International Research Journal of
BUSINESS STUDIES

ISSN: 2089-6271 | e-ISSN: 2338-4565 | https://doi.org/10.21632/irjbs

Vol. 17 | No. 3

The Adequacy of Cybersecurity in Financial Institutions in Zimbabwe

Margaret Mashizha & Pestalos Kanengoni

University of Zimbabwe, Department of Finance and Accounting, P.O. Box MP167, Harare, Zimbabwe

ARTICLE INFO

Keywords:
cybersecurity,
cybercrime,
banking,
Zimbabwe.

Kata Kunci:
keamanan siber,
kejahatan siber,
perbankan, Z
imbabwe.

Corresponding author:
Margaret Mashiza
margretmashizha@gmail.com

ABSTRACT

A well-protected cyber environment is virtually non-existent in the technical landscape of the 21st century, exposing financial institutions to risk. To preserve the well-being and trust of the public within financial systems, the financial sector needs a stable and robust cybersecurity system. This study sought to determine the causes and sources of cybercrime, the degree to which banks are aware of cybercrime, and to assess their understanding of cybersecurity and possible solutions to cyber threats. A sample of five commercial banks in Zimbabwe was surveyed and data was analyzed using descriptive statistics. Findings revealed low awareness of cybersecurity, the absence of anti-virus protection, and a cybersecurity framework. Further, the study established that financial institutions are not providing adequate financial support and training relating to cybersecurity. The study recommends investment in cybersecurity, training, and awareness campaigns to cultivate a culture of cyber alertness.

SARI PATI

Lingkungan siber yang terlindungi dengan baik hampir tidak ada dalam lanskap teknis abad ke-21, sehingga mengekspos lembaga keuangan pada risiko. Untuk menjaga kesejahteraan dan kepercayaan publik dalam sistem keuangan, sektor keuangan membutuhkan sistem keamanan siber yang stabil dan tangguh. Penelitian ini bertujuan untuk menentukan penyebab dan sumber kejahatan siber, tingkat kesadaran bank terhadap kejahatan siber, serta menilai pemahaman mereka tentang keamanan siber dan solusi yang mungkin untuk ancaman siber. Sampel yang terdiri dari lima bank komersial di Zimbabwe disurvei, dan data dianalisis menggunakan statistik deskriptif. Temuan menunjukkan rendahnya kesadaran tentang keamanan siber, tidak adanya perlindungan antivirus, dan kerangka kerja keamanan siber. Selain itu, penelitian ini menemukan bahwa lembaga keuangan di Zimbabwe tidak memberikan dukungan finansial dan pelatihan yang memadai terkait keamanan siber. Penelitian ini merekomendasikan investasi dalam keamanan siber, pelatihan, dan kampanye kesadaran untuk membangun budaya kewaspadaan siber.

INTRODUCTION

The African continent has witnessed exponential rise in cybercrimes and victimisation engendered by the increasing use of the internet (Ndubueze, 2022, Maphosa 2023). Nearly four billion people across the globe are online, meaning that half of the population is currently using the internet, and half of it began using it in 2017 ('Internet World Stats,' 2018). Ndubueze (2022) notes a significant positive association between the growth of internet users and the rate of cybercrime in Africa. Although the internet is beneficial in that it is easy to use, time-saving, and convenient, it has often made users more vulnerable to cybercrimes. As workers took their computers home during the COVID-19 pandemic, for example, industry experts report that cyberattacks quadrupled (Hajase et al 2021; Maphosa 2023; Ramadani et al 2018).

The growing number of internet users, coupled with emerging technologies, have increasingly exposed the information of organisations to a variety of risks (Mutunhu et al, 2022; Mutanda and Maireva 2022; Akinbowale et al 2022). Indeed, literature indicates that the rate of cybercrime is increasing globally, with dire consequences on customer satisfaction, the reputation, and economic growth of financial institutions (Maphosa 2023; Akinbowale 2022; Mutunhu et al 2022; Mutanda & Maireva 2022). Maphosa (2023) as well as Weforum (2022) note that Africa loses $4 billion annually to cybercrime, whilst Maphosa (2023) records that 90 percent of African businesses have no cybersecurity protocols to protect their businesses.

Zimbabwe has not been spared from the negative consequences of the introduction of the internet and the subsequent rise in cybercrime. The current Zimbabwe liquidity crisis and drive towards digital financial inclusion have also increased exposure to cybercrime. Many people are using digital banking platforms and payment systems, making the sector more vulnerable to cyber threats (Mugari 2016). By way of example, Zimbabwe's 2020 National Risk Assessment reports point out that the risk of cyber fraud contributes about $900 million annually in illicit proceeds of crime (Mutanda and Maireva 2023). In 2018, over 4000 cases of cybercrime were handled by the Zimbabwean police and the country lost US 40 million to it (Bulawayo 24 2021; Maphosa 2023).

According to the National Cybersecurity Index, Zimbabwe is ranked 129th due to its lack of policies that support cybersecurity (Maphosa 2023), and the absence of a national cybersecurity implementation plan and strategy (NCSI 2021). Additionally, Zimbabwe and Lybia had 90 percent of counterfeit and pirated software (Kshetri 2019; Maphosa 2023). Authorities and stakeholders are therefore becoming increasingly concerned about the sophistication and frequency of cyber fraud (RBZ 2021).

As opined by Kshetri (2015), cybercrime is on the increase in Africa because of the exponential increase in the use of the internet coupled with a lack of knowledge on how one can be protected from cyber threats. This is a serious problem in many developing countries, as people lack proficiency in the English language, which is the medium of communication in which instructions on how to prevent cybercrime is often received. Cybercrime has, therefore, become a global concern as frauds have been observed around the world, (Mutanda et al, 2022; Mutunhu et al 2022; Baur-Yazbeck 2020)

The alarming fact is that a substantial portion of the security mechanisms employed by most financial institutions in Zimbabwe are a step behind the methods currently used by cybercriminals (Raghavan, 2014). Even though an impressive number of network safety frameworks have been developed of late, the serious issue remains, for Zimbabwean institutions, in terms of the cost of updating such systems. It is therefore of great importance to determine the level of cyber exposure alertness and preparedness of institutions in the Zimbabwean financial sector (Magweregwede, 2014).

Problem Statement

Cybercrime has been on the rise, following the introduction of fintechs within the financial sector as the country moves towards financial inclusivity. Technological advancements have enabled banks to reach an increasing clientele base, but reports of cyberattacks have been on the increase, resulting in a loss of confidence in the banking sector. Customers have been hesitant to adopt fintech because of increasing incidents of hacking and various other cybercrimes, highlighting the need to tighten security measures within the banking sector in order to maintain customer confidence.

In the 2015 National Risk Assessment (NRA) Report of Zimbabwe, cybercrime was identified as one of the crimes leading to the estimated illicit proceeds of US$ 1.8 billion generated annually by criminal activity in Zimbabwe (NRA, Reserve Bank of Zimbabwe, 2015) and the number of reported cases have continued to rise as most financial institutions are still at high risk of cybercrime. This highlights the need for the financial service sector to understand the benefit of incorporating cybersecurity in their operations. There is a need to develop more online security to moderate risks for both the consumer and the bank and enable it to respond effectively to cybercrime incidents. Failure to take the security measures necessary will discourage customers from adopting digital financial services (Baur-Yazbeck, 2018).

This study calls on financial institutions to re-evaluate their current operating practices to regain the trust of current and prospective customers. It adds to the existing body of literature by assessing the extent to which banks are alert to cybercrimes and determining the level of preparedness of financial institutions to deal with cyberattacks. Additionally, Mutunhu et al (2022) note that the insufficiency of research focused on equipping users with knowledge about cybersecurity awareness and education. Zimbabwe has no awareness strategies developed and implemented. The study, therefore, contributes to addressing the dearth of literature from developing countries on cybercrime, as identified by Maphosa (2023).

Literature review

The literature documents several forms of cybercrime, namely: phishing (Shaikh et al, 2016; Chakkaravarthy et al, 2018), identity theft (Maphosa 2023, Srinivas et al, 2016) hacking (Mutunhu et al, 2022; Nurse, 2018), denial of service (BBC, 2016) and malware (RBZ 2015; Sunny 2020). According to the OECD report (2007), cybercriminals or malicious exploiters can be grouped into five sub-categories. These include innovators (who seek to find system holes to overcome protection measures implemented by the banks, and amateurs (who are beginners and whose expertise is limited to computer skills that are exploited by cybercriminals) (Raghavan, 2014). There are also insiders (who are working within the bank to leak out important information, copycats (who are interested in recreating simple tasks), and last but not least - criminals themselves! These are highly organised and very knowledgeable and may use all the above-mentioned stakeholders for their benefit (Raghavan, 2014). Shah (2019) suggests that cybercrimes can be reduced by establishing cyber forensic training centres, setting up cybercrime helplines, developing a framework to enhance security in cyberspace, setting up a computer emergency response team, keeping computers updated, and protecting one's identity online.

The theoretical body of knowledge on cybersecurity seeks to answer the following questions: Is it the knowledge of the employees or top management that contributes to cybercrime significantly? Is the management involved in cybersecurity awareness campaigns in their organisations? What kinds or versions of operating systems are used primarily by Zimbabwean financial institutions? Three main theories - the structuration theory, the complexity theory, and the deterrence theory - explain the phenomenon of cybersecurity. The structuration theory centres on rules that should be observed as people use the internet, which safeguard both the company and the customers from cyberattacks (Bolivar, 2016). The complexity theory is concerned about the interconnectedness of systems, intertwined with a people element, making IT systems un-isolable from the human element. The third theory is based on coming up with measures to prevent individuals from committing or becoming victims of cybercrimes.

Mugari (2016) conducted a study on a sample of four financial institutions to evaluate the dominant forms of cybercrimes in Zimbabwe's financial sector, establish measures used to curb cybercrime, and recommend measures to combat cybercrime in financial institutions. Findings revealed that forms of cybercrime in banks include hacking, phishing, data stealing, and malware and measures used to reduce cybercrime were updated antivirus software and firewalls.

Ombati et al (2017) studied the cybersecurity techniques used to reduce cybercrime in Kenyan banks, particularly the policy of cyber risk management and monitoring and cybersecurity safeguards. In addition, the study analysed the latest intelligence on cyberattacks as well as cyber incidents and response strategies used by the Kenyan banking sector in dealing with banking fraud. Results of the study showed that all independent variables (Cyber Incident Resolution and Resilience, Cyber Risk Control and Oversight) contribute 69.5 percent to the overall dependent variable variability (Combat Banking Fraud). Each strategy was found to be of vital importance in combating banking fraud in Kenya. The study concluded that these strategies be used as complementary to each other and that further research be conducted to find more strategies to deal with cybercrime.

Catota et al. (2018) researched on the challenges that Ecuadorian financial institutions face concerning cybersecurity, focusing mainly on computer security incident response teams (CSIRT) and information sharing. The study found that cybercrime emanated from outsiders as well as insiders and that financial institutions face constraints imposed by computer users' scarcity of financial and technical resources, and weaknesses in the legal framework. In the quest to improve cybersecurity, stakeholders suggested that this presents an opportunity to establish a better incident response strategy for Ecuadorian financial services through the creation of a CSIRT and an information-sharing system. To reduce uncertainty relating to threats, employees are more likely to share technical information as opposed to quantitative information about security incidents.

Kabanda (2018) as well as Kurebwa and Tanhara (2019) found out that Zimbabwe was lagging behind in terms of embracing cybersecurity awareness despite the significant increase in the adoption and use of ICTs. It was found that there was no framework in place to provide direction, focus, guidance, and a standardised way of addressing cybersecurity issues in Zimbabwe. Kurebwa and Tanhara (2019) stated that cybercrime was a threat to peace and security in the country and with no cybersecurity framework in place, dealing with cybersecurity issues becomes problematic as there is no guidance and direction on how to prevent, respond, and reduce cybersecurity breaches and risks as well as improve personnel awareness.

A cybersecurity framework that will support a cybersecurity culture to prevent cyber-attacks in Zimbabwe is therefore required. Kurebwa and Tanhara (2019) recommended prevention and awareness measures, training and development, development of new technology and introduction of new laws, and updating of current - and introduction of new - legislation as measures to curb cybercrime. Dongol (2019) also associates poor security implementation practices with cyber threats relating to payment systems and a discrepancy between the understanding and practice of banks related to the payment system in the banking industry in New Zealand.

Rawass (2019) examined the methods that the management of a small financial institution used to shield its data systems from cyber threats. The results of the study were that leaders of financial institutions protect their computer networks from cyber-attacks by handling data management activities effectively; establishing solid cybersecurity policies; and adopting a comprehensive operational approach. The study concluded that the protection of data systems through the reduction of cyber threats will improve organisational business practices.

Tam et al (2020) examined cybercrimes in the banking sector of Vietnam, which is one of the countries in the world experiencing extremely high levels of cybercrime. Based on a sample of 305 bank clients, they established common cyberattacks to be hacking, skimming, and phishing. Furthermore, the results showed that the reasons for the high cybercrime rate are associated with commercial banks (poor management and human capacity), an inadequate supporting environment, and absence of a legal framework. The country has high cybercrime rates, and clients therein have inadequate knowledge of how to prevent cybercrime and thus believed that greater banking security was in traditional banking methods. The study concluded that several solutions should be implemented by all stakeholders, so as to improve cybersecurity in Vietnamese banks.

Wang, Nnaji, and Jung (2020), conducted an online survey of 100 experienced professionals to establish cybersecurity breaches, competence and practices in the Nigerian Internet banking industry. The findings were that viruses, electronic spam mail, and hacking were the most common cyber breaches. Where cyber practices were concerned, it was established that sufficient training and support had been provided to professionals in the country's banking sector. Additionally, cybersecurity capabilities have been reduced by a lack of advanced technologies and failure to comply with legislation intended to curb cybercrime.

Mwila (2020) discussed the cyber threat preparedness policy for the public and private sectors in Zambia. The research sought to assess the current cyberattack preparedness measures, establish a system that can be used to curb cyberattacks and define the existence and types of cyberattacks. The findings of the study established a shortage of cybersecurity experts and that less than 50 percent of the workers have the requisite experience in cybersecurity whilst 48.2 percent do. The study found that cybersecurity is handled by IT workers instead of cybersecurity experts and that 70% of structured policies, manuals, rules, and controls aimed at improving cyber-attack security are likely to generate further results if only the problems covered by the policies are completely addressed. Finally, the study found that 63% of companies have implemented frameworks or standards for cybersecurity, but these frameworks are not effective.

Akinbowale et al (2022) conducted a study in South Africa to assess the impact of cyber fraud within the banking sector and suggest mitigating measures. Findings revealed that the impact of cyber threats was significant, adversely affecting confidence in the banking sector highlighting the need to establish stringent measures to curb cyber threats. Another study by Mutunhu et al (2022) sought to establish whether students and staff were aware of cybersecurity measures to be included in a proposed cybersecurity framework. Research findings were that staff and students did not have adequate knowledge of cybersecurity issues and how they impact their daily lives, neither were they aware of any preventative measures.

Mutanda and Maireva (2022) studied the efficiency of the measures to prevent cyber fraud in Zimbabwean commercial banks and the challenges associated with cyber fraud prevention. Findings were that measures implemented were not as effective as intended, leaving loopholes for further attacks, to the detriment of clients and the financial system as a whole. Challenges faced were that cybercriminals were always steps ahead in terms of tactics, and clients were ignorant of the messages sent to them to help prevent cyberattacks, as some still shared passwords and credit cards. Additionally, there was an absence of sophisticated systems to prevent cybercrimes and employees were seen as lacking the necessary knowledge about preventative measures.

Ekong (2023) studied the effect of cybercrime in commercial banks in Nigeria. The study sought to establish the types and causes of electronic fraud in the banking sector, as well as challenges and possible solutions for curbing cyber fraud in banks. Findings revealed that major types of cyber fraud in banking systems were accounting fraud, identity theft, money laundering, hacking/cracking, phishing, pharming, and computer viruses. Insufficient supervision by managers, high-set targets, inadequate data encryption, and third-party service providers were noted to be serious exposures to cybercrime. The research noted the absence of a functional database, the lack of standards, inadequate infrastructure, and a lack of awareness by customers about some of the cybersecurity challenges. The impact of cybercrime was felt in the form of financial loss, suppressed productivity, and exposure of the bank's confidential information. Measures to mitigate cybercrime were found to be the use of antivirus software, multifactor authentication, biometrics, and automatic logouts, among many others. The study emphasised the need to enhance cybersecurity within the banking sector.

The current study focuses on the need to determine the level of alertness to cybercrime exposure by banks in Zimbabwe and assess bank clients' general level of understanding of cybersecurity and knowledge of the available solutions to cyber threats. The research contributes to the body of existing literature on cybersecurity in Zimbabwe and the African context as a whole.

METHODOLOGY

The research adopted a descriptive approach and utilised questionnaires to collect data. The study population was drawn from 164 banks in the financial sector in Zimbabwe, from which a sample of five commercial banks were selected according to the range of banking and financial services that the institution offers to its corporate and individual customers. The main respondents were Information and Communication Technology (ICT) staff in the selected banks and these included Chief Digital Banking Officers, Chief Information Officers, Security Officers, IT support employees, Network Engineers as well as the general IT staff. The inclusion of some of the general IT employees in this study serves to measure the extent to which top management is engaging in issues about cybersecurity based on the current knowledge possessed by their lower-level subordinates.

A convenience sampling strategy was used hence the sampling units were approached based on their availability. This strategy was chosen because it enabled easy access to employees in the financial sector at a very minimum cost and effort, resulting in a high response rate. The utilisation of known contacts made it possible to achieve a high response rate since there is a significant level of trust between the researcher and the respondents. A generated web link for the questionnaire was created and shared through email addresses and in some cases through social media platforms such as WhatsApp. That link is clicked and redirects the respondent to the survey questionnaire. This method ensured saving on time and travelling costs and flexibility, enabling the respondents to multitask and answer the questionnaire. However, it had several drawbacks, which included late responses from the participants owing to a lack of data to browse the internet. In this research, content validity was ensured by restricting the questionnaire response to ICT staff with adequate knowledge of cybersecurity. This enhanced the chances of collecting honest and valid responses. A pilot test of the questionnaire was also conducted using a few experts, whose opinions were also incorporated. Data was presented using tables and figures and analysed using descriptive statistics generated using Microsoft Excel.

RESULTS AND DISCUSSION

A response rate of 70 percent was achieved, and this was deemed adequate for data analysis. One of the research objectives was to determine how cybersecurity alert financial institutions are. The study sought to examine the degree to which banks are alert to cybercrime exposures, assessing the general understanding of cybersecurity by respondents, time spent on cybersecurity-related issues, and knowledge of available solutions and cybersecurity concerns amongst the employees. Firstly, a general question was asked to determine whether employees were at all concerned about cybersecurity. Results are presented in Figure 1.

Findings indicated that 80 percent of IT employees are not concerned with cybersecurity, whilst only 20 percent are. The 20 percent concerned with it were mainly those whose daily routine required them to monitor the security systems of the bank. These results are indicative of the weak loopholes that may be found in cybersecurity systems, accounting for the high rise of cyber-attacks in many institutions.

To determine the level of alertness to cybercrime, data was collected to determine whether respondents received any notifications when there was an attack on the systems, and results are presented in Figure 2.

About 50 percent of the respondents indicated that they rarely receive notifications when there

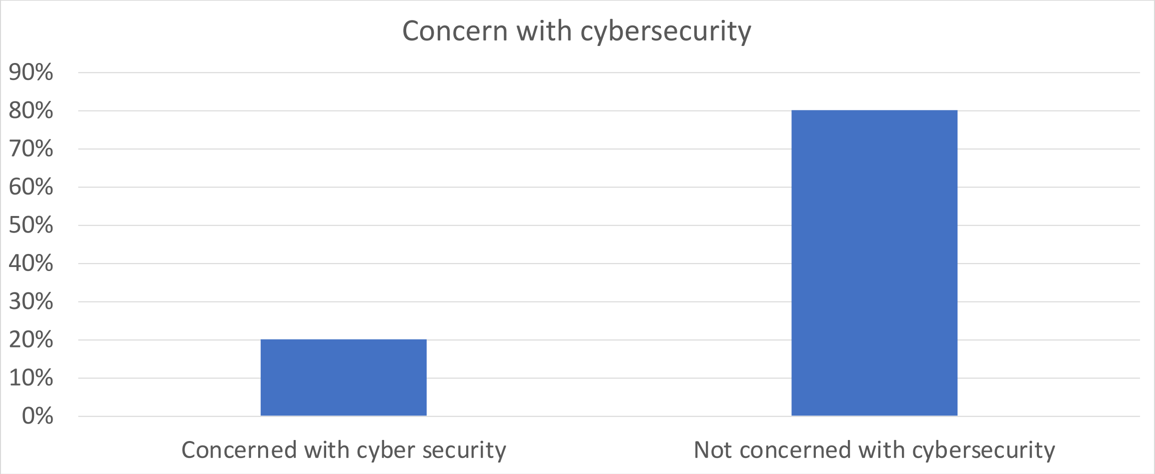

Figure 1. Concern with cybersecurity

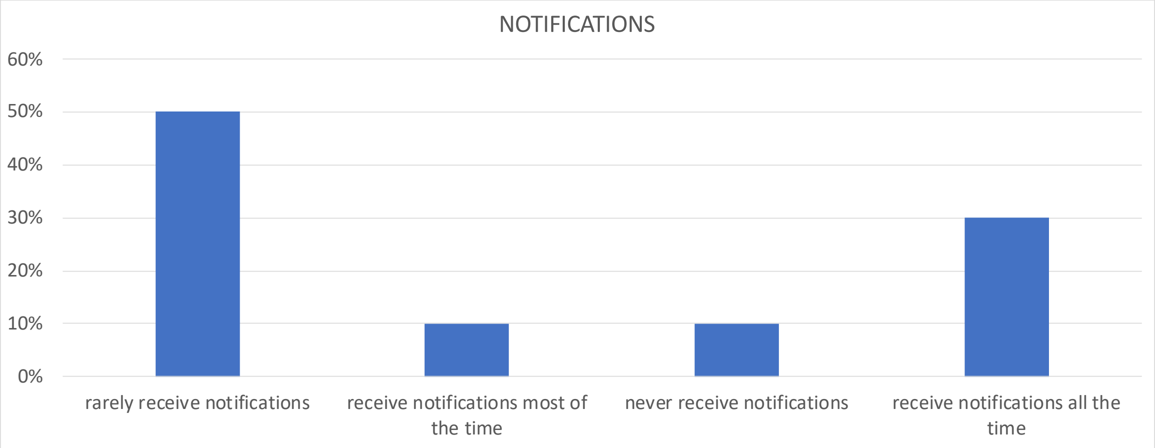

Figure 2. Notifications of cyberattacks

was an attack on their organisation's information systems. 10 percent of the respondents revealed that they receive notifications most of the time, another 10 percent of the respondents mentioned that they never receive any notification, while 30 percent always receive notifications whenever an attack occurred. This 30 percent comprises the top management, which makes company decisions. This finding can be backed by the idea that cyberattack notification is usually the responsibility of the IT managers, who include Chief Digital Officers and heads of Information Security and that the larger population of the respondents are low-level subordinates. These results show that management is not doing much to involve lower-level employees in cybersecurity matters.

Data was also collected to determine the participants' knowledge of available solutions to cyberattacks. Results are presented in Figure 3.

The findings revealed that 36.36 percent of the respondents claimed to know the solutions that are available for a few attacks, whilst 9.10 percent of them revealed that they knew solutions to some of the attacks, followed by 36.36 percent, who claimed know the solutions to most attacks. Only 9.10 percent of the respondents claimed they knew solutions to all possible cyberattacks, and another 9.10 percent of the respondents, surprisingly, did not know any solution available for any attack. The research found that those who did not know of any solution were IT support employees, who did not have anything to do with cybersecurity in their institutions. Generally, the level of knowledge of the solutions to cyberattacks is not at all within the acceptable range since it was less than 50 percent for all the responses received in the Zimbabwean financial sector.

Data was also collected to determine whether financial institutions in Zimbabwe are undertaking cybersecurity awareness campaigns so as to reduce the risk of cyber threats. Findings are presented in Figure 4.

From the responses given, 70 percent of financial institutions undertake cyber-security campaigns annually at different intervals. Of the 70 percent, 40 percent carry out campaigns more than 5 times per year, 30 percent do so 1-3 times per year and none of the institutions carry out campaigns 3-5 times per year. Nevertheless, the remaining 30 percent of the participants showed that there were no cybersecurity campaigns undertaken at their organisations. One could therefore conclude that financial institutions are providing cybersecurity awareness to their employees.

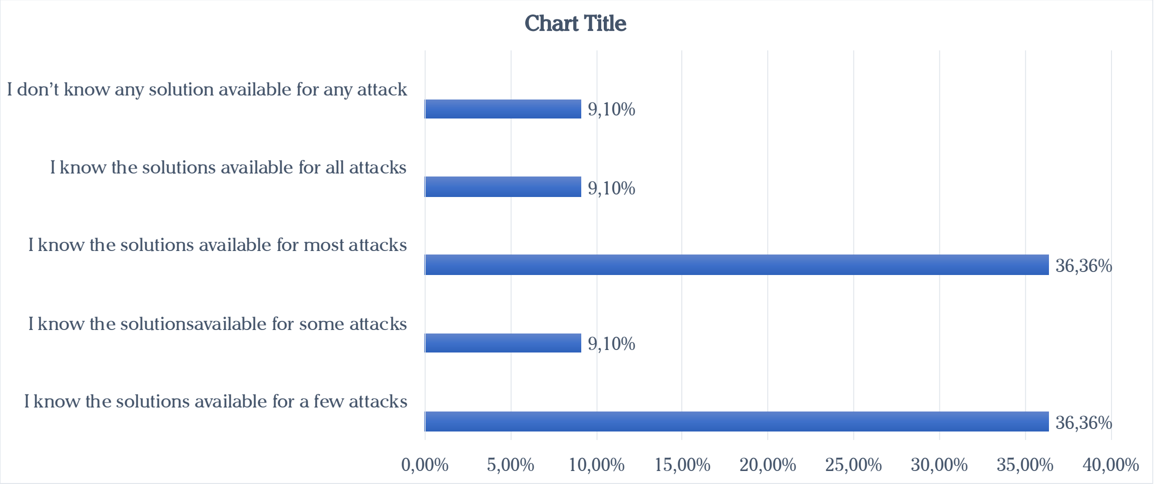

Figure 3. Knowledge of solutions to cyberattacks

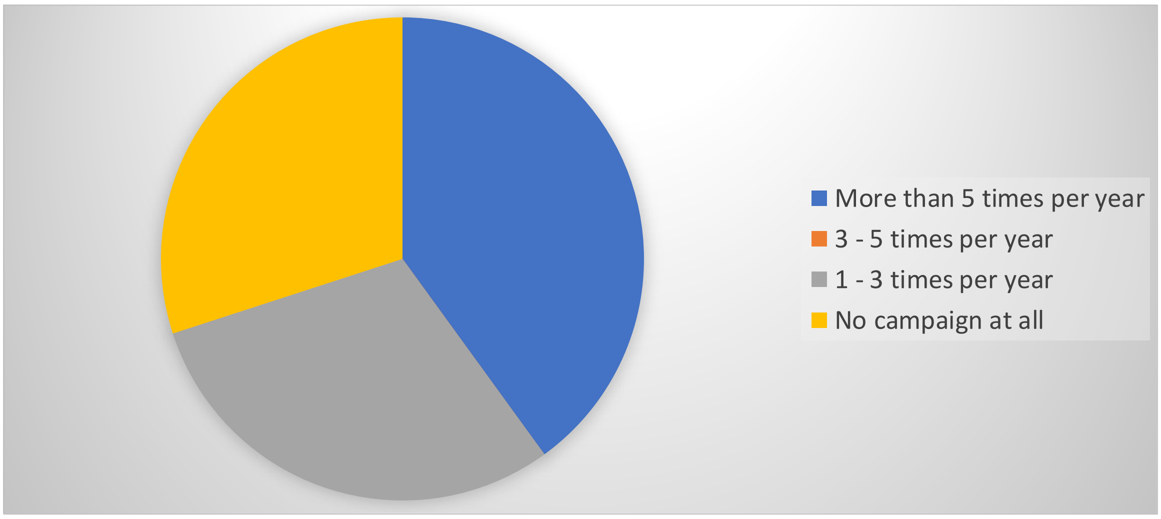

Figure 4. Cybersecurity awareness campaigns

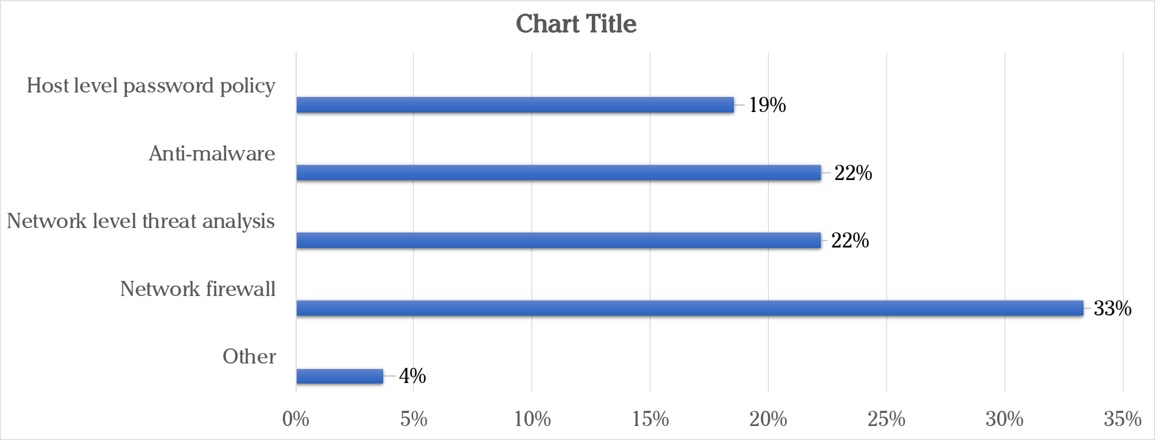

Figure 5. Cybersecurity tools and policies

Data was collected to determine the cybersecurity tools or policies that are in place. Results are presented in Figure 5.

Results showed that 33 percent had a network firewall, 22 percent had network-level threat analysis, 22 percent had antimalware, and 19 percent had a host-level password policy. From the figure above, one can conclude that financial institutions are generally not fully implementing cybersecurity tools. This might be the case, since some institutions that deal with a large amount of client data are required to invest in these tools and policies such as network firewalls and these may be the ones that constitute about 33% of the total percentage. However, since cyber criminals are usually a step ahead of some of the prevention tools and policies, there is a need for institutions to implement all policies and tools intended to support cybersecurity, so that client data is secured.

Data was also gathered to determine the cybersecurity testing procedures over the past 2 years. Findings are presented in Figure 6.

From the figure 6, it can be seen that many institutions are mostly prioritising network scanning and vulnerability assessment and penetration of their systems represented by 42 percent and 32 percent respectively. Less focus is being placed on

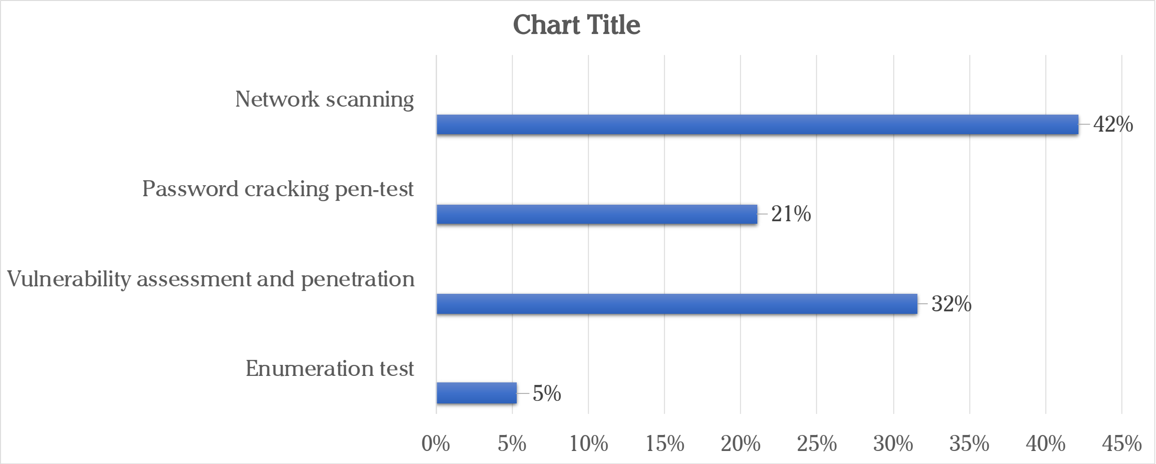

Figure 6. Cybersecurity testing procedures

the password cracking pen test and enumeration test, which have 21 percent and 5 percent respectively. Participants have demonstrated that lack of awareness of the significance of the enumeration test, even though, according to Chakravartula (2018), the enumeration test is very critical, since it is a systematic collection of details such as hostnames, IP tables, Audit configurations, and service settings. These details will be used to completely examine the systems, and detect the weak links of the systems, which can, in turn, help come up with strategies to strengthen the system.

Data was collected to determine the exposure levels of financial institutions in Zimbabwe, by analysing the perceived causes of cybercrimes. This was assessed based on several factors; whose absence contribute significantly to high levels of cybercrime exposure. Below is Table 1, which summarises responses from participants on various questions relating to the causes of cybercrime exposures.

The availability of firewall protection in financial institutions reduces cybercrime exposures since the attackers cannot easily access the company systems. The responses from the participants in Table 1 showed that 30 percent of the financial institutions in Zimbabwe have firewall protection in their organisations, whilst the remaining 70 percent do not. A firewall is a very critical and indispensable security device, as it protects a company's network by filtering traffic and blocking outsiders from gaining unauthorised access to the private data on a user device (Johansen, 2020). The participants revealed that most IT managers are not doing enough to safeguard company information, as reflected in the lack of firewall protection. Only 30 percent of the financial institutions have frameworks in place, whilst 70 percent do not. This shows that 70 of these institutions' information is vulnerable to cyberattacks, for lack of procedures on how to safeguard company information.

Table 1. Causes of Cybercrime Exposures

Question	Yes	No
Lack of firewall protection	30%	70%
Lack of framework specifically for cybersecurity implemented in your organisation	70%	30%
Lack of a breach incident response plan	30%	70%
Lack of intrusion detection software	80%	20%
Lack of anti-virus protection on computer systems	60%	40%

The incident response plan is a documented, written plan with 6 unique phases that assist IT employees to deal with a cybersecurity incident such as a data breach or cyberattack. Properly creating and managing an incident response plan involves regular updates and training (Ruefle, 2014). The availability of a breach incident response plan greatly reduces cybercrime exposures, as the institution can implement strategies to combat future cyberattacks. According to the survey, as shown in Table 1, 70 percent of the participants revealed that most institutions do not have a breach incident response plan, which is a major drawback, since such institutions will not be able to recover their data if it is lost or to use diverse strategies to combat such occurrences in the future. The survey proves that many IT managers of Zimbabwean financial institutions do not have breach response plans. Based on the table above, 80 percent of the financial institutions from the sample population have no intrusion detection system and only 20 percent of the institutions do. Hackers use a variety of attacks to get valuable data. Many intrusion detection techniques, methods, and algorithms help to detect those several attacks. Zimbabwean financial institutions are therefore prone to high cyber-attacks since they lack updated detection software to at least match current hacking technologies.

Table 1 shows that 60 percent of financial institutions do not have anti-virus protection for their systems, as indicated by the respondents. The protection can detect undesirable malware that might corrupt client or company data and these include spam emails. Anti-virus protection such as McAfee can prevent the installation of software that is not verified as free from viruses, thereby protecting the user's data from threats associated with viruses. Company IT managers are not prioritising the procurement of verified anti-virus software, which significantly benefits the company by countering such viruses. About 40 percent of the participants revealed that anti-virus protection is not among the causes of cybercrime exposure, pointing to the presence of anti-virus protection in their respective institutions and revealing that other factors are causing high levels of exposure.

Data was also gathered to show the sources of cyber threat(s) and Figure 7 indicates the potential threats that institutions in the Zimbabwean financial sector consider to be of great concern.

According to the figure above, 30.77 percent of the respondents revealed that internal attacks from company employees, including former employees, are a major threat(s). 19.23 percent of the participants highlighted that they also fear

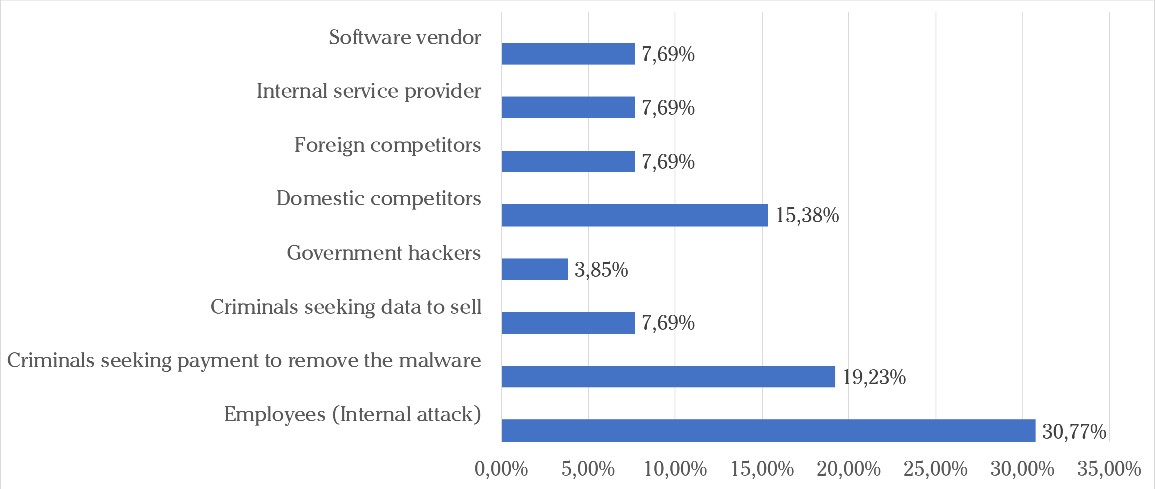

Figure 7. Potential cyber threats

criminals seeking payment to remove the malware, while domestic competitors were cited by 15.38 percent of respondents. Criminals seeking data to sell, government hackers, foreign competitors, internal service providers, and software vendors were the least suspected criminals. The responses from the study were in line with the survey by KPMG (2020), which found that threats that organisations are most vulnerable to are internal attacks by the organisation's workers.

Cybersecurity budgets

The study collected data on factors that influenced budget allocations for cybersecurity and the results are presented in Figure 8.

Based on the study, the researchers found out that most organisations' cybersecurity budget is influenced by audit suggestions (80 percent), regulatory requirements (50 percent), software vendor suggestions (50 percent), and, to a lesser extent, client requests (20 percent). From the study, one can conclude that cybersecurity budgets in most financial institutions in Zimbabwe are driven by audit suggestions, and client requests do, to a lesser extent, influence the budget decisions, as institutions seek to retain their client base.

Cybersecurity training

Data was collected to show whether financial institutions were training their staff. Findings are presented in Figure 9.

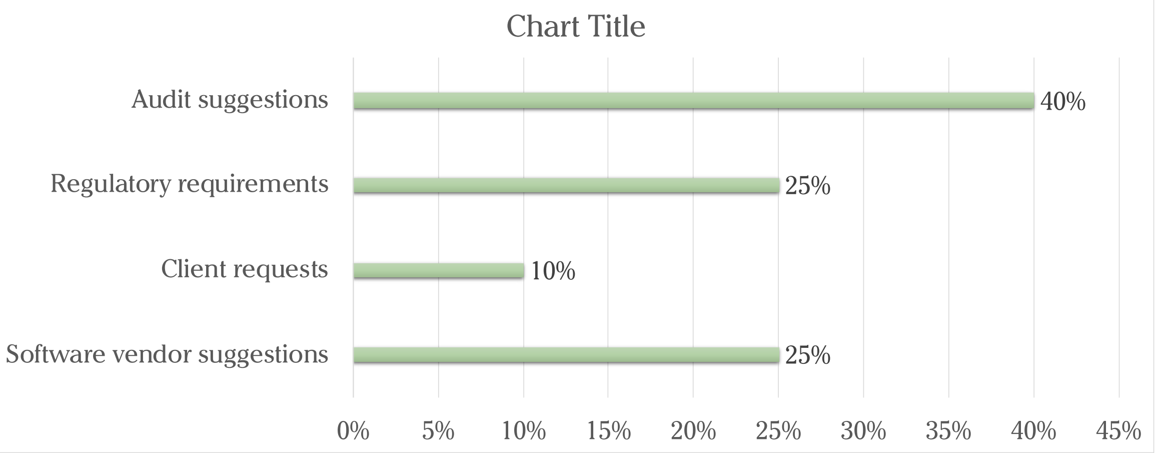

Figure 8. Cybersecurity budget influence

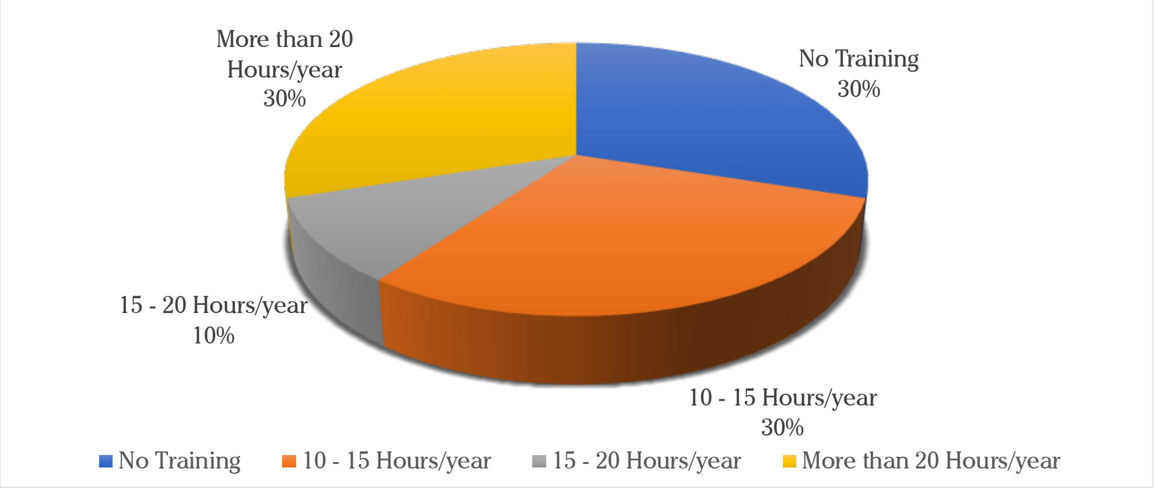

Figure 9. IT Training

Figure 9 reveals that some financial institutions in Zimbabwe are not making an effort to provide cybersecurity training for their IT staff. These institutions constitute 30 percent, meaning that their IT departments are lagging in terms of technological advancement. Based on the study 30 percent of organisation provide 10-15 hours per year of training, while 10 percent provide 15-20 hours of training. Some financial institutions (30%) are even providing cybersecurity training to their IT staff for more than 20 hours per year. This shows that management is ignorant of the consequences of cyberattacks, and therefore tends to neglect cybersecurity issues. Results showed that financial institutions in Zimbabwe do not fully invest in cybersecurity infrastructure, exposing themselves to cyberattacks. They usually focus on growing their client base so that they can be on par with already large and established institutions, rather than paying adequate attention on ways of reducing cybercrimes.

The results obtained from the respondents echo those of a study carried out by Mwila (2020) investigating the cyberattack preparedness strategy. It was discovered that the majority of organisations have understaffed cybersecurity departments where less than 50 percent of the staff, have cybersecurity training, and only 48.2 percent have the right skills. The cybersecurity compliance assessment revealed that only 10 percent of financial institutions in Zimbabwe are compliant, showing that some are still defaulting to manually monitoring cybersecurity compliance by their staff. These institutions account for about 20 percent of the sample population. Although monitoring compliance manually can be less costly, it is hard to monitor websites accessed by employees, password policy monitoring, and even check the integrity of emails sent, which might, in some cases, be spam

MANAGERIAL IMPLICATIONS

Findings from the study have several implications for management in terms of improving security systems and regaining client confidence. Management should demonstrate greater concern for cybersecurity and ensure that knowledge about it is imparted to their employees. To this end, management should increase budget allocations for cybersecurity, increase awareness campaigns, and offer training to their employees. This will ensure that employees become more knowledgeable about cybersecurity, enhance the level of alertness to it, and ensure a quick response in the event of an attack.

CONCLUSION

The study concluded that employees lack concern about and knowledge on how to deal with cybersecurity attacks. Although cybersecurity tools and policies are available, cybersecurity campaigns and training are inadequate to impart the necessary know-how to deal with cybersecurity. Cybercrimes are attributable mainly to company employees, those currently working in it or those who may have left the organisation. Additionally, cybercrimes result from a lack of anti-virus protection and the absence of a cybersecurity framework. Financial institutions do not have a breach incident response plan, which indicates the necessary steps to be followed when a cyber-attack occurs. Such a plan is critical, as it assists in the recovery of lost data and indicates how to avoid the reoccurrence of such attacks. The banks studied do not have intrusion software, which puts them at extremely high levels of cyber exposure since they cannot detect any malware attack on their systems.

Most of the institutions are not allocating enough of their cybersecurity budget to support the protection of confidential information and the training of staff is inadequate. The study recommended that the Zimbabwean government should impose minimum regulations to be implemented by every financial institution in the country to ensure compliance from each of them. Skilled cybersecurity personnel should be hired and also involved in the higher level decision making processes of the company. The time taken by administrators to close the accounts and rights of an employee who might have left the firm should be reduced to a very short time so that former employees cannot tamper with company accounts. Since the study concluded that the zeal of management in carrying out activities such as awareness campaigns to improve cybersecurity is low, this issue needs to be addressed as well. ■

REFERENCES

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2023). The assessment of the impact of cyber fraud in the South African banking industry. *Journal of Financial Crime.*

Mohsin, A. (2016). A manual for selecting sampling techniques in research. *Munich Personal RePEC Archive*, *2016*, 1-56.

BBC News (2016). http//www.bbc.co.uk/news/technology-36072240.

Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). Cyber Security in the Financial Sector Development. *CGAP Background Documents*, 5(2).

Bulawayo24: Italy offers cyber security training in Zimbabwe. 2021, April 18.

Camilo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions*, *10*(2), 196-200.

Catota, F., Morgan, M. & Sicker, D. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity*, *4*(1), tyy002.

Chakkaravarthy, S, Sangeetha, M., & Vaidehi, V. (2018). Futuristic cyber-attacks, *International Journal of Knowledge-based and Intelligent Engineering Systems. 22*(3), 195-204.

Chingoriwo, T. (2022). Cybersecurity Challenges and Needs in The Context of Digital Development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies*, *3*(2), 77-104.

Dongol, R. (2019). Robust Security Framework for Mitigating Cyber Threats in Banking Payment System, *Research Journal of Science, Technology and Management,* 1.

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe, *Risk Governance and Control: Financial Markets and Institutions*, 4(2), 16-26.

Dzomira, S. (2015). Cyber-banking fraud risk mitigation conceptual model, *Banks and Bank Systems*, 10 (2), 7-14.

Dzomira, S. (2017). Internet banking fraud alertness in the banking sector: South Africa, Banks and Bank Systems, 12(1),143-151.

Hejase, H. Fayyad-Kazan H, & Hejase A (2021). Cyber Security amid COVID-19. *Computer and Information Science.* 14(2), 10-25.

Jongbo, O. C. (2014). The role of research design in a purpose-driven inquiry. *Review of Publication Administration and Management,* 3(6), 87-94.

Kabanda, G., & Chingoriwo, T. (2021). A Cybersecurity Culture Framework For Grassroots Levels In Zimbabwe. Https://Www.Researchgate.Net/Profile/Gabriel-Kabanda/publication/359651454_A_Cybersecurity_Culture_Framework_for_Grassroots_Levels_in_Zimbabwe/links/626ba5106a39cb1180e3c46e/A-Cybersecurity-Culture-Framework-for-Grassroots-Levels-in-Zimbabwe.pdf.

Kabanda, G. (2018). A Cybersecurity culture framework and its impact on Zimbabwean organisations. *Asian Journal of Management, Engineering & Computer Science*, *3*(4), 17-34.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Management Technology*, 22(2), 77-81. DOI: 10.1080/1097198X.2019.1603527.

Kshetri, N. (2013). Cybercrime and cybersecurity in the global South. Basingstoke, U.K: *Palgrave Macmillan*: Houndmils.

KPMG (2020). Cybercrimes: A Financial Sector Review. Government and Public Sector. Available at: *https://www.kpmg.com/in/en/industry/publications/fs_cybercrime_booklet.pdf* [Accessed 18 March 2021].

Kurebwa, J., & Tanhara, J. R. (2020). Cybercrime as a Threat to Zimbabwe's Peace and Security. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*, 1107-1122, IGI Global.

Magweregwede, J. (2014). An evaluation of the adequacy of cyber security within the Zimbabwean banking sector. *Risk governance & control: financial markets & Institutions,* 4.

Maphosa, V. (2023). An overview of cybersecurity in Zimbabwe's financial services sector. *F1000Research*, *12*, 1251.

Mwila, K. A. (2020). An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia (Doctoral dissertation, The University of Zambia). *https://dspace.unza.zm/server/api/core/bitstreams/e7fecda3-7f89-4dbb-970b-9db11121d5fb/content.*

Mugari, I. (2016). Cybercrime- The emerging threat to the financial services sector in Zimbabwe, *Mediterranean Journal of Social Sciences*, 7(3).

Mutanda, B., & Chrispen, M. (2023). Towards a Cyber Resilient Banking System: Effectiveness of Cyber Fraud Risk Management Strategies Adopted by Commercial Banks in Zimbabwe. *Studies And Scientific Research Economics Edition*, (37).

Mutunhu, B., Dube, S., Ncube, N., & Sibanda, S. (2022). Cyber Security Awareness and Education Framework for Zimbabwe Universities: A Case of National University of Science and Technology. In *Proceedings of the International Conference on Industrial Engineering and Operations Management Nsukka, Nigeria*, 5-7.

Nurse, J.R. (2019). Cybercrime and you: how criminals attack and the human factors that they seek to exploit. *In: Attrill-Smith A, Fullwood C, Keep M, et al. (eds)* The Oxford Handbook of Cyberpsychology. Oxford: Oxford University Press.

Ombati, E. (2017). Evaluation of cybersecurity strategies used in combating banking fraud in the banking industry in Kenya. *International Journal of Innovative Finance and Economics Research* 5(4):12-22. Seahi Publications.

Rawass, J. (2019). Cybersecurity strategies to protect information systems in small financial institutions. Walden University Scholar Works. Dissertations and Doctoral Studies Collection *https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=8462&context=dissertations.*

Raghavana, A.R., Parthiban, L. (2014). The effect of cybercrime on a Bank's finances, *International Journal of Current Research & Academic Review*, 2(2), pp. 173 178.

Ramadani, S., Siahaan, A.P.U., Sutrisno, R.S., Amelia, W.R., Dalimunthe, H. and Munthe, R. (2018). Impact of cybercrime on technological and financial developments, *International Journal for Innovative Research in Multidisciplinary Field*, 4(10), 341-344.

Reserve Bank of Zimbabwe. (2015). Cybercrime in Zimbabwe and Globally, Harare: Reserve Bank of Zimbabwe.

Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics*, 18, 751-762.

Tam, LE & Chau, Nguyen & Mai, Pham & Phuong, Ngo & Tran, Vu. (2020). Cybercrimes in the banking sector: Case study of Vietnam. International Journal of Social Scienceand Economics Invention. 6. 10.23958/ijssei/vol06-i05/207.

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, 23(2), 1-11.

Tiwari, M. (2017). Intrusion detection system. *International Journal of Technical Research and Applications,* 5, 38-44.

Tiwari, S., Bhalla, A. and Rawat, R. (2016). Cybercrime and security, *International of Advanced Research on Computer Science and Software Engineering*, 6 (4), 46-52.

The United Nations, Cyberspace and International Peace and Security (2017) Available at: *https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf /*[Accessed 12 January 2021].

The Herald (2017). Man hacks into OK Zim system*, and* steals $70k. [Online] Available at: http://www.herald.co.zw/man-hacks-into-ok-zim-system-steals-70k/ [Accessed 12 June 2020].

Ekong, E. U. (2023). Impact of Cyber-Security on Financial Fraud in Commercial Banks in Nigeria: A Case Study of Zenith Banks in Abuja (Doctoral dissertation, AUST).*https://repository.aust.edu.ng/xmlui/bitstream/handle/123456789/5117/Ekong%20Eyo%20Unwana.pdf?sequence=1&isAllowed=y.*

Weforum: Global Cybersecurity Outlook 2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

Wang, V. Nnaji, H and Jung, J. (2020). Internet banking in Nigeria: Cybersecurity breaches, practices and capability. *International Journal of Law, Crime and Justice*