IMPACT OF CYBERSECURITY ON RISK MITIGATION STRATEGY BY COMMERCIAL BANKS IN EMERGING MARKETS: A LEGAL PERSPECTIVE CASE STUDY

Genius Kanyongo *, Newman Wadesango **

* Midlands State University, Gweru, Zimbabwe
** *Corresponding author,* University of Limpopo, Polokwane, South Africa
Contact details: University of Limpopo, 0727 Polokwane, South Africa

OPEN ACCESS

How to cite this paper: Kanyongo, G., & Wadesango, N. (2025). Impact of cybersecurity on risk mitigation strategy by commercial banks in emerging markets: A legal perspective case study. *Corporate Law & Governance Review, 7*(1), 28–37. https://doi.org/10.22495/clgrv7i1p3

ISSN Online: 2664-1542
ISSN Print: 2707-1111

Received: 22.05.2024
Accepted: 09.01.2025

JEL Classification: M41, M49
DOI: 10.22495/clgrv7i1p3

Abstract

This study examined the impact of cyber security on risk mitigation strategy by commercial banks in the emerging market. The objectives included exploring the relationship between cyberspace and cyber threats, identifying the causes and challenges of these threats, and proposing solutions. A quantitative research approach was adopted, utilizing questionnaires for data collection from a sample of 25 respondents. Results indicated that major cyber risks included phishing, hacking, and internal accounting fraud (Johnson, 2016). Key challenges identified were inadequate oversight by managers, insufficient data encryption, reliance on third-party services, and lack of national standards and infrastructure, which hinder efforts to combat cyber threats (Alsayed & Bilgram, 2017). The study concluded that enhancing cyber security is crucial for Zimbabwean banks. Recommendations for NEWMAN Bank (NB) include implementing stringent monitoring of staff activities related to customer confidentiality, conducting regular cyber security audits, raising customer awareness, and adopting measures such as multifactor authentication, automatic logout features, and strong firewalls to mitigate cyber risks effectively.

Keywords: Cyber Security, Risk Mitigation, Commercial Banks

Authors' individual contribution: Conceptualization — G.K. and N.W.; Methodology — G.K. and N.W.; Software — G.K. and N.W.; Validation — G.K. and N.W.; Formal Analysis — G.K. and N.W.; Investigation — G.K. and N.W.; Resources — G.K. and N.W.; Data Curation — G.K. and N.W.; Writing — Original Draft — G.K. and N.W.; Writing — Review & Editing G.K. and N.W.; Visualization — G.K. and N.W.; Supervision — G.K. and N.W.; Project Administration — G.K. and N.W.; Funding Acquisition — G.K. and N.W.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

Acknowledgements: The Authors acknowledge Midlands State University for ethical clearance.

1. INTRODUCTION

This study examines the impact of cyber security on risk mitigation strategies employed by commercial banks in emerging markets, with a specific focus on Zimbabwe. A literature gap identified within the existing body of research is the limited understanding of how cyber threats uniquely affect banks in emerging markets, as most studies have focused on developed economies. The research aims to explore the relationship between cyberspace and various cyber threats, identify the causes and challenges posed by these threats, and propose actionable solutions tailored to the context of Zimbabwean banks. The primary research question guiding this study is:

RQ: How does cyber security influence the risk mitigation strategies of commercial banks in emerging markets?

The relevance of this study lies in its potential to enhance the understanding of the intricate relationship between cyber security threats and risk management strategies within commercial banks in emerging markets, enabling them to fortify their defenses against increasingly sophisticated cyber attacks. Additionally, the significance of the research extends to fostering trust and confidence among bank customers by promoting awareness and proactive measures that safeguard their personal financial information, ultimately contributing to a more resilient financial ecosystem. This study contributes to enhancing the understanding of how cyber security threats impact risk mitigation strategies in commercial banks within emerging markets, ultimately guiding banks and regulatory bodies like the Reserve Bank of Zimbabwe (RBZ) in implementing more effective security measures to protect clients and strengthen the overall financial ecosystem against cyber threats.

To analyze this issue, a quantitative research approach was employed, utilizing questionnaires to gather data from a targeted sample of 25 respondents representing different roles within the banking sector. The theoretical framework that guided the research is built on risk management theory, emphasizing the need for effective strategies to minimize exposure to cyber risks.

Findings revealed that key cyber risks faced by Zimbabwean banks include phishing, hacking, and internal accounting fraud. Major challenges identified include inadequate managerial oversight, insufficient data encryption, reliance on third-party services, and a lack of national standards and infrastructure, all of which impede effective cyber threat mitigation. The study concluded that enhancing cyber security is crucial for the sustainability and operational integrity of Zimbabwean banks. Recommendations for NEWMAN Bank[1] (NB) include implementing stringent monitoring of staff activities related to customer confidentiality, conducting regular cyber security audits, raising customer awareness, and adopting technical measures such as multifactor authentication, automatic logout features, and strong firewalls to effectively mitigate cyber risks.

The paper is structured as follows. Section 1 is an introduction outlining the significance of the study and the identified literature gaps. Section 2 reviews the literature. Section 3 details the research methodology, which includes the sampling process and data collection techniques. Section 4 present the research results. Section 5 discusses these results in the context of existing literature. Section 6 concludes the paper with a summary of key findings and practical recommendations aimed at enhancing the cyber security resilience of commercial banks, thus contributing to the growing body of knowledge on cyber risk management in emerging markets.

2. LITERATURE REVIEW

2.1. The Reserve Bank of Zimbabwe

The Reserve Bank of Zimbabwe (RBZ) is the oversight body over financial services firms, striving to create a reliable and effective financing system in the interests of clients and the country's economy in compliance with the Banks Act (RBZ, 2021). Banking is done electronically in this modern era because of computer advancements also banking and withdrawals are done over networks. This modern era encompasses bank robberies to develop new and more efficient methods to exploit digital financial ecosystems. All these technological concerns point to a cyber security study area and propose how to limit risk on banks.

The protection of computerized data as well as the system that underpins it is referred to as cyber safety. Recently, Acharya and Joshi (2020), pointed out that technological advancement has resulted in significant returns for the banking industry, in addition to cyber attacks constitute a serious risk to the same organization. The report suggests computer safety audits, electronic safety education, cyber protection assessments, and security strengthening. Acharya and Joshi (2020) released a risk-based systems approach and recommendations to address the risk of cyber attacks in financial institutions. The book is organized into six categories: computer security governance and surveillance, cyber defense threat mitigation system, technological resilience assessment, cyber security functional resilience, cyber security intelligence, and metrics, surveillance, and reporting. National Risk Assessment (2020) mentions that 900 million dollars are recorded annually in Zimbabwe due to digital financial pathways. The Central Bank's continuing attempts to combat cyber economic criminal behavior complement and dovetail with the Government's National information and communication technologies (ICT) strategy and national cyber security policy, both of which aim to secure Zimbabwean cyberspace against cyber attacks.

Cobb (2019) suggested that digital safety is required as a solution when a crime is committed. Hacking, virus dissemination, logic bombs, denial of service attacks, phishing, jacking, and other forms of cybercrime exist. Cobb (2019) declares that the world's cyber skills gap is growing and reveals that 86% of information security managers polled believed that there is a scarcity of experienced cyber security workers. Cyber warfare is proposed as a way of cybercrime safeguarding, software programs are proposed and executed. Connection surveillance systems, according to Cobb (2019), are a form of computer programs that analyze system operations in order to discover unusual breaches of safety regulations and differentiate between malicious and lawful network users.

In terms of Zimbabwean commercial lending institutions, it is crucial to stress that they are embracing cutting-edge innovations such as electronic lending, psychometric models for scoring credit, mobile payments, and biometric technology (RBZ, 2021). Financial institutions in Zimbabwe are contemplating the importance of FinTech in encouraging reliable and effective service delivery, as they are proactively embracing and leveraging

[1] NEWMAN Bank is a pseudo name for ethical reasons.

innovation to offer a varied range of financial services and goods. NB, Zimbabwe's biggest bank, has signed a Letter of Association with an American startup. The National FinTech Steering Committee has been constituted by the RBZ (RBZ, 2021). Although commercial banks have good financial success, usage of internet-based banking services is low. It is distressing to discover that just 13% of Zimbabwean banking users use digital banking services, (Wadesango & Muwishi, 2024). Ensuring electronic safety, on the other hand, is a major priority for Zimbabwean banks (RBZ, 2021). This could be one of the reasons Zimbabwean consumers are wary about digital banking. There is evidence that while doing online business transactions, clients are more concerned with the protection of their confidential data.

NB upgraded its digital banking platforms, NB Touch and NB Pay, on July 28, 2021, as part of its efforts to improve client satisfaction and security when transacting. The latest version of the NB Touch application was effective on August 5, 2021, has a considerably better visual appeal, and contains more visuals and designs, making it faster than its predecessor.

Bhasin (2016) suggested that cyber security professionals in their fields highly driven, committed, and competent to avoid, identify, react to, or decrease the consequences of such threats were of vital importance to address this issue. To that end, various cyber security teaching programs have been established in recent years, as have government-set standards efforts in the field of cyber security. According to internal NB statistics, the number of online clients at NB Gweru Branch is still relatively low compared to offline customers, even after NB has spent considerably on their digital service, according to Wadesango and Magaya (2020). Fear of online threats proves to be a barrier to digital banking. Ohrimenco and Valeriu (2023) proposed a short description of critical infrastructure, dedicating optimization model of cyber attack influence on critical infrastructure. Cyber security insurance (cyber resilience program plans, cyber liability, first-party and third-party insurance) is investigated. Cyber insurance is considered dependent on the following categories of cyber liability: unlawful exposure to data, publication of secret information, and destruction of data or digital property are all examples of data breaches. Bhasin (2016) identifies and analyzes the most comprehensive list of cyber attacks and threats extortion assaults, data manipulation attacks, many device attacks, backdoor, mobile device attacks, hacking everyday gadgets, phishing.

According to Mugari et al. (2016), cybercrime is a danger to all parts of a country's economic activity, and it is most severe in financial institutions. With the global expansion of non-cash payment technologies, the possibility of cyber attacks in banking systems has become greater. According to Mugari et al. (2016), the present liquidity crisis in Zimbabwe has increased the utilization of facilities such as credit card transactions and the real gross settlement mechanism. New payment methods, according to Mugari et al. (2016), have widened financial systems' vulnerability to risk, including forged e-wallet transactions and digital card theft. Combating and avoiding cyber attacks in emerging nations, on the other hand, becomes more challenging than in Western nations due to considerations such as insufficient awareness, ineffective legislation and regulations, and the costly nature of antivirus programs, among others. Sussmann (1999) claims that due to the rapid advancement of technology, regulatory agencies have been unable to efficiently tackle digital crime, especially in emerging nations. According to the conclusions of the preceding research, the authors propose more stringent law enforcement, education, and the use of more technologically advanced machinery to mitigate these risks. In this research, we will discuss the possibilities of employing machine learning methodologies to overcome some of the present constraints of cyber threats and cyber forensic tools. Additionally, we will concentrate on ways to decrease the relationship between cyberspace and cyber attacks to promote cyber warfare. As a result of these unlawful allegations, the researchers will study the consequences of cyber security on risk mitigation. In this research, we will discuss the possibilities of employing machine learning methodologies to overcome some of the present constraints of cyber threats and cyber forensic tools. Additionally, concentrate on ways to decrease the relationship between cyberspace and cyber attacks to promote cyber warfare (Wadesango, Karaga, et al., 2024).

2.2. Empirical studies

2.2.1. The relationship between cyberspace and cybercrime

According to Bayraymova et al. (2021), cyberspace has a set of characteristics that must be observed and taken care of so that they do not have a negative impact on the operation of the digital realm. This is the location where data and information are transmitted using proper and secure standards. Furthermore, one of the most important aspects of this domain is that it has technology that detects and controls complicated cyber attacks, as well as determines the necessary steps to prevent these attacks. According to Bayraymova et al. (2021), cybercrime is a negative act that has an immense effect on the operation of the digital realm via manipulation, espionage, extortion, or the distribution of illegal information targeting clients or businesses. Cybercriminals try to breach safeguards of computers, smartphones, tablets, networks, and other internet-connected devices. A cyber threat can be perpetrated by one individual or a gang of hackers. Military espionage, extortion to get money or information, extortion and running people's reputations, vengeance, and challenges are all common motivations for cyber threats. All crimes performed in cyberspace are referred to as cybercrime. Cyberspace is our surroundings that results from the interconnection of hardware and software infrastructure. In Zimbabwe, cybercrime is on the rise. According to the banking regulator of Zimbabwe, internet criminal activity costs the country an average of 1.8 billion dollars every year. According to Bhasin (2016), there are numerous kinds of cybercrime in Zimbabwe including identity theft, phishing, hacking, and malware victimization. According to Acharya and

Joshi (2020), there has been a massive surge in cyber intrusion and attacks over the last decade. Cybercrime causes a worldwide loss of 114 billion dollars virtually every year, with the expense of countering the crime totaling 274 billion dollars. In July 2016, the Indian banking industry lost 171 million dollars because of a phishing email attack on Union Bank, as well as a ransomware attack that locked down thousands of computers.

Statistics show that India is responsible for 7% of all electronic fraud incidences globally. Potential state and non-state actors, criminal gangs, and attackers have frequently targeted Indian banks. The incident of cyber attacks on central banks in 2016 explains this better, as bank payments attempted to be prevented by attacking its website through the insertion of malicious software by a hacker from Pakistan, as reported by Saravade and Bhalla (2018). Union Bank of India suffered an incident in July 2017, in which almost 170 million dollars was stolen from the Nestro account. According to the investigation, the criminals got access through spear phishing. The published statement of the KPMG report on illegal acts happened in 2017, financial institutions originally did not have adequate infrastructure to secure data and other essential information, causing them to fall into rampant cyber danger. According to Deloitte (2015), 93% of participants outlined that there has been a skyrocketing of illegal deception cases in the financial sector in the last two years, due to the time gap between online assaults and the identification of the risk and intruders, just under twenty-five percent of the fraudulent transactions can be recovered.

2.2.2. Cyber risk management by commercial banks

Cyber risk identification, evaluation, measurement, mitigation, and comprehension are all critical components for tackling cyber risk, just as they are for managing any other financial risk. Mugari et al. (2016) contended that the risk management method for cyber threats is controlled by adopting the risk-mitigation control procedure. Effective cyber fraud risk mitigation reduces the chance of significant adverse impacts on an organization by obviating risks, controlling effects, and reducing susceptibility (RBZ, 2021). Prevention and mitigation of risks for cyber fraud must be continuous and proactive, requiring control over both the technology itself and the people and systems that utilize and support it (RBZ, 2021). Because of the continually changing risk environment, the approach must be dynamic (RBZ, 2021).

ISO/IEC 27005:2022 suggested that cyber risk identification is the process of identifying and assessing potential threats and vulnerabilities in an organization's information systems and digital assets (International Organization for Standardization [ISO], 2022). It involves recognizing the potential risks and their potential impact on the confidentiality, integrity, and availability of data and systems. There are several reasons for conducting cyber risk identification including understanding the threat landscape, cyber risk identification helps organizations gain a comprehensive understanding of the current threat landscape. It allows them to identify potential threats, vulnerabilities, and attack vectors that could compromise their information systems and digital assets. According to Tarala (2023), banking industries have specific regulatory requirements for managing cyber security risks. Cyber risk identification helps organizations identify and address risks to ensure compliance with relevant regulations and standards. SANS Institute suggested that to identify cyber risk is to assess stakeholder confidence. Demonstrating a proactive approach to cyber risk identification instills confidence in stakeholders, including customers, partners, and investors. It shows that the organization takes cyber security seriously and is committed to protecting sensitive information and maintaining operational resilience.

2.2.3. Security practices that can mitigate cyber risks

Ghelani et al. (2022) stated that having innovation at the leading edge, the financial services industry has revolutionized, and online financial services have emerged as a more practical means to conduct transactions. South African banks often use external platforms like PayPal to complete foreign and local payments. This system is not under the bank's control, and its reliance on external systems to ensure quality in terms of how they provide internet services to clients represents a significant safety concern. As networks evolve, increasingly interconnected, reliance increases, as would the possibility of assault or harm on a computer system. Managing these risks includes restricting and neutralizing incidents before happen, a process called managing risks. Deloitte as risk management has established the first cyber artificial center (CIC) in Africa in Nairobi, Kenya, to give the highest level of cyber protection worldwide. The center is related to other centers utilizing the latest innovations on seven different continents. According to Johnson (2016), this center helps financial companies build a risk-specific, preventive digital safety approach that can help in computer attack avoidance, detection, and mitigation. These services are offered by Deloitte CIC: cyber surveillance, cyber watch, and cyber response. A computer monitoring is an actual time surveillance information system as well as a system for organizing events that identifies, analyzes, notifications, reports, and conducts a reaction process 24 hours a day, seven days a week. Cyber checks provide continuous vulnerability monitoring and control, as well as risk information which are precise and tailored to detect prospective assault before its occurrence. Gupta et al. (2021) and Khalghani (2022) concur Bhasin (2016) who explained that in an environment in which cyber assaults become increasingly complicated and common, the combination of the three ideas of cyber shield, internet space, and cyber resilience would offer a strong foundation for successfully reacting to safety issues in the age of technology. This concept refers to a strong cyber system that protects systems and networks from threats. Strong protection protocols, and modern technical installation for attack discovery, mitigation, and intervention, and it also includes early detection of fresh risks components of the cyber shield. The basic safeguard used to defend businesses from cyber attacks is known as a cyber security guard. Second, according to Czejdo et al. (2014), the idea of cyber resistance, which we name "cyberspace", is a strategic section where organizations can enhance that when faced with cyber assaults, organizations must strengthen their security procedures and safeguard system reliability. Finally, we introduce what we name the concept of cyber resiliency "cyber sword". This concept refers to a business's capacity to respond to and defend against cyber assaults. Sword of the cyberspace employs protective and reactive tactics that rely on a thorough awareness of online risk, as well as reactive methods like electronic forensics assessment, the development of fresh safety features, as well as the implementation of modern protection practices. Wadesango and Muwishi (2024) claimed that cyber security frameworks and controls, such as the NIST Cyber Security Guidelines and ISO/IEC 27001:2022 Information Security Management System (ISMS) Benchmark, can be utilized to reduce risks related to cyber security.

2.2.4. Cyber security risk associated with the banking industry

Ojeniyi et al. (2019) conducted a study in Nigeria to examine the controlling risks associated with electronic financial institutions in Nigeria, utilizing Diamond Bank and other banks as case studies. The purpose of this study was to assess the threat to safety associated with various parts of digital transactions to identify the amount of security priorities required to ensure their privacy, access, and authenticity. Questionnaires were utilized to collect data to assess the degree to which bank clients mostly affected them (Ojeniyi et al., 2019). Respondents included risk officers from Nigerian institutions. To obtain replies from respondents, the survey was graded on a rating system of occasionally, regularly, very frequently, seldom, and never. In addition, a scale grading system was established to quantify the dangers of internet money transfers. It was carried out in the following way, the combination of very often and frequently scales yielded an amount of a small effect risk, whilst moderate risk's effect was immediately mapped to the sometimes scale, and a significant influence of risk was obtained by combining rarely and never scales. According to the results, most of the respondents kept their accessible via the internet including operations credentials as well as private information to their mobile devices, according to research and analysis. If another individual gains access to the gadget used for online transactions, this might put bank users in danger. Banks, according to Ojeniyi et al. (2019), state that they ought to tell their customers how to manage their online access and usernames when making financial transactions online. Aside from the threat of password retention, the researchers also mentioned that exchanging internet login credentials with other persons poses much harm giving unauthorized gaining of user's information. Information is subject to being illegally gained by hackers using a free Wi-Fi access point. According to the survey, many customers' confidential information is routinely charged without authentication from their users and this implies that financial institutions are supposed to create awareness campaigns to inform consumers about the dangers, like NB does to its customers. NB Holdings Limited values your security as you transact online, and we are pleased to give you tips from time to time. Fraudsters normally send emails, text messages as well and pop-up messages on websites and social media sites to clients asking for login details, internet banking passwords, and/or user's ID, this is called web phishing. If you receive such an e-mail do not open the e-mail or any of the given links, just ignore and delete the email without replying.

According to the research outcomes, a substantial percentage of those polled had a rudimentary understanding of the safety concerns associated with sharing their online bank transaction details. Furthermore, Ojeniyi et al. (2019) emphasized the need to warn users not to keep credentials and details of transactions on transaction terminals. Financial institutions must regularly upgrade their financial interaction programs to ensure that they remain trustworthy in the public domain of customer account material.

According to Choudhary and Sharma (2020), banks face a range of cyber security threats due to the sensitive nature of the data they handle and the potential financial gains for attackers. Banks are vulnerable to malware and ransomware attacks that can compromise their systems and networks. Malicious software can be used to steal sensitive customer information, gain unauthorized access, or encrypt data for ransom. Palan (2019) suggested smishing is a type of phishing attack, that often aims to trick bank customers or employees into revealing their login credentials. Attackers can then use these stolen credentials to gain unauthorized access to online banking accounts, conduct fraudulent transactions, or even compromise internal banking systems. Once attackers obtain login credentials through phishing, they can take control of customer accounts. This enables them to monitor account activities, manipulate transactions, transfer funds to unauthorized recipients, or initiate further financial fraud. According to Pal et al. (2019), breaches can lead to identity theft, financial loss, and reputational damage for both the bank and its customers. Phishing attacks often involve creating fake emails, messages, or websites that mimic legitimate bank communications or online banking platforms. These spoofed emails or websites may use similar design elements, logos, and branding to deceive recipients into believing they are interacting with the bank. Customers who unknowingly provide their login credentials or other sensitive information on these spoofed platforms can become victims of fraud (Dzomira, 2014). Banks may be targeted by more sophisticated spear phishing attacks, where attackers meticulously research and personalize their phishing attempts. They may impersonate bank executives or employees to trick other employees into divulging sensitive information, providing access to internal systems, or initiating fraudulent transactions. According to Okpa et al. (2022), phishing emails may also include malicious attachments or links that, when clicked or opened, can infect a user's device with malware. This malware can then be used to gather sensitive information, capture keystrokes, or gain unauthorized access to the bank's systems (Wadesango, Tatenda, et al., 2024).

2.2.5. Analysis of the effects of cyber threat on the ecosystem of banks

According to Mugari et al. (2016), cyber risk can have a substantial impact on a bank's ecosystem, affecting different stakeholders and parts of its operations. A successful cyber attack on a bank might result in financial damages. Direct losses from stolen funds, fraudulent transactions, or operational disruptions that impede income creation are examples of this. Indirect expenses may also be incurred because of incident response, cleanup activities, legal actions, and prospective regulatory action. According to Bhasin (2016), cyber security events can significantly harm a bank's reputation. News of a data breach, client information theft, or other cyber attacks can destroy trust in the bank's capacity to safeguard sensitive information. Rebuilding a damaged reputation can be a difficult and time-consuming process that can influence client retention and acquisition. Cyber risk occurrences have a direct impact on customers. When a person's personal and financial information is compromised, it can lead to identity theft, financial fraud, or unauthorized access to their accounts. Customers may lose trust in the bank's ability to protect their data and opt to switch to other financial institutions, resulting in customer attrition, as mentioned by Dzomira (2014). Banks are governed by a regulatory framework that imposes certain cyber security obligations. Cyber risk occurrences can result in violations of these standards, which can result in financial penalties, legal ramifications, or regulatory restrictions (Makuya et al., 2024). Failure to comply with data protection laws, privacy regulations, or industry standards can have serious ramifications for the bank. Cyber attacks, according to Acharya and Joshi (2020), can interrupt the bank's business operations, resulting in service failures, system unavailability, or transaction processing delays. These disruptions can have an impact on client experiences, impede day-to-day operations, and result in financial losses. Banks frequently work with other financial institutions, vendors, or partners. A cyber attack on one party might have a domino effect, jeopardizing the security and operations of other businesses (Wadesango & Muwishi, 2024). This emphasizes the significance of analyzing and controlling cyber risks related to the bank's ecosystem. Alsayed and Bilgram (2017) researched the techniques employed by phishing hackers in Saudi Arabia to attempt the theft of information and money laundering. The research also outlined security strategies that bank customers may take to safeguard their online financial transactions. Regardless of the advantages that financial institutions offer to their clients by way of online channels, including money transfers among accounts, payment of bills, monetary balance approval, and the ability to transmit and receive confidential data between financial institutions and their clients, digital banking has caused many safety issues (Alsayed & Bilgram, 2017; Akinbowale et al., 2020).

3. RESEARCH METHODOLOGY

In conducting the research, a structured quantitative methodology was employed to gather empirical data from specifically targeted groups within the NB. The primary method of data collection involved the use of questionnaires, which were designed to facilitate the collection of objectively measurable data regarding perceptions and practices within the bank's various departments. This approach was deemed appropriate for capturing a comprehensive statistical overview of the targeted population — comprised of bank supervisors, information technology (IT) staff, internal auditors, risk officers, and customers across 49 branches in Harare. The structured nature of the questionnaire ensured that responses were standardized, thus enhancing the reliability and validity of the findings (Bloomfield & Fisher, 2019). Additionally, piloting the questionnaire before the main study could have further refined the instrument and minimized misunderstandings among respondents, ensuring the clarity of the constructs being measured.

While the current study utilized a quantitative approach with random sampling methods, alternative research methods could also have been suitable for exploring the perceived impact of technological innovations in banking. For instance, a qualitative research design, incorporating focus group discussions or in-depth interviews, would allow for a richer exploration of the nuanced experiences and perceptions of the participants, providing insight into the qualitative dimensions of technological adoption and its implications for banking operations (Bloomfield & Fisher, 2019). Mixed-method approaches that combine both qualitative and quantitative data could also be considered beneficial, as they would draw on the strengths of both methodologies, allowing for a comprehensive analysis that captures both statistical generalizations and in-depth personal narratives.

Moreover, longitudinal studies could serve as a viable alternative, enabling the investigation of changes over time concerning attitudes toward technological innovations within the bank. Such studies could help to identify trends and relationships that are not observable in a static, cross-sectional snapshot. Utilizing these alternative methods could enrich the findings by providing a more holistic view of how technological innovations are perceived and implemented within banking settings (Wadesango, Karaga, et al., 2024). Furthermore, employing methods such as stratified sampling would ensure that different subgroups within the population are adequately represented, thereby enhancing the generalizability of the research outcomes.

Table 1. Target population and sample size

Sample components	*Targeted population*	*Sample size*	*Population sampled*
RBZ supervision and surveillance employees	7	4	57%
Information technology	8	6	75%
Risk managers	3	3	100%
Internal auditors and financial accountants	9	7	78%
Total	27	20	74%

The information was analyzed qualitatively as well as quantitatively. Quantitative analysis was used to enhance the subjective information that focused on the goals. Pearson correlation was used to determine the connection between cyber safety procedures and risk factors using the Statistical Program for the Social Sciences (SPSS).

4. RESULTS

4.1. The solutions and practices used by NEWMAN Bank to solve and resolve the risk of cyber threats

The answer to cyber fraud in banks is shown in Table 3. The mean score is important when it exceeds 2.5. With a mean of 4.60 and a standard deviation of 0.59824, Table 3 demonstrates that a forensic security audit is required to mitigate the occurrence of cyber risk in banks. Similarly, it is demonstrated that banks must utilize firewalls to avoid cyber attacks and forgeries in financial institutions, with a mean of 3.95 and a standard deviation of 1.05006. Finally, with a mean of 3.75 and a standard deviation of 1.20852, it demonstrates the necessity to sensitize bank customers to cyber security through cyber security education.

Table 2. Solutions and methods to eliminate and mitigate cyber threats

Solutions and methods	*Disagree*	*Strongly disagree*	*Neutral*	*Agree*	*Strongly agree*
Forensic audit	0.0%	0.0%	5.0%	30.0%	65.0%
Cyber security education to banks' customers	5.0%	10.0%	25.0%	25.0%	35.0%
Firewall	0.0%	10.0%	25.0%	25.0%	40.0%

Table 3. Cyber security practices to mitigate cyber threats: Descriptive statistics

Solutions and methods	*N*	*Minimum*	*Maximum*	*Mean*	*Std. Deviation*
Forensic audit	20	3.00	5.00	4.6000	0.59824
Firewall	20	1.00	5.00	3.7500	1.20852
Cyber security to bank customers' firewall	20	2.00	5.00	3.9500	1.05006
Valid N (listwise)	20				

4.2. Major challenges faced by NEWMAN Bank to mitigate cyber risk occurrence (2019–2023)

Table 5 details the difficulties encountered in reducing the extent of cyber incidents in NB institutions. The average benchmark is noteworthy at greater than 2.5. The investigation revealed that a lack of infrastructure management causes a major barrier in reducing electronic breaches of money and other confidential information, with a mean of 4.7 and a standard deviation of 0.47016. Furthermore, the chart found that the mean of 3.95 and a standard deviation of 1.35627 are the issues of decreasing online theft in institutions that were impacted by a shortage of effective databases and insufficient awareness among bank clients.

Table 4. The major challenges to mitigate cyber risk

Challenges	*Disagree*	*Strongly disagree*	*Neutral*	*Agree*	*Strongly agree*
Inadequate awareness by bank customers	10.0%	5.0%	15.0%	20.0%	50.0%
Lack of infrastructure	0.0%	0.0%	0.0%	30.0%	70.0%

Table 5. The major challenges to mitigate cyber risk: Descriptive statistics

Challenges	*N*	*Minimum*	*Maximum*	*Mean*	*Std. Deviation*
Inadequate awareness by bank customers	20	1.00	5.00	3.9500	1.35627
Lack of infrastructure	20	4.00	5.00	4.7000	0.47016
Valid N (listwise)	20				

4.3. The effects of cyber security threats on the banking ecosystem

According to the findings presented in Table 7, financial loss is the most significant effect, with a mean of 3.45 and a standard deviation of 1.46808. Furthermore, NB recorded a loss in repute, with a mean of 3.35 and a standard deviation of 1.53125. At ≥ 2.5, the mean score is significant.

Table 6. Effects of cyber security threats on the banking ecosystem

Effects	*Disagree*	*Strongly disagree*	*Neutral*	*Agree*	*Strongly agree*
Loss of reputation	20.0%	10.0%	15.0%	25.0%	30.0%
Financial loss	10.0%	25.0%	10.0%	20.0%	35.0%

Table 7. Effects of cyber security threats on the banking ecosystem: Descriptive statistics

Effects	*N*	*Minimum*	*Maximum*	*Mean*	*Std. Deviation*
Loss of reputation	20	1.00	5.00	3.3500	1.53125
Financial loss	20	1.00	5.00	3.4500	1.46808
Valid N (listwise)	20				

Table 8. Pearson correlation using SPSS bivariate analysis

		Cyber risk	*Security measures*
Cyber risk	Pearson correlation	1	0.237
	Sig. (2-tailed)		0.314
	N	20	20
Security measures	Pearson correlation	0.237	1
	Sig. (2-tailed)	0.314	
	N	20	20

Sources: Authors' computation using SPSS, 2023.

Table 8 shows a mathematical calculation of Pearson correlation with SPSS. The independent variable was internet safety risk, and the dependent variable was cyber practices. The Pearson correlation of 0.237 between cyber risk and security measures is shown in the bivariate analysis with a Sig. (2-tailed)/p-value of 0.314. Because the correlation is close to +1, it indicates that there is a substantial positive relationship between cyber risk and security measures. R = 0.237 (Sig. = 0.314).

5. DISCUSSION

Kremer and Mu̇ller (2014) proposed that cyberspace refers to the visual world formed by computers and networks, where information is stored, processed, and communicated. It includes numerous digital platforms such as the internet and cloud infrastructures. Cyber dangers, on the other hand, are potential risks that can result in harm or bad outcomes from the use of cyberspace. It comprises a wide variety of threats and vulnerabilities that can damage an organization in the setting of NB. These risks include illegal access to personal information such as banking details, banking systems, and so on, as well as virus infection, financial theft, hacking, and phishing. Bhasin (2016) argued that the relationship between cyberspace and cyber risk is complex and interconnected. Stiawan et al. (2017) suggested that the rise of cyberspace has enlarged the prospects for innovation and progress but has also introduced much risk to the industry that requires much attention as cyber security procedures to secure the organization.

When questioned about the prevalence of cyber assaults in financial institutions using cyberspace, NB staff responded that generally, the problem of cyber attacks emanates from external and internal factors, with internal factors mentioning disgruntled employees and those with access to systems and data can misuse their privileges, as well as outsider hackers. Personnel of the NB also indicated that they obtain such notifications on a minimum of three occasions a year, and additionally that they are aware of bank personnel being prosecuted for reporting such threats. According to McGuire and Dowling (2013), hacking/cracking, spamming, and running fraudulent software and spyware applications are ways used to deceive bank clients.

According to the other research findings (Bhasin, 2016; Okpa et al., 2022; Dzomira, 2014; Alsayed & Bilgram, 2017), there are several opportunities for banks to commit cyber threats during sloppy or incompetent risk administration and minimal concentration on internal oversight. When such opportunities are combined with incentives, the potential for cyber danger increases. When questioned what steps they considered could be implemented to address online risks, participants from the RBZ figured that this might be accomplished by continuously tracking the efficiency of banks in order to support the setting up of more restrictive control systems, continually informing banks about the significance of online security not only to the bank involved but to the financial service industry as a whole, and supporting banks to undertake forensic audits as an ongoing audit instead of as a statistical measure. However, both bank employees and auditors agreed that hiring forensic auditors was the most effective strategy.

Cyber security education for bank customers is another practice that can be used to mitigate cyber risk. According to Table 2, 35% of respondents strongly agree that education is the best way to curtail cyber breaches, as illustrated in Section 2 where NB informs and educates its customers about phishing, 25% of respondents agree and are neutral, 10% disagree, and 5% strongly disagree.

Another method for mitigating cyber risk is to utilize a firewall. A firewall is an internet connection security device that serves as an obstruction between a company's network and a third-party network or a different network. It tracks and controls network traffic that comes and goes based on predetermined security parameters. The primary role of a firewall is to protect the internal network from unauthorized access and to mitigate various cyber dangers. Access control, packet filtering, network address translation, application control, and intrusion prevention systems are examples of firewall features that can help to reduce risk (Okpa et al., 2022; Seissa et al., 2017).

The study's findings revealed that banks face numerous hurdles in reducing cyber risk. The challenges were a lack of guidelines and national oversight, a lack of structures, and a lack of education among bank customers. The outcomes were supported by Mugari et al. (2016), who stated that digital users in Africa do not have fresh technological advances in safety precautions such as anti-virus packages, and many of the operating system versions used are not frequently patched, impinging on the elimination of online risks. The results of the research suggested the adverse consequences of cyber security risks on banks, such as monetary losses, diminished efficiency, and vulnerability of the banking industry's ICT networks and structures.

6. CONCLUSION

In conclusion, this study highlighted key findings regarding the impact of cyber security on risk mitigation strategies employed by commercial banks in the emerging market of Zimbabwe. The research identified major cyber threats, including phishing, hacking, and internal accounting fraud, which pose significant challenges to financial institutions. These risks are exacerbated by factors such as inadequate managerial oversight, insufficient data encryption, reliance on third-party services, and a lack of established national standards and infrastructure. The implications of these findings underscore the urgent need for Zimbabwean banks to enhance their cyber security frameworks to effectively mitigate these risks, particularly by implementing robust monitoring systems, conducting regular audits, and educating customers about potential cyber threats.

While this research provides valuable insights into the current state of cyber security within the banking sector, it is subject to certain limitations. The study's small sample size of 25 respondents may not fully capture the diverse experiences and perspectives across the banking industry in Zimbabwe, and the focus on a single bank limits the generalizability of the findings. Future research could explore broader geographical contexts or include a larger sample size to draw more comprehensive conclusions. Additionally, longitudinal studies assessing the effectiveness of the recommended cyber security measures over time would be beneficial. Investigating the evolving landscape of cyber threats and developing adaptive mitigation strategies will be essential for enhancing the resilience of banks in emerging markets against cyber risks.

Regarding the effects of cyber security procedures on risk reduction by financial institutions, some pieces of advice that should be followed to reduce risks linked to bank operations are as follows.

According to our research, NB ought to boost its investment in cyber security to reduce risks and assure responsive information privacy, reliability, and accessibility. Banks should host additional gatherings aimed at awareness-raising campaigns to inform clients, and institutions ought to give out free T-shirts to individuals who attend the gatherings because motivated people are more inclined to engage in awareness campaigns. Banking firms should hire more skilled and knowledgeable IT security staff to protect their data from attacks via the Internet. Additionally, employee email learning ought to be given on an ongoing schedule to guarantee that staff are always alerted of the risks. To avoid monetary losses and harm to their reputations, institutions should concentrate on increasing ways to mitigate risks such as penetration testing, the use of encrypted passwords, and software that prevents malware despite this, corporate rules must be created to describe the protocols that would be taken in the incidence of a cyber incident.

The researchers suggest that NB implement several authentication methods and a strong firewall to protect the security of customer information and funds.

REFERENCES

Acharya, S., & Joshi, S. (2020). Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures. *PalArch's Journal of Archaeology of Egypt/Egyptology, 17*(6), 4656–4670. https://archives.palarch.nl/index.php/jae/article/view/1714

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card. A survey of literature. *Journal of Financial Crime, 27*(3), 945–958. https://doi.org/10.1108/JFC-03-2020-0037

Alsayed, O. A., & Bilgram, A. L. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and Advanced Engineering, 7*(2), 98–102. https://www.researchgate.net/publication/315399380_E-Banking_Security_Internet_Hacking_Phishing_Attacks_Analysis_and_Prevention_of_Fraudulent_Activities

Bayramova, A., Edwards, D. J., & Roberts, C. (2021). The role of blockchain technology in augmenting supply chain resilience to cybercrime. *Buildings, 11*(7), Article 283. https://doi.org/10.3390/buildings11070283

Bhasin, M. L. (2016). The role of technology in combatting bank frauds; Perspectives and prospects. *Ecoforum, 5*(2), 200–212. http://www.ecoforumjournal.ro/index.php/eco/article/viewFile/412/255

Bloomfield, J., & Fisher, M. J. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses Association, 22*(2), 27–30. https://search.informit.org/doi/10.3316/informit.738299924514584

Boparai, J. K., Singh, S., & Kathuria, P. (2018). How to design and validate a questionnaire: A guide. *Current Clinical Pharmacology, 13*(4), 210–215. https://doi.org/10.2174/1574884713666180807151328

Bursal, M., & Polat, O. (2020). Middle school students' line graph skills and affective states about common graph types used in science courses. *International Journal of Education in Mathematics, Science and Technology, 8*(4), 290–303. https://doi.org/10.46328/ijemst.v8i4.1026

Choudhary, S., & Sharma, A. (2020). Malware detection & classification using machine learning. In *Proceedings of 2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3).* IEEE. https://doi.org/10.1109/ICONC345789.2020.9117547

Cobb, S. (2019). Mind this gap: *Criminal hacking and the global cybersecurity skills shortage, a critical analysis* [Paper presentation]. Virus Bulletin Conference, October 5–7, 2016, Denver, USA. https://www.virusbulletin.com/conference/vb2016/abstracts/mind-gap-criminal-hacking-and-global-cybersecurity-skills-shortage-critical-analysis

Czejdo, B. D., Iannacone, M. D., Bridge, R. A., Ferragut, E. M., & Goodall, J. R. (2014). Integration of external data sources with cyber security data warehouse. In R. K. Abercrombie & J. T. McDonald (Eds.), *Proceedings of the 9th Annual Cyber and Information Security Research Conference* (pp. 49–52). ACM. https://doi.org/10.1145/2602087.2602098

Deloitte. (2015). *Consumer data under attack: The growing threat of cyber crime.* https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf

Denning, D. E. R., & Denning, P. J. (1998). *Interest besieged: Countering cyberspace scofflaws.* ACM Press.

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry Zimbabwe. *Risk Governance and Control: Financial market and Institutions, 4*(2), 17–27. https://doi.org/10.22495/rgcv4i2art2

Ghelani, D., Hua, T. K., & Koduru, S. K. (2022). Cyber security threats, vulnerability, and security solution models in banking. *American Journal of Computer Science and Technology, 7*(6), 34–47. https://doi.org/10.22541/au.166385206.63311335/v1

Gupta, K., Sahoo, S., Panigrahi, B. K., Blaabjerg, F., & Popovski, P. (2021). On the assessment of cyber risk and attack surface in a real-time co-simulation cyber security test bed for inverter-based microgrids. *Energies, 14*(16), Article 4941. https://doi.org/10.3390/en14164941

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001 — Information Security Management System.* IMSM. https://www.imsm.com/us/iso-27001/?utm_medium=cpc&utm_source=google&utm_term=iso%2027001&utm_campaign=LOL+-+Search+-+SA+27001&hsa_

Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber attacks mitigation. *NC Banking Institution, 20*(1), Article 277. https://scholarship.law.unc.edu/ncbi/vol20/iss1/15

Khalghani, M. R., Verma, V., Solanki, S. K., & Solanki, J. M. (2022). Resilient networked control of inverter-based microgrids against false data injection. *Electronics, 11*(5), Article 780. https://doi.org/10.3390/electronics11050780

Kremer, J.-F., & Müller, B. (2014). *Cyberspace and international relations: Theory, prospects, and challenges.* Springer, Berlin. https://doi.org/10.1007/978-3-642-37481-4

Makuya, N. K., Wadesango, N., & Sitsha, L. (2024). An evaluation of the effects of hyperinflation on capital budgeting: A case study of National Foods Holdings Ltd (NFHL). *Journal of Economic and Social Development (JESD) — Resilient Society, 11*(1), 156–170. https://www.jesd-online.com/articles/an-evaluation-of-the-effects-of-hyperinflation-on-capital-budgeting-a-case-study-of-national-foods-holdings-ltd-nfhl.pdf

McGuire, M., & Dowling, S. (2013). Improving the cyber crime evidence base. In *Cyber crime: A review of the evidence* (Home Office Research Report 75). Home Office. https://assets.publishing.service.gov.uk/media/5a7caa0340f0b65b3de0a624/horr75-chap4.pdf

Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime — The emerging threat to the financial service sector in Zimbabwe. *Mediterranean Journal of Social Science, 7*(3 S1), Article 135. https://doi.org/10.5901/mjss.2016.v7n3s1p135

National Risk Assessment. (2020). *National Risk Assessment: Money laundering 2020* (Report). https://www.gov.je/Industry/Finance/FinancialCrime/NationalRiskAssesmnents/pages/nationalriskassessmentmoneylaundering.aspx

Ohrimenco, S., & Valeriu, C. (2023). Cyber conflict: Indicators and assessments. In E. Ozen, S. Grima, A. Hazar, L. Mistrean, & E. Sackes (eds.), *Proceedings of International Applied Social Sciences Congress (C-IASOS 2023)* (pp. 528–537). https://www.researchgate.net/publication/376990905_Cyber_Conflict_Indicators_and_Assessments

Ojeniyi, J. A., Edward, E. O., & Abdulhamid, S. M. (2019). Security risk analysis in online banking transactions: Using diamond banking as a case study. *International Journal of Education and Management Engineering, 9*(2), 1–14. https://doi.org/10.5815/ijeme.2019.02.01

Okpa, J. T., Ugwuoke, C. U., Ajah, B. O., Eshiotse, E., Igbe, J. E., Ajor, O. J., Nnana Okoi, O., Eteng, M. J., & Nnamani, R. G. (2022). Cyberspace, black-hat hacking and economic sustainability of corporate organization in Cross-River state, Nigeria. *SAGE Open.* https://doi.org/10.1177/21582440221122739

Pal, A., De, R., Herath, T., & Rao, H. R. (2019). A review of contextual factors affecting mobile payment adoption and use. *Journal of Banking and Financial Technology, 3*, 43–57. https://doi.org/10.1007/s42786-018-00005-3

Palan, C. (2019, September 16). *Smishing explained: What it is and how to prevent it.* Webroot. https://www.webroot.com/blog/2019/09/16/smishing-explained-what-it-is-and-how-you-can-prevent-it/

Reserve Bank of Zimbabwe (RBZ). (2021). *Annual report.* https://www.rbz.co.zw/documents/ar/ANNUAL-REPORT-2021.pdf

Saravade, N., & Bhalla, K. (2018). *Emerging trends and challenges in cyber security.* Reserve Bank Information Technology Private Limited.

Seissa, I. G., Ibrahim, J., & Yahaya, N.-Z. (2017). Cyberterrorism definition patterns and mitigation strategies: A literature review. *International Journal of Science and Research (IJSR), 6*(1), 180–186. https://doi.org/10.21275/ART20163936

Shati, M., Wadesango, N., & Lovemore, S. (2023). Impact of articled clerk turnover on audit quality: A study of BDO Zimbabwe Chartered Accountants. *Journal of Accounting, Finance and Auditing Studies, 9*(4), 388–397. https://doi.org/10.56578/jafas090401

Stiawan, D., Idris, M. Y., Abdullah, A. H., Aljaber, F., & Budiarto, R. (2017). Cyber-attack penetration test and vulnerability analysis. *International Journal of Online and Biomedical Engineering, 13*(01), 125–132. https://doi.org/10.3991/ijoe.v13i01.6407

Sussmann, M. A. (1999). The critical challenge from international high-tech and computer-related crime at the millennium. *Duke Journal of Comparative and International Law, 9,* 451–489. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1235&context=djcil

Tarala, J. (2023, October 25). *Cybersecurity regulations and risk assessment requirements.* SANS. https://www.sans.org/blog/cybersecurity-regulations-risk-assessment-requirements/

Wadesango, N., & Magaya, B. (2020). The impact of digital banking services on performance of commercial banks. *Journal of Management Information and Decision Sciences, 23*(S1), 343–353. https://www.abacademies.org/articles/THE-IMPACT-OF-DIGITAL-BANKING-SERVICES-ON-PERFORMANCE-OF-COMMERCIAL-BANKS-1532-5806-23-S1-204.pdf

Wadesango, N., & Muwishi, G. (2024). Enhancing operational efficiency and financial performance through internal audit: A case study of BLESSING Finance. *Journal of Accounting, Finance and Auditing Studies, 10*(3), 157–167. https://doi.org/10.56578/jafas100304

Wadesango, N., Karaga, C. K., & Sitsha, L. (2024). Effects of enterprise resource planning (ERP) on the financial performance of funeral companies. *Journal of Accounting and Management, 14*(*1*), 21–38. https://dj.univ-danubius.ro/index.php/JAM/article/view/2765

Wadesango, N., Tatenda, N., & Sitsha, L. (2024). The role of information technology in enhancing property tax administration in decentralized local government: A case study of Zimbabwe. *Journal of Accounting, Finance and Auditing Studies, 10*(2), 65–73. https://doi.org/10.56578/jafas100202