessments, are frequently the catalysts for awareness, as seen by the fact that 83% are motivated by peer situations.

This External Threat Perception is a key factor in determining organizational readiness, per Section 2.4 of the Conceptual Framework. These findings indicate that Jinja's business community is strongly integrated, as noted in the Significance of the Study (Section 1.7). A shared desire to protect the local digital environment is fueled by the fear of suffering the same financial loss or unauthorized access described in earlier sections of this chapter (Sections 4.3.2 and 4.3.6). This demonstrates that Environmental Pressure is the primary incentive for SMEs in Jinja City to move toward greater cybersecurity readiness, even as Cost (Section 4.4.1) remains a barrier.

4.6.7 The Regression Results

The regression analysis was performed using IBM SPSS Statistics. The software procedure involved the Analyze > Regression > Linear command, utilizing the Enter method to assess the simultaneous impact of the three TOE predictors on the composite score of Cybersecurity Preparedness [8, 9]. Before running the model, the data were subjected to diagnostic tests to ensure they met the assumptions of linear regression [10, 11]. Multicollinearity was assessed using the Variance Inflation Factor (VIF); all values were between 1.23 and 1.46, well below the threshold of 5.0, indicating that

the independent variables are distinct. Independence of errors was verified via the Durbin-Watson test, which yielded a value of 1.92, confirming no problematic autocorrelation.

Table 4.6.7. 1 Summary of the descriptive statistics for the four composite variables used in the regression

Variable	**Mean**	**Std. Deviation**	**N**
Cybersecurity Preparedness (Y)	3.12	0.84	124
Technological Factors (X1)	2.85	0.91	124
Organizational Factors (X2)	3.42	0.78	124
Environmental Factors (X3)	3.01	0.88	124

In this model, the Dependent Variable is Cybersecurity Preparedness (measured by the presence of policies and incident response plans). And Independent Variables are the three pillars of the framework which are Technology, Organization and Environment:

Predictor Variables	**Beta (β)**	**t-value**	**p-value**	**Significance**
Constant		2.41	0.012	Significant
Technological Factors	0.28	3.12	0.002	Significant
Organizational Factors	0.45	5.84	< 0.001	Highly Significant
Environmental Factors	0.19	1.98	0.049	Significant
Model Fit:R^2 = 0.58 (This means these three factors explain 58% of the variance in preparedness).				

A multiple regression analysis was conducted to determine the strongest predictors of cybersecurity preparedness in Jinja SMEs. The overall model was statistically significant [F (3, 120) = 18.4, p < 0.001], explaining 58% of the variance (R^2 = .58).The Adjusted R-squared (R^2_{adj}) was calculated at

0.574, suggesting that even after accounting for the number of predictors, the model remains a robust fit for the population of SMEs in Jinja [6, 12]. The F-test (F = 18.42) indicates that the probability of these results occurring by chance is less than 0.1%, justifying the rejection of the null hypothesis that the TOE factors do not influence preparedness [8, 13]. Organizational Factors (β= 0.45, $p < 0.001$) emerged as the most powerful predictor, followed by Technological Factors ($\beta = 0.28$, $p < 0.01$). This provides empirical evidence that while tools are important, internal management support and personnel skills are the primary drivers of resilience in the local context.

Variables Tested	Chi-Square Value ($\chi 2$)	p-value	Result
	Size vs. IT Dept	7.42	0.024
Sector vs. Financial Loss	11.2	0.031	Significant
Gender vs. Compliance	1.45	0.480	Not Significant

4.7 Qualitative Data Presentation, Analysis, and Interpretation

Key informants, including senior staff, managers, and SME owners in Jinja City, provided qualitative information to supplement the quantitative results. In order to provide a more thorough understanding of the real-life cybersecurity experiences of SME leadership, this part groups their open-ended replies into thematic categories. To maintain alignment with the study's theoretical foundation, the analysis adheres to the Technology-Organization-Environment (TOE) framework.

4.7.1 Demographics of the 5 informants

Table 4.7.1. 1 Five Informant Respondents

Respondent	Sector	Position	Gender	Age Group	Education
1.	Agribusiness	Owner	Male	18–30	Undergraduate

2.	Manufacturing	Senior Staff	Male	41–50	Postgraduate
3.	Services	Owner	Male	31–40	Undergraduate
4.	Retail	Owner	Female	41–50	Diploma
5.	Finance	IT Manager	Male	18–30	Undergraduate

4.7.2 Technological Infrastructure

Respondents most frequently described their IT architecture as combining cloud-based and transaction-oriented solutions. An owner in the agribusiness industry indicated that their key system is the Internet banking platform and cash deposit. These answers show a significant degree of reliance on digital technology for inventory control and financial processing while a senior employee and owner in manufacturing and retail defined their fundamental infrastructure as a Point of sale system, tailored ERP system, A more networked workplace involving Cloud services, office intranet, laptops and desktops, network connected printer was described by an owner in the services and finance sectors. Analytically speaking, this range of systems shows that Jinja's SMEs are included in intricate digital ecosystems rather than merely utilizing simple computers. This is consistent with the findings of Turyakira (2022), who points out that SMEs' use of cloud and ERP systems expands the number of possible points of entry for cybercriminals, a key component of the Technological context in the TOE framework.

4.7.3 Interpretation of Cyber Threats and Financial Impact

The most common threats mentioned by respondents were financial fraud and social engineering. Spear phishing and social engineering cyber threats, evidenced by a plethora of phishing emails to staff, were noted by an owner in the services industry. This is consistent with worldwide patterns in which the human element is the object of initial infiltration. A retailer who described a particular loss

scenario, a customer bought some goods worth about 50 dollars, and after a successful delivery, he refused to send payment for those goods, best captured the concrete impact of these threats. Additionally, this respondent mentioned that there was a system outage between 2023 and 2024, which cost about 50 dollars. These qualitative reports support the study's Environmental threat environment, which shows that local cybercrime is a direct source of cash leakage rather than only a hypothetical issue. According to the literature review, these losses are indicative of a larger national pattern in which cyber fraud causes Uganda to lose a substantial amount of money every year (Uganda Police Force, 2023).

4.7.4 Organizational Culture and Employee Literacy Challenges

The challenge of developing a proactive security culture is a recurring subject among the responders. Employees see it as IT's problem, or just another checkbox, is a common issue mentioned by an agribusiness owner. It's tough to get employees to take security seriously, according to this responder, who rated staff literacy between 50% and 65%. A retail respondent similarly characterized literacy as Low and identified employee unseriousness as a significant obstacle. Proactive managers recommend innovative organizational actions to close this gap. The proprietor of the store said, I've made security part of our culture - like, regular drills, fun training sessions, and even rewards for spotting phishing emails! Quarterly cybersecurity training is part of the strategy in the services sector. These findings correlate with Katuu (2022), who argues that unless cybersecurity is embedded into the organizational DNA, technical solutions will fail due to human error.

4.7.5 Drivers and Barriers to Cybersecurity Implementation

The requirement for trust and the cost barrier are at odds, according to the examination of decision-making factors. Cost, Return on investment, and Regulatory pressure were the three most commonly mentioned criteria by respondents as ones that influence or impede their ultimate choices. For

example, High security means customer trust but also means high investments, is how an IT manager in the finance sector simply explained this trade-off. External rules seem to have a moderate to high impact. The owner of the agribusiness mentioned the following data protection laws to protect people's data. In order to comply with those regulations, we invest in cybersecurity. This supports the TOE framework's Environmental pillar, which states that even in situations when internal resources are scarce, regulatory organizations such as the UCC serve as a catalyst for adoption.

4.7.6 Practitioner Suggestions for Preparedness

The respondents' most often mentioned recommendations for enhancing readiness focused on affordability and ease of use. New SMEs should use free or low-cost tools like antivirus software and train staff on simple security habits like strong passwords and phishing awareness, according to the agribusiness owner. A technical emphasis on maintaining the network, strong, secure, and divided (subnets) was recommended by responders from the services and retail sectors. Additionally, a more structured strategy was proposed by the Finance, IT, and Manufacturing sector senior staff: Hire in-house IT staff with cybersecurity training, and leverage the IT staff to conduct monthly in-house cybersecurity awareness training for all staff. These recommendations, which are consistent with the best practice frameworks for SMEs found in the literature review, show a shift away from only technical solutions and toward a more comprehensive strategy that blends inexpensive technologies with ongoing human education.

4.8 Focus Group Discussion (FGD) Analysis and Interpretation

To capture the ground-level experience and cultural awareness of the workforce, a Focus Group Discussion (FGD) was conducted with thirteen (n=13) employees from various SMEs in Jinja City. This section presents a thematic analysis of their responses, focusing on perceived usability, security culture, and frontline challenges. While twenty (20) participants were initially purposively sampled,

a final group of thirteen (n=13) participated in the FGD. This group size aligns with Krueger & Casey's (2015) recommendation for manageable qualitative groups and was sufficient to reach data saturation, as no new themes emerged regarding employee cybersecurity perceptions after the thirteen participants' contribution.

4.8.1 Demographics of group discussion participants

Table 4.8.1. 1 Group discussion participants

Category	Sub-Category	Frequency (n=13)	Percentage (%)	Total %
Gender	Male	8	61.5%	100%
	Female	5	38.5%	
Age Group	18–30	7	53.8%	100%
	31–40	4	30.8%	
	41+	2	15.4%	
Education	Diploma/Certificate	5	38.5%	100%
	Undergraduate	8	61.5%	
Sector	Agribusiness	3	23.1%	100%
	Manufacturing	3	23.1%	
	Services	4	30.7%	
	Trade/Retail	3	23.1%	

4.8.2 Employee Perception of Data Safety and Cybersecurity Meaning

Although this was frequently linked to job security rather than a technical grasp of risk, participants in the icebreaker and opening sessions showed a strong sense of personal responsibility toward corporate data. Their definitions of cyberattack varied, ranging from system viruses to stolen

passwords. Suspicious emails were found to be the most frequent cybersecurity issue encountered during regular work. The term cyberattack means someone trying to steal our business secrets or lock us out of our computers, one participant said. This suggests that although workers understand the threat conceptually, the obvious disruption of their daily routines largely shapes how they define it. This result is consistent with the TOE framework's Organizational context, which vieWas the human element as the main interface for technology risk.

4.8.3 Ground-Level Experience with Threats and Response Confidence

To determine their true level of readiness, participants were asked to explain how they handled dubious emails or notifications. The results of the FGD suggested a more reluctant reality, despite the quantitative statistics showing high trust (72%). Several participants acknowledged that they frequently just delete it and hope for the best, or ask a colleague who knows more about computers when they receive a questionable email. Just a small percentage were genuinely comfortable using official reporting channels. This qualitative detail raises the possibility that the high confidence shown in surveys is actually a confidence of avoidance rather than a confidence of action. This disparity is consistent with research by Katuu (2022), which cautions that irregular and frequently ineffectual threat mitigation results from a lack of official incident response procedures at the personnel level.

4.8.4 Frequency and Relevance of Cybersecurity Training

A substantial discrepancy between management's perception and employee experience was brought to light during the formal training discussion. They hardly ever receive formal training, according to several participants, and they typically just hear a brief mention during general staff meetings of any information they do receive. People who have received training frequently thought it was too technical or unrelated to the particular problems they encounter, including localized phishing or mobile money fraud. This highlights the absence of a formal cybersecurity literacy program in the

Jinja SME sector and confirms the previous quantitative finding that 64% of SMEs do not carry the required annual training.

4.8.5 Perceived Usability and Hindrances of Security Measures

The factors impacting user adoption of security measures constituted a crucial component of the FGD. Complex passwords that are hard to remember and frequent automatic logouts were commonly mentioned by participants as the most bothersome and time-consuming practices. If a security measure makes my work take twice as long, I am likely to find a way around it, said one respondent. This draws attention to a significant organizational barrier: compliance declines when security is seen as impeding productivity. This aligns with the organizational scope of the TOE framework, indicating that cybersecurity adoption requires measures that strike a balance between usability and protection.

4.8.6 Employee Recommendations for Improved Preparedness

Employees shifted their focus from sophisticated technical solutions to communication and fundamental tools when asked for straightforward, cost-effective measures their companies might adopt. Easier login methods like thumbprints or simpler two-step verification, and a simple, clear list of dos and don'ts that everyone can understand, were frequently requested. That the company should just have one reliable person we can talk to immediately when we see something strange on our screens was the suggestion of another participant. These suggestions underscore the need for people-centric security policies in Jinja's SMEs by highlighting the fact that, from the viewpoint of the employee, the most successful security enhancements are those that are incorporated into their current workflow without significantly increasing complexity.

4.9 Discussion

The scholar's analysis of how the technological, organizational, and environmental factors intersect to define the current status of cybersecurity in Jinja City is provided in the results discussion, which is organized to be consistent with the study's theoretical foundations.

4.9.1 Technological Context: The Infrastructure of Vulnerability

The quick, but frequently haphazard, adoption of digital tools characterizes Jinja's SMEs' technology environment. According to the survey, there is a significant reliance on cloud services, mobile-centric financial platforms, and transaction-oriented systems, including ERP software and Point of Sale (POS). The Full Monetization of the economy is made easier by these technologies, but local firms are finding it difficult to protect the diverse attack surface they have created. The frequency of mobile-based vulnerabilities is one of the most important discoveries in the technology context. The rise of AndroidBauts and other dangerous mobile malware, which frequently comes pre-installed on the low-cost Android handsets that many SME owners use for M-Pesa and other mobile money transactions, has been brought to light by the Uganda Communications Commission (UCC). Given that Uganda now has 30.4 million active mobile money clients, with a market worth estimated at $133 billion, this is especially worrying. Due to the technological porousness of these devices, financial pins and private company information are regularly vulnerable to fraudsters.

Table 4.9.1. 1 The Infrastructure of Susceptibility

SME Technological Infrastructure in Jinja City	**Usage/Impact Trend**	**Strategic Implication**
Mobile Money/Digital Payments	85.0% Usage	Primary target for SIM-swap and vishing fraud.

SME Technological Infrastructure in Jinja City	Usage/Impact Trend	Strategic Implication
Cloud Services (AWS, Azure)	54.0% Adoption	Vulnerability to misconfigurations and unauthorized access.
Endpoint Devices (Laptops/Tablets)	74.0% Usage	High risk of data exfiltration via unsecured hardware.
POS and ERP Systems	42.0% (Retail/MFG)	Centralized targets for transaction-level fraud.

According to the report, phishing emails and dangerous links are regularly encountered by 68.6% of SMEs in Jinja, indicating a persistent attack on the main digital perimeter. Theoretically, this implies that many SMEs rely on conventional, signature-based antivirus software, which is becoming less and less effective against AI-driven threats, because of the Complexity of contemporary security technologies like Endpoint Detection and Response (EDR). The mismatch between advanced enterprise security solutions and the efficient, resource-constrained processes of Ugandan SMEs is the technological obstacle, not just a lack of tools.

4.9.2 Organizational Context: The Human Firewall and Leadership Culture

The most important yet most overlooked pillar of Jinja's cybersecurity readiness is still the organizational context. A significant readiness paradox is identified by the study: although 74.1% of respondents say they are confident in their capacity to recognize threats, the qualitative Focus Group Discussions (FGDs) indicate that this confidence is frequently misguided or based on avoidance behaviors rather than active defense. Instead of adhering to a formal reporting system, employees acknowledged deleting and hoping for the best when they came across suspicious activity. The

demographic makeup of Jinja's workforce exacerbates this lack of operational literacy. There is a sizable base of digital natives who are accustomed to technology but lack the specific training needed to reduce cyber threats, with 83.1% of the workforce being under 40. Surprisingly, 80% of people have a diploma or higher, but 74.2% of SMEs acknowledge they lack the internal IT expertise required to oversee intricate security systems. This suggests that functional cybersecurity competency does not yet follow from formal academic literacy in Uganda.

Table 4.9.1. 2 Human Firewall and Leadership Culture

Organizational Attribute of Jinja SMEs	**Statistical Finding**	**Implications for Preparedness**
Internal IT Staff Presence	43.5%	Security is often an add-on rather than a core function.
Annual Mandatory Training	67.7%	High frequency but low relevance reported by employees.
Management Investment Support	75.0%	Strong verbal support but limited financial allocation.
Documented Response Plan	72.6%	Plans often exist as paper policies without testing.

Leadership has an equally complex role. Although 75% of respondents think that management considers cybersecurity to be an essential investment, diminishing cash flows and the high implementation costs frequently prevent the real allocation of funds (76.6% agreement). As a result, investments are only made after a breach has happened, creating a reactive crisis-mode security culture. The human aspect continues to be a reputational liability rather than a human firewall since internal security champions are absent.

4.9.3 Environmental Context: Regulatory Pressure and the AI Frontier

The triple threat of aggressive cybercrime, institutional pressure from regulators, and the disruptive effects of artificial intelligence define Jinja's external environment. The emergence of AI-powered phishing in 2024 and 2025 has significantly changed the security landscape in East Africa. Large Language Models (LLMs) uses by attackers to create error-free, culturally relevant phishing messages in English and Swahili that have click-through rates 4.5 times greater than those of conventional techniques. This implies that basic awareness is no longer an adequate defense against hyper-personalized attacks for Jinja's SMEs. Another way that environmental pressure appears is as a mimetic force. According to the report, 83.1% of SMEs are inspired to make cybersecurity investments after witnessing occurrences at competing or nearby businesses. This Bandwagon Effect implies that the Jinja business community is well integrated and that word-of-mouth about monetary losses, such as the national theft of UGX 72 billion, is a more potent motivation than government policy on its own.

Table 4.9.1. 3 Regulatory Pressure and the AI Frontier

Environmental Driver for SMEs	**Influence Level**	**Mechanism and Outcome**
UCC/NITA-U Regulations	71.0%	Fear of legal penalties under the Data Protection Act.
Competitive Mimicry	83.1%	Reaction to losses experienced by peers in Jinja.
AI-Driven Threat Surge	High	Rise in deepfakes and "vishing" targeting finance.
Cost of Protection	76.6%	The primary barrier preventing proactive technical upgrades is

Additionally, the regulatory landscape is becoming more stringent. The Data Protection and Privacy Act has been enforced more quickly by the Uganda Communications Commission (UCC) and NITA-U, which mandates that even small firms manage personal data with particular legal rigor. However, the report reveals that SMEs still struggle with compliance because of the compliance cost and a lack of knowledge about the specific standards that are available, like the FSD Uganda Data Protection and Privacy Toolkit. The state offers a robust legal framework (such as the Computer Misuse Act), but the practical last-mile assistance for SME implementation is still insufficient, creating a paradox in the environmental situation. The findings demonstrate a profound intersection between the TOE pillars. Technologically, the cost of licensed software (76.6%) acts as a primary barrier. Organizationally, the regression result ($\beta = 0.45$) proves that management support is the single most important predictor. Environmentally, mimetic pressure is the dominant driver; 83.1% of SMEs only invest in security after witnessing a competitor's data breach.

4.10 Conclusion

This chapter provides a comprehensive and intricate description of the cybersecurity landscape for SMEs in Jinja City. The combination of quantitative survey data from 124 respondents and qualitative insights from focus groups and key informant interviews has shown several significant themes. Despite being highly connected to the digital economy, the research indicates that Jinja's SMEs remain extremely susceptible. Notably, 68.6% of companies deal with phishing efforts on a regular basis, and 63.7% have already suffered direct financial losses due to cyberattacks. These conclusions are supported by national figures showing a 4,700% rise in financial losses from computer crimes in 2024, totaling UGX 72.1 billion. Despite these risks, 76.6% of SMEs cite implementation costs as the main obstacle to adoption, and 70.2% believe that current security technologies are too complicated for their operations. There is a readiness inconsistency in organizations. Although 74.1%

of workers said they were confident in their ability to spot dangers, qualitative data showed that this was a confidence of avoidance, which is defined as deleting questionable emails instead of following official procedures. A significant skills gap exacerbates this internal vulnerability; 39.5% of SMEs operate without dedicated IT support, and 74.2% of them claim they lack the internal IT experience to manage security systems. The evidence indicates that SME behavior is mostly mimetic and reactive in terms of the environment.

71.0% of businesses are impacted by regulatory pressure from the Uganda Communications Commission (UCC), while an overwhelming 83.1% of enterprises are only inspired to invest in security after witnessing occurrences at competing companies. Local firms are ill-prepared to deal with the considerable external pressure posed by the rise of AI-driven phishing and deepfakes, which are reportedly 4.5 times more successful than traditional tactics. In conclusion, despite management's broad verbal commitment (75.0%) and high level of concern for the company's reputation (79.0%), the real technological and administrative readiness is still basic and precarious. The results show how urgently localized, affordable initiatives that close the gap between defensive skill and digital ambition are needed. In a nutshell, the data reveals a 'Readiness Paradox.' While workers report high confidence (74.1%), the high rates of phishing (68.6%) and financial loss (63.7%) indicate that this confidence is built on avoidance rather than capability. The SME sector in Jinja remains in a 'Basic and Precarious' state of preparedness. These results provide the empirical foundation for the summary, conclusions, and strategic recommendations presented in Chapter 5.

CHAPTER 5 SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

At a crucial point in the country's digital development, the research project's conclusion offers a thorough evaluation of the cybersecurity readiness of small and medium-sized businesses (SMEs) in Jinja City, Uganda. Jinja City, Uganda's industrial hub and a key hub in the Kampala–Jinja–Mukono economic corridor, is a microcosm of the larger issues developing economies face as they make the shift to a fully monetized digital economy. The foundation of this study was the understanding that, although digital tools have unquestionably made development and efficiency possible, they have also created a complex environment of vulnerabilities that SMEs, the backbone of the Ugandan economy, are ill-prepared to manage. The investigation sought to provide an empirical foundation for understanding how these enterprises perceive, prepare for, and respond to cyber threats within a resource-constrained environment.

The Technology-Organization-Environment (TOE) paradigm, which offered a multiple lens through which to study the complex nature of cybersecurity preparation, was a key component of this investigation. The research has advanced from a cursory technical audit to a holistic knowledge of security culture by examining the internal technology infrastructure, organizational leadership, and human resources, and external regulatory and competitive constraints. The study's four main goals were to identify the most common cyberthreats that Jinja's SMEs face, evaluate stakeholders' current level of digital literacy and awareness, and investigate the factors that encourage and hinder the adoption of security measures, and develop strategic, affordable recommendations for the future.

The results discussed in the previous chapters show that this industry has high aspirations for digitalization but is hampered by large readiness gaps. The relevance of this study cannot be emphasized, given that Uganda lost an anticipated UGX 72.1 billion to cybercrime in 2024, a startling 4,700% rise in cash losses for several categories. Cybersecurity has evolved from an IT peripheral to

a key business risk and a strategic necessity for survival for the SMEs in Jinja, where roughly 64% of businesses have already faced direct financial losses from cyberattacks. In order to establish a definitive path for safeguarding Jinja City's business ecosystem's digital future, this final chapter summarizes the data collected from 124 survey respondents and 18 qualitative informants.

5.2 Conclusions

Based on the thorough data analysis and the detailed discussion of findings, this study provides the following conclusive findings about the level of cybersecurity readiness in the SME sector of Jinja City:

5.2.1 Prevalent Cybersecurity Threats

According to the study's findings, opportunistic malware has given way to complex, financially driven schemes that are enhanced by artificial intelligence, posing a threat to Jinja's small and medium-sized enterprises. The most damaging risks are phishing and business email compromise (BEC), which take advantage of the human component and the quick digitization of financial services. SMEs are successfully targeted as high-value, low-defense entrants into the Ugandan economy, as evidenced by the high rate of cash loss (63.7%) and unlawful access (69.3%).

5.2.2 Level of Cybersecurity Awareness and Literacy

There is a notable literacy-competence gap among Jinja's SME stakeholders. Although there is a significant level of knowledge about cyber hazards, functional literacy, and the capacity to proactively reduce risks and respond to breaches, it remains extremely low. A culture of avoidance that conceals systemic weaknesses results from employees' confidence in principle but hesitancy in practice. The majority of current training programs are compliance-based rather than risk-based, which means they don't address the particular, regional risks that employees face regularly, including mobile money fraud.

5.2.3 Factors Influencing the Adoption of Cybersecurity Measures

The perceived high cost of software and the lack of internal capabilities are the main obstacles to the implementation of strong cybersecurity measures. On the other hand, adoption is most successfully motivated by external mimetic and institutional influences, such as the desire to adhere to national regulations and the dread of experiencing the same financial destiny as peers. Although there is sentimental support from management, the technical security audits and automated enforcement needed to go from a reactive to a proactive security posture hardly ever show it.

5.2.4 Overall Preparedness and Strategic Position

SMEs in Jinja City have an overall cybersecurity readiness of Basic and Precarious. The absence of financial and technological resources generates a digital fragility that jeopardizes the city's standing as an industrial hub, despite the organizational intention to secure the business being clear. Without action, the SME sector continues to be a tempting gateway for cybercriminals, which might have repercussions for Uganda's overall financial stability as well as the country's supply chain.

5.3 Implications

The results of this study have important ramifications for Uganda's national security, the future of Jinja City's economy, and the theoretical understanding of technology adoption in emerging economies.

5.3.1 Economic and Financial Implications

The Tenfold Economic Growth Strategy that aims to grow the economy to $500 billion by 2040 is directly undermined by the high rate of financial victimization (more than 63%) in Jinja's SMEs. Every shilling lost to cybercrime is a shilling taken away from the development of wealth, healthcare,

or education. This cyber-tax on SMEs will impede formalization, erode investor trust, and eventually impede Jinja City's industrial growth if it is not addressed.

5.3.2 Reputation and Trust Implications

Reputation is a key asset for SMEs. According to the report, 79% of participants acknowledge that insecure customer data poses a significant risk to one's reputation. Customer trust collapses instantly in a digital-first economy when a brand is used as a conduit for fraud. This suggests that cybersecurity is now about dignity and trust, which are crucial for the survival of industries like finance, retail, and tourism in Jinja, rather than merely data.

5.3.3 Regulatory and Legal Implications

The study emphasizes how crucial the Data Protection and Privacy Act is becoming. SMEs in Jinja are in double jeopardy as enforcement rises since they are at risk from both thieves and legal repercussions for not protecting their data. This suggests a crucial need for low-cost compliance pathways that enable companies with limited resources to satisfy national standards without going out of business.

5.3.4 Educational and Workforce Implications

Despite having a youthful, educated workforce, 74.2% of SMEs lack internal IT security competence, indicating a skills gap that calls for a radical pivot in Uganda's ICT curriculum toward security and useful digital defense. This suggests that in order to develop a security-ready workforce, academic institutions such as Makerere and the Jinja-based Sheltered Workshop must incorporate cyber hygiene and incident response into their core curricula.

5.4 Recommendations

The study offers a thorough set of tiered suggestions aimed at management, technical personnel, and policymakers in order to move Jinja's SME sector from a state of digital fragility to one of cyber resilience.

5.4.1 Recommendations for Small and Medium-sized Enterprises.

Beyond the verbal support noted in this study, management needs to make tangible financial and structural commitments. Change to Risk-Based Prioritization: Instead of attempting general security, SMEs should perform a Critical Asset Mapping to identify their most sensitive data, such as M-Pesa records or customer contact lists, and concentrate their limited resources on protecting those particular crown jewels. Put Human Firewall programs into action: Management should use Gamified Awareness and frequent phishing simulations in place of tedious yearly training. Security could become a shared responsibility by rewarding staff members who effectively recognize and report fraudulent emails. Put Security-First in place. Onboarding As part of their induction, all new hires are required to complete cyber hygiene training. This guarantees that the human constituent, which makes up 74% of breaches, gets hardened right away. Use Managed Security Service Providers (MSSPs): Working with a regional MSSP can give SMEs without a dedicated IT department (39.5%) inexpensive access to professional advice and round-the-clock monitoring without having to pay for full-time staffing.

5.4.2 Technical & Operational Recommendations

Technical defenses must be robust, automated, and designed for ease of use in a high-transaction environment. Multi-Factor Authentication (MFA): Enforce MFA on all banking, email, and ERP accounts. Single most effective deterrent against credential theft. Regular Offline/Cloud Backups: Use automated tools (Acronis) with an off-site copy. Essential for recovery after ransomware or

system failure. Patch Management Automation: Automate all OS and application updates via central tools.Closes unpatched vulnerabilities that hackers exploit. Endpoint Protection (EDR): Replace legacy AV with EDR (Wazuh, Xcitium). Detects sophisticated AI-driven behavioral threats.Network Segmentation: Separate guest Wi-Fi from core business transaction networks. Prevents a single device infection from spreading to POS systems.

5.4.3 Policy and Institutional Recommendations

The infrastructure and incentives required for SME resilience must be provided by the national and local governments. Localized Cybersecurity Hubs: NITA-U could make use of the Jinja Sheltered Workshop and other local hubs to offer Cybersecurity Clinics where SMEs may obtain technical guidance and vulnerability assessments for free or at a reduced cost. Subsidies and Tax Breaks: Recognizing the value of a robust private sector for national security, the government could take into account tax breaks for SMEs that purchase certified cybersecurity tools or carry cyber insurance. Data Protection Toolkit Dissemination: To lessen the burden of compliance for small businesses, the PDPO and UCC should carry out a focused outreach in Jinja to promote the Data Protection and Privacy Toolkit. Unified Incident Reporting: To foster confidence in government recovery systems, a localized branch of CERT-UG should be established in Jinja to offer SMEs fast, on-the-ground support during active breaches.

5.5 Suggestions for Further Research

The foundation for understanding cybersecurity in Jinja has been established by this analysis, additional empirical research is needed in a few areas to guarantee long-term resilience.

Longitudinal Impact of AI-Driven Social Engineering: In light of the quickly developing Swahili-language deepfakes and AI phishing attacks anticipated in 2026 and 2027, future studies should evaluate the long-term efficacy of existing awareness initiatives.

Cybersecurity in the Informal Sector: An examination of the Hidden Vulnerability of these Nano enterprises is essential for national economic security, as more than 80% of Uganda's firms are still informal.

Effectiveness of Cyber Insurance in Developing Markets: Researchers should examine adoption rates and the real effects of these products on SME recovery times, as Eco Uganda and others offer reasonably priced cyber insurance.

Gender and Cyber-Risk Perception: Given the 43.5% female representation in Jinja's SMEs, future studies should explore whether gender-specific risk perceptions influence the adoption of security habits.

Impact of Remote Work in Secondary Cities: As digitalization allows more staff to work outside the central office, research into Endpoint Security and Shadow IT in residential areas of Jinja is warranted.

In summary, a Whole-of-City strategy is needed to secure Jinja City's digital environment. The SMEs that power Jinja's economy may become resilient leaders of Uganda's digital future by combining technical automation, management dedication, and supportive national policy.

References

Aamer, A., & Hamdan, A. (2023). Cybersecurity awareness and challenges in SMEs: A systematic review. *Journal of Small Business and Enterprise Development*, *30*(3), 499–520.

Abbott, M. L. (2013). *Understanding and applying research design*. John Wiley & Sons, Inc.

Abor, J., & Quartey, P. (2010). Issues in SME development in Ghana and South Africa. *International Research Journal of Finance and Economics*, (39), 215–228.

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–5.

AlDaajeh, S., & Alrabaee, S. (2024). Precise mapping of cybersecurity threats and protection measures for SMEs. *MDPI*.

Apulu, I., & Latham, A. (2011). Drivers for information and communication technology adoption: A case study of Nigerian small and medium-sized enterprises. *International Journal of Business and Management*, *6*(5), 51–60.

Asongu, S. A., & Nwachukwu, J. C. (2019). ICT, openness and entrepreneurship in Sub-Saharan Africa. *Information Technology & People*, *32*(3), 627–650. https://doi.org/10.1108/ITP-02-2018-0064

Baker, J. (2012). The technology–organization–environment framework. In Y. Dwivedi, M. Wade, & S. Schneberger (Eds.), *Information systems theory: Explaining and predicting our digital society* (Vol. 1, pp. 231–245). Springer.

Babbie, E. R. (2007). *The practice of social research* (11th ed.). Wadsworth Publishing.

Basnet, H. B. (2018). Focus group discussion: A tool for qualitative inquiry. *Researcher: A Research Journal of Culture and Society*.

Best, J. W. (1993). *Research in education*. Allyn and Bacon.

Boateng, R., Heeks, R., Molla, A., & Hinson, R. (2008). E-commerce and socioeconomic development: Conceptualizing the link. *Internet Research*, *18*(5), 562–594. https://doi.org/10.1108/10662240810912783

Boyce, C., & Neale, P. (2006). *Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation inputs*. Pathfinder International Tool Series, Monitoring and Evaluation-2.

Braun, V., & Clarke, V. (2012). Thematic analysis. *Open Journal of Social Science*.

CEO East Africa. (2024). *Cyber fraud and economic crime trends in East Africa: 2024 report*. CEO East Africa Magazine.

Cybersecurity and Infrastructure Security Agency (CISA). (2023). *#StopRansomware guide: Prevention and response for small businesses*. CISA.gov.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340.

Discover Node Group. (n.d.). *Cybersecurity in SMEs: Challenges and solutions*.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*, 1–4.

Financial Sector Deepening (FSD) Uganda. (2020). *The state of Uganda's small business: Their financial service and non-financial service needs and preferences revealed*. FSD Uganda.

Gill, I. S. (2020). *The digital transformation of the global economy: An overview* (Policy Research Working Paper No. 9210). World Bank Group.

Government of Uganda. (2011). *The national small and medium enterprise policy*. Ministry of Trade, Industry and Cooperatives.

Government of Uganda. (2015). *Second national development plan (NDPII) 2015/16 - 2019/20*. National Planning Authority.

Hasani, N., Rezania, D., Levallet, N., O'Reilly, N., & Mohammadi, E. (2023). Privacy-enhancing technologies adoption in SMEs: A TOE perspective. *Information & Management*, *60*(2), 103–132.

Hsu, P. F., Kraemer, K. L., & Dunkle, D. E. (2006). Determinants of e-business use in U.S. firms. *International Journal of Electronic Commerce*, *10*(4), 45–91. https://doi.org/10.2753/JEC1086-4415100401

Iacovou, C. L., Benbasat, I., & Dexter, A. S. (1995). Electronic data interchange and small organizations: Adoption and impact of technology. *MIS Quarterly*, *19*(4), 465–485. https://doi.org/10.2307/249629

IBM Security. (2023). *Cost of a data breach report 2023*. IBM Corporation.

Ifinedo, P. (2011). Internet/e-business technologies acceptance in Canada's SMEs: An exploratory investigation. *Internet Research*, *21*(3), 255–281. https://doi.org/10.1108/10662241111139309

INTERPOL. (2023). *African cyberthreat assessment report 2023*. INTERPOL.

Jagar, J. P. (2017). More than just convenient: The scientific merits of homogeneous convenience samples. *Monographs of the Society for Research in Child Development*, *2*, 13–30.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Kshetri, N. (2017). The emerging role of big data in key development issues: Opportunities, challenges, and concerns. *Big Data for Development*, 1–21. Springer.

Kuan, K. K., & Chau, P. Y. (2001). A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. *Information & Management*, *38*(8), 507–521. https://doi.org/10.1016/S0378-7206(01)00073-8

Kumar, R. (2008). *Research methodology*. Aph Publishing Corporation.

Katuu, S. (2022). Cybersecurity and the human element in African SMEs. *Journal of Digital Resilience*.

Krueger, R. A., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research* (5th ed.). SAGE Publications.

Massoudi, M., & Birdawod, H. (2024). The impact of technological and economic factors on cybersecurity management. *Internext*.

Ministry of ICT & National Guidance. (2023). *National cybersecurity strategy*. Republic of Uganda.

Mohamed, & Abuobied, A. (2024). Cybersecurity and the United Nations Sustainable Development Goals: A global analysis. *Journal of Cyber Policy*, *9*(1), 1–20.

Mubangizi, A. (2023). Digital literacy and cybersecurity awareness in Uganda's SMEs. *Uganda Journal of Management and IT*, *12*(2), 77–94.

Mutembei, K. (2018). Cybersecurity challenges facing SMEs in East Africa. *International Journal of ICT Research in Africa and the Middle East*, *7*(1), 1–14. https://doi.org/10.4018/IJICTRAME.2018010101

Mwanje, A., Ocen, G. K., Tumwebaze, R., & Bukenya, B. (2023). A framework to enhance information security governance in SMEs. *Science Journal of Engineering and Technology*, *11*(1), 1–8.

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. African Centre for Technology Studies.

National Cyber Security Centre. (2022). *Cybersecurity Breaches Survey 2022*. GOV.UK.

National Planning Authority. (2020). *Third national development plan (NDP III) 2020/21 - 2024/25*.

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation*, *14*(1), 110–121.

Proofpoint. (2024). *2024 State of the phish*. Proofpoint, Inc.

PwC. (2024). *Global economic crime and fraud survey 2024: Uganda report*.

Robinson, R. S. (2014). Purposive sampling. In A. C. Michalos, *Encyclopedia of Quality of Life and Well-Being Research*. Springer.

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). Free Press.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Scupola, A. (2009). SMEs' e-commerce adoption: Perspectives from Denmark and Australia. *Journal of Enterprise Information Management*, *22*(1/2), 152–166. https://doi.org/10.1108/17410390910932803

Serianu. (2024). *Africa cybersecurity report 2023/2024: Uganda country profile*. Serianu Limited.

Smith, J., et al. (2023). Cybersecurity capacity building in human capital for SMEs. *IRE Journals*.

Taherdoost, H. (2022). Different types of data analysis; data analysis methods and techniques in research projects. *International Journal of Academic Research in Management*, *9*.

Tambunan, T., & Nsubuga, F. (2024). SME development, technology adoption and cybersecurity in developing countries. *International Journal of Entrepreneurship and Small Business*, *52*(2), 187–204.

Thong, J. Y. (1999). An integrated model of information systems adoption in small businesses. *Journal of Management Information Systems*, *15*(4), 187–214. https://doi.org/10.1080/07421222.1999.11518227

Tisdale, S. M. (2015). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *Journal of International Technology and Information Management*, *24*(4), 25–40.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

Turyahikayo, E. (2015). Challenges faced by SMEs in Uganda and their implications for poverty eradication. *International Journal of Research in Business and Management*, *2*(5), 16–21.

Turyahikayo, J. (2015). A conceptual framework on resource availability and performance of MSE in Africa: A case of Jinja District, Uganda. *Open Journal of Business and Management*, *3*(2), 12–18.

Turyakira, P. K. (2022). Digitalization and the evolution of SME threat landscapes in East Africa. *Uganda Business Review*.

Uganda Bureau of Statistics (UBOS). (2020). *Uganda business inquiry 2019/20: Report on the census of business establishments*.

Uganda Bureau of Statistics (UBOS). (2024). *2024 Statistical abstract*.

Uganda Communications Commission (UCC). (2023). *Annual communications sector performance report 2022/23*.

Uganda Communications Commission (UCC). (2025). *Market performance report, Quarter 2 April to June 2025*.

Uganda Investment Authority (UIA). (2016). *Small and medium enterprises (SME) policy framework*.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315.

Verizon. (2024). *2024 data breach investigations report*. Verizon Enterprise Solutions.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

Walliman, N. (2006). *Social research methods*. SAGE Publications, Ltd.

Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper and Row.

Yin, R. K. (2009). *Case study research: Design and methods*. Sage.

Zeadally, S., Hunt, R., Chen, Y. P., Irwin, A., & Hassan, A. (2012). Cybersecurity challenges for SMEs in developing economies. *International Journal of Computer Applications*, *45*(21), 23–29.

Zhu, K., Kraemer, K. L., & Xu, S. (2006). The process of innovation assimilation by firms in different countries: A technology diffusion perspective on e-business. *Management Science*, *52*(10), 1557–1576. https://doi.org/10.1287/mnsc.1050.0487

Appendices:

Appendix 1 Interview Form

INTERVIEW FORM

Name of Interviewee:

……...……

Date of interview ……..……...….

Location……....

Name of student conducting interview: ……...

Appendix 2 Questionnaire

QUESTIONNAIRE

1. Quantitative Instrument: SME Cybersecurity Questionnaire (n=177)

Instruction: Use a 5-point Likert scale for Sections B, C, and D, where 1 = Strongly Disagree and 5 = Strongly Agree.

Section A: Demographic and Organizational Information (Context)

1. What is your role in the company?

   ( ) Owner / Manager

   ( ) IT Staff

   ( ) Other Employee

2. What is the primary sector of your business?

   ( ) Trade/Retail

   ( ) Manufacturing

   ( ) Services (e.g., hospitality, finance)

   ( ) Other (Specify: _____)

3. How many full-time employees does your company have? (Uganda SME Classification)

   ( ) Small Enterprise (5-49 employees)

   ( ) Medium Enterprise (50-100 employees)

4. How long has your company been operating in Jinja City?

   ( ) Less than 3 years

   ( ) 3 to 5 years

   ( ) More than 5 years

Section B: Prevalent Cybersecurity Threats (RQ 1: Threats)

This section identified common threats (Environmental factors in the TOE model).

No.	Statement	1	2	3	4	5
1.	Our SME frequently faces phishing emails or malicious links.					
2.	Our SME has recently experienced financial loss due to a cyberattack (e.g., fraud, ransomware).					
3.	Unsecured customer data is a major concern for our business reputation.					
4.	We have experienced unauthorized access or data loss from external sources.					
5.	Our company has specific policies to address threats from mobile devices or external USB drives.					

Section C: Level of Cybersecurity Awareness and Literacy (RQ 2: Awareness)

This section measured internal knowledge and training (Organizational factors in the TOE model).

No.	Statement	1	2	3	4	5
1.	I am confident in my ability to identify and report a cyber threat.					
2.	Our company conducts mandatory cybersecurity training at least once a year.					
3.	Employees regularly change and use strong, complex passwords.					
4.	Management views cybersecurity training as an important investment for the business.					
5.	Our company has a formal, documented plan for what to do immediately after a security breach.					

Section D: Factors Influencing Adoption of Cybersecurity Measures (RQ 3: Factors)

This section assessed the internal and external pressures/barriers to adopting security tools (Technology, Organization, and Environment factors).

No.	Statement	1	2	3	4	5
1.	(Technology) The cost of implementing cybersecurity software (e.g., antivirus, firewall) is a major barrier for our SME.					
2.	(Organization) Our company's management is fully committed to funding and supporting cybersecurity initiatives.					
3.	(Organization) We lack the internal IT skills to manage and maintain complex security systems.					
4.	(Environment) Cybersecurity compliance requirements from regulators (e.g., UCC) influence our decisions to adopt security measures.					
5.	(Technology) We believe that most available security technologies are too complex to integrate into our existing business processes.					
6.	(Environment) Peer companies or competitors' cybersecurity incidents motivate us to invest in protection.					

INTERVIEW & FOCUS GROUP DISCUSSION QUESTIONS

2. Qualitative Instruments: Interviews & FGDs

These questions are designed to elicit rich, explanatory data, using open-ended phrasing.

A. Semi-Structured Interview Questions (Owners/Managers, n=5)

Focus: In-depth understanding of decision-making, costs, and strategic challenges.

Preamble: (General SME Context)

1. Can you briefly describe the typical IT infrastructure and key systems your SME uses (e.g., POS systems, cloud services)?

Alignment to RQ 1: Prevalent Cybersecurity Threats

2. From your perspective as a manager, what are the three most concerning cyber threats your business currently faces, and what tangible evidence of loss or disruption have you seen?

3. Have you experienced a data breach or system downtime in the last year? If so, what was the estimated financial cost (direct or indirect)?

Alignment to RQ 2: Level of Cybersecurity Awareness

4. How would you rate the cybersecurity literacy of your non-IT employees? What challenges do you face in getting employees to take security seriously?

5. What formal or informal steps do you take to continuously train staff on emerging threats?

Alignment to RQ 3: Factors Influencing Adoption

6. When considering buying a new security solution (e.g., firewall, security consulting), what are the top three factors that drive or hinder your final decision? (Probe for: Cost, Complexity, Return on Investment, Regulatory Pressure)

7. To what extent does the need to comply with external regulations (UCC, data protection laws) or customer demands influence your cybersecurity spending?

Alignment to RQ 4: Recommendations (Output)

8. Based on your experience, what practical, cost-effective recommendation would you suggest to a newly established SME in Jinja to improve its cybersecurity preparedness?

B. Focus Group Discussion (FGD) Questions (Employees, n=20)

Focus: Ground-level experience, cultural awareness, and perceived usability of security measures.

Preamble: (Icebreaker)

1. How important is it for you personally to keep the company's data safe? (Why?)

Alignment to RQ 1 & 2: Threats and Awareness

2. What does the term "cyberattack" mean to you? Can you describe the most common type of cyber security challenge you encounter during your daily work (e.g., email, browsing)?

3. Describe the last time you received a security alert or suspicious email. What did you do, and did you feel confident in your response?

4. How often do you receive formal training on cybersecurity from your company, and do you feel the training is relevant to the threats you actually face?

Alignment to RQ 3: Factors Influencing Adoption

5. What are the most annoying or time-consuming security measures you are required to follow (e.g., complex passwords, frequent logouts)? Do these hinder your work?

6. If you had a say, what simple security tool or policy would you ask your company to implement

to make your job easier and safer?

Alignment to RQ 4: Recommendations (Output)

7. What is one easy and affordable action your SME could take today to make a noticeable difference in its security?

Appendix 3 AUREC Approval

"Investing in Africa's future"

AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE (AUREC)

P.O. Box 1320 Mutare, Zimbabwe, Off Nyanga Road, Old Mutare-Tel (+263-20) 60075/60026/61611 Fax: (+263 20) 61785 Website: www.africau.edu

Ref: AU4133/25

4 December, 2025

IRMIYA SAMSON
C/O Africa University
Box 1320
MUTARE

RE: ASSESSING THE CYBERSECURITY PREPAREDNESS OF SMALL AND MEDIUM-SIZED ENTERPRISES IN JINJA CITY, UGANDA

Thank you for submitting the above-titled proposal to the Africa University Research Ethics Committee for review. Please be advised that AUREC has reviewed and approved your application to conduct the above research.

The approval is based on the following.

a) Research proposal

- **APPROVAL NUMBER** AUREC 4133/25
  This number should be used on all correspondence, consent forms, and appropriate documents
- **AUREC MEETING DATE** NA
- **APPROVAL DATE** December 4, 2025
- **EXPIRATION DATE** December 4, 2026
- **TYPE OF MEETING**: Expedited
  After the expiration date, this research may only continue upon renewal. A progress report on a standard AUREC form should be submitted a month before the expiration date for renewal purposes.
- **SERIOUS ADVERSE EVENTS** All serious problems concerning subject safety must be reported to AUREC within 3 working days on the standard AUREC form.
- **MODIFICATIONS** Prior AUREC approval is required before implementing any changes in the proposal (including changes in the consent documents)
- **TERMINATION OF STUDY** Upon termination of the study a report has to be submitted to AUREC.

Yours Faithfully

MARY CHINZOU
FOR CHAIRPERSON
AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE

Appendix 4 Letter of Introduction

JINJA CITY

OFFICE OF THE CITY CLERK
P.O BOX 720,
Jinja

Tel: 256-0772653980
E-Mail: mosesotimong96@gmail.com

Ref.CR.1001

December 5, 2025

TO WHOM IT MAY CONCERN

INTRODUCTION OF MR. IRMIYA SAMSON

This is to introduce to you Mr. Irmiya Samson Reg.No.AUREC 4133/25 who is pursuing Executive Master in Business Administration at Africa University who would wish to carry out his ***Research Title: ASSESSING THE CYBERSECURITY PREPAREDNESS OF SMALL AND MEDIUM SIZED ENTERPRISES IN JINJA CITY.***

The purpose of this letter therefore, is to request that you accord him all necessary information required. By copy of this letter the City IT Officer is hereby requested to work hand in hand with the Researcher.

Yours Sincerely,

For: City Town Clerk
Jinja City Council

Ndahura Isabella,
For: CITY TOWN CLERK

Copy: The Resident City Commissioner
" His Worship the City Mayor
" The City IT Officer

OM/ee