Article

Bridging the Cybersecurity Gap: Tailored Strategies for Zambia's SMEs

Goni Saar
https://orcid.org/0009-0003-9582-5864
The DaVinci Institute
gonisaar2011@gmail.com

Rabelani Dagada
https://orcid.org/0000-0002-3025-6678
University of South Africa
dagadr@unisa.ac.za

Abstract

This research examines cybersecurity awareness and implementation within Zambia's small and medium-sized enterprises (SMEs), a sector increasingly targeted by cyberattacks that cause substantial financial losses. The study aimed to enhance cyber awareness and develop actionable guidelines for SMEs in Zambia. Utilising an interpretive philosophy and inductive approach, the methodology encompassed semi-structured interviews, cross-sectional analysis, and a comprehensive review of CISA, ENISA guidelines, and Zambia's Data Protection Act. Findings indicate a notable deficit in cybersecurity training and awareness among SMEs. Key concerns include inadequate data security measures, a lack of formal cybersecurity policies, and a reliance on basic tools like antivirus software. In response, the study formulated targeted guidelines that emphasise integrating cyber awareness into SME governance and risk management. These guidelines have garnered significant interest from Zambian government entities, highlighting their potential influence on national cybersecurity policy. The study contributes theoretically by contextualising international cybersecurity standards within Zambia's unique SME landscape. Methodologically, it pioneers a cyber awareness framework tailored to Zambian SMEs, underscoring the critical role of human factors in cybersecurity. In practice, the research has sparked engagement among SMEs and government bodies, demonstrating its applicability and potential to shape policy. However, limitations include reliance on outdated demographic data and a focus on digitally enabled SMEs, potentially overlooking broader IT governance aspects and less digitised businesses. Future research should aim for comprehensive, up-to-date analyses across all SME sectors, contributing to a more inclusive and resilient cybersecurity landscape in Zambia.

UNISA
Southern African Journal of Security
Volume 3 | 2025 | #15713 | 43 pages

https://doi.org/10.25159/3005-4222/15713
ISSN 3005-4222 (Online)

Keywords: cybersecurity awareness; SMEs; Zambia; data protection; cybersecurity guidelines; financial impact of cyberattacks

Introduction

Cybersecurity threats are among the most pressing challenges negatively affecting businesses and nations worldwide in the 21st century. Modern lifestyle is characterised by people's reliance on technology for their daily activities, such as shopping, financial transactions, and other aspects of their daily routines (Rajasekharaiah, Dule, and Sudarshan 2020). Additionally, with the growth and popularity of social media, cybercrime has increased in parallel. Most government leaders, in both developing and developed nations, have embarked on providing cybersecurity because it is the key to stimulating prosperous and enhanced national security (Shafqat and Masood 2016). However, cyber threats continue to increase despite these efforts. In the digital age, cybersecurity has emerged as a critical issue due to the rising number of cyberattacks and data breaches. This has led to significant financial repercussions. The economic significance of cybersecurity is a notable factor in the digitalisation of national economies (Demchyshak and Shkyria 2021). This multifaceted aspect can be examined from various angles, including the cost of cybercrime, the impact of cyberattacks on businesses, and the economic benefits associated with cybersecurity investments.

Morgan (2022) highlights the escalating costs of cybercrime, projecting damages of US$8 trillion in 2023 and US$10.5 trillion in 2025, compared to US$3 trillion in 2015. Such statistics underscore the growing financial consequences of cyber threats and the urgency to address them effectively.

In the business sector, the connection between businesses and cybersecurity has become indisputable in the 21st century. Dagada (2021) emphasises the pervasive adoption of digital platforms by businesses worldwide. The Fourth Industrial Revolution, characterised by rapid technological advancements such as artificial intelligence, the Internet of Things, and robotics, further accentuates the need to address the cybercrime associated with these technological developments. With both the government and private sectors embracing digitalisation, cybersecurity is no longer an optional consideration but an imperative investment to mitigate substantial losses incurred through cyberattacks.

Cyberattacks can inflict significant damage on businesses, ranging from reputational harm and financial losses to legal liabilities. A study conducted by the Ponemon Institute found that the average cost incurred by a breach of data for a company in 2020 was US$3.86 million (Ponemon Institute 2020). Business-related cyberattacks can also have wider implications and pose a national threat to nations.

Kozak (2017) accentuates the criticality of regional economies, wherein small and medium-sized enterprises (SMEs) are prominent in driving a country's economic development. This importance is particularly pronounced in rural areas, where SMEs

serve as primary employers, fostering local economic growth (Kozak 2017). According to the Zambia Development Agency (ZDA), SMEs account for an estimated 70% of the employed population and contribute about 20% to the GDP (Zambia Development Agency 2020).

Every year, Zambia is subjected to an increasing number of cyberattacks that result in losses of hundreds of millions of Kwacha (National Assembly of Zambia 2022). ICT use in Zambia has grown rapidly (ZICTA 2021), making dealing with this substantial cybersecurity issue a major challenge for the country's economy. The challenge to cybersecurity in Zambia may be caused by businesses or companies having limited expertise in cybersecurity. Cyber threats have significantly harmed the Zambian economy, with the Zambia Computer Incident Response Team reporting a surge in cyberattacks, culminating in losses of over 150 million Zambian Kwacha in 2021 alone, including losses from deceptive investment schemes (National Assembly of Zambia 2022). Contributing to the rise of such cyber incidents is a notable deficiency in cybersecurity awareness. This is highlighted by a study on information security awareness among Zambian higher education employees. This study found a lack of adequate information, limited security training, and a dearth of support from the upper echelons of management (Halubanza, Kunda, and Musonda 2016).

Zambia's legislative advancements, particularly the enactment of the Data Protection Act No. 3 of 2021, established a foundational legal framework for personal data protection through the establishment of the Office of the Data Protection Commissioner (Government of Zambia 2021). Despite these steps, Zambia encounters continuous cybersecurity challenges, including technical skill shortages, infrastructural inadequacies, and a general lack of cyber threat awareness (Mwila 2020). A comprehensive strategy that integrates legislative efforts, capacity building, and public education, augmented by international collaboration, is essential to navigating these challenges (Khunga and Kunda 2017; ZICTA 2022).

Research Problem and Purpose of the Study

Cybercrime is having a huge impact globally, with damages increasing from US$3 trillion in 2015 to 10.5 trillion by 2025 (Morgan 2022). Within this context, SMEs are identified as particularly at risk, lacking robust cybersecurity knowledge and measures, leading to significant financial and reputational losses (Sangani and Vijayakumar 2012). These are more pronounced in SMEs due to a lack of early detection and preventive strategies, as well as pervasive misunderstandings about cybersecurity (Yudhiyati, Putritama, and Rahmawati 2021; Imsand, Tucker, Paxton, and Graves 2020; Berry and Berry 2018), unlike larger enterprises with more resources for fostering cyber risk awareness (Hadlington 2018). This study responds to such challenges by examining cybersecurity knowledge and practices among Zambian business employees.

The study aimed to explore knowledge and practices of cybersecurity amongst individuals in the Zambian business sector, as well as to develop guidelines that enhance cyber awareness among employees. To attain the set purpose, the objectives were outlined as follows:

1. To explore the knowledge and practices of cybersecurity among employees in the business sector in Zambia.

2. To identify key factors influencing the implementation of cyber awareness among employees in the business sector in Zambia.

3. To create feasible guidelines that promote greater cybersecurity awareness within the business sector.

Before embarking on the study, the principal researcher found that there was a lack of literature regarding cyber awareness in Zambia. There was no substantive literature discussing the state of cyber awareness in Zambia's business sector, nor how to help business owners create it.

Within this context, the research question is formulated as follows:

1. What are the knowledge and practices of cybersecurity in the business sector in Zambia, and how can guidelines be created to enhance cyber awareness among employees?

To answer the research question, it was necessary to answer the following sub-questions:

1.1. How do employees in the business sector of Zambia view and implement cybersecurity practices, and why do they hold those views?

1.2. What are the key factors that influence the implementation of cyber awareness among employees in the business sector in Zambia?

1.3. How can feasible guidelines be created to promote greater awareness of cybersecurity within the business sector?

The Vulnerability of SMEs to Cyberattacks

Cybersecurity in Zambia, and more broadly throughout Africa, has emerged as a significant concern amid the rapid technological advancement that characterises the region. The burgeoning use of digital services like mobile money has paradoxically expanded the cybersecurity threat landscape (Dagada 2013). A notable 3.8% increase in cyberattacks in 2020 highlights a critical need for fortified cybersecurity frameworks to protect an increasingly digital-dependent economy, especially within the Zambian

business sector. This literature review explores the cybersecurity environment, emphasising the necessity of heightened cyber awareness being acutely attuned to the unique requirements of Zambian enterprises (Yokohama 2016; Ofori-Sarpong and Adomako 2020; Serianu 2020).

The economic ramifications of cybercrime are profound, with anticipated costs possibly reaching an unprecedented US$10.5 trillion by 2025 (Morgan 2022). Data breaches, which on average inflict costs of US$3.86 million, starkly illustrate the deep interconnection between a firm's operational sustainability and cybersecurity (Ponemon Institute 2020). The World Economic Forum has highlighted the potential for cybersecurity investments to unlock considerable economic value by defending infrastructural assets and fostering reliable digital interactions (World Economic Forum 2018).

SMEs are the cornerstone of economic growth, accounting for a substantial portion of GDP and employment in emerging economies. Zambia's reliance on SMEs for socio-economic development, employment, and fiscal income underscores their critical role in maintaining national economic resilience (World Bank n.d.; Kozak 2017; Nuwagaba 2015). Consequently, cybersecurity emerges as a strategic economic safeguard, essential for protecting SMEs against the detrimental impacts of cyber threats, which can destabilise their operations, erode customer confidence, and result in severe financial losses.

Globally, businesses confront the financial and operational consequences of cyber threats, with reports by the FBI revealing significant monetary losses and major cyber incidents like the Colonial Pipeline and Target breaches demonstrating the potential for substantial financial repercussions (Federal Bureau of Investigation 2020; Robles-Carrillo and García-Teodoro 2022; Eaton and Dustin 2021). Intellectual property theft and the legal consequences of non-compliance with data protection regulations, such as GDPR, emphasise the imperative for stringent cybersecurity frameworks (European Commission 2016; Dagada 2014).

SMEs are susceptible to cyber threats, leading to significant financial and operational setbacks, and in many cases, culminating in the closure of affected businesses. Their vulnerability is often magnified by limited resources and a deficiency in specialised cybersecurity knowledge and personnel (Federation of Small Businesses 2019; Lambeth and Høglo 2020). Despite the prevalence of fundamental cybersecurity measures like firewalls and data backups, the lack of comprehensive IT and cybersecurity expertise leaves SMEs vulnerable to sophisticated cyber threats (ENISA 2021; Senarathna, Wilkin, Warren, Yeoh, and Salzman 2018).

The challenge of cybersecurity is inherently global, with threats that transcend national borders and affect regions differently. Developed areas like North America and Europe exhibit enhanced cyber awareness owing to comprehensive regulatory initiatives like

GDPR. In contrast, Africa presents a marked variance in cybersecurity readiness. Nations such as South Africa have demonstrated significant progress in cybersecurity, while others are just beginning to formulate cyber defences (Clough 2014; ITU 2020; Cassim 2017).

The Zambian business environment, a substantial contributor to the nation's GDP and employment, is undergoing a dynamic transition fuelled by digital innovation. SMEs, which make up a significant portion of employment and national GDP, are challenged by factors including limited resources and a nascent understanding of cybersecurity (Zambia Development Agency 2020; Bwenbya 2022). Furthermore, the informal sector, despite its significance, is characterised by a paucity of comprehensive data, and the expansion of the IT sector necessitates rigorous cybersecurity measures to uphold confidence in digital transactions and services (Mukubesa 2021; Banda and Hapompwe 2023). In Zambia's evolving digital economy, which depends on secure data and system operations, cybersecurity has become indispensable. The country's ongoing digital revolution is inextricably linked with the need for robust cybersecurity measures. The Zambia Information and Communications Technology Authority (ZICTA), through the 2009 ICT Act and subsequent cybersecurity legislation, spearheads initiatives to counteract cybercrime and enhance data protection. However, the current Data Protection Act's lack of specific guidelines for businesses indicates a need for more comprehensive regulations (Government of Zambia 2009; Government of Zambia 2021). Zambia is witnessing an increase in cyber incidents, with significant consequences for the financial sector and government entities. Annual reports reveal millions of cyber incidents, with common threats including phishing, malware, and distributed denial-of-service (DDoS) attacks leading to considerable disruption in operations and economic distress (National Assembly of Zambia 2022; Kaspersky 2021; Minnaar 2019; Akamai 2021). Notable cyber breaches at prominent financial institutions and government agencies underscore the urgency of a multifaceted cybersecurity strategy to secure Zambia's digital future (Lusaka Times 2019; Lusaka Times 2022; Zambian Observer 2023).

The pressing issues presented in this review underline the critical juncture at which Zambia's cybersecurity readiness stands. The need for a strategic layered defence mechanism to secure Zambia's digital landscape against the escalating sophistication of cyber threats is more urgent than ever. It is an imperative that encompasses not only technological and regulatory frameworks but also a broader cultural shift towards heightened cyber awareness and resilience.

Theoretical Framework

This research utilises the Cyber Security Awareness and Education Framework, formulated by Kortjan and von Solms (2014). This framework was originally designed to enhance cybersecurity culture at a national level within South Africa. The framework, informed by an analysis of cybersecurity practices in OECD countries, proposes a five-

layered structure for cybersecurity awareness. However, for this research, only three layers most pertinent to the organisational context have been utilised:

1. **Strategic Layer:** Outlines the overarching vision and policies for cybersecurity within an organisation, as well as delineating the "responsible unit" for implementing these measures. The study examines whether employees are aware of and adhere to these policies and how responsibility is perceived within the company structure.

2. **Tactical Layer:** Involves actionable steps taken by an organisation, such as cybersecurity training and education programmes. The research assesses an organisation's commitment to educating its employees and the effectiveness of these programmes in changing behaviour.

3. **Monitoring Layer:** Deals with the ongoing evaluation of cybersecurity initiatives. This study focuses on whether organisations monitor employee compliance and how they respond to infractions.

Although this framework was intended for national use, it also offers valuable insights for the private sector. By considering a company as a "microcosm of a country," it is possible to apply similar measures to instil cybersecurity awareness within the business sector.

The conceptual framework of this study, derived from the theoretical framework and supplemented by a concept identified through the comprehensive literature review, is built upon a selection of core concepts pertinent to the business sector:

1. **Cybersecurity Policy:** This involves an exploration of company policies related to cybersecurity, aiming to understand how these policies are perceived and implemented by employees, and the extent to which they contribute to a secure corporate culture.

2. **Responsibility:** The research explores perceptions of responsibility for cybersecurity within organisations, distinguishing between the roles and expectations of employees and upper management.

3. **Training:** An exploration of educational initiatives in place to assess whether training efforts are effective and how they shape employees' cybersecurity behaviours and attitudes.

4. **Monitoring:** The study explores organisational practices in monitoring cybersecurity measures, including the impact of such oversight on employee behaviour and policy compliance enforcement.

5. **Actions:** This examines the proactive steps employees take to secure organisational data and assets, reflecting on the overall cybersecurity mindset within the company.

These concepts resonate with the broader definitions provided by Schatz et al. (2017) and Shaw et al. (2009), which emphasise the importance of policy, training, and individual responsibility in creating a robust cybersecurity environment.

Figure 1 below illustrates the conceptual framework relations, whose path begins with organisational actions, followed by employees' actions and knowledge:

Figure 1: Conceptual Framework Relations

Table 1 below, definitions and concept alignment, has been meticulously compiled following a comprehensive review of CISA's and ENISA's guidelines for SMEs. This analysis was conducted in alignment with the previously defined concepts of cybersecurity and cyber awareness, as well as the established conceptual framework. The primary objective of this tabulation is to determine the most suitable guidelines for enhancing cyber awareness among businesses in Zambia and augmenting the cybersecurity posture of enterprises in the country. This systematic approach ensures that the selected guidelines are not only relevant to the Zambian context but also effectively address the twin objectives of raising cyber awareness and strengthening cybersecurity in the business sector.

	Definitions		Concepts				
Guideline	**Cyber security**	**Cyber awareness**	**Cyber security policy**	**Responsibility**	**Training**	**Monitoring**	**Actions**
CISA Small Business Guidelines Presentation							
Shared Responsibility	✓	✓		✓			
Assess Risk and Identify Weaknesses	✓	✓		✓			✓
Create a Contingency Plan	✓		✓	✓			
Educate Employees	✓	✓		✓	✓		
Back-Up Critical Information	✓		✓				✓
Secure Your Internet Connection	✓		✓				
CISA Small Business Tip Card							
Equipping All Computers with Anti-Virus and Anti-Spyware	✓		✓				
Regularly Updating Antivirus and Antispyware	✓		✓				
Require Employees to Use Strong Passwords	✓	✓	✓	✓			✓
Protect All Pages on Your Websites	✓		✓				
CISA Cyber Guidance for Small Businesses							

Appointment of Roles	✓	✓	✓	✓	✓		
Establish a Culture of Security	✓	✓	✓	✓			
Select and Support a "Security Programme Manager"	✓					✓	
Review and approve the Incident Response Plan (IRP)	✓		✓				
Participate in tabletop exercise drills (TTXs)	✓		✓		✓		
Support the IT leaders	✓					✓	
Multi-Factor Authentication	✓		✓				
Training	✓	✓		✓	✓		✓
Host Quarterly Tabletop Exercises	✓	✓	✓	✓	✓		✓
Ensure MFA is Mandated Using Technical Controls, Not Faith	✓		✓			✓	
Patch	✓		✓				
Remove Administrator Privileges from User Laptops	✓		✓				
Enable Disk Encryption for Laptops	✓		✓				
On-Premises vs. Cloud	✓		✓				

ENISA SMEs Guidelines							
Publish Cybersecurity Policies	✓	✓	✓	✓			✓
Conduct Cybersecurity Audits	✓		✓			✓	
Remember Data Protection	✓		✓				
Provide Appropriate Training	✓	✓	✓	✓	✓		✓
Ensure Effective Third-Party Management	✓		✓				
Employ Email and Web Protection Tools	✓		✓			✓	
Implement Mobile Device Management	✓		✓			✓	
Improve Physical Security	✓	✓	✓	✓			✓
Secure Online Sites	✓		✓				

Research Methodology

The study adopted Saunders' research onion, which outlines the entire process of determining a research philosophy and defining theoretical approaches:

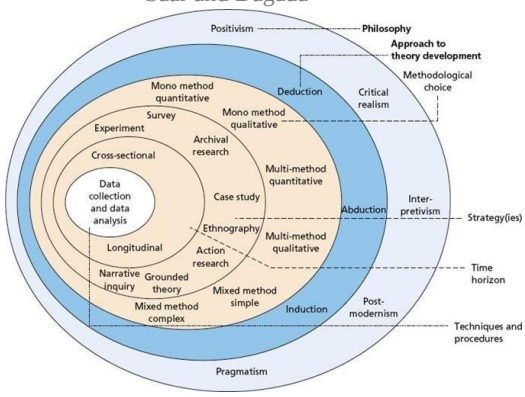

Figure 2: Saunders et al.'s Research Onion

Research Philosophy: Interpretivism

Interpretivism played a central role in this qualitative research, emphasising the subjective construction of reality through language and shared meanings (Myers 2008). It valued diverse perspectives, acknowledging that values differ rather than being right or wrong (Aliyu and Adamu 2015). In this study on cybersecurity awareness, the principal researcher's professional insights informed the interpretive approach premised on a commitment to being open to various viewpoints and experiences throughout the research process.

Research Approach: Inductive

The inductive approach, aligning with the second layer of the research "onion," guided this study within the qualitative methodology. It proved effective in handling raw data from individuals across various businesses. This bottom-up research harnessed participant views to form broader themes and theories on cybersecurity challenges in Zambia's business sector (Creswell 2011), facilitating a nuanced analysis of the qualitative data.

Methodological Choice (Strategy): Multi-Method Qualitative

The adopted strategy was grounded in a humanistic and interpretive perspective, aiming to understand human experiences deeply. It underscored the significance of preserving and scrutinising the form, content, and intricacies of social interactions as they occur naturally, avoiding the simplification often associated with quantitative analysis (Jackson, Drummond, and Camara 2007; Lindlof and Taylor 2002; Chesebro and Borisoff 2007). The choice of this approach was particularly effective for exploring cybersecurity awareness among professionals in Zambia's business sector, facilitated through semi-structured interviews. Additionally, document analysis provided a complementary method, helping to extract pertinent themes, best practices, and

legislative frameworks. This combination of techniques ensured a thorough and dependable foundation for the study's conclusions.

Research Type: Exploratory

This exploratory study was driven by a notable gap in the existing literature on cybersecurity awareness in Zambia's business sector. Adopting the exploratory research design facilitated a deeper understanding of this under-investigated area (Hunter and Howes 2019; Sehularo, Du Plessis, and Scrooby 2012). Questions were specifically designed to elicit insights into the current state of cyber awareness among professionals, thereby laying the groundwork for future scholarly work and practical interventions.

Data Collection Instruments

The following data collection instruments were employed in this study: semi-structured in-depth interviews, cross-sectional tools, and document analysis.

Semi-structured in-depth interviews

The study conducted semi-structured in-depth interviews following a cross-sectional approach. Guided by research objectives, a systematic set of questions was crafted from the literature to elicit targeted data from participants. Each interview began with obtaining consent for recording, assuring confidentiality, and ensuring the interviewee's comfort. These one-on-one interviews, conducted in person, adhered to a recommended duration of 20 minutes (Koshy 2010).

Cross-sectional tool

The research employed a cross-sectional study to capture a snapshot of cybersecurity awareness at a single point in time. This approach is suitable for estimating characteristics, attitudes, and knowledge—the core objectives of the study. It facilitated data collection from different individuals simultaneously, providing a robust view of current cybersecurity practices in Zambia's business sector and lending credence to the research findings (Levin 2006; Kesmodel 2018).

Document analysis

Document analysis was conducted on five essential texts. Four documents from the globally recognised cybersecurity authorities, CISA and ENISA, provided targeted cybersecurity guidelines for SMEs. Additionally, Zambia's Data Protection Act was analysed. The Act outlines legal obligations for businesses to manage personal data. This comprehensive document review was necessary to validate the research findings against established cybersecurity practices and statutory requirements, ensuring that the study's recommendations are both actionable and compliant for SMEs in Zambia. The analysis further deepened the study's insights by correlating the established guidelines and legal framework with the literature review and conceptual framework, enhancing the study's overall validity and relevance to the Zambian business context.

Population and Sampling

This section discusses the targeted population, sampling strategy, and sampling size.

Target Population

Small and medium-sized enterprises' employees formed the target population for the study. The selection of employees from the enterprises acknowledged the vulnerability of SMEs to cyber threats due to typically limited resources and less stringent policies than larger firms. The research included employees at different organisational levels rather than focusing only on senior management. This recognises that cyberattacks can target any employee and that the entire organisation is responsible for cybersecurity (Hadlington 2018; Tischer et al. 2016).

Sampling strategy: Purposive Sampling

The study employed purposive sampling, a non-probability technique ideal for qualitative research, allowing for in-depth exploration of specific traits within the participant pool (Creswell 2014; Palinkas et al. 2015). Participants were chosen for their direct experience with cybersecurity in the Zambian business context, leveraging the principal researcher's industry connections to identify individuals who could provide relevant insights (Patton 2015). This sampling method ensured that interviewees could contribute meaningfully to the research objectives based on their knowledge and experience.

Table 2 below summarises the participants involved in the study:

Serial No.	Designation	Sector of Operation
Participant 1	Employee	Technology
Participant 2	Manager	Logistics and customs clearing
Participant 3	Employee	Customs clearing
Participant 4	Employee	Agriculture and retail
Participant 5	Administrative Assistant	Technological solutions
Participant 6	Manager	Customs clearing and forwarding
Participant 7	Employee	Logistics
Participant 8	Head of Finance and Administration	Technology
Participant 9	Employee	Logistics
Participant 10	Employee	Logistics
Participant 11	Employee	Logistics
Participant 12	Employee	Hospitality
Participant 13	Operations Manager	Communications and security
Participant 14	Employee	Hotel
Participant 15	Manager	Agric-manufacturing
Participant 16	Employee	Logistics and clearing
Participant 17	Manager	Hospitality
Participant 18	Employee	Logistics
Participant 19	Executive	Hospitality
Participant 20	Middle Management	Hospitality
Mr. Likando Lyuwa	Data Protection Commissioner	Government

Sampling Size

Saturation is essential for sampling and ensuring the quality of qualitative research. However, opinions differ about the number of interviews that should be conducted for saturation to be reached. Some argue for as few as six interviews to develop themes meaningfully (Guest, Bunce, and Johnson 2006) while others recommend more for credibility (Tran, Porcher, Tran, and Ravaud 2017; Mason 2010). There is no clear definition of saturation, as it is fluid, impacted by the interview analysis sequence (Constantinou, Georgiou, and Perdikogianni 2017).

Research on cybersecurity awareness often employs quantitative methods with large samples. However, qualitative studies in this area are limited, suggesting a knowledge gap in understanding the reasons behind the phenomena that quantitative studies identify. For instance, Paul and Whitley (2013) used six interviews to explore cyber

situation awareness, while Johansson et al. (2022) included 14 participants from five organisations.

Determining a sample size is a complex process influenced by a variety of factors, including the phenomenon's nature, complexity, and existing knowledge. An insufficient sample can lead to non-saturated data with superficial results (Morse 2015). Considering the pervasive nature of cyber awareness and risks in the Zambian business sector and the scant research, this study conducted 20 interviews. This number exceeds the suggested saturation point and compares favourably with participant numbers in prior qualitative research, ensuring comprehensive data collection without the risk of non-saturation.

Data Analysis

Thematic analysis was the primary method for analysing interview data in this study, involving a six-step process recommended by Kiger and Varpio (2020). It began with examining the interview data, coding to categorise the information, and identifying themes relevant to the research context. Coding was essential for comparing data segments and facilitating the formulation of theoretical constructs (Creswell 2014; Williams and Moser 2019).

Interview data were analysed for semantic content, with themes cross-referenced against literature to provide comprehensive insights. Additionally, document analysis of CISA and ENISA guidelines and Zambia's Data Protection Act informed the findings, ensuring industry relevance and legal compliance. This multi-layered analysis yielded a robust and holistic understanding of cybersecurity challenges and practices in Zambia's SME sector.

Trustworthiness of the Study

To ensure this study's trustworthiness, the methodology incorporated Creswell's (2014) guidelines for maintaining objectivity. Every interview was audio-recorded and supplemented with detailed notes to capture the full breadth of responses. Following the interviews, all responses were transcribed verbatim to facilitate a detailed and precise analysis, making these transcriptions the primary data for thematic analysis.

Once the data analysis and interpretation were complete, the derived conclusions and recommendations were presented to the interviewees for validation, enhancing the study's credibility. This feedback loop not only allowed for possible amendments but also provided interviewees with a comprehensive view of the research outcomes on cyber awareness. This contributed value to both the participants and the wider academic and professional community.

Research Ethics

To ensure ethical rigour in this research, the principal researcher obtained ethical clearance from the Da Vinci Institute, affirming adherence to their standards. Transparency with participants was prioritised; they were informed about the study's aims and how the data acquired from them would be used. This ensured that their participation was informed and voluntary. The respondents reiterated consent at the beginning of each interview.

Professional boundaries were strictly observed to prevent bias. Active listening was central to capturing unbiased data, and reflexivity helped manage potential researcher biases. Participant confidentiality was prioritised. Focus was on cyber awareness insights rather than personal information.

Finally, to validate the findings, participants were invited to review and evaluate the study conclusions, solidifying the trustworthiness of the research.

Findings of the Study

The findings of this study established several critical insights into cybersecurity awareness and practices among Zambian SMEs. These findings were guided by the study's objectives and research questions and informed by international guidelines from CISA and ENISA specifically designed for SMEs. The analysis drew on a nuanced thematic examination of in-depth interviews, a comprehensive review of Zambia's Data Protection Act, and an expert discussion with the Data Protection Commissioner.

This multi-layered approach, illustrated in Figure 3, structures the findings sequentially, with each layer contributing to a deeper understanding of cyber awareness and security within the Zambian business context. The practical guidelines developed from this process are integrated into the discussion and conclusion sections, providing recommendations tailored to enhance cyber awareness and cybersecurity measures for businesses in Zambia.

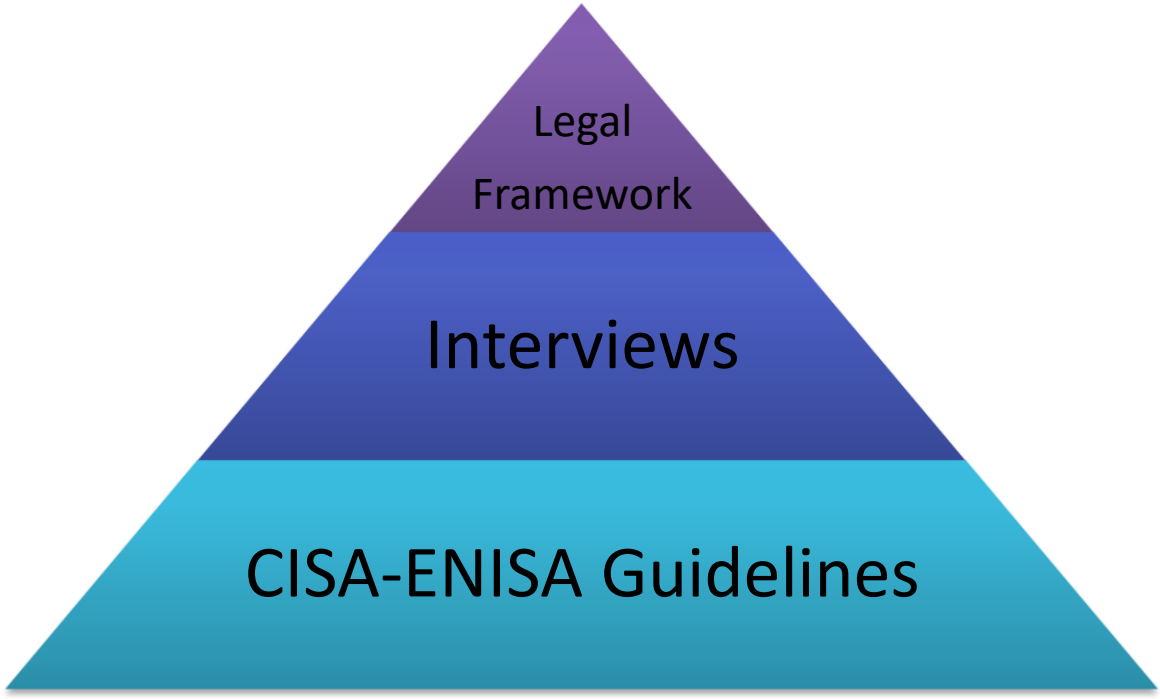

Figure 3- Layers of the Research Results

Interviews Analysis, Results, and Findings

This sub-section presents an in-depth analysis of data from semi-structured interviews with Zambian business sector participants, focusing on identifying patterns, themes, and sub-themes in cybersecurity knowledge, practices and perceptions. Employing qualitative research and thematic analysis aligns key themes with research objectives, incorporating relevant literature for context. The sections detail these themes, their relation to the research questions, and provide interpretations, culminating in a synthesis of findings that contribute to understanding cybersecurity in Zambia's business landscape.

Major Theme 1: Cybersecurity Knowledge and Practices among Employees

In an increasingly digital landscape, cybersecurity is essential for safeguarding assets (Gundu 2019). Employees are a key line of defence against cyber threats (Nifakos et al. 2021). Major Theme 1, Cybersecurity Knowledge and Practices among Employees, explores employees' cybersecurity awareness and actions in Zambia's business sector. This theme investigates their understanding of cyber threats, engagement in preventive measures, response to incidents, and their role in organisational cybersecurity. It aligns with the study's first objective: exploring employee cybersecurity knowledge and practices in Zambia to identify gaps and training needs. Subsequent sections analyse

this theme, offering a detailed view of employees' cybersecurity awareness and practices in Zambia.

Sub-Theme 1.1. Use of IT Systems and Cybersecurity

IT systems have transformed organisational operations, enhanced efficiency and innovation (Baskerville, Rowe, and Wolff 2018), while also raising cybersecurity stakes (Slusky 2020). The first sub-theme, Use of IT Systems and Cybersecurity, under Major Theme 1, examines the relationship between employees' IT usage and cybersecurity. It focuses on how tasks like emailing, data management, financial transactions, and business processes (Boyce et al. 2011) intertwine with cybersecurity. This sub-theme explores employees' perceptions and integration of cybersecurity in IT usage, probing their awareness of technology and security interplay.

The focus is on whether employees see cybersecurity as inherent in IT usage and understand the risks of a lax approach. It also examines the demand for enhanced security in IT systems use. This analysis aligns with the theme's goal of dissecting Zambian employees' cybersecurity knowledge and practices. The following sections examine these aspects, revealing how employees' interaction with IT systems intersects with their cybersecurity awareness.

Integration of IT systems in professional duties

IT systems are integral to professional duties, with cloud-based tools like Sage 200 enhancing financial tasks through real-time access (*"I'm using an accounting package which is Sage 200 and that's connected on the cloud..."*). Essential daily tools include desktop printers, computers, the internet, emails, and WhatsApp (*"Desktop printers, Computers, Internet, Wifi, Emails and WhatsApp"*).

Dual usage of IT systems—personal and professional

IT system use often overlaps between work and personal life, with common tools like laptops, phones, and the internet serving both purposes *("...We use the laptops and the phones... Gmail. Emails we have."*). While emails and the internet are primarily used for professional purposes, they are also used for personal interactions. This is indicated by participants' usage of computers for email and internet tasks (*"...The computer where we receive mail..."; "Not complex ones, but I do. Internet, emails"*).

Varied approaches to IT system usage

Individuals use IT systems differently, with some prioritising security through tools like Google Drive and official emails (*"...upload PODs in the Google Drive"*), while others use a broader array of tools, including personal apps like WhatsApp for work. Examples include using the internet, office tools, SAGE, and emails for various tasks ("*...financial packages, emails*"). This sub-theme also explores how Zambian employees integrate

diverse IT systems into their professional tasks, focusing on the alignment with cybersecurity considerations.

Diverse spectrum of IT systems usage

Professional settings utilise a broad spectrum of IT systems, including desktop printers, computers, the internet, emails, and WhatsApp, reflecting diverse technology integration ("*desktop printers, computers, Internet, wifi, emails and WhatsApp*").

Specialised IT tools and applications

The use of specialised tools like NetSuite, WAN, and tracking systems illustrates the adoption of diverse technologies tailored to specific organisational needs *(*"*...using a tracking system...*"*;* "*...our programmes, NetSuite, WAN*"). This indicates a deliberate effort to integrate technology that meets unique business requirements.

Dual usage and flexibility

Employees often use IT resources like laptops, emails, and payroll systems beyond office hours, merging work and personal life ("*Just the laptop, sending emails, receiving emails*"). This highlights the flexibility and accessibility of modern technology ("*We've got a payroll system, a system that captures data...*").

Leveraging IT for Efficient Reporting

IT systems are essential for efficient reporting in organisations, with practices like sending reports via the internet and using software like WIN (ERP system) and NetSuite enhancing communication and decision-making ("*Sending reports, when I'm doing my reports IT is involved. I use the Internet, the computer*"*;* "*Emails*"*,* "*WIN*"*,* "*NetSuite*").

These findings emphasise the significant role of IT systems in work efficiency and effectiveness, but also the need to balance enhanced productivity with robust cybersecurity, considering the overlap of personal and professional use. The diversity and adaptability of IT system usage in the workplace, from standard to specialised applications, are highlighted, showing their importance in organisational communication and data management.

Sub-Theme 1.2. Perception and Understanding of Cyber Threats

This sub-theme examines how Zambian business employees perceive and understand various cyber threats, focusing on their awareness, knowledge of different threats, and assessment of their severity and impact. It explores their awareness sources, including training, personal experience, or media, and aims to understand the mental frameworks they use to interpret these threats. This understanding is necessary for developing effective cybersecurity measures and strategies to enhance awareness and prevention. It also aligns with the second research objective: identifying factors influencing cyber

awareness implementation among employees. The following sections analyse how these employees view and respond to the dynamic cyber threat landscape.

Perception

Interview participants recognised phishing and malware as major cyber threats, understanding the tactics used by cybercriminals (*"Phishing malware...they extort information from you which they later use to threaten you or bribe you..."*). They demonstrated awareness of the evolving cyber threat landscape and its potential harm, emphasising the importance of proactive security measures (*"What I know about cyber risks is that we need to protect ourselves from the cyber risks or the cybercrimes..."*).

Participants acknowledged the vulnerability of personal information in the digital sphere, highlighting the need for protective measures against data exposure (*"They mostly expose sensitive information that should not be revealed to the public"*). Concerns about hacking and the risk of unauthorised access to systems were prevalent, underscoring the necessity for strong defences (*"If you're on the internet and you see some link from a certain individual that you don't even know about, then you open that link, it might corrupt your PC or they might steal information from you..."*). Negligence was also seen as a significant threat, pointing to the need for a culture of vigilance and responsibility (*"It's negligence"*).

Furthermore, the awareness of cyber threats extended to specific organisational sectors, with particular emphasis on protecting guest information (*"So that one I might say, reviewing guest information which is confidential guest information"*) and identifying fraud as a key concern (*"Fraud, maybe"*). The vulnerability of IT infrastructure, especially a single server, was recognised as a critical issue (*"I think the biggest threat is that we have a few we have a single server"*). Email communication was also noted as a potential risk area, particularly regarding the transmission of sensitive information (*"Information. On the information part, especially because we deal with lots of emails and those emails, there are some which are very sensitive"*).

Overall, participants exhibited a clear understanding of various cybersecurity threats, recognising the need for comprehensive protective measures and strategies to mitigate these risks. This insight reflects a growing consciousness of the importance of cybersecurity in both personal and organisational domains.

Experience of and response to cyberattacks

Participants reported varied personal experiences with cyber incidents. Some faced cyber-attacks, while others took proactive steps like password protection to prevent threats (*"Yes, we had to put some measures, like block back pacing and put some security measures on our group, add a password to it"*). A few, particularly those with an IT background, hadn't experienced incidents, attributing this to their knowledge or cautious practices (*"Personally, yes, but since I have a bit of IT background, I know*

how to handle them"). However, many participants did encounter cyber-attacks, highlighting their widespread and persistent nature (*"I think I've also encountered, I'll call it cyber-attack..."*). These experiences underline the necessity of proactive and robust cybersecurity measures to effectively mitigate potential threats.

Training to counter cyberattacks

Participants highlighted a significant lack of cybersecurity training, with many noting the absence of formal programmes (*"No, I've never had one", "No", "No, we've never really had any sort of training or any sort of awareness pertaining to the risks"*). Responses varied from a complete lack of training to some training that was deemed insufficient or not focused on cybersecurity risks (*"No, I would like to start from the beginning the basics..."*).

Despite this gap, there was an eagerness among employees to learn more about cybersecurity and how to tackle cyber threats (*"Through training...You need to learn more on how to identify risks"*). The overarching theme was the absence of structured cybersecurity training in organisations (*"No, we've never really had any sort of training or any sort of awareness pertaining to the risks","No" "Personally, no"*).

These findings emphasise the need for comprehensive and regular training programmes that are tailored to employees' needs and roles, highlighting the importance of enhancing knowledge and awareness to strengthen the organisation's defence against cyber threats.

Response To / Countering Cyber Attacks

Participants altered their behaviour after cyber incidents, becoming more cautious and less trusting online (*"Yeah, so I've learned not to trust anyone"; "If you are not sure of anything don't click on anything that we're not sure"*). They adopted practices like changing passwords and avoiding risky online behaviour (*"Yeah, like on my personal, I've changed my passwords..."; "I just don't involve myself in these malicious pages, like especially porn sites"*).

There was a strong desire for more cybersecurity knowledge, with employees emphasising the importance of training ("*Training, training can do*"; "*I think it's something that we are, it's about just awareness and training, it's something that we are working on*"; "*I would just love to have a little bit more knowledge about cybersecurity*"). This underscores the need for regular training and proactive practices to foster a culture of cybersecurity awareness and enhance organisational resilience against cyber threats.

Cyber awareness and training

Participants highlighted the crucial need for increased cybersecurity awareness and education, pointing out the lack of sufficient training in their organisations and the

importance of sensitisation to foster a security-conscious mindset (*"...we need proper sensitisation on cybersecurity..."; "I have, but not here I have with my former company"*). They expressed a strong desire for improved awareness about evolving cyber threats and showed keen interest in training programmes (*"I think it's something that we are, it's about just awareness and training, it's something that we are working on"*).

Many suggested that raising awareness and improving practices could be achieved through systematic training and advocacy campaigns (*"I think through training"; "Trainings, campaigns"*). These findings emphasise the importance of training and awareness initiatives in cultivating a cybersecurity culture within organisations, highlighting the need to address existing training gaps and to advocate for continuous awareness to enhance cybersecurity resilience.

Data security concerns and needs

Employees voiced concerns about data security, emphasising the need to protect sensitive information and enhance cybersecurity infrastructure (*"I think it will be our information data, our rates, our clients as well as suppliers"*). They stressed the urgency of implementing effective cybersecurity measures and the importance of having dedicated personnel or consultants for this purpose (*"My thoughts are we would need to engage a consultant"; "I think we don't have proper controls here"*).

There was a call for improvements in the cybersecurity framework, including hiring full-time IT professionals to ensure better control over cybersecurity protocols (*"If we can have somebody just specifically trained in IT employed full-time to look at such things, then we are better off"*).

These findings underscore the need for robust data security measures and the importance of allocating the necessary resources and expertise to strengthen cybersecurity efforts in organisations.

Major Theme 2: Factors Influencing Cyber Awareness Implementation

This major theme explores the various elements crucial for the effective integration of cybersecurity awareness programmes in organisations. It covers a range of factors, including leadership support, organisational culture, resource availability, and technological infrastructure, essential for fostering a cybersecurity-conscious environment. The findings in this theme highlight the key determinants for successful cyber awareness initiatives, offering insights for organisations looking to strengthen their cybersecurity posture.

Cyber risks/threats; awareness and training

The sub-theme reveals that perceiving and understanding potential cyber risks and threats is fundamental to establishing a proactive cybersecurity defence (Yildirim 2016).

Integrating awareness and training is vital for enhancing organisational resilience against the evolving cyber threat landscape (Chen and He 2013). Participants unanimously recognised the ubiquity and diversity of cyber risks, with hacking and blackmailing through hacking cited as common concerns (*"Cyber risks have advanced, people hacking emails, even your personal laptop can be hacked"; "With this advanced internet, there are so many risks. Mostly the hackers"*). The fear of cyber violence and bullying was also prevalent among respondents.

Interestingly, many participants, especially those knowledgeable in IT, hadn't experienced cyber attack incidents, attributing this to proactive security measures like strong passwords. However, some noted a lack of adequate protection for organisational systems, emphasising the need for enhanced security measures (*"The biggest threat, if our system is not well protected..."*).

These findings underscore the importance of fostering awareness and training to empower employees with the necessary skills to effectively identify and mitigate cyber risks. Additionally, they highlight the need for improving protective measures and strengthening security infrastructure as critical steps towards a resilient cybersecurity posture.

Awareness

Awareness of cyber threats is necessary for a robust cybersecurity framework (Ifinedo 2023). This sub-cluster explores how individuals learn about cyber incidents and their understanding of digital threats. Respondents identified various sources, including media reports (*"I have read the newspapers about cybercrimes, like hacking of information..."*) and personal experiences with cyber-attacks (*"On several occasions, I've received phone calls from people I don't know demanding money, so I really get scared"*). Some noted a lack of information within their organisation, pointing to a potential communication gap (*"I think mainly it's most of it is self-researched or self-read because every now and then on these social media platforms will talk about cyber awareness and all that"*).

Awareness was often self-acquired through research and workshops, underscoring the need for proactive learning about cyber risks (*"I just started doing a bit of research here and there. I also attended a workshop..."*). These findings emphasise the importance of diverse sources and proactive efforts in gaining cyber threat awareness in order to enhance cybersecurity strategies within organisations.

Training to understand cyber risks

Training and education are central to awareness and understanding of cyber risks (Tam, Moara-Nkwe, and Jones 2020; Stephanou and Dagada 2008). In this sub-cluster, the focus is on the perspectives of individuals regarding their training, or lack thereof, in cyber risks. A prevalent theme among responses was the absence of formal training and

awareness programmes in organisations, highlighting a need for comprehensive educational initiatives on cyber risks (*"No"; "Management, but also the employee must have a certain amount of responsibility"*).

Participants expressed the importance of fostering a culture where reporting security incidents is encouraged, indicating a proactive approach to cybersecurity (*"Sometimes, they just tell us to say if you receive a mail from an unknown person that you're not too sure of, don't respond to that mail"; "There is encouragement to report"*). Many have enhanced their cyber risk understanding through self-driven research and reading (*"Reading a lot, research and just becoming more and more aware with the cyber happenings"*), while others suggested workshops as an effective method for learning (*"Maybe if we are given workshops to learn about the cyber system"*).

The responses underscore a critical need for formal training and education on cyber risks within organisations. Encouraging incident reporting and individual efforts like reading, research, and attending workshops can contribute to building a knowledgeable and cyber-resilient workforce. These measures are important for developing a vigilant and proactive cybersecurity culture in organisations.

Concerns and impact of and preparedness for cyber incidents

Understanding the impact of cyber incidents is essential for effective cybersecurity strategies in organisations (Plėta, Tvaronavičienė, Della Casa, and Agafonov 2020). Participants recognised the varying impacts of cyber incidents, from shutting down devices to acknowledging severe consequences, indicating an awareness of threats and efforts to mitigate damage (*"It's very severe very extremely severe..."; "I think it would be severe if that happened because it's a chain of it"*). However, some admitted not taking action despite being aware of risks, revealing a gap in translating awareness into proactive measures (*"No, they haven't because I can't change my personal line because I normally use it for work"*).

The perceived impact of data breaches included concerns about competition and potential financial distress, highlighting the far-reaching consequences of such incidents (*"Because we have got competitors out there who are in the same business... "It can lead to bankruptcy"*). Bridging the gap between awareness and action and using monitoring as a deterrent are crucial for a resilient cybersecurity posture.

Preparedness for cyber incidents involves identifying improvement areas and taking proactive steps, such as enhancing control over risks (*"I think the controls we don't have proper controls here"*), updating antivirus software (*"Improvement, I would say maybe updating the antivirus we use on our machines..."*), and employing dedicated IT personnel for effective threat management (*"If we can have somebody just specifically trained in IT employed full-time to look at such things then we are better off"*). These measures are central to building a strong cybersecurity defence in organisations.

Enhancing Awareness and Practices: Participants emphasised the need to enhance cybersecurity awareness and practices within organisations, highlighting the benefits of training and awareness campaigns for creating a workforce that is vigilant against cyber threats (*"Also the second one is the slow pace in which we upgrade"; "Trainings, campaigns"; "I think through training"*). These efforts are viewed as necessary for improving cybersecurity preparedness.

The findings emphasise the significant impact of cyber incidents, particularly the critical nature of data leaks, and the importance of immediate response measures. The link between awareness, action, and the role of monitoring in shaping behaviour is highlighted as key for a resilient cybersecurity posture. Additionally, the varied perceptions of cyber incident impacts show the need for robust and tailored security strategies within organisations to address specific risks and concerns effectively.

Cybersecurity policies and compliance

In cybersecurity, policies and compliance are fundamental for maintaining a secure organisational environment. Participants noted the existence of clear codes of conduct and sanctions for non-compliance, emphasising the importance of adhering to cybersecurity policies (*"Yes, there are sanctions. We have a code of conduct"; "Some they might be given warning letters"; "There is, however, there hasn't been an instance whereby we can enforce such sanctions"; "Yes, apparently, you are supposed to be charged"*).

The presence of formal cybersecurity policies varied across organisations. While some had established policies (*"Yes, we have a policy"*), most indicated a lack of such formal guidelines (*"No, it's not in our company"; "Not that I know"*). The role of a designated cyber risk manager was considered crucial for handling cybersecurity concerns effectively (*"There's the IT manager"*), although in some instances, there was ambiguity about who was responsible (*"No, that I know of"; "Yes, it is"*).

Participants expressed the need for continuous improvement of these policies to keep pace with evolving cyber threats and to address operational limitations (*"I feel we need to do more"; "There are certain things that we are not supposed to use on these computers that we have as a company"*). Additionally, the data protection officer pointed out a lack of regulation in data handling, suggesting a gap in policy enforcement and compliance (*"There has been no regulation, therefore, the way the data was being handled, it really does not control"*).

Overall, these findings highlight the importance of having clear, enforceable cybersecurity policies and a designated individual for cybersecurity management. Continuous policy evaluation and enhancement are necessary to adapt to the changing cybersecurity landscape and ensure effective protection against potential risks.

Major Theme 3: Guidelines for Promoting Cybersecurity Awareness

In today's digital age, fostering a culture of cybersecurity awareness is necessary (Kortjan and von Solms 2014). Major Theme 3 focuses on strategies to create a vigilant organisational environment. The goal is to equip employees with the knowledge and skills to effectively identify and mitigate cybersecurity risks, making them the first line of defence against cyber threats. Cybersecurity is a collective responsibility, extending beyond the IT department to every employee. This theme bridges the gap between cybersecurity policies and their practical application, offering actionable guidelines to cultivate a cybersecurity-centric mindset. It explores how organisations can raise awareness, educate their workforce, and instil a cybersecurity-first approach, addressing communication, training, and culture-building in the face of evolving threats. Major Theme 3 provides a roadmap for organisations to strengthen their defences and ensure a safer digital environment.

Cybersecurity tools and measures

Tools

The adoption of Kaspersky, known for its comprehensive security features against various threats, as a cybersecurity tool in organisations indicates a proactive approach to protecting digital assets (*"We're using Kaspersky"*). However, the common citation of only antivirus software points to a potential gap in cybersecurity knowledge, with businesses possibly underestimating the need for more comprehensive measures beyond antivirus (*"We have the antivirus. It's just the antivirus"*). Only a few organisations employ a range of technological tools and strategies, such as antivirus software, site restrictions, and frequent Wi-Fi password changes, to enhance security. The installation of firewalls on Wi-Fi networks further demonstrates a commitment to network security (*"There is a blanket antivirus thing"; "Site limitations"; "Regular change of Wi-Fi passwords"; "We have a firewall installed on our Wi-Fi..."*).

Instances where no proactive cybersecurity measures were reported highlight significant gaps in organisational cybersecurity posture and underscore the importance of developing a proactive cybersecurity culture (*"No"*). Assigning temporary IT personnel for IT systems monitoring suggests a need for more permanent and sustainable cybersecurity solutions (*"We just have an IT person though he's not fully employed by the company..."*).

These findings reveal various cybersecurity measures and tools utilised in organisations, suggesting a combination of positive security practices and areas needing enhancement. The reliance on basic tools like antivirus software, without additional measures, and instances of no proactive measures, indicate areas where organisations can focus to strengthen their cybersecurity posture. The deployment of diverse technological tools and security measures reflects an integrated approach to cybersecurity required for a robust defence against evolving cyber threats.

Measures

Consistent network monitoring is a key cybersecurity measure, enabling real-time detection of threats and contributing to smooth operations (*"The networks have been monitored, but I know that they have been monitored, but I don't know how"*). Organisations benefit from learning from past cyber-attacks, using these experiences to enhance preparedness and adaptability (*"I think the last attack that I mentioned earlier, I think that gave them a wake-up call"*). However, the absence of formalised cybersecurity policies suggests a need for improvement. Creating comprehensive cybersecurity policies is essential for secure practices and fostering a culture of awareness and compliance (*"Official policy, no"*). The Data Protection Commissioner highlighted the legal requirement for local data storage, suggesting the use of data centres as a measure to safeguard information (*"We also have data centres, which we believe that their cost is becoming reasonably affordable for them"*). These insights underline the significance of proactive cybersecurity strategies, including constant monitoring, learning from previous incidents, and formalising policies within organisations.

IT department and security measures

The need for a dedicated IT department is recognised as a central requirement in addressing cybersecurity, highlighting a gap in expertise and the importance of having specialised personnel (*"We just need an IT department"*). This reflects a proactive approach to continuously improving and updating cybersecurity measures in response to evolving threats (*"The slow pace in which we upgrade"*).

These findings underscore the importance of a specialised IT team to effectively manage cybersecurity challenges and the commitment to ongoing improvements to bolster the organisation's cybersecurity posture.

Responsibilities and measures

The concept that cybersecurity is a collective responsibility underscores a culture of shared vigilance in organisations, with each employee playing a key role in security (*"It's my responsibility"; "It's both"; "It's everyone's responsibility"*). The presence of a designated IT manager for cybersecurity implies a structured approach to handling cyber threats and emphasises the importance of coordination in cybersecurity efforts (*"There's the IT manager"*). Encouraging the reporting of incidents fosters prompt response and resolution, enhancing overall cybersecurity readiness (*"We do communicate"*).

Conclusion

This study examined cybersecurity practices and perceptions in various organisations and individuals, focusing on understanding the current state of cybersecurity awareness,

challenges faced, and guidelines for improvement. The analysis culminated in key themes and findings that summarise the study's insights:

Cybersecurity Awareness and Training

A central theme from the study is the critical role of cybersecurity awareness and training. Respondents highlighted the need for a better understanding of cyber risks like hacking and data breaches, emphasising proactive measures through education and training. The study found a lack of cybersecurity training in some organisations, underscoring the need for enhanced awareness and best practices.

Data Security Concerns and Needs

Data security was a major concern among respondents, with many desiring stronger cybersecurity measures to protect sensitive information. The study revealed concerns about inadequate data protection and the risks of data breaches, leading to calls for improved security measures like updated antivirus software and dedicated IT personnel.

Cybersecurity Policies and Compliance

The study highlighted that while some organisations had established cybersecurity policies, most lacked a clear framework. It noted the presence of sanctions and enforcement mechanisms for policy violations. The importance of guidelines and training for compliance, particularly for SMEs, was emphasised.

Cybersecurity Measures and Tools

The theme of cybersecurity measures and tools in the study highlighted the use of technologies such as antivirus software, firewalls, and network security for enhancing cybersecurity. It noted that some organisations employed IT personnel for effective monitoring and management, emphasising the importance of proactive measures and awareness in safeguarding data.

Responsibilities and Measures

The final theme of the study emphasised shared responsibility for cybersecurity within organisations, highlighting the importance of reporting security incidents and having dedicated teams for risk management.

In summary, the research emphasises the critical need for cybersecurity education, training, and clear policies. The effective use of technological tools and IT teams is essential for robust cybersecurity practices. The study advocates for prioritising cybersecurity awareness and the development of guidelines for data protection and localisation.

This analysis underscores the ongoing importance of cybersecurity awareness and implementation in the face of advancing technology, crucial for data protection and safeguarding against cyber threats.

The Third Layer—Legal Framework

The research endeavours to create guidelines that address the Zambian business sector. The legal framework is necessary for promoting such guidelines as being valuable to businesses so that it does not simply serve to increase their cyber awareness and cybersecurity, but will also promote compliance with Zambian legislation, in this case, the Data Protection Act.

For this study, the principal researcher undertook two approaches that could inform the legal guidelines: document analysis of the Data Protection Act and an interview with the Data Protection Commissioner of Zambia, Mr Likando Lyuwa.

Data Protection Commissioner

In an interview, Mr Likando Lyuwa, Zambia's Data Protection Commissioner since 9 June 2023, outlined the Commission's roles, including enforcing data protection laws, educating on data rights, and setting national standards. His insights added depth to the research, offering a current perspective on implementing Zambia's Data Protection Act. This contribution enhances the study's relevance with respect to the nuances of Zambian data governance.

The Commission's approach centres around three pillars fundamental to its data protection mandate.

Data Privacy: The Commission is committed to protecting individual privacy rights, ensuring respectful and lawful handling of personal data. It rigorously monitors adherence to privacy standards, prioritising the rights of data subjects in organisational data practices.

Data Localisation: The Commission emphasises the importance of data localisation, advocating for storing and processing personal information within Zambia. This strategy enhances data security and upholds national sovereignty over personal data.

Data Protection: The Commission enforces a strict emphasis on data protection, mandating comprehensive security protocols to prevent breaches, loss, or unauthorised dissemination of data. This includes various strategies from technical measures to organisational policies, all aimed at creating a secure environment for personal data.

In addition to the primary focus areas, the Data Protection Commission in Zambia is mandated to fulfil several critical responsibilities:

Registration of Data Controllers and Data Processors: The Commission handles the registration of all entities dealing with personal data, establishing accountability and transparency for those managing personal information. This registration process creates a detailed record of data processors, the data they handle, and the processing purpose.

Incident Reporting and Breach Management: Data controllers and processors must legally report data breaches to the Commission within 24 hours of their occurrence. This prompt reporting helps the Commission accurately assess Zambia's cybersecurity situation. Reports should detail the nature of the breach, the corrective actions implemented, and any adverse consequences. This rapid communication enables the Commission to assess the impact, recommend additional remedial actions, and coordinate with other agencies for broader security issues or data misuse.

The Data Protection Commission of Zambia enforces data protection laws using auditors, as provided for in Chapter 6 of the Act. These auditors are necessary for ensuring compliance and conducting inspections to verify adherence with legal requirements by data controllers.

With the Commission in its early stages, it often subcontracts external auditors for wider coverage and efficient monitoring of organisations handling personal data. These auditors function as the Commission's agents, scrutinising data protection practices.

After audits, Commission inspectors review the findings, establishing a two-tier process for thorough oversight. This system, where inspectors verify auditor reports, strengthens the rigour of the oversight and promotes accountability among data controllers. This approach reflects the Commission's dedication to robust data governance in Zambia.

The Act (chapter 6, section 38) defines the functions of a data auditor as follows (Government of Zambia 2021): promote adherence to principles of data protection by controllers and processors of data; ensure that data controllers and data processors implement adequate policies and procedures to regulate the processing of personal data; enhance public and stakeholder awareness of data protection principles and rights; and check that data controllers implement adequate safeguards to prevent data leaks and data breaches.

The Data Protection Act of 2021 took effect with the establishment of the Data Protection Commission in 2023. With full enforcement beginning on 1 January 2024, the Commission is prioritising auditor recruitment to ensure Zambian data centres comply with the data localisation requirements as set out in Chapter 10, Section 70(1) of the Act, thereby strengthening data protection in Zambia.

The Current Situation of Data Protection in Zambia

In Zambia's previous regulatory framework, data protection was inadequately controlled, as Commissioner Likando Lyuwa noted. He described prevalent practices,

such as logging personal details without consent: “Institutions will put a log at the entrance, and they will literally want you to leave all your details, name, contact number, email address.” He drew attention to illegal practices like publishing personal information in recruitment ads: “Institutions could go on and publish names of recruitments in the papers, and that would include their personal ID, their name, and phone number. All that was totally against the law.”

Commissioner Lyuwa attributed these issues to a widespread lack of understanding about data rights: “The data subjects not knowing their rights, not knowing that it is illegal for somebody to use their data in a way in which they want without their consent.” The enactment of the Data Protection Act marks a shift towards rectifying these issues by providing public information on lawful data usage.

Data Controllers and Data Processors

Appointing Data Controllers and Processors is required for all organisations handling data, a task that is challenging for those without IT resources or knowledge. Data Protection Commissioner Likando Lyuwa addressed this, stating that, “Currently, there are no guidelines, but they’ll provide them in the future that will address who is suitable to be a data controller and what are their responsibilities.” Plans include training data auditors to educate data controllers on their roles.

Lyuwa further noted that formal training and qualifications for data controllers will become necessary: “In the long run they’ll provide formal training to data controllers and they’ll need to have certain qualifications in order to become data controllers.” He suggested that smaller entities could outsource these roles: “We are not forced that within the institution you need to have a data protection officer, but all can subcontract and can go and get it outsourced,” a recommendation particularly pertinent for SMEs: “Small businesses, we would encourage them to subcontract.”

This approach indicates a process of developing a structure for clearly defining and supporting the roles of data controllers and processors, aiding organisations in meeting their data protection obligations.

Cyber Awareness

The Data Protection Commissioner of Zambia, Mr Likando Lyuwa, stressed the crucial role of cyber awareness in data protection, considering it a primary defence against breaches, noting that, “The weakest link in all these breaches is the human being themselves… the other tools are secondary.”

Mr Lyuwa advocated for ongoing cyber awareness education within organisations, emphasising its necessity as a continuous effort: “The employer themselves they need to put in place some little measures that will make the employees be aware of what they need to do, what they don’t need to do, because the consequences are quite high.” He

suggested regular updates to this training: “Knowledge also grows and is evolving. It should be something that can be continuously done, maybe quarterly, half-yearly.”

The Commission plans to assist SMEs in understanding cyber awareness and the Data Protection Act through an educational campaign, in collaboration with ZICTA, using SMS technology. Additionally, partnerships with entities like the “patents and the company’s registrar” and the use of social media and flyers aim to enhance public cyber awareness, focusing on the business community.

Enforcing the Law

Before fully enforcing the Data Protection Act, the Zambian Data Protection Commission intends to conduct assessments to gauge the volume of data held by entities. Commissioner Likando Lyuwa explained, “We’ll run questionnaires to the entities to understand the magnitude of data that they hold.” These findings will guide the development of specific guidelines for legal compliance.

Addressing the challenge of data storage as per Chapter 10, Section 1 of the Act, which requires data storage within Zambia, the Commissioner recognised the gap between this mandate and current global technological capabilities, noting the availability of local data centres and the potential acceptance of international centres like AWS and Azure after finalising guidelines.

Enforcement will be gradual, starting with understanding current practices and helping businesses adapt. The Commissioner noted, “It will be very, very gradual. Of course, we’ll start with the bigger ones and then we’ll start coming downwards,” indicating an incremental rollout, prioritising larger companies first. This phased approach is designed to ease businesses into compliance with the Act.

The Need for the Study’s Outcomes

The Data Protection Commissioner of Zambia showed keen interest in the research, particularly its benefits for SMEs, and was open to applying its findings in practice. The Commissioner expressed, “Even before you finalise, if you’ve got any ideas about the guidelines which you think that can be very helpful to the SME, we would love that you can share that with us and we can discuss better.”

This openness to collaboration highlights the Data Protection Commission’s proactive approach to incorporating academic research into practical policies. This strategy aims to ensure that SME guidelines are not only research-based but also specifically catered to the distinct challenges SMEs may encounter in data protection.

Contributions of the Study

This study makes contributions in the theoretical, methodological, and practical domains for cybersecurity and cyber awareness in Zambia's SME sector. Theoretically, it integrates international guidelines with Zambian realities, providing a model for adapting global cybersecurity standards to local needs. It identifies gaps in cybersecurity implementation among Zambian SMEs and proposes an adaptive compliance model within Zambia's legal framework, enhancing the understanding of cybersecurity in emerging economies.

Methodologically, the research develops Cyber Awareness and Cybersecurity guidelines specifically for Zambian SMEs, combining international best practice with local SME conditions and legal frameworks. Those guidelines, designed through literature reviews and stakeholder interviews, focus on building a cyber-aware culture and provide a structured blueprint for enhancing employee cyber awareness at all organisational levels. It represents a significant advancement in cyber awareness research, filling a gap in the global discourse on cybersecurity methodologies.

Practically, the research advocates integrating cyber awareness into the governance and risk management of Zambian SMEs. It has generated interest among business owners and government bodies, including the Data Protection Commissioner and the Ministry of Small and Medium Enterprises, who are keen to review and potentially adopt its findings. This research offers actionable guidelines for Cyber Awareness and Cybersecurity, aligning them with business objectives and operational practices. Its adaptability across different SMEs highlights its practical utility and potential to shape national policy, positioning the research as a blueprint for elevating cyber awareness at both corporate and national levels in Zambia.

Limitations of the Study

This study on cybersecurity awareness in Zambia's SME sector has several limitations. Firstly, the lack of current official data on the number of operational businesses in Zambia posed a foundational challenge. The study's reliance on 2012 secondary data may not accurately reflect the dynamic business sector's current state. This limitation was compounded by the study's generalised approach across the SME sector without delving into the variegated nature of different industries, each with its unique cybersecurity challenges and needs.

Another gap arises from focusing solely on digitally enabled enterprises, leaving out SMEs outside the digital sphere. This exclusion neglects a segment that, while presently less exposed, remains unprotected and uninformed about cyber threats. The rapidly evolving technology and cyber threat landscape also mean the study's findings might quickly become outdated, highlighting the need for continual research and updates.

Finally, the study's intense focus on cybersecurity possibly overlooked other critical IT governance and risk aspects, which are necessary for Zambian SMEs.

These limitations suggest the need for future research offering more detailed analysis, updated business demographics, and extending to less digitised sectors. This approach would provide a comprehensive roadmap for strengthening all SMEs in Zambia against cyber threats.

Ideas For Future Research

This study on cybersecurity in Zambia's SMEs opens avenues for future research, addressing its inherent limitations. Future work could explore industry-specific cybersecurity frameworks to tailor strategies for diverse sectors. Understanding the evolving nature of cyber threats through longitudinal studies will provide insights into the long-term effectiveness of cybersecurity policies.

Investigating how SMEs across varying digital integration levels navigate cyber threats is a key requirement for a deeper understanding of national cyber resilience. Developing quantitative cybersecurity metrics and engaging in cross-country comparisons within the southern African region could lead to more effective cybersecurity frameworks.

Research should examine the role of cybersecurity in corporate governance and the impact of emerging technologies like IoT and AI on the cybersecurity paradigm. Assessing the effectiveness of different cybersecurity training methodologies and understanding the implications of evolving legal mandates on organisational practices are necessary for refining policies and strategies.

By focusing on these areas, future research can address the multifaceted challenges of cybersecurity, contributing to a robust and resilient cyber ecosystem for SMEs in Zambia and potentially influencing broader regional practices.

Final Word

Zambia's progression towards a connected world underscores the criticality of cybersecurity, transforming it from a mere option to an essential obligation. The rising frequency of cyberattacks and their cumulative impact necessitate proactive measures from both the government and business sectors to mitigate these risks effectively.

This research demonstrates that guidelines from international bodies like CISA and ENISA are applicable and beneficial in enhancing cyber awareness and cybersecurity knowledge within Zambia's business environment. The study's findings, derived from in-depth interviews with employees in the Zambian business sector, reveal a notable deviation from the perspectives outlined by Tischer et al. (2016). Contrary to the argument that employees predominantly assign cybersecurity responsibility to senior

management, the study revealed a prevalent perception among Zambian employees that cybersecurity is a shared responsibility.

A significant finding from the research is the lack of formal cyber awareness training within the Zambian business sector. Employees express a keen desire to learn more about cyber risks but face a void in official training resources. This gap in cyber awareness training is critical, as the knowledge it provides is fundamental for employees to safeguard their work environments effectively. The absence of initiatives from businesses and the government in conducting such training is a glaring oversight, especially considering the potentially catastrophic consequences of cyber-attacks, including bankruptcy, as highlighted by several interviewees.

Furthermore, the research indicates the general absence of dedicated IT personnel in Zambian businesses, a necessary role for implementing contemporary cybersecurity measures. The prevalent reliance on antivirus software is insufficient in today's evolving threat landscape, underscoring the need for skilled IT professionals to implement more robust protections.

The impending enforcement of Zambia's Data Protection Act marks a significant advancement in the nation's legal framework. Businesses must adapt in order to remain compliant with the law, or risk potential penalties for non-compliance. The Data Protection Commissioner and the Ministry of SMEs of Zambia have demonstrated a proactive stance, expressing interest in the outcomes of this study for potential adoption as formal guidance for businesses. This engagement highlights the study's significant and unique contribution to Zambia's national interest and specifically to its business sector.

References

Akamai Technologies. 2021. *State of the Internet / Security: A Year in Review.* Akamai Technologies.

Aliyu, A. A., and Adamu, H. 2015. "Ontology, Epistemology and Axiology in Quantitative and Qualitative Research: Elucidation of the Research Philosophical Misconception." *Proceedings of the Academic Conference: Mediterranean Publications and Research International on New Directions and Uncommon* 2(1).

Banda, F., and Hapompwe, C. 2023. "An Assessment of Informal Sector's Business Registration Patterns: Nature and Size among Micro, Small and Medium Enterprises in Lusaka." *Journal of Economics, Finance and Management Studies* 6(1):342–357.

Baskerville, R., Rowe, F., and Wolff, F. C. 2018. "Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective." *ACM SIGMIS Database: The Database for Advances in Information Systems* 49(1): 33–52.

Berry, C. T., and Berry, R. L. 2018. "An Initial Assessment of Small Business Risk Management Approaches for Cybersecurity Threats." *International Journal of Business Continuity and Risk Management* 8(1):1–10.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., and Lockett-Reynolds, J. 2011. "Human Performance in Cybersecurity: A Research Agenda." *In Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 55(1):1115–1119.

Bwenbya, J. 2022. "Addressing Challenges in Accessing Finance by Small and Medium Enterprises (SMEs) in Zambia: A Pragmatic Approach." Master's Thesis, University of Zambia.

Cassim, F. 2017. "Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study." *PER* 12(4):35–79.

Chen, Y. He, W. 2013. Security Risks and Protection in Online Learning: A Survey." *The International Review of Research in Open and Distributed Learning* 14(5).

Chesebro, J. W. and Borisoff, D. J. 2007. "What Makes Qualitative Research Qualitative?" *Qualitative Research Reports in Communication* 8(1):3–14.

Clough, J. 2014. "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation." *Monash University Law Review* 40(3): 698–736.

Constantinou, C. S., Georgiou, M., and Perdikogianni, M. 2017. "A Comparative Method for Themes Saturation (CoMeTS) in Qualitative Interviews." *Qualitative Research* 17(5): 571–588.

Creswell, J. W. 2011. “Controversies in Mixed Methods Research.” *The Sage Handbook of Qualitative Research* 4(1):269–284.

Creswell, J. W. 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (4th ed.). London: Sage Publications Ltd.

Dagada, R. 2013. “Digital Banking Security, Risk and Credibility Concerns in South Africa.” *In The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensics* (CyberSec2013)

Dagada, R. 2014. “Legal and Policy Aspects to Consider When Providing Information Security in the Corporate Environment.” Doctoral thesis, University of South Africa.

Dagada, R. 2021. *Digital Commerce Governance in the Era of Fourth Industrial Revolution in South Africa.* Pretoria: Unisa Press.

Demchyshak, N., and Shkyria, A. 2021. “Risk Management in the Financial Sector of Ukraine in the Context of Cyber Threats and Post-Pandemic Economic Recovery.” *Innovative Economy* 3–4..

Eaton, C., and Dustin, V. 2021. “Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom.” May 21, 2021. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

ENISA. 2021. *Cybersecurity for SMEs: Challenges and Recommendations.* Athens: European Union Agency for Cybersecurity, ENISA.

European Commission. 2016. “Regulation (EU) 2016/679 of the European Parliament and of the Council.” *Official Journal of the European Union.*

Federal Bureau of Investigation. 2020. “2019 IC3 Annual Report.” Federal Bureau of Investigation.

Federation of Small Businesses. 2019. *Cyber Threat Assessment.* Blackpool:: Federation of Small Businesses.

Government of Zambia. 2009. The Information and Communication Technologies Act No. 15 of 2009. Government of Zambia.

Government of Zambia. 2021. The Cyber Security and Cyber Crimes Act No. 2 of 2021. Lusaka: Government of Zambia.

Government of Zambia. 2021. The Data Protection Act No. 3 of 2021. Lusaka: Government of Zambia.

Guest, G., Bunce, A., and Johnson, L. 2006. “How Many Interviews Are Enough? An Experiment with Data Saturation and Variability.” *Field Methods* 18(1):59–82.

Gundu, T. 2019. “Acknowledging and Reducing the Knowing and Doing Gap in Employee Cybersecurity Compliance.” *In ICCWS 2019 14th International Conference on Cyber Warfare and Security, 94–102.* Stellenbosch University.

Hadlington, L. 2018. “Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom.” *International Journal of Cyber Criminology* 12(1):262–274.

Halubanza, B., Kunda, D., and Musonda, Y. 2016. “An Assessment of Information Security Awareness among Employees in the Higher Education Sector in Zambia.” Kabwe: Mulungushi University.

Hunter, D., and Howes, D. 2019. “Defining Exploratory-Descriptive Qualitative (EDQ) Research and Considering Its Application to Healthcare.” *Journal of Nursing and Health Care* 4(1).

Ifinedo, P. 2023. “Effects of Security Knowledge, Self-Control, and Countermeasures On Cybersecurity Behaviors.” *Journal of Computer Information Systems* 63(2):380–396.

Imsand, E., Tucker, B., Paxton, J., and Graves, S. 2020. “A Survey of Cybersecurity Practices in Small Businesses.” In *Intelligent Systems and Applications (Advances in Intelligent Systems and Computing*, edited by K. Arai, S. Kapoor, and R. Bhatia, 44–50. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-29513-4_4

ITU. 2020. *Global Cybersecurity Index.* Geneva: International Telecommunication Union-ITU.

Jackson, R. L., Drummond, D. K., and Camara, S. 2007. “What is Qualitative Research?” *Qualitative Research Reports in Communication* 8(1):21–28.

Johansson, K., Paulsson, T., Bergström, E., and Seigerroth, U. 2022. *Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry*. IOS Press.

Kaspersky. 2021. *Spam and Phishing in Q3 2021.* Moscow: Kaspersky.

Kesmodel, U. S. 2018. “Cross-Sectional Studies - What Are They Good For?” *Acta Obstetricia et Gynecologica Scandinavica* 97(4):388–393.

Khunga, B., and Kunda, D. 2017. “Impact of NRENs in Universities – The ZAMREN Experience.” *MANAS Journal of Engineering* 5(2):13–23.

Kiger, M. E., and Varpio, L. 2020. “Thematic Analysis of Qualitative Data: AMEE Guide No. 131.” *Medical Teacher* 42(8):846–854.

Kortjan, N., and von Solms, R. 2014. “A Conceptual Framework for Cyber-security Awareness and Education in SA.” *South African Computer Journal* 52(1):29–41.

Koshy, V. 2010. *Action Research for Improving Educational Practice: A Step-by-Step Guide* (2 ed.). London: Sage Publications Ltd.

Kozak, S. 2017. "The Role and Importance of the Small Business Sector in the Economic Development of the Mazowieckie Province." *Scientific Journals of the University of Natural Sciences and Humanities, Series Administration and Management* 41(114):61–70.

Lambech, M., and Høglo, K. S. 2020. "Assessing Different Levels of Time Retention for Business Interruption Coverage on Cyber Insurance." Master's thesis, Handelshøyskolen BI.

Levin, K. A. 2006. "Study Design III: Cross-Sectional Studies." *Evidence-Based Dentistry* 7: 24–25.

Lindlof, T. R., and Taylor, B. C. 2002. *Qualitative Communication Research Methods* (2nd ed.). Thousand Oaks, CA: Sage Publications Ltd.

Lusaka Times. 2019. "ZANACO Xapit Suffers Major Hack, Thousands Lose Savings.*"* 7 May 2019. July 5, 2019. https://www.lusakatimes.com/2019/07/05/zanaco-xapit-suffers-major-hack-thousands-lose-savings/

Lusaka Times. 2022. "BoZ Says Hackers Attacked Its Computer System." May 17, 2022. https://www.lusakatimes.com/2022/05/17/boz-says-hackers-attacked-its-computer-system/ (Accessed August 6, 2023)

Mason, M. 2010. "Sample Size and Saturation in PhD Studies Using Qualitative Interviews." *Forum Qualitative Sozialforschung/Forum / Qualitative Social Research* 11(3).

Minnaar, A. 2019. "Cybercriminals, Cyber-Extortion, Online Blackmailers and the Growth of Ransomware." *Acta Criminologica: African Journal of Criminology and Victimology* 32(2).

Morgan, S. 2022. *Official Cybercrime Report.* Northport: Cybersecurity Ventures.

Morse, J. M. 2015. "Critical Analysis of Strategies for Determining Rigor in Qualitative Inquiry." *Qualitative Health Research* 25(9):1212–1222.

Mukubesa, M. 2021. *Broadening the Tax Base and Enhancing Revenue Collection: A Case Study for the Small and Medium Enterprises in the Informal Sector in Zambia.* Lusaka: Cavendish University.

Mwila, K. A. 2020. "An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia." Master's Thesis, The University of Zambia.

Myers, M. D. 2008. *Qualitative Research in Business and Management.* London: Sage.

National Assembly of Zambia. 2022. "Information Brief on Cyber Security and Cybercrime Trends in Zambia."Lusaka: Research Department. National Assembly of Zambia.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., and Bonacina, S. 2021. “Influence of Human Factors on Cybersecurity within Healthcare Organisations: A Systematic Review.” *Sensors* 21(15): 5119.

Nuwagaba, A. 2015. “Enterprises (SMEs) in Zambia.” *International Journal of Economics, Finance and Management* 4(4).

Ofori-Sarpong, E. K. and Adomako, F. D. 2020. “Cybersecurity Awareness and Practices: A Study of Mobile Money Users in Ghana.” *International Journal of Computer Applications Technology and Research* 9(6): 239–244. https://doi.org/10.7753/IJCATR0906.1001

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., and Hoagwood, K. 2015. “Purposeful Sampling for Qualitative Data Collection and Analysis.” *Administration and Policy in Mental Health* 42(5):533–544.

Patton, M. Q. 2015. *Qualitative Research and Evaluation Methods* (4th ed.). Thousand Oaks, CA: Sage Publications.

Paul, C. L., and Whitley, K. 2013. *A Taxonomy of Cyber Awareness Questions for the User-Centered Design of Cyber Situation Awareness*. Berlin: Berlin Heidelberg.

Plėta, T., Tvaronavičienė, M., Della Casa, S., and Agafonov, K. 2020. *Cyber-Attacks to Critical Energy Infrastructure and Management Issues: Overview of Selected Cases. Insights into Regional Development.* Vilnius: Entrepreneurship and Sustainability Center.

Ponemon Institute. 2020. *Cost of a Data Breach Report 2020.* New York: IBM Security.

Rajasekharaiah, K. M., Dule, C. S., and Sudarshan, E. 2020. “Cyber Security Challenges and its Emerging Trends on Latest Technologies.” *IOP Conference Series: Materials Science and Engineering* 2(981): 022062.

Robles-Carrillo, M., and García-Teodoro, P. 2022. “Ransomware: An Interdisciplinary Technical and Legal Approach.” *Security and Communication Networks* 2022: 1–17.

Sangani, N. K., and Vijayakumar, B. 2012. “Cyber Security Scenarios and Control for Small and Medium Enterprises.” *Informatică economică* 16: 58–71.

Schatz, D., Bashroush, R., and Wall, J. 2017. “Towards a More Representative Definition of Cyber Security.” *The Journal of Digital Forensics, Security and Law* 12(2): 8.

Sehularo, L. A., Du Plessis, E., and Scrooby, B. 2012. “Exploring the Perceptions of Psychiatric Patients Regarding Marijuana Use.” *Health SA Gesondheid* 17(1):1–13.

Senarathna, I., Wilkin, C., Warren, M., Yeoh, W., and Salzman, S. 2018. “Factors That Influence Adoption of Cloud Computing: An Empirical Study of Australian SMEs.” *Australian Journal of Information Systems* 22.

Serianu LTD. 2020. *Africa Cybersecurity Report 2019–2020*. Nairobi: Serianu Ltd.

Shafqat, N., and Masood, A. 2016. “Comparative Analysis of Various National Cyber Security Strategies.” *International Journal of Computer Science and Information Security* 14(1): 129.

Shaw, R. S., Chen, C. C., Harris, A. L., and Huang, H.-J. 2009. “The Impact of Information Richness on Information Security Awareness Training Effectiveness.” *Computers and Education* 52(1): 92–100.

Slusky, L. 2020. “Cybersecurity of Online Proctoring Systems.” *Journal of International Technology and Information Management* 29(1):56–83.

Stephanou, T., and Dagada, R. 2008. “The Impact of Information Security Awareness Training on Information Security Behavior: The Case of Further Research.” ISSA University of Johannesburg, 2 to 4 July 2008.

Tam, K., Moara-Nkwe, K., and Jones, K. 2020. “The Use of Cyber Ranges in the Maritime Context: Assessing Maritime-cyber Risks, Raising Awareness, and Providing Training.” University of Plymouth.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., and Bailey, M. 2016. “Users Really Do Plug in USB Drives They Find.” *IEEE Symposium on Security and Privacy (SP)*, 306–319.

Tran, V.-T., Porcher, R., Tran, V.-C., and Ravaud, P. 2017. “Predicting Data Saturation in Qualitative Surveys with Mathematical Models from Ecological Research.” *Journal of Clinical Epidemiology* 82:71–78.

Williams, M., and Moser, T. 2019. “The Art of Coding and Thematic Exploration in Qualitative Research.” *International Management Review* 15(1): 45–55.

World Bank. (n.d.). *Small and Medium Enterprises (SMEs) Finance*. https://www.worldbank.org/en/topic/smefinance (Accessed April 6, 2023).

World Economic Forum. 2018. “Cybersecurity: The $1 Trillion Opportunity.” World Economic Forum.

Yildirim, E. 2016. “The Importance of Information Security Awareness for the Success of Business Enterprises.” In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity*, July 27–31, 2016, Walt Disney World®, Florida, USA, 211-222.

Yokohama, S. 2016. *Cybersecurity for Business Executives: An NTT Publication for Top Management.* https://group.ntt/en/topics/CfBE/pdf/Cybersecurity_for_Business_Executives2.pdf (Accessed on June 13, 2023).

Yudhiyati, R., Putritama, A., and Rahmawati, D. 2021. “What Small Businesses in a Developing Country Think of Cybersecurity Risks in the Digital Age: Indonesian Case.” *Journal of Information, Communication and Ethics in Society* 19(4):446–462.

Zambia Development Agency. 2020. *Promoting SME Competitiveness in Zambia*. Lusaka: Zambia Development Agency.

Zambian Observer. 2023. “The Official Bank of Zambia Facebook Page Has Been Hacked.” July 24, 2023. https://zambianobserver.com/the-official-bank-of-zambia-facebook-page-has-been-hacked/ (Accessed on July 25, 2023)

ZICTA. 2021. *2020 Annual Report.* Lusaka: ZICTA.

ZICTA. 2022. *Collaborative Framework For the Oversight of Digital Financial Services in Zambia.* Lusaka, Zambia: Zambia Information and Communications Technology Authority (ZICTA), Bank of Zambia (BoZ) and the Rural Finance Expansion Programme (RUFEP).