Building Cybersecurity Capacities in Zambia's Business Sector: Guideline for SMEs

Goni Saar[1] and Rabelani Dagada[2]
[1]The Da Vinci Institute for Technology Management, Zambia
[2]Graduate School of Business Leadership, University of South Africa, South Africa

Gonisaar2011@gmail.com
dagadr@unisa.ac.za

Abstract: This research explores cybersecurity awareness and implementation within Zambia's small and medium-sized enterprises (SMEs), a sector increasingly targeted by cyberattacks that lead to substantial financial losses. The study's primary aim was to enhance cyber awareness and develop actionable guidelines for SMEs in Zambia. Utilising an interpretivist 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, emphasising the integration of 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. Practically, the research has sparked engagement among SMEs and government bodies, demonstrating its applicability and potential for shaping policy. However, limitations include reliance on outdated demographic data and a focus on digitally enabled SMEs, potentially overlooking broader IT governance aspects and less digitized businesses. Future research should aim for comprehensive, up-to-date analysis across all SME sectors, contributing to a more inclusive and resilient cybersecurity landscape in Zambia.

Keywords: Cybersecurity awareness, SMEs, Zambia, Data protection, Cybersecurity guidelines, Financial impact of cyberattacks

1. Introduction and Background

Among the most pressing challenges of the 21st century is cybersecurity threats, which negatively affect businesses and nations worldwide. Due to the modern lifestyle that prevails, people nowadays rely on technology for their daily activities such as shopping, financial transactions, and other aspects of their daily routines (Rajasekharaiah, et al., 2020). Additionally, with the growth and popularity of social media, cybercrime has concomitantly increased.

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 & 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 resulted in significant financial repercussions. The economic significance of cybersecurity is a notable factor in the digitalization of national economies. 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 (Dagada, 2013).

Morgan (2022) highlights the escalating costs of cybercrime, projecting damages of 8 trillion dollars in 2023 and 10.5 trillion dollars in 2025, compared to 3 trillion dollars 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, characterized by rapid technological advancements such as artificial intelligence, the Internet of Things, and robotics, further underscores the need to address cybercrimes 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 potentially substantial losses incurred through cyberattacks (Dagada, 2014).

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 sustained through a

breach of data for a company in 2020 was $3.86 million (Ponemon Institute, 2020). Business-related cyberattacks can have wider implications and pose a national threat to nations.

Kozak (2017) emphasises the criticality of regional economies, wherein small and medium-sized enterprises (SMEs) hold prominence 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) (2020), SMEs account for an estimated 70% of the employed population and contribute about 20% to GDP.

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). Together with the rapid growth of ICT use in Zambia (ZICTA, 2021), dealing with this substantial cybersecurity issue has become a major challenge for the country's economy. The challenge of cyber security in Zambia may be attributed to businesses or companies not being sufficiently knowledgeable about cybersecurity.

Zambia has sustained significant economic impairment due to cyber threats, 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 fraudulent 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, which found a lack of adequate information security training and a dearth of support from the upper echelons of management.

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 faces ongoing cybersecurity challenges, including technical skill shortages, infrastructural inadequacies, and a general lack of cyber threat awareness. A comprehensive strategy that integrates legislative efforts, capacity building, and public education, augmented by international collaboration, is essential to navigating these challenges (ZICTA, 2022).

The purpose of the study was to explore knowledge and practices of cyber security amongst individuals in the Zambian business sector, and furthermore to develop guidelines that enhance cyber awareness amongst employees.

2. Theoretical and Conceptual Framework

This research utilizes the "Cyber Security Awareness and Education" framework as formulated by Kortjan and von Solms (2014). This framework was originally designed for enhancing cyber security culture at a national level within South Africa. The framework, informed by an analysis of cyber security practices in OECD countries, proposes a five-layered structure for cyber security awareness. However, for the purpose of this research, only three layers most pertinent to the organizational context have been utilised: strategic, tactical, and monitoring.

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", we can 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. These include cybersecurity policy, responsibility, training, monitoring, and actions.

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.

A comprehensive review of CISA's and ENISA's guidelines for SMEs was undertaken in this study. 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 the analysis is to discern which guidelines are most conducive to enhancing cyber awareness among businesses in Zambia and which are instrumental in augmenting the cybersecurity posture of Zambian enterprises. 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.

3. Research Methodology

The qualitative research methodology was adopted for the study. And the following data collection instruments employed: semi-structured in-depth interviews, cross-sectional tool, and document analysis. The adopted strategy was grounded in a humanistic and interpretive perspective, aiming to deeply understand human experiences. 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.

Population and Sampling

Employees from small and medium-sized enterprises formed the target population for the study, acknowledging the vulnerability of SMEs to cyber threats due to typically fewer resources and less stringent policies than larger firms. The research included employees across organisational levels rather than focusing on senior management alone, recognizing that cyberattacks can target any employee and that responsibility for cybersecurity spans the entire organisation.

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. Twenty 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. This sampling method ensured that interviewees could contribute meaningfully to the research objectives based on their knowledge and experience.

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.

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.

4. Findings of the Study

The findings of this study are grounded in a methodical examination of three primary sources: the guidelines from CISA and ENISA specifically designed for SMEs; the nuanced thematic analysis of in-depth interviews; and a thorough review of Zambia's Data Protection Act, which is further enriched by an in-depth discussion with the Data Protection Commissioner. The structure of the research findings is sequential, with each layer contributing to a more profound understanding of cyber awareness and security in the Zambian business context. The guidelines developed from this process are presented in the appendices, tailored to enhance cyber awareness and cybersecurity measures for businesses in Zambia.

Major Theme 1: Cybersecurity Knowledge and Practices among Employees

In an increasingly digital landscape, cybersecurity is essential in seeking to safeguard assets (Gundu, 2019). Employees are a principal defence line 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 organizational cybersecurity. It aligns with the study's first objective, exploring employee cybersecurity knowledge and practices in Zambia, aiming 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 organizational operations, enhancing efficiency and innovation (Baskerville, et al., 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 looks at 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 to 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 explore 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"). Emails and the internet, while primarily for professional use, are also used for personal interactions, as indicated by participants' usage of computers for email and internet tasks ("...The computer where we receive mail..."; "Not really complex ones, but I do. Internet, emails").

Varied Approaches to IT System Usage

Individuals vary in their IT system usage, with some prioritizing 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 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 utilize 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"*).

Specialized IT Tools and Applications

The use of specialized tools like NetSuite, WAN, and tracking systems illustrates the adoption of diverse technologies tailored to specific organizational 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 indispensable 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 specialized applications, are highlighted, demonstrating 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 used to interpret these threats. This understanding is crucial 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 recognized 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, emphasizing 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 unauthorized access to systems were prevalent, underscoring the necessity of 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 organizational 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 recognized as a critical issue (*"I think the biggest threat is that, we have a few, we have a single server"*). Email communication was 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, recognizing 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 organizational 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, had not 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 emphasise 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 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 organizations (*"No, we've never really had any sort of training or any sort of awareness pertaining to the risks"; "No"; "Personally, no"*).

These findings emphasize 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 organization's defence against cyber threats.

Response to / Countering Cyberattacks

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 of"*). They adopted practices like changing passwords and avoiding risky online behaviour (*"Yeah like on my personal space 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 emphasizing 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 cyber security"*). This underscores the need for regular training and proactive practices to foster a cybersecurity-aware culture and enhance organisational resilience against cyber threats.

Major Theme 2: Factors Influencing Cyber Awareness Implementation

This Major Theme explores the various elements necessary 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 organizations looking to strengthen their cybersecurity position.

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 organizational resilience against the evolving cyber threat landscape (Chen & He, 2013). Participants unanimously recognized the ubiquity and diversity of cyber risks, with hacking and blackmailing through hacking cited as common concerns (*"Cyber risks has 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, had not experienced cyber incidents, attributing this to proactive security measures like strong passwords. However, some noted a lack of adequate protection for organizational systems, emphasizing 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 toward 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 organization, pointing to a potential communication gap (*"I think mainly most of it is self-researched or self-read because every now and then 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 emphasize the importance of diverse sources and proactive efforts in gaining cyber threat awareness, necessary for enhancing cybersecurity strategies within organizations.

Training to Understand Cyber Risks

Training and education are key to awareness and understanding of cyber risks (Tam, et al., 2020; Stephanou & 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 organizations, 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 promoting 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 a known 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 demonstrate a critical need for formal training and education on cyber risks within organizations. 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 when developing a vigilant and proactive cybersecurity culture in organizations.

Cybersecurity Policies and Compliance

In cybersecurity, policies and compliance are fundamental for maintaining a secure organizational environment. Participants noted the existence of clear codes of conduct and sanctions for non-compliance, emphasizing 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 organizations. 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 of"*). 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 designated individuals for cybersecurity management. Continuous policy evaluation and enhancement are necessary to adapt to the changing cybersecurity landscape and ensure effective protection against potential risks.

5. Contributions of the Study

This study makes significant 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 practices 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 organizational levels. Such guidelines represent 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.

6. Limitations of the Study

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 generalized 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 less exposed now, 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.

7. 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 essential 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.

8. 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 revelation 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 potential catastrophic consequences of cyber-attacks, including bankruptcy, as highlighted by several interviewees.

Another important finding is the general absence of dedicated IT personnel in Zambian businesses, a role that is essential 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 to remain compliant with the law, otherwise face potential penalties for non-compliance. The Data Protection Commissioner and the Ministry of SMEs of Zambia have shown 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, (2021). State of the Internet / Security: A Year in Review, s.l.: Akamai Technologies.

Baskerville, R., Rowe, F., & 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), pp 33-52.

Boyce, M. W. et al. (2011). Human performance in cybersecurity: a research agenda. In Proceedings of the Human Factors and Ergonomics Society annual meeting, 55(1), pp 1115-1119.

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).

Dagada, R. (2013). Digital banking security, risk and credibility concerns in South Africa. Second International Conference on Cybersecurity, pp 148-161.

Dagada, R. (2014). Legal and policy aspects to consider when providing information security in the corporate environment. Thesis submitted in accordance with the requirements for the degree of Doctor of Philosophy in Information Systems at the University of South Africa, November 2014.

Dagada, R. (2021). *Digital Commence governance in the era of fourth industrial revolution in South Africa*. Pretoria: Unisa Press.

Federal Bureau of Investigation. (2020). IC3 Annual Report, s.l.: Federal Bureau of Investigation.

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

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

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. 14th International Conference on Cyber Warfare and Security, pp94-102.

Ifinedo, P. (2023). Effects of security knowledge, self-control, and countermeasures on cybersecurity behaviors. *Journal of Computer Information Systems*, 63(2), pp 80-396.

Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide, No. 131. *Medical Teacher,* 42(8), pp 846-854.

Kortjan, N., & von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in South Africa. *South African Computer Journal*, 52(1), pp 29-41.

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), pp 61-70.

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

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

Nifakos, S. et al. (2021). Influence of human factors on cybersecurity within healthcare organisations: A systematic review. *Sensors*, 21(15), pp 5119.

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

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

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

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

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), pp 92-100.

Slusky, L. (2020). Cybersecurity of online proctoring systems. *Journal of International Technology and Information Management*, 29(1), pp 56-83.

Stephanou, T. & Dagada, R. (2008). The impact of information security awareness training on information security behaviour: the case of further research. *ISSA 2008*, University of Johannesburg, 2 to 4 July 2008.

Tam, K., Moara-Nkwe, K., & Jones, K. (2020). The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training.. s.l.:s.n.

World Economic Forum. (2018). Cybersecurity: The $1 Trillion Opportunity, s.l.: 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, pp 211-222.

Zambia Development Agency. (2020). Promoting SME competitiveness in Zambia. Lusaka, Zambia: Zambia Development Agency.

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).