Mitigating Cybersecurity Risks in the Digitization of Banking Operations: Strategies, Challenges, and Best Practices for Zambian Commercial Banks

Sidney Kawimbe[1*], Mubukwanu Kwalombota[2]

[1]ZCAS University, P O Box 35422, Lusaka

[2]FNB Bank – Zambia, J859+G8J, Thabo Mbeki Rd, Lusaka, Lusaka

[*]Corresponding Author

DOI: https://dx.doi.org/10.47772/IJRISS.2024.803213S

Received: 16 July 2024; Accepted: 22 July 2024; Published: 28 August 2024

ABSTRACT

This study explores cybersecurity risk mitigation strategies within the Zambian banking sector amidst rapid digitization. Utilizing a mixed methods approach, data from a survey involving 123 bank employees/managers from banks operating in Zambia and expert interviews with bank cybersecurity staff. The study offers comprehensive insights into stakeholders' perceptions, challenges, opportunities, implemented strategies, and recommended best practices for Cybersecurity Risk Mitigation (CSRM). The findings highlight a diverse landscape of digitization efforts among banks, influencing their exposure to cybersecurity vulnerabilities ranging from fundamental lapses to sophisticated threats like advanced persistent threats (APTs) and ransomware. Current cybersecurity strategies, including security audits and regulatory compliance, are prevalent but exhibit varying effectiveness, particularly in areas such as encryption and incident response readiness. Employee training emerges as a pivotal factor despite mixed perceptions regarding its efficacy, underscoring its critical role in mitigating human-induced vulnerabilities and adapting to evolving cyber threats effectively. Best practices identified in the study emphasize rigorous regulatory compliance tailored to the banking sector, secure software development practices, and robust vendor risk management protocols. Recommendations derived from the study advocate enhancing regulatory adherence, investing in advanced encryption technologies, and prioritizing comprehensive, context-specific employee training programs to foster a resilient cybersecurity culture across Zambian banks. These insights contribute valuable perspectives on cybersecurity challenges specific to the Zambian banking sector, advocating adaptive strategies to safeguard digital operations effectively amidst evolving cyber threats. This study not only addresses current gaps in cybersecurity resilience but also provides practical recommendations such as enhanced regulatory compliance, improved encryption and incidence response, prioritization of employee training and implementation of secure software practices aimed at enhancing overall preparedness and resilience against cybersecurity threats in Zambian banking operations undergoing digital transformation.

Keywords: Resilience, Cybersecurity, Banking Sector, Cyber threat, Risk Management

INTRODUCTION

The growing fourth industrial revolution, characterized by the convergence of digital technologies, is transforming the knowledge economy. As Pariso & Marino (2020) suggest, organizations across public and private sectors are harnessing these technologies to generate value and secure a competitive edge. The banking industry, a fervent adopter of digitization (Girling, 2022), has reaped significant benefits from this transformation. However, this digital metamorphosis also presents substantial cybersecurity vulnerabilities, as Strelicz (2021) aptly highlights. This chapter serves as an introduction to the research project titled *Cybersecurity risk mitigation in digitizing banking operations: the case of Zambia's commercial banks*. It establishes the conceptual, theoretical, and knowledge-based context of the study, illuminating existing research gaps in a concise problem statement. Furthermore, the chapter outlines the research methodology and the organizational structure of the entire dissertation.

LITERATURE REVIEW

As noted, the digitization of banking operations has revolutionized the financial industry, offering greater convenience and efficiency to customers while presenting new challenges and risks for banks. This transformation has fundamentally changed how financial services are delivered, creating a landscape that requires banks to constantly adapt to remain secure and efficient. A comprehensive examination of existing studies reveals several significant cybersecurity risks arising from the digitization of bank operations. Most studies in this regard relied on reviews of existing literature to identify the threats. This reliance highlights a crucial gap, the need for more empirical research to deepen our understanding of these risks and the effectiveness of various mitigation strategies. Some studies find that digitization expands the attack surface for cybercriminals.

With the introduction of new channels such as mobile banking, online portals, and APIs, banks are exposed to a wider range of potential vulnerabilities. This increased attack surface provides cyber attackers with more opportunities to exploit weaknesses within the banking infrastructure, as highlighted by Zabala Aguayo & Ślusarczyk (2020) and Thach et al. (2021). Moreover, the interconnectedness between internal systems and external partners further amplifies this risk. Khan and Malaika (2021) and Asgarimehr & Maghsoodlou (2023) emphasize that if one element of the interconnected system is compromised, it could potentially compromise the entire ecosystem. Rapid advancements in digital technologies have enhanced efficiencies of various sectors including the banking and financial services sector (Chakraborty, 2020; Girling, 2022).

Chakraborty (2020) is of the view that technology developments increased innovative possibilities for improving productivity and changing traditional banking procedures. The emergence of digital platforms makes it feasible for the banking and financial services sector to operate across national borders, resulting in the industry's globalization (Abdellah & Benyacoub, 2023). Owing to digital innovation, the banking and financial services industry has experienced a significant transition in recent years (Kondratyeva, Svirina, & Tsvetkov, 2021). To offer consumers easy and easily available services, traditional brick and retail banks are progressively utilizing digital channels including digital wallets, smartphone apps, and online banking (Rodrigues, Ferreira, Teixeira, & Zopounidis, 2022).

Digitization brings about significant data security concerns for banks according to extant literature. The proliferation of digital channels results in a substantial increase in the volume and complexity of sensitive customer data stored by banks. This data, including financial information and personal details, becomes a prime target for cybercriminals seeking unauthorized access, as discussed by Khan and Malaika (2021) and Kondratyeva et al. (2021). Consequently, the risk of data breaches and leaks becomes heightened due to the challenges associated with managing data across multiple systems and channels, as indicated by Najaf et al. (2021) and Saeed et al. (2023). Ensuring the integrity and confidentiality of this data requires robust encryption protocols, advanced threat detection systems, and regular security audits to identify and rectify potential vulnerabilities.

Regulatory compliance adds another layer of complexity, requiring banks to continuously update their policies and procedures to align with new laws and standards. However, as indicated, the studies cited and reviewed mostly relied on reviews of literature to identify the cybersecurity risks faced by banks as they undergo digitization of operations. The approach applied in this regard may have been justified by sensitivities around the research area which may deter empirical data collection. Conducting empirical research in cybersecurity can be challenging due to the sensitive nature of the data and the potential repercussions of disclosing security weaknesses. Nevertheless, the reliance on literature reviews limits the depth of understanding that can be achieved. Empirical studies, involving direct observation, case studies, or experiments, could provide more context-intelligent insights into the effectiveness of different cybersecurity measures and the specific challenges faced by banks. Thus, from the reviewed studies, it is evident that while the digitization of banking operations offers significant benefits in terms of convenience and efficiency, it also introduces a range of cybersecurity risks that must be carefully managed.

Existing studies provide a valuable overview of these risks and highlight the importance of comprehensive, evidence-based training and robust organizational practices. However, there is a clear need for more empirical research to better understand the specific threats and to develop targeted, effective strategies for mitigating them. By addressing these gaps, banks can better protect their operations and their customers, ensuring that the benefits of digitization are realized without compromising security.

Studies on Efficacy of Cybersecurity Risk Mitigation Strategies

The existing research provides insights into cybersecurity risks in banking digitization but lacks direct focus on the efficacy of specific mitigation strategies. Several studies offer indirect observations. This subsection describes relevant studies and their lessons. Chakraborty (2020) studied multiple banks in India using surveys and interviews with IT managers and cybersecurity experts. The research stressed the need for robust risk management to address vulnerabilities from digitization. Findings showed many banks had basic but insufficient cybersecurity measures, needing further development in continuous monitoring and advanced threat detection. Khan & Malaika (2021) reviewed banking cybersecurity practices in Europe and North America through case studies and secondary data analysis. They emphasized effective risk management strategies, highlighting improvements needed in organizational structures and cybersecurity training for personnel. Despite awareness of risks, comprehensive risk management execution was often lacking.

The literature underscores the necessity of effective cybersecurity risk mitigation in banking. It recognizes digitization introduces new vulnerabilities that require comprehensive and adaptable risk management. Effective organizational structures, skilled personnel, and third-party risk management are crucial. Case studies provide practical examples but have limitations in generalizability and long-term effectiveness assessments. Most studies lack empirical evidence directly assessing specific strategy efficacy. Chakraborty (2020), Khan & Malaika (2021), and Saeed et al. (2023) mainly relied on reviews and theoretical discussions, limiting concrete conclusions about real-world effectiveness. Moşteanu (2020) highlighted organizational adaptation and skill development but lacked empirical support. Farooqui & Husain (2021) emphasized third-party risk management without detailed evaluations of measures' performance.

Studies on Employee Training and Cybersecurity Risk Mitigation

Various recent studies have also explored the theme of employee training and mitigation of cybersecurity risks. Cryer & Zounlome (2018) study was conducted within the academic setting of IU South Bend, focusing on undergraduate research.

They examined the gap between cybersecurity training and the effective knowledge base of employees, particularly in the context of cyber threat mitigation. The authors emphasized the need for more practical, hands-on training that can bridge the theoretical and practical aspects of cybersecurity knowledge. Their findings highlighted that theoretical training alone is insufficient, and that employees require more practical experience to effectively mitigate cyber threats.

Despite their common ground, the studies differ in their methodologies and specific focuses. Cryer & Zounlome (2018) primarily examine the academic context, which may limit the applicability of their findings to broader organizational settings. He et al (2020) utilize a robust, evidence-based approach, emphasizing the practical implications of their training methods but do not delve into the long-term impacts of such training. He & Zhang (2019) provide a broader organizational perspective, focusing on the implementation and sustainability of training programs but lack detailed case studies or examples of successful applications. The studies are interconnected in their overarching goal of improving cybersecurity through effective employee training. Cryer & Zounlome (2018) provide a foundational understanding of the gap between theoretical and practical knowledge, suggesting the need for more experiential learning. He et al (2020) build on this by demonstrating the effectiveness of practical, evidence-based training programs. He & Zhang (2019) further expand the conversation by offering comprehensive strategies for maintaining effective training programs within organizations.

Collectively, these studies contribute valuable insights into the effectiveness of cybersecurity training programs in banking and other sectors. Cryer & Zounlome (2018) highlight the existing gaps and the need for bridging theoretical and practical knowledge. He et al. (2020) demonstrates the effectiveness of evidence-based training, emphasizing real-world application. He & Zhang (2019) provide actionable recommendations for creating and maintaining effective training programs.

Studies on Best Practice in Cybersecurity Risk Mitigation

The theme of best practices in cybersecurity risk mitigation has been prominently featured as the digitization of banking operations becomes more widespread. Key studies provide valuable insights into various aspects of cybersecurity. For example, Khan & Malaika (2021) conducted an international review of banking cybersecurity practices in Europe and North America. Their research emphasized the importance of strong cybersecurity governance within organizations, which includes clear roles, responsibilities, and accountability. Additionally, they highlighted the need for a comprehensive risk management framework that includes regular risk assessments and penetration testing to proactively identify and mitigate cybersecurity risks.

Despite their common goal, the studies differ in their specific areas of focus and methodologies. Khan & Malaika (2021) provide a broad international perspective on governance and risk management, whereas Asgarimehr & Maghsoodlou (2023) offer a detailed case study of an Iranian bank. Manoj (2021) and Rodrigues et al. (2022) focus on technological aspects, with Manoj concentrating on basic security controls and Rodrigues et al. highlighting advanced technologies like AI and machine learning. Chakraborty (2020) bridges these aspects by discussing both basic and advanced technological measures. Moşteanu (2020) uniquely emphasizes the importance of employee training and cultural integration, a perspective not deeply explored in the other studies. Farooqui & Husain (2021) provide a detailed analysis of third-party risk management, while Abdellah & Benyacoub (2023) focus on compliance with legal regulations, an area less addressed by others.

RESEARCH METHODOLOGY

The concept of research approach refers to the overarching strategy or plan of action chosen to guide the investigation and interpretation of research findings (Bryman, 2012). It determines how data will be collected, analysed, and interpreted to address the research questions effectively (Pandey, 2019). Two primary research approaches are deductive and inductive reasoning, each offering distinct methodologies and applications suited to different research contexts (Pandey, 2019). Deductive reasoning involves deriving specific hypotheses from general theories or principles. In the context of this study, deductive reasoning was employed during quantitative data analysis (Natow, 2020). This approach allowed the researcher to test hypotheses derived from existing theories and literature on cybersecurity risks and mitigation strategies in the banking sector. By applying deductive reasoning, the study aimed to validate or refute theoretical propositions through statistical analysis of quantitative data collected from surveys and structured questionnaires (Woiceshyn & Daellenbach, 2018).

Inductive reasoning, on the other hand, involves developing generalized conclusions or theories based on specific observations or empirical evidence (Azungah, 2018). Qualitative data collection methods, such as semi-structured interviews, were utilized in this study to facilitate inductive reasoning (Woiceshyn & Daellenbach, 2018). Through in-depth exploration of participant experiences and perspectives, the study aimed to identify emerging themes and patterns related to cybersecurity challenges faced by Zambian banks. Inductive reasoning allowed for the generation of new insights and hypotheses grounded in the specific context of the banking sector, informing broader understandings of cybersecurity practices (Woiceshyn & Daellenbach, 2018).

The choice of a mixed methods research approach in this study integrated both deductive and inductive reasoning (Cresswell, 2014). This approach was selected because it combines the strengths of qualitative and quantitative methods, offering a comprehensive exploration and validation of cybersecurity issues in Zambian banks. Unlike purely deductive or inductive approaches, a mixed methods approach allowed for triangulation of data sources, enhancing the robustness and credibility of findings by corroborating different types of evidence and perspectives (Woiceshyn & Daellenbach, 2018). By employing a mixed methods approach, the study aimed to provide enhanced insights into cybersecurity challenges and mitigation strategies within the Zambian banking sector, contributing to both theoretical advancements and practical applications in cybersecurity management (Azungah, 2018).

Strategy Justification

Research Paradigm

A research paradigm refers to the philosophical framework guiding a study, influencing the researcher’s worldview and approach to understanding the research problem. In this study, a pragmatic research paradigm was adopted. Pragmatism emphasizes practical solutions to real-world problems, bridging the gap between theory and practice (Creswell & Creswell, 2018 (Heras-Escribano, 2021)). The choice of a pragmatic research paradigm was justified by the need to address real-world cybersecurity issues encountered by commercial banks in Zambia. Unlike purely theoretical paradigms, which may prioritize abstract concepts and generalizable theories, pragmatism focuses on actionable insights and recommendations that can directly impact cybersecurity practices within the banking sector. By adopting a pragmatic approach, the study aimed to provide practical solutions and recommendations that are applicable and relevant to the specific challenges faced by Zambian banks in managing cybersecurity risks (Flick, 2017). This paradigmatic choice allowed the research to consider the practical implications of cybersecurity strategies, considering the contextual factors and operational realities of commercial banks in Zambia.

By emphasizing practical outcomes, the study aimed to contribute directly to enhancing cybersecurity resilience and management practices within the banking sector, thereby addressing critical issues in a manner that aligns with the pragmatic philosophy of problem-solving and application (Heras-Escribano, 2021).

Time Horizon

The study focused on the experiences of Zambian banks over the past three years (2021-2024), aligning with recent legislative developments in cybersecurity.

This temporal scope was chosen to ensure that findings were current and relevant to contemporary challenges faced by banks in Zambia.

Sampling Frame

The sampling frame encompassed all commercial banks operating in Lusaka, Zambia. This inclusive approach aimed to provide a representative sample that reflected the diversity and operational scale of the banking sector in the city. By including all banks, the study ensured comprehensive coverage of perspectives and practices related to cybersecurity.

Sample Size and Sampling

The study population consisted of all employees/managers across commercial banks in Zambia. A purposive sampling technique was employed to select participants, ensuring representation from various managerial levels and diverse roles within the banks (Campbell, et al., 2020). The sample size was calculated to be 162, based on a confidence level of 95% and a margin of error of 5.5% and a proportion of 15% of the population deemed to be closely involved in cybersecurity risk mitigation and bank digitization processes. This size was deemed sufficient to provide robust statistical analysis and ensure the reliability of findings.

$$n = Z\alpha^2 * p * \frac{1-p}{E^2} = 1.96^2 * 0.15 * \frac{1-0.15}{0.055^2} \approx 162$$

In-depth interviews on the other hand were conducted with 18 risk Managers from each of the commercial banks that took part in the study.

Data Collection

Data were collected through semi-structured questionnaires and face-to-face interviews. The questionnaires were distributed in hard copy and made available to respondents online to enhance accessibility and convenience (Krosnick, 2018). This mixed-methods approach enabled the gathering of qualitative insights into perceptions and experiences, as well as quantitative data on awareness levels and practices related to cybersecurity. The choice of methods aimed to triangulate findings and provide a comprehensive understanding of the research problem (Natow, 2020). The appendix includes both the questionnaire and the interview guide that were used in these processes.

DISCUSSIONS

This study was conducted to investigate the specific cybersecurity landscape of commercial banks in Zambia in the context of digitization, assess the effectiveness of current mitigation strategies, and identify tailored best practices for mitigating cyber risks.

This was achieved through a mixed methods research study that focused on the experiences of commercial banks in Zambia over the past three years (2021-2024) considering developments such as the Data Privacy Act (DPA), Cybersecurity and Cyber Crimes Act (CCCA) and Cyber and Information Risk Management Guidelines (CIRMG) (Siampondo et al, 2023). The previous chapter described the methodological choices that were made to support the attainment of the objectives of the study. This chapter presents and analyses the findings of the study. The data for analysis was effectively collected from a survey involving 123 respondents from Zambia's banking sector. This represented a response rate of 88% of the target sample size of 140 as was estimated in Chapter Three. Data was also collected using in-depth interviews involving 18 cybersecurity specialists/risk managers from Zambia's banking sector. The chapter begins by presenting data that was collected from the survey before using thematic analysis to present qualitative data from the interviews that were conducted.

Survey Respondent Profiles

Data in Figure No 1 below shows the distribution of respondents according to the years they had been operating in risk management in the bank. The results show that the highest ratio of respondents, 47.97%, had been operating in bank risk management for over 4 years, indicating a significant proportion of experienced professionals in the field.

This was followed by those who had been operating in bank risk management for 2 to under 4 years, comprising 32.52% of the respondents, suggesting a substantial number of moderately experienced individuals. The least relative frequency was related to respondents with less than 2 years' experience in 47.97% of respondents who answered in the negative, indicating that nearly half of the professionals had not received specialized training in cybersecurity.

On the other hand, 52.03% of respondents indicated that they had undergone specialized cybersecurity training, suggesting a slight majority had received specific training to handle cybersecurity threats in the banking sector.

This data underscores the importance of continuous professional development and training in cybersecurity to ensure that bank risk management professionals are well-equipped to handle emerging threats.

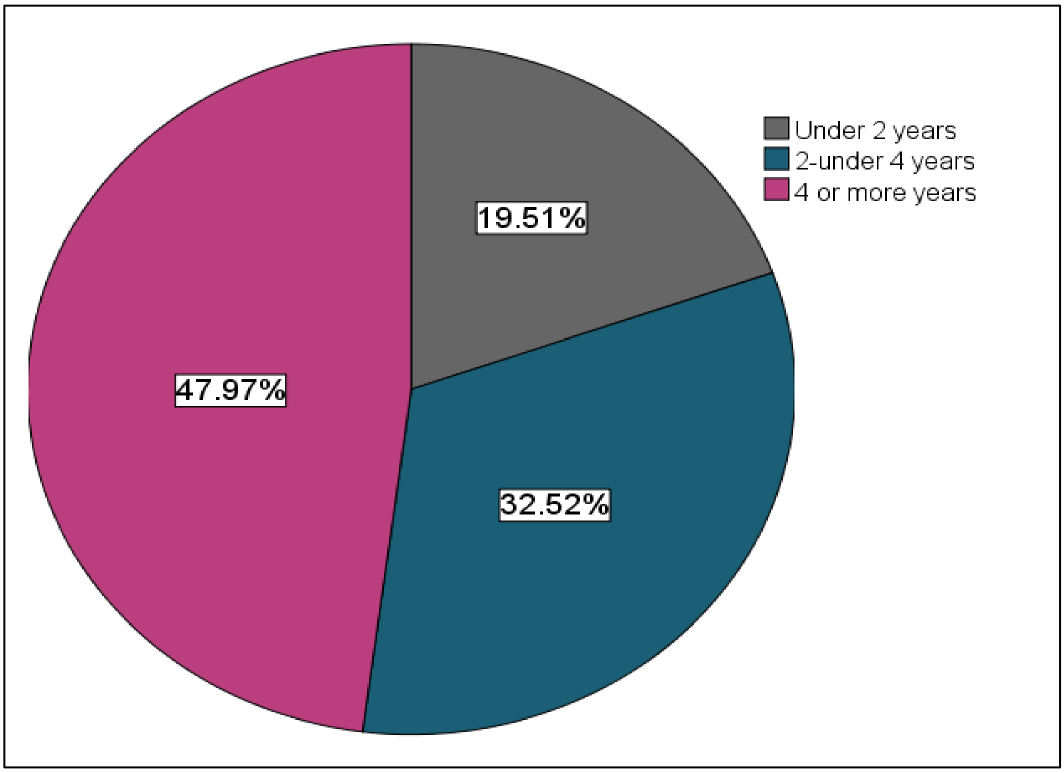

Figure 1 Distribution by Experience of Bank Risk Management

Source: Researcher (2024)

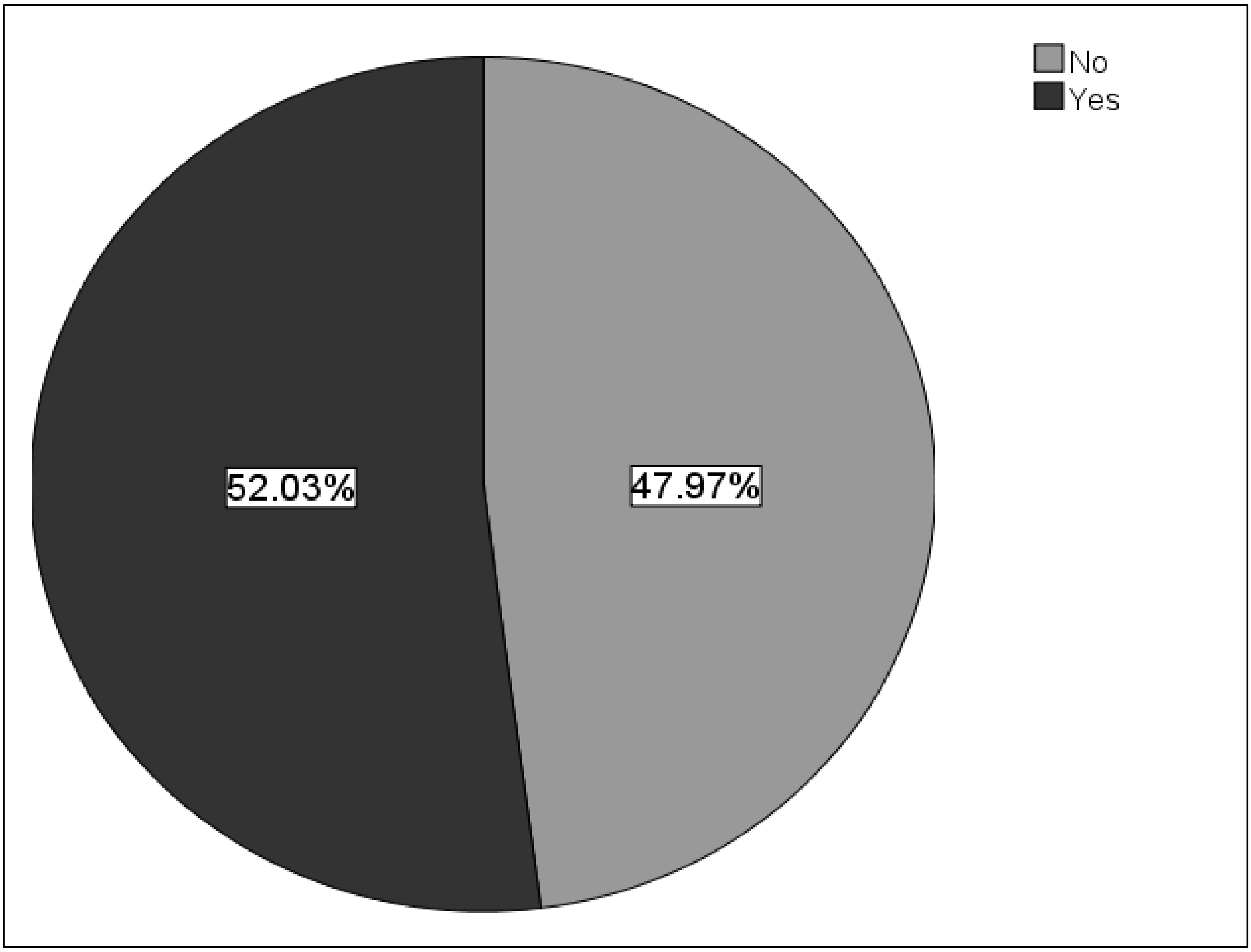

Figure 2 Distribution based on Whether Cybersecurity Trained or Not

Source: Researcher (2024)

Bank Digitization and Critical Cybersecurity Threats in Zambia

Respondents were asked to indicate the extent to which operations in their banks were digitized. Figure 4.3 shows the results that were obtained. The results in the figure show that there was a very low to negligible response frequency identifying with the *“No digitization at all”* (0.44%). On the other hand, there were 23.58% of respondents who reported that their banking institutions had minimal digitization comprising basic online services. There were 28.46% of respondents who suggested that their banking operations were *“mostly digitized*” with majority of banking operations automated. Only 18.70%, the second lowest after the no digitization response, was associated with the full digitization response. These results suggested that commercial banks in Zambia are at varying stages of digital transformation, with a significant proportion still in the early to mid-stages of digitization. This uneven level of digitization indicates that while some banks have embraced advanced digital solutions and automation, many are still reliant on basic online services and partial digitization. Consequently, this disparity presents different levels of exposure to cybersecurity threats. Banks with minimal digitization might face lower immediate risk from sophisticated cyber-attacks but could be vulnerable due to weaker basic security measures. In contrast, banks that are mostly or fully digitized might have more robust cybersecurity frameworks but face higher risks from advanced persistent threats and sophisticated cyber-attacks due to the extensive use of digital platforms.

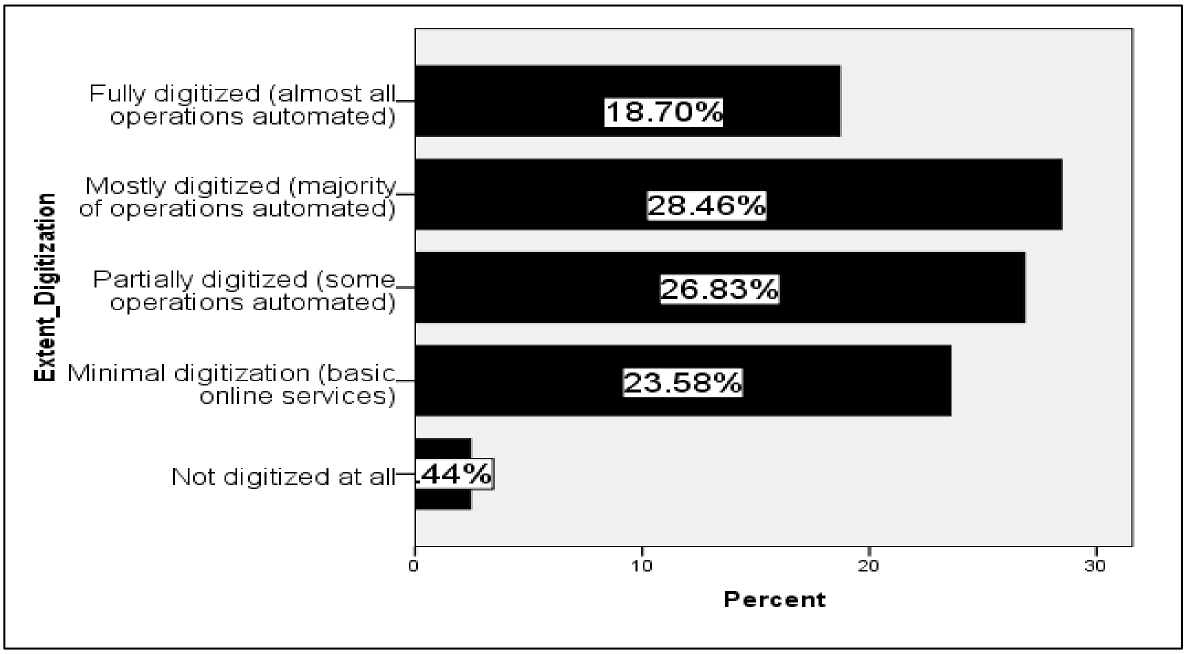

Figure 3 Degree of Digitization of Banks. Source: Researcher (2024)

Critical Vulnerabilities of Banking Digitization in Zambia

Survey respondents were asked in an open-ended question to provide information on the most critical vulnerabilities arising from digitization of banking operations in Zambia. The data that was obtained was subjected to thematic analysis. The thematic analysis identified critical vulnerabilities in the digitization of banking operations in Zambia, including inadequate cybersecurity infrastructure and governance, insufficient training and awareness among staff and customers, outdated software and systems, various types of cyber threats and attacks, weak data protection measures, poor incident response and recovery plans, inconsistent policies and controls, weak third-party and vendor management practices, inadequate monitoring and auditing, insufficient investment in advanced technology and tools, and vulnerabilities in communication and transaction security. Table 1 below offers a summary of the textual data that was collected and analyzed from the 32 responses recorded by the themes that were observed in the data. There were 11 themes that were identified in the data.

Table No 1: Themes on Most Critical Vulnerabilities

Theme	*Description*
Infrastructure and Governance (1)	
**** Lack of robust cybersecurity infrastructure***	Weak firewalls, outdated systems
**** Poor network security controls***	Unmonitored network activity, inadequate access controls
**** Weak security governance frameworks***	Lack of clear policies and procedures, insufficient oversight
**** Inadequate regulatory compliance***	Failure to meet industry standards and regulations
**** Weak governance of third-party risk***	Inadequate oversight of security practices by vendors and service providers
Training and Awareness (2)	
**** Insufficient training for bank staff on cybersecurity measures***	Staff unaware of latest threats and best practices

**** Limited awareness among customers about online banking risks***	Customers susceptible to phishing attacks and social engineering
**** Weak security awareness culture among staff***	Lack of emphasis on cybersecurity as a shared responsibility
Software and Systems (3)	
**** Outdated software systems still in use***	Vulnerable to known exploits
**** Unpatched software vulnerabilities***	Failure to install security patches in a timely manner
**** High dependency on legacy systems***	Difficulty implementing security updates due to compatibility issues
**** Inconsistent updates of security patches***	Patching not prioritized or unevenly applied across systems
Threats and Attacks (4)	
**** Frequent phishing attacks targeting bank customers***	Deceptive emails or websites designed to steal login credentials
**** Increasing ransomware attacks***	Malware that encrypts data and demands a ransom for decryption
**** Social engineering attacks on bank employees***	Manipulation tactics used to gain access to sensitive information or systems
**** Inadequate protection against DDoS attacks***	Denial-of-service attacks that overwhelm systems and prevent legitimate users from accessing them
Data Protection (5)	
**** Weak encryption methods for sensitive data***	Data easily accessible in case of a breach
**** Lack of encryption for data in transit***	Unsecured communication channels expose data to interception
**** Data breaches due to insider threats***	Malicious or negligent actions by employees or contractors
Incident Response and Recovery (6)	
**** Inadequate incident response plans***	Lack of clear procedures for identifying, containing, and recovering from security incidents
**** Insufficient data backup and recovery plans***	Difficulty restoring critical data and systems in case of a cyberattack or outage
Policies and Controls (7)	
**** Weak password policies and enforcement***	Easily guessable passwords or infrequent password changes
**** Inadequate multi-factor authentication for transactions***	Reliance on single factor authentication methods vulnerable to compromise
**** Poorly managed access controls***	Excessive access privileges or lack of user access reviews
**** Inconsistent application of security policies across branches***	Variations in security practices create vulnerabilities
**** Weak policies for mobile device security***	Unsecured mobile devices can be a gateway to corporate networks
**** Inconsistent enforcement of cybersecurity policies***	Policies not effectively communicated or enforced
Third-party and Vendor Management (8)	
**** Third-party service providers not adhering to strict security protocols***	Weaknesses in vendor security practices create risks for the bank
**** Poor vendor management practices***	Lack of due diligence in selecting and monitoring vendors

**** Limited collaboration with cybersecurity experts***	Failure to leverage external expertise to improve security posture
Monitoring and Audits (9)	
**** Lack of regular security audits and assessments***	Vulnerabilities remain undetected due to infrequent security reviews
**** Inadequate logging and monitoring of system activities***	Difficulty identifying suspicious activity or tracing the source of an attack
**** Lack of real-time threat monitoring***	Inability to detect and respond to threats in a timely manner
Technology and Tools (10)	
**** Over-reliance on outdated antivirus solutions***	Antivirus software may not be effective against new and emerging threats
**** Limited investment in advanced security technologies***	Failure to invest in modern security tools and threat intelligence
**** Vulnerabilities in cloud-based banking services***	Cloud environments introduce new security considerations
**** Lack of penetration testing***	Failure to proactively identify vulnerabilities in systems and applications
Communication and Transaction Security 11)	
**** Lack of secure communication channels for sensitive transactions***	Unencrypted communication channels expose data to eavesdropping
**** Unsecured Wi-Fi networks within bank premises***	Public Wi-Fi networks are vulnerable to interception
**** Weak security protocols for ATM networks***	Outdated ATM security protocols can be exploited by attackers

Data on Emerging Cyber Threats for Banking Digitization in Zambia

Respondents were also asked to provide data on emerging cyber threats for banking digitization. There were 25 responses that were collected for this question. The responses that were obtained were also suggested to thematic analysis and results presented in Table 4.2 below.

The thematic analysis identified several critical cybersecurity threats to Zambia’s banking sector, including phishing, ransomware, insider threats, DDoS attacks, identity theft, and advanced persistent threats. Key concerns also include cloud vulnerabilities, data breaches, mobile security, crypto jacking, and deepfake technology. Emphasizing security awareness, robust authentication, endpoint security, and regulatory compliance are essential measures to mitigate these risks and enhance overall cybersecurity resilience.

Table 2: Emerging Cyber Threats for Bank Digitization

Cybersecurity Threat	**Description**	**Frequency**
Phishing and Social Engineering	Exploits human vulnerabilities; necessitates robust employee training and awareness programs.	18
Ransomware and Malware	Increasing prevalence highlights need for advanced malware detection and response systems.	20
Insider Threats	Risks from intentional and unintentional actions by insiders; requires stringent access controls and monitoring.	15

DDoS and Network Attacks	Disrupt services and compromise communication; necessitates enhanced network security measures.	12
Identity and Credential Theft	Protecting customer information through stronger authentication methods.	14
Advanced Persistent Threats	Continuous monitoring and timely patching of systems essential to defend against sophisticated threats.	11
Cloud and Third-Party Vulnerabilities	Ensuring security in cloud services and third-party interactions.	10
Data Breaches	Protecting databases and sensitive information from breaches is a top priority.	13
Mobile and IoT Security	Strengthening the security of mobile banking apps and IoT devices as these platforms are increasingly targeted.	9
Cryptojacking	Monitoring for unauthorized cryptocurrency mining activities within networks.	7
Security Awareness and Training	Regular training programs to mitigate risks stemming from human error.	8
Deepfake Technology	Being vigilant about new technologies used for fraud.	6
Supply Chain Attacks	Securing the supply chain to prevent compromises.	5
Regulatory and Compliance Issues	Keeping up with evolving regulations to avoid legal and financial repercussions.	4
Password and Authentication	Implementing multi-factor authentication to significantly enhance security.	3
Endpoint Security	Ensuring robust endpoint protection to prevent unauthorized access.	2

Effectiveness of Cyber Security Strategies

Respondents were asked to share their views of the effectiveness of different Cyber Security strategies within the context of banking digitization. Table 4.3 below summarizes the structured data that was collected. Among the respondents, 27.6% rated firewalls as Somewhat Effective, making it the highest category. A significant portion, 22.0%, found them Somewhat Ineffective, while 18.7% were Neutral and Very Ineffective respectively. Only 13.0% rated firewalls as Very Effective, indicating mixed perceptions regarding their efficacy. Responses to encryption measures showed that 30.9% of participants viewed them as Somewhat Ineffective, the highest percentage among the categories. Neutral responses accounted for 19.5%, and Somewhat Effective received 16.3%. Very Effective ratings were given by 17.9%, while Very Ineffective responses were at 15.4%. This suggests a notable skepticism about the robustness of encryption strategies.

Intrusion Detection Systems were seen as Somewhat Effective by 24.4% of respondents, and 22.0% were Neutral. Very Effective responses were at 20.3%, indicating a favorable view from a significant minority. Somewhat Ineffective was 14.6%, and Very Ineffective was 18.7%. The data reveals a balanced yet slightly positive perception of intrusion detection systems. Opinions on security audits were diverse. The highest percentage, 23.6%, considered them Very Effective, while 22.8% saw them as Somewhat Ineffective. Responses were equally split between Very Ineffective and Somewhat Effective at 18.7% each. Neutral responses were 16.3%. This indicates a general approval of security audits with some reservations. Incident response plans were viewed as Very Ineffective by 26.0% of respondents, the highest percentage for any measure in this category. Somewhat Ineffective followed closely at 23.6%. Neutral responses were 14.6%, and Somewhat Effective was 19.5%. Only 16.3% found them Very Effective. This suggests a considerable concern regarding the adequacy of incident response plans.

Table 3 Effectiveness of Cyber Security Strategies

Measure	Very Ineffective	Somewhat Ineffective	Neutral	Somewhat Effective	Very Effective
Firewalls	18.7	22.0	18.7	27.6	13.0
Encryption	15.4	30.9	19.5	16.3	17.9
Intrusion Detection	18.7	14.6	22.0	24.4	20.3
Regular Security Audits	18.7	22.8	16.3	18.7	23.6
Incident Response Plans	26.0	23.6	14.6	19.5	16.3

Data on Employee Training and Awareness

The theme of employee training for enhancing effectiveness of bank cyber security in the era of digitization of banking operations was a key part of this study. Respondents were therefore asked to indicate their satisfaction with the level of awareness that employees in their organizations could be considered to have vis-à-vis cyber security issues arising from digitization of banking operations. Data in Figure 4.4 shows the results that were obtained in this regard.

The data reveals a divided perception among respondents regarding the effectiveness of employee training in cybersecurity. While there is a notable portion of respondents who were very satisfied (22.8%), an equally significant percentage were very dissatisfied (22.8%), pointing to a need for more robust and widespread cybersecurity training programs in the banking sector.

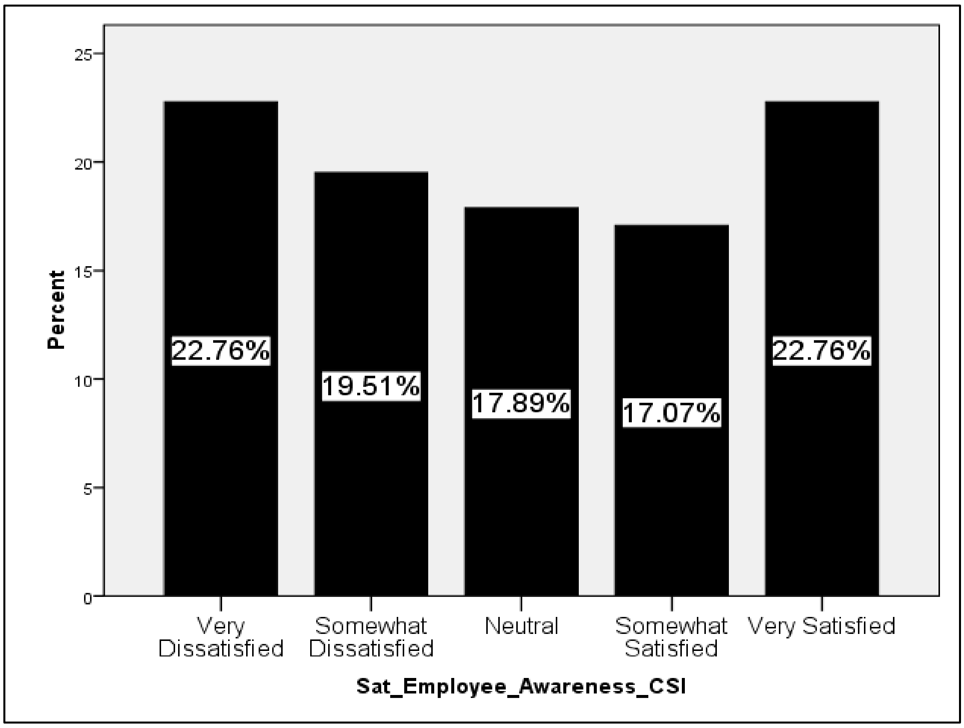

Figure 2: Satisfaction with Level of Employee Awareness of Cyber Security Issues

Source: Researcher (2024)

Respondents were also asked to indicate the extent to which employee training and awareness programs significantly increase the effectiveness of cybersecurity measures in their organizations in the context of digitization of banking operations. Data in Table 4.4 below shows the results that were obtained. The data in the table shows mixed perceptions regarding the impact of employee training and awareness programs on the effectiveness of cybersecurity measures. While a notable proportion of respondents perceive training as beneficial, a significant percentage believe it either has no effect or negatively impacts cybersecurity effectiveness. This highlights the need for more effective training programs and possibly a reevaluation of current training methodologies to enhance their impact.

Table 4: Training Programs Impact on Effectiveness of Cyber Security Measures

		Freq.	Percent	Valid %	CMLT %
Valid	Not Applicable (No training yet)	12	9.8	9.8	9.8
	Significantly Decrease Effectiveness	22	17.9	17.9	27.6
	Somewhat Decrease Effectiveness	27	22.0	22.0	49.6
	Neutral	33	26.8	26.8	76.4
	Somewhat Increase Effectiveness	29	23.6	23.6	100.0
	Total	123	100.0	100.0	

Respondents were also asked how often their organizations have provided or provide training to employees on cyber security risks and their mitigation. Data in Table 4.5 shows the results that were obtained.

Table 5: Frequency of Employee Training on Cyber Security Risks

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Never	22	17.9	17.9	17.9
	As Needed	20	16.3	16.3	34.1
	Annually	30	24.4	24.4	58.5
	Bi-Annually	31	25.2	25.2	83.7
	Quarterly	20	16.3	16.3	100.0
	Total	123	100.0	100.0	

Data on Best Practices for Cyber Security Risk Mitigation (CSRM)

Respondents were also asked to provide their evaluations of the significance of various best practice recommendations around cyber security mitigation within the context of digitization of banking operations. Data in Table 4.6 shows the summarized position for the data that was collected. Approximately 36.6% of respondents viewed regulatory compliance as not at all or slightly important, while 35.0% considered it very or extremely important, revealing mixed perceptions with a cautious inclination. Regarding regular updates, 48.0% of participants emphasized their importance, contrasting with 37.4% who were less convinced, indicating a significant emphasis on system maintenance. Secure software development practices were met with skepticism by 43.1%, yet an equal proportion recognized their critical role, demonstrating a balanced perspective. Vendor risk management mirrored regulatory compliance, with 38.7% uncertain and 41.4% acknowledging its importance, showing cautious optimism. User access control policies drew varied responses, with 34.3% uncertain, yet 35.0% emphasized their critical nature, highlighting a crucial requirement despite reservations.

Table 6: Importance of Best Practice Recommendations for CSRM

Recommendation Area	**Not at all important (%)**	**Slightly important (%)**	**Not Sure (%)**	**Very Important (%)**	**Extremely Important (%)**
Regulatory Compliance	19.5	18.7	26.8	17.9	17.1
Regular Updates	22.0	26.0	15.4	19.5	17.1
Secure Software Dev. Practices	16.3	24.4	16.3	21.1	22.0
Vendor Risk Management	17.9	23.6	21.1	19.5	17.9
User Access Control Policies	22.8	21.1	21.1	22.8	12.2

Respondents were also asked to provide a description of what they consider best practice for CSRM within the context of their banking organizations as they undergo digitization of operations. Results in Table 4.7 show the transcribed responses to the question. Only 6 responses were recorded in a form that could be considered helpful for the analysis with majority of respondents not providing data on the question. The table illustrates varying approaches among Zambian banks towards CSRM best practices. Responses emphasize regulatory adherence through regular audits and updates, coupled with a focus on secure software development and vendor risk management. Key themes include the importance of continuous compliance monitoring, robust user access controls, and proactive measures like staff training. These practices underscore a holistic approach to cybersecurity, emphasizing both regulatory requirements and operational strategies to safeguard digital operations effectively.

Table No 7: CSRM Best Practice for Banks in the Study

"Our organization strictly adheres to regulatory guidelines by implementing regular security audits and updates. We ensure robust user access control policies to safeguard against unauthorized access, complemented by continuous staff training on emerging cyber threats."-**Response 1**

"In line with regulatory requirements, we prioritize secure software development practices and vendor risk management. Our approach includes regular updates to mitigate vulnerabilities, alongside proactive monitoring of network traffic to detect and respond to potential threats promptly." –**Response 2**

"To mitigate cybersecurity risks effectively, we integrate regulatory compliance into our operational framework. This involves regular audits and updates, coupled with stringent user access controls and encrypted data transmission protocols to protect sensitive information."-**Response 3**

"Our organization employs a comprehensive approach to cybersecurity that includes regular compliance checks and updates. We emphasize secure software development practices and vendor risk assessments to ensure robust protection against evolving cyber threats."–**Response 4**

"In our operational context, we focus on regulatory compliance through frequent security audits and updates. We prioritize user access control and encryption measures, supported by staff training programs that enhance awareness of cybersecurity risks."-**Response 5**

"To mitigate cybersecurity risks, we follow stringent regulatory requirements by conducting regular audits and updates. We prioritize secure software development and maintain robust vendor risk management protocols to safeguard our digital operations."-**Response 6**

SUMMARY OF FINDINGS

Perceptions of Critical Vulnerabilities and Emerging Threats

The study confirms significant variations in perceptions among stakeholders regarding critical vulnerabilities and emerging threats associated with digitization in Zambian banks. These perceptions are shaped by the varying levels of digitization across institutions, exposing them to risks ranging from basic security lapses to sophisticated threats like advanced persistent threats (APTs) and ransomware.

Effectiveness of Current Cybersecurity Strategies

While Zambian banks employ various cybersecurity strategies such as security audits and regulatory compliance, our findings indicate mixed effectiveness. Areas of concern include encryption measures and incident response plans, which are viewed sceptically by stakeholders despite their critical importance in mitigating cyber risks.

Impact of Employee Training on Cybersecurity Measures

Employee training emerges as a crucial factor in enhancing cybersecurity resilience, despite mixed perceptions of its effectiveness. Continuous and context-relevant training programs are essential to mitigate human-induced vulnerabilities and adapt to evolving cyber threats effectively.

RECOMMENDATIONS

The study offers the following recommendations arising from the findings.

1. Enhance Regulatory Compliance: Ensure rigorous adherence to cybersecurity regulations and standards tailored to the banking sector’s digital operations.

2. Improve Encryption and Incident Response: Invest in robust encryption technologies and refine incident response plans to enhance effectiveness in mitigating cyber threats.

3. Prioritize Employee Training: Develop comprehensive and frequent training programs that address specific cybersecurity risks and foster a culture of awareness among banking staff.

4. Implement Secure Software Practices: Integrate secure software development practices to mitigate vulnerabilities inherent in digital banking operations.

5. Strengthen Vendor Risk Management: Establish stringent protocols for assessing and monitoring third-party vendors to minimize supply chain vulnerabilities.

Practical/Managerial Implications of Findings/Recommendations

Managers in Zambian banks should prioritize cybersecurity investments aligned with regulatory requirements and best practices. They should also foster a proactive cybersecurity culture through continuous training and robust incident response frameworks.

Financial Implications

Investments in cybersecurity technologies and training programs may incur initial costs but are critical for safeguarding against potential financial losses due to cyber incidents.

Operational Implications

Operational strategies should integrate cybersecurity considerations at every level, from technology adoption to vendor management, ensuring resilience against evolving cyber threats.

LIMITATIONS OF THE STUDY AND DIRECTIONS FOR FUTURE RESEARCH

While this study provides valuable insights, it is not without limitations. The sample size and scope of data collection may limit generalizability. Future research could explore the effectiveness of emerging technologies like AI and machine learning in enhancing cybersecurity resilience in Zambian banking.

CHAPTER SUMMARY

In conclusion, this study underscores the critical need for adaptive cybersecurity strategies tailored to the varying levels of digitization in Zambian banks. By addressing identified vulnerabilities, improving current strategies, and prioritizing employee training, banks can bolster their resilience against cyber threats and maintain trust in digital banking operations.

REFERENCES

1. Bryman, A. (2012). *Social Research Methods* (4th ed.). Osford: Oxford University Press.
2. Chakraborty, G. (2020). Evolving profiles of financial risk management in the era of digitization: The tomorrow that began in the past. *Journal of Public Affairs,, 20*(2), e2034.
3. Cresswell, J. (2014). *A Concise Introduction to Mixed Methods Research.* SAGE Publications, Inc .
4. Flick, U. (2017). Triangulation in data collection. In *The SAGE Handbook of Qualitative Data Collection* (p. 736). SAGE Publications.
5. Ghelani, D., Hua, T. K., & Koduru, S. K. (2022). *Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. .* Authorea Preprints.
6. Girling, P. X. (2022). *Operational Risk Management: A Complete Guide for Banking and Fintech.* John Wiley & Sons.
7. Heras-Escribano, M. (2021). Pragmatism, enactivism, and ecological psychology: towards a unified approach to post-cognitivism. . *Synthese, 198*(s1), 337-363.
8. Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). *Utilizing bio metric system for enhancing cyber security in banking sector: a systematic analysis.* IEEE Access.
9. Khan, M. A., & Malaika, M. (2021). *Central Bank Risk Management, Fintech, and Cybersecurity.* . International Monetary Fund.
10. Kondratyeva, M. N., Svirina, D. D., & Tsvetkov, A. I. (2021). The role of information technologies in ensuring banking security. *IOP Conference Series: Materials Science and Engineering (Vol. 1047, No. 1)* (p. 012069). IOP Publishing.
11. Krosnick, J. A. (2018). Questionnaire design. In *The Palgrave handbook of survey research* (pp. 439-455.). Palgrave .
12. Moşteanu, N. R. (2020). Challenges for organizational structure and design as a result of digitalization and cybersecurity. *The Business & Management Review, 1*(1), 278-286.
13. Natow, R. S. (2020). The use of triangulation in qualitative studies employing elite interviews. . *Qualitative research, 20*(2), 160-173.
14. Pandey, J. (2019). Deductive approach to content analysis. In *Qualitative techniques for workplace data analysis* (pp. 145-169). IGI Global.
15. Pariso, P., & Marino, A. (2020). From digital divide to e-government: re-engineering process and bureaucracy in public service delivery. *Electronic Government, an International Journal,, 16*(3), 314-

325.

16. Rezigalla, A. A. (2020). Observational study designs: synopsis for selecting an appropriate study design. *Cureus, 12*(1), e6692.
17. Rodrigues, A. R., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance, 60*, 101616.
18. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 25*(15), 6666.
19. Strelicz, A. (2021). Risks and threats in cyberspace–The key to success in digitization. *Journal of Physics: Conference Series, 1935*(1), 012009.
20. Thach, N. N., Hanh, H. T., Huy, D. T., & Vu, Q. N. (2021). Technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research, 15*(3), 845.
21. Woiceshyn, J., & Daellenbach, U. (2018). Evaluating inductive vs deductive research in management studies: Implications for authors, editors, and reviewers. . *Qualitative Research in Organizations and Management: An International Journal, 13*(2), 183-195.