RESEARCH ARTICLE

# REVISED An overview of cybersecurity in Zimbabwe's financial services sector [version 2; peer review: 2 approved, 2 approved with reservations]

Vusumuzi Maphosa

Department of Information and Communication Technology Services, National University Science and Technology, Bulawayo, Bulawayo, 263, Zimbabwe

**v2** **First published:** 29 Sep 2023, **12**:1251
https://doi.org/10.12688/f1000research.132823.1
**Latest published:** 14 Mar 2024, **12**:1251
https://doi.org/10.12688/f1000research.132823.2

## Abstract

### Background

As nations, businesses, and individuals rely on the Internet for everyday use, so are cybercriminals manipulating systems to access information illegally and disrupting services for financial gain. The global cost of cybercrime eclipsed one trillion US Dollars in 2020, with Africa losing US $3.5 billion.

### Methods

A quantitative research methodology was adopted to investigate factors affecting cybercrime in Zimbabwean financial institutions. The study focused on the technical aspects of cybersecurity. Data were collected from July 2022 to October 2022, targeting technology experts in the financial services sector. Participants were recruited from 13 institutions to rank cybersecurity constructs, frameworks, and challenges associated with cybersecurity. Data was collected using a questionnaire distributed to participants. Descriptive statistics were used to extract meanings from the responses that measure mean and standard deviation.

### Results

Network and data security were the most highly ranked cybersecurity constructs, while physical security was the least. The top three barriers are increasing sophistication of threats, limited skills and emerging technologies, while lack of executive support was the least.

## Open Peer Review

**Approval Status** ✓ ? ✓ ?

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| **version 2**<br>(revision)<br>14 Mar 2024 | ✓<br>view | | ✓<br>view | ?<br>view |
| **version 1**<br>29 Sep 2023 | ?<br>view | ?<br>view | | |

1. **William Vambe**, Walter Sisulu University, Mthatha, South Africa
2. **Nomusa Dlodlo**, Rhodes University, Grahamstown, South Africa
3. **Dinesh Kalla**, Colorado Technical University, Colorado Springs, USA
   **Samaah Fnu**, Northeastern Illinois University (Ringgold ID: 2458), Chicago, USA
4. **Simon Kaggwa**, Hult International Business School, Boston, USA

Any reports and responses or comments on the article can be found at the end of the article.

The top frameworks used are the Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and Related Technologies (COBIT), while a fifth is yet to adopt cybercrime frameworks.

**Conclusions**

The study proposes that financial institutions establish a cybersecurity culture to fight cybercrime, addressing cybersecurity barriers and following best practices. Financial institutions should invest in cybersecurity technologies, train security specialists, and employ a Chief Information Security Officer (CISO). The study's small sample may affect the generalisability of the results. Financial institutions should implement strategies to raise awareness and collaborate with institutions to train cybersecurity security specialists to close the skills gap.

**Keywords**
cybersecurity, cybercrime, threats, barriers, frameworks

This article is included in the Artificial Intelligence and Machine Learning gateway.

This article is included in the Cybersecurity collection.

**Corresponding author:** Vusumuzi Maphosa (vusumuzi.maphosa@nust.ac.zw)

**Author roles: Maphosa V**: Conceptualization, Data Curation, Investigation, Methodology, Writing – Original Draft Preparation, Writing – Review & Editing

**Competing interests:** No competing interests were disclosed.

**Grant information:** The author(s) declared that no grants were involved in supporting this work.

**How to cite this article:** Maphosa V. **An overview of cybersecurity in Zimbabwe's financial services sector [version 2; peer review: 2 approved, 2 approved with reservations]** F1000Research 2024, **12**:1251 https://doi.org/10.12688/f1000research.132823.2

**First published:** 29 Sep 2023, **12**:1251 https://doi.org/10.12688/f1000research.132823.1

**REVISED** **Amendments from Version 1**

I have responded to the issues raised by the reviewers e.g. providing a global view of cybersecurity and focusing on Zimbabwe. The other issues related to sampling are also addressed.

**Any further responses from the reviewers can be found at the end of the article**

## Introduction

The internet supports today's knowledge economy and affects every way of life. The internet is growing in volume and complexity, and without due care, it exposes private data and information to criminals. Businesses use information and communication technologies to drive production and automation, while consumers use technology for entertainment and services (Maphosa, 2022a). The International Telecommunication Union (ITU) reports that fixed broadband access has increased globally. In Zimbabwe broadband penetration rose to 59.9% from 0.4% in 2000, while mobile phone penetration surpassed 100% (Maphosa, 2022b). Although data costs are still high in Zimbabwe, the last decade witnessed a significant decrease from US $180.00 per giga byte in 2010 to US $15.50 in 2020 (POTRAZ, 2021). Decreasing data costs have fueled teleworking, electronic commerce (e-commerce), distance learning, remote entertainment, and telemedicine (Katz and Jung, 2021). The over-dependency on information technology (IT) systems and the rise of e-commerce make societies more vulnerable to cyber-attacks than ever. Nations, institutions, and individuals utilise cyberspace, a digital or virtual environment where they connect and access digital resources. Devices, networks, and systems that harness information and knowledge for economic development should be secured. Cyberattacks disrupt services and critical infrastructure such as electric grids, water supply and transport systems, banking, and social network systems. Cybersecurity breaches impact national security, economies, and individual livelihoods as attackers leverage the vulnerabilities on multiple devices connected to the internet.

The cost of cybercrime and cybersecurity in 2020 exceeded 1% of the world's gross domestic product eclipsing one trillion US dollars (Sviatun *et al.,* 2021). New forms of businesses purely mediated by the internet, such as cryptocurrencies, virtual reality, and cloud computing, have emerged. The adoption of new technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT), among others, offers the hacker community new methods and skills to breach and undermine the security of organisations that suffer irrecoverable losses (Radzikowski, 2015). When systems have been compromised, attackers may lock the data illegally and demand ransoms to restore compromised data. The internet provides significant advantages as customers can flip through virtual online systems to acquire goods and services. However, criminal elements are lurking, intercepting, and tracking these transactions for fraud. Industry experts report that IoT devices will surpass 75 billion units by 2025 (Hejase *et al.,* 2021), offering more opportunities for cybercriminals to breach insecure systems and homes and access sensitive data.

Cyberspace comprises of three layers: infrastructure, software, and data. The infrastructure layer includes physical devices and network equipment, the software layer includes computer systems and applications, and the data layer includes the data held in storage devices. To reduce the impact of cyberattacks, institutions harden cyber resources through software upgrades and patches and train employees, constantly identify vulnerabilities, and mitigate effects through backups. Institutions deploy solutions to protect their cyber resources, from physical security to application and data security. Physical cybersecurity refers to using biometric controls, physical locks, alarm systems, human security guards, and video surveillance cameras to safeguard the tangible cyber assets of an organisation (Goldstein, 2016). Cybersecurity controls and measures are applied to an organisation's cyber applications to reduce the risk of breach. Data cybersecurity protects the confidentiality, integrity, and availability of cyber data to meet the data user's requirements. Network security safeguards systems against unauthorised access. Network cybersecurity refers to measures taken to protect data during transmission over interconnected networks (Awodele, Onuiri, and Okolie, 2012). Network cybersecurity entails enforcing policies and modifying the network architecture to include security controls such as firewall rules, intrusion detection, monitoring, and patch management.

Identity theft is the illegal use of another person's private information for fraud. It involves impersonating an individual's identity to steal personal information, including banking details, credit cards, and social security information (Arachchilage and Love, 2014). Phishing is a social engineering technique where an attacker seeks to access a legitimate user's credentials illegally or personally sensitive information by impersonating electronic communications from a trusted source (Jakobsson and Myers, 2006; Jang-Jaccard and Nepal, 2014). During phishing, an unsuspecting victim is redirected to a malicious website after receiving an email with an embedded link using social engineering techniques (Gupta *et al.,* 2015). Malware refers to software programs illegally installed on a victim's computer to steal identifying information and cause malicious damage to cyberinfrastructure.

Developed countries have enacted effective cybersecurity frameworks and policies to strengthen operations, raise awareness and support training programmes (Russell *et al.*, 2017). Countries such as the United States of America (USA), Australia, Canada and the United Kingdom (UK) use cybersecurity to secure and fortify critical infrastructure which drives socioeconomic development (Catota *et al.*, 2019). The USA's National Security Agency fortified its cybersecurity posture by setting academic centres of excellence to lead in cybersecurity research and quality education, disseminate information, lead the country in cybersecurity best practices and spearhead public and private sector partnerships (Kallberg and Thuraisingam, 2012). The Australian Federal Police's computer crimes unit collaborates with foreign intelligence units to respond to cyberattacks on the country's national infrastructure and digital assets (Smith and Ingram, 2017). The European Union's NATO warned potential cyber criminals that the bloc had a full range of capabilities to detect cybercrime and respond to all threats using all possible means (Goel, 2020). The UK adopted a large scale cybersecurity framework that shows the government's ability to detect and defend its infrastructure against cyberattacks, involving collaborations with the private sector, military and educational institutions (Neville-Jones and Phillips, 2012). Despite the unprecedented adoption of ICTs in the last two decades (Maphosa, 2022b), developing countries lag in the adoption of cybersecurity frameworks and policies. Kabanda (2019) noted that cybersecurity systems in Africa are underdeveloped due to limited infrastructure, lack of funding, inadequate policies and legislation, lack of education and awareness, and limited reporting and data-sharing platforms. Only 11 African countries have cybersecurity policies (Kshetri, 2019).

As banks go digital, customers use electronic devices to conduct banking services such as creating accounts, conducting financial transactions and paying bills anytime and anywhere, increasing exposure to cybercrime. Most of Africa's economy is informal; therefore, cyberattacks target financial institutions and mobile network operators who drive the mobile money ecosystem (Mukiibi, 2019). The outbreak of the COVID-19 pandemic forced organisations to shift from the physical to the virtual environments to deliver services (Maphosa, 2021; Maphosa, 2022b), putting a strain on cybersecurity. Cybercrimes continue to increase despite the availability of technical cybersecurity infrastructures such as firewalls, encryption, and antiviruses. Developing countries should strengthen cybersecurity measures as attacks on critical infrastructure are rising. Africa loses over four billion USD annually to cybercrime; other critical losses include data, intellectual property, reputation, and brand name (Weforum, 2022).

According to the national cybersecurity index (CGI), a global tracker of countries' progress in cybersecurity, Zimbabwe is ranked 129th due to a lack of policies that support the cybersecurity (NCSI, 2021). Cybersecurity breaches are rising in Zimbabwe due to a lack of a national cybersecurity implementation plan and strategy in Zimbabwe (NCSI, 2021). Not much has been done in cultivating a cybersecurity culture and combating cybercrimes in Zimbabwe. Zimbabwe has a massive shortage of cybersecurity specialists and this is compounded by the lack of frameworks and policies to drive national implementation programmes. Kabanda (2019) notes that cybersecurity is regarded as an afterthought and is usually not part of the core business strategies and this is worsened by the unprecedented brain drain of skilled personnel in Zimbabwe. Zimbabwe faces challenges such as a lack of programmes and opportunities to equip the general public with skills, knowledge and awareness to fight cybercrime (Mutunhu *et al.*, 2022). Zimbabwe's Cyber Security and Data Protection Bill promulgation is a critical step in fighting cybercrime, but it has been widely criticised and viewed as a tool for the State to gag and muzzle civil society and the media in the fight against corruption (Transparency International, 2020). There is a need to involve non-state actors in the development and review of the Bill.

In a 2018 survey, 64% of industry leaders acknowledged that organisations had failed to manage cybersecurity risks; therefore, improvements were proposed (Deloitte, 2018). This calls for researchers to propose and evaluate technical cybersecurity solutions for combating cybercrime. The study aims to assess the state of cybersecurity in a developing country to raise awareness and compliance and fight cybercrime. The study also adds to the dearth of literature from developing countries on cybercrime.

## Literature review

Cyberspace is the fastest evolving technology in human history, where new emerging platforms such as IoT, social media, big data, and cloud computing provide new threats and opportunities. Despite the recent adoption of digital platforms in Africa, organisations still need to prioritise cybersecurity; unfortunately, only a few have developed comprehensive policies to improve security. Criminals have expanded their attacks as many systems are vulnerable due to lax cybersecurity practices in most African countries. Mukiibi (2019) reported that less than ten African countries have cybersecurity legislation. In 2018, only 13 of the 54 African countries had Computer Emergency Response Teams (CERT), and 14 had personal data protection laws (AUC, 2018). By 2022, 29 of the 54 African countries had cybersecurity legislation (Weforum, 2022). Mukiibi (2019) reports that only 18 countries have Computer Security Incident Response Teams (CSIRTs). As a result, many organisations are vulnerable, and assessment results revealed that only 52% of African companies could handle large-scale cyber-attacks (Weforum, 2022). In the 12 months ending

February 2021, South Africa had 230 million attacks, followed by Kenya and Morocco, which recorded 72 and 71 million attacks, respectively (KPMG, 2022). Interpol reports that 90% of African businesses have no cybersecurity protocols to protect their businesses, leaving them vulnerable to threat actors (Weforum, 2022). Zimbabwe and Libya had 90% of counterfeit and pirated software, the highest percentage, accelerating the spread of malware and system breaches (Weforum, 2022; Kshetri, 2019).

## Cybercrime

Cybercrimes are known as crimes of the Internet; specifically, they refer to criminal activities perpetrated through computer-related devices in cyberspace (Kharb, 2017). As more workers took their computers to work from home during the COVID-19 pandemic, industry experts report that cyberattacks quadrupled (Menn, 2020). The World Economic Forum reports that cyberattacks increased to 125% globally in 2021, and indications show an upward increase in 2022 (Weforum, 2022). Ever since the outbreak of the COVID-19 pandemic, cybercrimes have increased by 300%, costing the world over six trillion USD (Hejase *et al.,* 2021). Sviatun *et al.* (2021) reported that 87.6% of cybercrime attacks targeted the financial sector, with the retail industry coming second with 82.7%, while the communication and technology sector had 81.9%. African businesses face cyber threats such as online scams, ransomware, botnets and email compromise (KPMG, 2022). The most common cybercrimes in Zimbabwe are identity theft, hacking, email phishing, and malware victimisation (RBZ, 2015).

A study carried out by Kahn and Roberds (2008) showed that identity theft was driven by the need to steal money on one side and the need to avoid being monitored. Alkhalil *et al.* (2021) postulated that phishers attack a technical system by tricking employees into clicking on malicious links or downloading harmful files to steal their private information required to commit fraud. Molinaro and Bolton (2018) highlighted the importance of the double lens model in preventing phishing attacks. Hacking has been attributed to low self-control (Kranenbarg, Holt, and Gleder, 2017). Odunze (2018) employed the differential association theory and the routine activity theory to explain hacking and found that women were more vulnerable to hacking than their male counterparts due to the prevalence of romance scams.

## Cybersecurity

Cybersecurity combines procedures and processes to protect infrastructure, systems, and data from cyberattacks. Cybersecurity ensures data integrity and confidentiality by guarding against unauthorised access to sensitive information (Mukiibi, 2019). Cybercriminals exploit flaws and other vulnerabilities in emerging technologies to counter security offered by firewalls, antivirus scanners, and data encryption tools (Jang-Jaccard and Nepal, 2014). On average, organisations are paying US $3.6 million per attack, with ransomware attacks increasing by 151% as organisations witnessed a 31% increase in attacks (Bissell *et al.,* 2021). A major cyber-attack on a power grid left over 1.4 million people without electricity in Ukraine (Knake, 2017). Financial institution systems have become a significant target for hacking, phishing, malware, and identity theft (Weforum, 2022). Industry trends show exponential cyber-attack growth; Price Waterhouse Cooper (PWC) reported that 93% of financial institutions suffered security breaches in 2016 (Airehrour, Vasudevan, and Madanian, 2018). The financial services sector can become bankrupt after a security breach, with millions of dollars demanded to pay lawsuits and settle ransomware (Reddy and Reddy, 2014). After a phishing attack in 2017, the Bank of India lost US $170 million (Acharya and Joshi, 2020). Another bank in Brazil lost US $243 million to cyber criminals (Tabassum, 2020). Industry experts reported that Africa lost over US $3.5 billion in 2017, with Nigeria accounting for 18.5% (US $649m), Kenya losing 6% (US $210m), and South Africa losing 4.5% (US $157m) through cyberattacks (Kshetri, 2019). Klynveld Peat Marwick Goerdeler (KPMG) reported that Kenya's interconnected supply chain networks had suffered ransomware attacks (KPMG, 2022). In contrast, its banking sector has suffered from distributed denial-of-service (DDoS) attacks. Cyber threats have disrupted South Africa's maritime infrastructure, and its cities' social services payment systems have suffered ransomware and data breach (KPMG, 2022). In 2018, over 4,000 cases of cybercrime were handled by Zimbabwean police, and the country lost US $40 million to cybercrime in 2018 (Bulawayo24, 2021).

Cybercriminals target and exploit technical vulnerabilities and pry on users with limited cyber training or ethics to breach systems. Physical security is achieved using human guards, video surveillance cameras, physical locks, and biometrics to protect cyberspace. Skopak and Sakanovic (2016) confirmed that physical security is necessary to protect information resources comprehensively. Kazemi (2018) asserted that physical security was among the factors helping to preserve confidentiality. This view was supported by Elnaim (2016), who found out that physical security helped to protect information against attacks. DiMase *et al.* (2015) highlighted the importance of physical security in denying access to hardware resources. Georgiadou *et al.* (2021) reported that it was easy to control machines as they were more predictable than humans. There is growing interest and broader emphasis on human factors in the fight against cybercrime.

As financial institutions move some of their services online, potential breaches and security attacks increase exponentially. Reaves *et al.* (2015) analysed branchless banking applications and reported increased cybersecurity threats.

ENISA (2016) showed that application security influences cybersecurity. Elkhodr *et al.* (2012) proposed improving mobile banking's application security in Australia and found that mobile application security significantly impacted cybersecurity. Ahluwalia (2016) postulated that biometrics were pivotal in mitigating cybersecurity breaches. Experimental results from a study conducted by Zhang and Wang (2010) showed that network security performance contributed to cybersecurity.

Globally, internet traffic increased by over 30%, with significant changes in geographic distributions of the connections from enterprise locations to residential access (Katz, 2020). As workers move to work from home due to COVID-19 and flexible working in line with 21$^{st}$-century jobs, vulnerabilities intensify, and measures are required to protect data during transmission over interconnected networks. Gyabi and Shrivas (2016) used encryption to secure data in the rural bank of Ghana. A simulation analysis by Hossain *et al.* (2017) revealed that data security in the cloud could be achieved through encryption and a location-based salt algorithm. Durumeric *et al.* (2017) sought to avoid HTTPS interception through heuristics deployed on different networks. A study carried out by Subramanian and John (2017) revealed that a data security algorithm reduced malicious insider attacks. Kaiwartya *et al.* (2017) investigated biometric Internet security and found it suitable for Internet authentication. Tseng *et al.* (2015) realised the importance of internet security and proposed an anti-phishing-based video game to enhance the learners' internet security.

## Methods

### Ethical statement

This study received ethical approval from the Lupane State University Institutional Ethics Committee (LSU00022). The online questionnaire explained the research objectives, participants' expectations, voluntariness and respondents' anonymity. Participants gave their written consent before participating in the online survey.

### Study design

The study applied a descriptive quantitative survey design. The comprehensive literature review identified critical technical factors influencing cybersecurity, such as physical security, data security, application security, network security, and internet security. These factors shaped the thrust of the study. The study's questionnaire was adapted from the International Organization for Standardization (ISO)/International Electrotechnical Commission (ISOC/IEC) (ISOC/IEC, 2012). ISOC/IEC is a task force responsible for crafting and reviewing industry-wide cybersecurity standards after every five years. Since the targeted participants are professionals with post-secondary education, the questionnaire was administered in English, the country's official language.

A pilot study was conducted to verify the questionnaire's appropriateness and completeness and gauge the meaning of the questions (Maphosa, 2023c). The instrument was piloted in June 2022 to six network and security personnel at the University. Participants made comments and suggestions on the online questionnaire, which the researcher captured. This ensured that the questions were not ambiguous, difficult to answer or prone to many interpretations, which could lead to biased responses. Before the survey instrument was disseminated, some questions were edited to ensure clarity and answerability, while some were re-arranged to improve the flow of responses. Other changes involved altering some binary responses 'yes' or 'no' to the Likert scale type and providing options to other questions.

The final questionnaire contained two key sections with 38 items based on the literature reviewed. Cybersecurity literature and security governance standards were contextualised to the Zimbabwean context to develop the questionnaire. Data were collected from early July 2022 to early October 2022. Section A contains the respondent's age, financial institution's name, and gender profile as shown in Appendix A. Section B consisted of the main questions on a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree (Maphosa, 2023b).

### Participant selection and data collection

The study targeted IT experts from the country's financial institutions comprising commercial banks, merchant banks, discount houses, building societies, and finance houses. The survey questionnaire for the study was self-administered to IT experts in the financial services sector to obtain an overview of cybercrime. Electronic mail was sent to personnel in the networks and infrastructure departments of the randomly selected financial institutions. Professional networks such as LinkedIn and Twitter and distribution lists such as the Computer Society of Zimbabwe and the Internet Society of Zimbabwe were used. Convenience sampling was used to recruit participants. The sample includes participants working in the networks and infrastructure department within their financial institutions. Data were collected electronically and stored in Google Drive, which was password encrypted.

## Results

The 76 responses received were from ICT managers (16), network security specialists (12), database and systems administrators (10), developers (28), and risk and compliance officers (10), giving an 84.4% response rate. Most (72%)

**Table 1. Demographics of the 76 participants.**

| Demographic variables | Demographic variables values |
|---|---|
| Gender | Male (72%); Female (28%) |
| Age | Mean 29; range 19-55 years |
| Qualification | Diploma (14%), undergraduate (51%), postgraduate (35 %) |
| IT experience in a financial institution | Mean = 9.5 years, range 1-40 years |
| Occupation | Developers, Database administrators, Systems administrators, Network security specialists, Managers, and Risk compliance officers |

respondents were male, while about a third were female. More than half of the respondents had an undergraduate degree, as shown in Table 1. The average age of the respondents was 29 years, while the IT experience in the financial services sector was 9.5. The respondents' names and those of their financial institutions were kept anonymous (Maphosa, 2023a).

The study evaluated cybersecurity security constructs for initial threat areas from physical security to data security. The study used descriptive statistics and percentages to measure the constructs' means and standard deviations (SD). The mean and the SD of the cybersecurity constructs are shown in Table 2. The mean values ranged between 3.699 and 4.854, while SD values ranged between 0.655 and 0.779. Participants ranked network security highly, with a mean of 4.854 and a standard deviation of 0.739. The following ranked construct was data security, with a mean of 4.739 and an SD of 0.655. The penultimate construct was identity theft, with a mean of 3.802 and an SD of 0.715. The last ranked construct was physical security, with a mean of 3.699 and an SD of 0.770. Physical security is easily fortified through security guards, CCTV, biometrics, electronic locks or other related devices.

Respondents ranked the framework used by their financial institution; almost half (44.74%) used the Information Technology Infrastructure Library (ITIL), followed by Control Objectives for Information and Related Technology framework (COBIT), with 36.84% and about 10.53% of the institutions adopted other frameworks as shown in Table 3.

Figure 1 shows the top cybersecurity barriers, which include increasing sophistication of threats (89.5%), limited technical skills (85.5%) and emerging technologies (81.6%). The least ranked barriers are lack of executive support (22.4%), lack of adequate budget (30.3%) and lack of cybersecurity policies (53.9%).

**Table 2. Security constructs and ranking.**

| Constructs | Items | Mean | SD |
|---|---|---|---|
| Physical Security | 5 | 3.699 | 0.770 |
| Application Security | 5 | 4.731 | 0.779 |
| Data Security | 4 | 4.739 | 0.655 |
| Network Security | 4 | 4.854 | 0.739 |
| Internet Security | 5 | 3.964 | 0.703 |
| Identity Theft | 4 | 3.802 | 0.715 |

**Table 3. Frameworks: cybersecurity.**

| Cybersecurity Framework | Frequency | Percentage |
|---|---|---|
| ITIL | 34 | 44.74% |
| COBIT | 28 | 36.84% |
| NIST | 19 | 25% |
| ISO/IEC27000 | 17 | 22.37% |
| No framework used | 15 | 19.74% |
| Others | 8 | 10.53% |

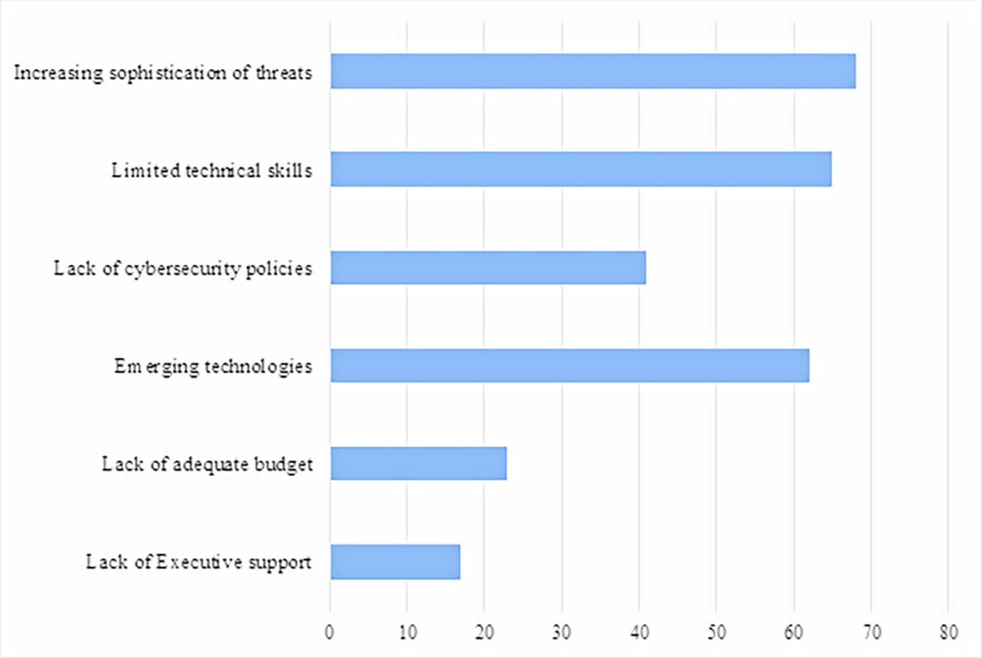

**Figure 1. Barriers to cybercrime management.**

## Discussion

The top three barriers for this study are increasing sophistication of threats, limited skills and emerging technologies. Insufficient cybersecurity personnel, limited budgets, and executive support followed these. Financial institutions should adopt cybersecurity policies and engage in extensive end-user training programmes to fight cybercriminals. This study confirmed the findings by Norris *et al.* (2019), who established that lack of skills, inadequate policies, limited funding and management support impacted cybersecurity. Institutions must balance the drive to increase revenues and reduce operating costs while ensuring compliance and investing in cybersecurity frameworks.

The high ranking of network security aligned with findings by Praveena and Smys (2017), who identified network security as a substantial concern in protecting financial information. Acharya and Joshi (2020) also contended that networks should be audited at fixed intervals to test for security breaches.

Bendovschi (2015) also ranked data security highly, noting that when organisations lose their data, they lose their market share and customer relationship. Verizon reports that 37% of security breaches resulted from identity theft, while social engineering or phishing accounted for 22% (Verizon, 2020). KPMG (2022) recommended that organisations perform penetration tests regularly and demonstrate response and readiness to evaluate the institution's network security.

The minimal technical skills mean institutions have limited capacity to secure networks and information systems, configure servers, recover data, and continuously scan for vulnerabilities and remediation. Figure 1 shows the barriers to cybercrime in line with Norris *et al.* (2019), who ranked cybersecurity management barriers as limited technical skills caused by the inability of institutions to pay competitive salaries. The findings align with observations by the World Economic Forum, which reported that only 53.7% of African countries had cybersecurity policies (Weforum, 2022). The establishment of cybersecurity policies demonstrates management's intent to create a security conscious culture and provide guidance to employees.

Cavusoglu *et al.* (2004) lamented that most African countries needed meaningful budgets to support cyber security. Although management support was lowly ranked, none of the financial institutions had established a Chief Information Security Officer (CISO) to handle cybersecurity issues at a strategic level. Management support also influences budgetary allocations and prioritises cybersecurity issues within the institution. Richards (2014) noted that organisations had established the CISO to strengthen the institution's cybersecurity portfolio, managing enterprise cybersecurity risks and mitigation measures to maintain the institutional brand.

Cybercriminals rely on sophisticated technologies that are difficult to detect and threaten even the savviest targets (Microsoft, 2020). The lack of policies hinders sharing cybersecurity information between institutions, resulting in fragmented knowledge across the domain. Caulkins *et al.* (2018) also identified a lack of cybersecurity personnel globally, affecting the availability of skilled and experienced staff who can handle cybersecurity tasks and challenges. Financial institutions should train and retain cybersecurity specialists to fight cybercrime.

Microsoft (2020) identified emerging threats, such as using AI-enabled capabilities to commit cybercrime and the increased adoption of IoT and teleworking. Such tools are available on the black market and online. Financial institutions can take practical steps to raise awareness and training and ensure that cybersecurity frameworks are adopted. Lack of cybersecurity awareness by employees can have devastating consequences on the organisation as they can quickly become a security loophole if they are not concentrating, are distracted, or are stressed. This aligns well with KPMG's (2022) recommendations, which suggested that institutions conduct cyber awareness and training, establish firewalls and maintain backup while ensuring their security systems have the latest patches.

Developing countries have rapidly increased access to cyberspace, without corresponding effort to fortify cyberspace and improve security measures deter cybercrime (Muller, 2015). The results show that about a fifth (19.74%) of the financial institutions are yet to adopt cybercrime frameworks, this is worrying as public funds and investments are exposed to risks. The most common cybersecurity frameworks in Zimbabwe are the ITIL and COBIT, while other frameworks such as the NIST and ISO 27002 are quickly gaining recognition.

The study has the following limitations. The small sample size impacts the generalisability of the findings; more responses would have improved the value of the study's findings. Using a quantitative data collection approach may have restricted the probing of participants to elicit more information and further explain specific responses. The use of self-reported data raises fears that participants could have portrayed a positive outlook on the image of their institution since data breaches are sensitive in the financial services sector.

## Conclusion

Literature shows that cybercriminals constantly attack financial institutions, yet results show that their cybersecurity practices are poor. As technology evolves, the means and opportunities to commit cybercrime also increase, and therefore, many organisations will suffer security breaches leading to irrecoverable losses. The study provides an overview of Zimbabwe's cybersecurity landscape and threats while providing a roadmap to manage cybercrime in other developing countries with a similar socioeconomic environment. Research has been conducted to identify the motivations, techniques, and countermeasures to cybercrime; however, there is no single solution due to the heterogeneous nature of the attack vector. Financial institutions should embrace a strong awareness culture, invest in cybersecurity technologies, train security specialists, and employ CISOs and executives knowledgeable in cybersecurity.

The study established technical factors such as physical security, application security, data security, network security, and internet security. Network security and data security were the highly ranked cybersecurity constructs, while physical security was the least ranked. There are several barriers that financial institutions face in managing cybercrime. The top three barriers are increasing sophistication of threats, limited skills and emerging technologies. The top frameworks used by financial institutions are the ITIL and COBIT, while about a fifth are yet to adopt cybercrime frameworks. The study's small sample may affect the generalisability of the results. The study focused on technical aspects of cybersecurity, and future studies could focus on social engineering aspects that compromise the security of systems. This study raises awareness of the ever-present cybersecurity threat in the financial services sector. The study provides a baseline on the state of cybercrime in developing countries. More research will be required to validate these findings by developing models and using advanced statistical analysis on independent and dependent variables to test for causality and correlation.

The Government should proactively provide an environment that supports cybersecurity research and reporting of cases so that institutions can learn from others and continuously improve their detection and protection systems. The study recommends developing a national cybersecurity framework for an improved cybersecurity strategy for protecting Zimbabwean financial institutions. This framework must include establishing a cybersecurity culture, addressing cybersecurity barriers and following best practices such as adopting frameworks and establishing the office of the CISO. This will improve the protection of critical assets, minimise service disruption and loss of resources and strengthen financial institutions' public confidence and reputation. The practical implication of this study is improving cybersecurity risks, given the rising adoption of emerging technologies and frameworks that support participation in the global economy. More awareness and education programmes are required to equip cyberspace users. A cybersecurity culture should be developed in the early stages of schooling such as the primary school level. There should be deliberate effort to grow cybersecurity skills which are extremely important to the financial services sector and are in short supply due to the brain drain. The government and the private sector should partner to set up CERT for the financial services sector and other sectors. The cybersecurity bill should be flexible to allow for the continuous review of the roles played by the state and non-state actors and align with the dynamic threat levels. Tax rebates on cybersecurity equipment are required to ensure that organisations can invest in basic cybersecurity equipment.

Future studies could investigate the effects of social media-based cybercrimes as emerging threats are predicted to increase significantly over the following years. The government should also implement and strengthen policies, laws and legislations that curb cybercrime to mitigate economic losses. Financial institutions must create strategies to raise awareness of cybercrime and collaborate with higher education institutions to introduce programmes addressing cybersecurity challenges to close the skills gap. Financial institutions can use social media platforms for cybersecurity literacy and awareness.

## Data availability

### Underlying data

Zenondo: Cybersecurity. https://doi.org/10.5281/zenodo.7824605. (Maphosa, 2023a).

The project contains the following underlying data:

- Cyber security survey.xlsx. (Anonymised responses from IT experts on cybersecurity in the financial services sector).

Data are available under the terms of the Creative Commons Attribution 4.0 International license (CC-BY 4.0).

### Extended data

Zenondo: An Overview of Cybersecurity in Zimbabwe's Financial Services Sector. https://doi.org/10.5281/zenodo.7824658. (Maphosa, 2023b).

This project contains the following extended data:

- Cybersecurity questionnaire.pdf. (Final version of the cybersecurity survey questionnaire in the financial services sector).

Zenondo: An Overview of Cybersecurity in Zimbabwe's Financial Services Sector. https://doi.org/10.5281/zenodo.7825562. (Maphosa, 2023c).

- Questionnaire pilot.pdf (Pilot version of the Cybersecurity survey questionnaire in the financial services sector).

Data are available under the terms of the Creative Commons Attribution 4.0 International license (CC-BY 4.0).

## References

Acharya S, Joshi S: **Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures.** *PalArch's J. Archaeol. Egypt/Egyptol.* 2020; **17**(6): 4656–4670.

Ahluwalia R: **Banking's biometric future.** *Biometric Technology Today.* 2016; **2016**(10): 7–9.
Publisher Full Text

Airehrour D, Vasudevan Nair N, Madanian S: **Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user-reflective mitigation model.** *Information.* 2018; **9**(5): 1–18.
Publisher Full Text

Alkhalil Z, Hewage C, Nawaf L, *et al.*: **Phishing Attacks: A Recent Comprehensive Study and a New Anatomy.** *Front. Comp. Sci.* 2021; **3**(563060): 1–23.
Publisher Full Text

Arachchilage NAG, Love S: **Security awareness of computer users: a phishing threat avoidance perspective.** *Comput. Hum. Behav.* 2014; **38**: 304–312.
Publisher Full Text

AUC: *Cyber Security and Cybercrime Policies for African Diplomats.* 2018.
Reference Source

Bendovschi A: **Cyber-Attacks – Trends, Patterns, and Security Countermeasures.** *Procedia Economics and Finance.* 2015; **28**: 24–31.
Publisher Full Text

Bissell K, Fox J, LaSalle RM, *et al.*: **How aligning security and the business creates cyber resilience.** *Accenture.* 2021.
Reference Source

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

Catota FE, Morgan MG, Sicker DC: **Cybersecurity education in a developing nation: the Ecuadorian environment.** *J. Cybersecur.* 2019; **5**: 1–19.
Publisher Full Text

Caulkins B, Marlowe T, Reardon A: **Cybersecurity skills to address Today's Threats.** Ahram T, Nicholson D, editors. *Advances in Human factors in Cybersecurity, AHFE 2018. Advances in Intelligent Systems and Computing.* Springer; 2018; pp. 782–788.
**Publisher Full Text**

Cavusoglu H, Mishra B, Raghunathan S: **The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers.** *Int. J. Electron. Commer.* 2004; **9**(1): 70–104.
**Publisher Full Text**

Deloitte: *Transforming Risks into Opportunities.* 2018. Retrieved July 2022.
**Reference Source** | **Reference Source**

DiMase D, Collier ZA, Heffner K, *et al.*: **Systems engineering framework for cyber physical security and resilience.** *Environ. Syst. Decis.* 2015; **35**(2): 291–300.
**Publisher Full Text**

Durumeric Z, Ma Z, Springall D, *et al.*: *The Security Impact of HTTPS Interception.* NDSS; 2017.
**Publisher Full Text**

Elkhodr M, Shahrestani S, Kourouche K: **A proposal to improve the security of mobile banking applications.** *2012 Tenth International Conference on ICT and Knowledge Engineering.* Bangkok, Thailand: 2012; 260–265.
**Publisher Full Text**

Elnaim BME: **The Impact Of Information Security Management For E- Banks Performance In Kingdom Of Sudi Arabia.** *Int. J. Eng. Res. Technol.* 2016; **5**(11): 266–271.
**Publisher Full Text**

European Network and Information Security Agency (ENISA): **NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies.** 2016. accessed on: 29 May 2019.
**Reference Source**

Georgiadou A, Mouzakitis S, Askounis D: **Detecting Insider Threat via a Cyber-Security Culture Framework.** *J. Comput. Inf. Syst.* 2021; **62**(4): 706–716.
**Publisher Full Text**

Goel S: **National cyber security strategy and the emergence of strong digital borders.** *Connections.* 2020; **19**(1): 73–86.
**Publisher Full Text**

Goldstein P: *Why Physical Security Should Be as Important as Cybersecurity.* 2016. accessed 21 March 2021.
**Reference Source**

Gyabi MO, Shrivas MK: **Data Security in Rural Banking Sector: A Case Study in Ashanti Region.** *Internation Journal of Advanced Research in Computer Science and ETechnology.* 2016; **4**(2): 99–106.
**Reference Source**

Gupta P, Srinivasan B, Balasubramaniyan V, *et al.*: **Phoneypot: data-driven understanding of telephony threats.** *Proceedings 2015 network and distributed system security symposium.* Reston, VA: Internet Society; 2015; 8–11.
**Publisher Full Text**

Hejase H, Fayyad-Kazan H, Hejase A, *et al.*: **Cyber Security amid COVID-19.** *Computer and Information Science.* 2021; **14**(2): 10–25.
**Publisher Full Text**

Hossain MA, Al-Amin M, Hossain N, *et al.*: **User Location Time and Entropy (ULTE) based Salt generation for Password Based Key Derivation Function (PBKDF) in Cloud Computing.** *Int. J. Sci. Eng. Res.* 2017; **8**(2): 1399–1408.
**Publisher Full Text**

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC): *2012 Information—Security Techniques—Guidelines for Cybersecurity, ISO/IEC 27032.* 2012. Retrieved January 2023.
**Reference Source**

Jang-Jaccard J, Nepal S: **A survey of emerging threats in cybersecurity.** *J. Comput. Syst. Sci.* 2014; **80**(5): 973–993.
**Publisher Full Text**

Jakobsson M, Myers S (editors): *Phishing and countermeasures: understanding the increasing problem of electronic identity theft.* John Wiley & Sons; 2006.

Kabanda G: **A Bayesian Network Model for a Zimbabwean Cybersecurity System.** *Orient. J. Comp. Sci. Technol.* 2019; **12**(4): 147–167.
**Publisher Full Text**

Kahn CM, Roberds W: **Credit and identity theft.** *J. Monet. Econ.* 2008; **55**(2): 251–264.
**Publisher Full Text**

Kaiwartya O, Prasad M, Prakash S, *et al.*: **An Investigation on Biometric Internet Security.** *Int. J. Netw. Secur.* 2017; **19**(2): 167–176.
**Publisher Full Text**

Kallberg J, Thuraisingam B: **Towards Cyber Operations The New Role of Academic Cyber Security Research and Education.** *IEEE International Conference on Intelligence and Security Informatics.* Washington, USA. 2012: pp. 132–134

Katz R: *Economic impact of COVID-19 on digital infrastructure.* Geneva: International Telecommunications Union; 2020.
**Reference Source**

Katz R, Jung J: **The Economic impact of broadband and digitalization through the COVID-19 pandemic.** *International Telecommunication Union.* 2021.
**Reference Source**

Kazemi U: **A Survey: Information Security Management System.** *Journal of Analog and Digital Devices.* 2018; **2**(3): 1–6.
**Reference Source**

Kharb L: **Cyber Crimes Becoming Threat to Cyber Security.** *International Journal of Engineering and Management Research.* 2017; **7**(2): 48–51.
**Reference Source**

Knake RK: *A cyberattack on the US power grid.* Council on Foreign Relations; 2017.

KPMG: *Africa Cyber Security Outlook.* 2022, September.
**Reference Source**

Kranenbarg MW, Holt TJ, Gleder J-L: **Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap.** *Deviant Behav.* 2017; **40**(1): 40–55.
**Publisher Full Text**

Kshetri N: **Cybercrime and Cybersecurity in Africa.** *J. Glob. Inf. Technol. Manag.* 2019; **22**(2): 77–81.
**Publisher Full Text**

Maphosa V: **Developing an App for Improving Access to COVID-19 Information in Underserved Communities.** *Int. J. Inf. Eng. Electron. Bus.* 2022b; **14**(3): 19–29.
**Publisher Full Text**

Maphosa V: **COVID-19 and the Digital Ecosystem: Using a Mobile App to Connect a Rural Community.** *Aqua.* 2021; **5**(1): ep21002.
**Publisher Full Text**

Maphosa V: **Rethinking Sustainability: A Bibliometric and Visualisation of E-Waste Management in Africa.** *Journal of Higher Education Theory and Practice.* 2022a; **22**(1): 123–135.
**Publisher Full Text**

Maphosa V: An Overview of Cybersecurity in Zimbabwe's Financial Services Sector. [Dataset]. *Zenodo.* 2023a.
**Publisher Full Text**

Maphosa V: An Overview of Cybersecurity in Zimbabwe's Financial Services Sector. Dataset. *Zenodo.* 2023b.
**Publisher Full Text**

Maphosa V: An Overview of Cybersecurity in Zimbabwe's Financial Services Sector. Dataset. *Zenodo.* 2023c.
**Publisher Full Text**

Menn J: *Hacking against corporations surges as workers take computers home, Reuters.* 2020, April 17. Retrieved March 15, 2021.
**Reference Source**

Microsoft: *Microsoft report shows increasing sophistication of cyber threats. Microsoft on issues.* 2020, September 29.
**Reference Source**

Molinaro KA, Bolton ML: **Evaluating the applicability of the double system lens model to the analysis of phishing email judgments.** *Comput. Secur.* 2018; **77**: 128–137.
**Publisher Full Text**

Mukiibi H: **Cyber security in Africa: The boring technology story that matters.** *Crossroads.* 2019; **26**(2): 56–59.
**Publisher Full Text**

Muller LP: *Cyber security capacity building in developing countries: challenges and opportunities.* Norway: Norwegian Institute of International Affairs; 2015.

Mutunhu B, Dube S, Ncube N, *et al.*: **Cyber Security Awareness and Education Framework for Zimbabwe Universities. A Case of National University of Science and Technology.** *Proceedings of the International Conference on Industrial Engineering and Operations Management.* Nsukka, Nigeria; 2022.

NCSI: 2021. Accessed 13 July 2021.
**Reference Source**

Neville-Jones P, Phillips M: **Where next for UK cyber-security.** *Rusi Journal.* 2012; **157**(6): 32–40.
**Publisher Full Text**

Norris DF, Mateczun L, Joshi A, *et al.*: **Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity.** *Public Adm. Rev.* 2019; **79**(6): 895–904.
**Publisher Full Text**

Odunze D: **Cyber Victimization by Hackers: A Criminological Analysis.** *Public Policy and Administration Research.* 2018; **8**(1): 8–15.
**Reference Source**

POTRAZ: *Mobile data prices in Zimbabwe. cyber behaviour.* Harare, Zimbabwe; 2021.
Reference Source

Praveena A, Smys S: **Prevention of inference attacks for private information on social networking sites.** *2017 International Conference on Inventive Systems and Control (ICISC).* Coimbatore, India: IEEE; 2017; (pp. 1–7).

Radzikowski S: *Cybersecurity: Origins of the advanced persistent threat (APT).* 2015. accessed on: 10 January 2020.
Reference Source

RBZ: *Cybercrime in Zimbabwe and Globally.* 2015.
Reference Source

Reaves B, Scaife N, Bates A, *et al.*: **Analysis of Branchless Banking Applications in the Developing World.** *24th USENIX Security Symposium.* 2015.
Reference Source

Reddy GN, Reddy GJ: **A study of cyber security challenges and its emerging trends on the latest technologies. arXiv preprint arXiv: 1402.1842.** 2014; 1–5.
Publisher Full Text

Richards K: **Has the CISO role changed under the spotlight?** *Inf. Secur. Mag.* 2014; **2014**: 56. accessed 21 March 2021.
Reference Source

Russell JD, Weems CF, Ahmed I, *et al.*: **Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors.** *J. Cyber Secur. Technol.* 2017; **1**(3-4): 163–174.
Publisher Full Text

Skopak A, Sakanovic S: **Adoption of standards for information security ISO/IEC 27001 in Bosnia and Herzegovina.** *ICESoS.* 2016; **2016**.
Reference Source

Smith F, Ingram G: **Organising cyber security in Australia and beyond.** *Australian Journal of International Affairs.* 2017; **71**(6): 642–660.
Publisher Full Text

Subramanian K, John FL: **Enhanced Security for Data Sharing in Multi Cloud Storage (SDSMC).** *Int. J. Adv. Comput. Sci. Appl.* 2017; **8**(3).
Reference Source

Sviatun O, Goncharuk O, Chernysh R, *et al.*: **Combating cybercrime: economic and legal aspects.** *WSEAS Trans. Bus. Econ.* 2021; **18**: 751–762.
Publisher Full Text

Tabassum L: **State of Cyber Crime Safety and Security in Banking.** *Int. J. Sci. Res. Engineering Dev.* 2020; **3**(4): 72–76.

Transparency International: **Zimbabwe: Cyber Security and Data Protection Bill would restrict anti-corruption watchdogs.** 2020.
Reference Source

Tseng S-S, Yang T-Y, Weg J-F, *et al.*: **Building a Game-Based Internet Security Learning System by Ontology Crystallization Approach.** *Int'l Conf. e-Learning, e-Bus., EIS and e-Gov.* 2015.
Reference Source

Verizon: *Data breach investigations report (DBIR) 2020. Verizon.* 2020.
Publisher Full Text

Weforum: **Global Cybersecurity Outlook 2022.** 2022.
Reference Source

Zhang L, Wang Q: **A Network Security Evaluation Method Based on Fuzzy and RST.** *2nd International Conference on Education Technology and Computer (ICETC).* Shanghai, China: 2010.

# Open Peer Review

## Current Peer Review Status: ✓ ? ✓ ?

Version 2

Reviewer Report 02 April 2024

https://doi.org/10.5256/f1000research.163228.r257448

?

**Simon Kaggwa**
Hult International Business School, Boston, Massachusetts, USA

Review at each Stage

**1. Title and Abstract**

Title: The title accurately reflects the report's focus on cybersecurity in Zimbabwe's financial services sector. It is informative and concise.

**2. Introduction**

The introduction effectively sets the context for the study, highlighting the importance of the internet in today's knowledge economy and the risks posed by cyberattacks. It provides relevant statistics and examples to underline the urgency of addressing cybersecurity in Zimbabwe. However, it would benefit from a clearer statement of the research questions or objectives towards the end to guide the reader on what the study specifically aims to address.

**3. Literature Review**

The literature review is detailed and covers a wide range of topics relevant to cybersecurity, including the evolution of cyberspace, the impact of cybercrimes, and the state of cybersecurity frameworks worldwide and in Africa. While comprehensive, the review could be improved by organizing the themes more clearly and critically evaluating the sources. For instance, discussing the gaps in current research that this study aims to fill would strengthen this section.

**4. Methods**

The methodological approach is well-detailed, explaining the survey design, participant selection, and data collection process. Ethical considerations are also addressed. However, the rationale for choosing a descriptive quantitative survey and the justification for the sample size and selection criteria could be elaborated on to enhance the method's section.

**5. Results**

The results section presents findings on the ranking of cybersecurity constructs, the frameworks used by financial institutions, and barriers to effective cybercrime management. The inclusion of statistical data, such as means and standard deviations, is commendable. However, the presentation of these results could be improved with the use of tables or figures for a more straightforward interpretation of the data.

**6. Discussion**

The discussion provides a good synthesis of the findings in relation to the literature review. It identifies key barriers to cybersecurity and suggests practical steps for improvement. However, the discussion could be strengthened by more directly linking the results to the specific objectives of the study and by offering a more critical analysis of the implications of the findings.

**7. Conclusion and Recommendations**

The conclusion summarizes the main findings and their implications. Recommendations are practical and relevant. The call for future research is appropriate, although more specific suggestions for areas of investigation would be beneficial. The report could also benefit from a stronger emphasis on the limitations of the study, as acknowledging these can help contextualize the findings.

**Overall Assessment**

This report provides valuable insights into the state of cybersecurity in Zimbabwe's financial services sector, highlighting significant challenges and offering practical recommendations. The authors have compiled a thorough analysis, though there are areas where clarity and depth could be improved, particularly in the abstract, methods justification, results presentation, and critical analysis in the discussion. Enhancing these areas would make the report an even more valuable contribution to the field of cyber security.

**Is the work clearly and accurately presented and does it cite the current literature?**

Yes

**Is the study design appropriate and is the work technically sound?**

Yes

**Are sufficient details of methods and analysis provided to allow replication by others?**

Partly

**If applicable, is the statistical analysis and its interpretation appropriate?**

Partly

**Are all the source data underlying the results available to ensure full reproducibility?**

Yes

**Are the conclusions drawn adequately supported by the results?**

Yes

***Competing Interests:*** No competing interests were disclosed.

***Reviewer Expertise:*** Finance and Cyber Securities case of America economies

**I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.**

Reviewer Report 28 March 2024

https://doi.org/10.5256/f1000research.163228.r257453

✓ **Dinesh Kalla**
Department of Computer Science,, Colorado Technical University, Colorado Springs, Colorado, USA
**Samaah Fnu**
Northeastern Illinois University (Ringgold ID: 2458), Chicago, Illinois, USA

This paper highlights the increasing sophistication of cyber threats, the limited skills available to combat these threats, and the challenges posed by emerging technologies. Maphosa emphasizes the need for financial institutions to establish a robust cybersecurity culture, invest in cybersecurity technologies, and employ specialized security professionals such as Chief Information Security Officers (CISOs) .Maphosa's study reveals that network and data security are the most highly ranked cybersecurity constructs, signifying their critical importance in safeguarding the sector. Conversely, physical security was ranked the least, suggesting a potential area for improvement or a shift in focus towards digital threats. Interestingly, the study found that a significant portion of financial institutions relied on the Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and Related Technologies (COBIT) frameworks, with a noteworthy percentage yet to adopt any cybercrime frameworks .

One of the paper's key recommendations includes the development of a national cybersecurity framework to enhance the strategic protection of Zimbabwean financial institutions. This framework should focus on creating a cybersecurity culture, addressing barriers to effective cybercrime management, and following best practices such as adopting established frameworks and appointing CISOs .The paper also underscores the importance of raising awareness about cybersecurity, suggesting that financial institutions collaborate with educational institutions to close the skills gap and enhance cybersecurity literacy. Furthermore, Maphosa calls for the government and private sector to partner in establishing Computer Emergency Response Teams (CERT) for the financial services sector, underscoring the critical need for improved cybersecurity infrastructure and readiness .

In conclusion, "An Overview of Cybersecurity in Zimbabwe's Financial Services Sector" provides a comprehensive examination of the challenges and necessary steps to fortify the cybersecurity posture within Zimbabwe's financial services sector. The study's recommendations offer a roadmap for stakeholders to improve cybersecurity awareness, infrastructure, and policies, thereby enhancing the resilience of financial institutions against cyber threats .

**Is the work clearly and accurately presented and does it cite the current literature?**
Yes

**Is the study design appropriate and is the work technically sound?**
Yes

**Are sufficient details of methods and analysis provided to allow replication by others?**

Yes

**If applicable, is the statistical analysis and its interpretation appropriate?**
Yes

**Are all the source data underlying the results available to ensure full reproducibility?**
Yes

**Are the conclusions drawn adequately supported by the results?**
Yes

***Competing Interests:*** No competing interests were disclosed.

***Reviewer Expertise:*** Cybersecurity, AI , Big Data and Data Science

**We confirm that we have read this submission and believe that we have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.**

Reviewer Report 25 March 2024

https://doi.org/10.5256/f1000research.163228.r255953

✓

**William Vambe**
Walter Sisulu University, Mthatha, Eastern Cape, South Africa

The issues raised previously were addressed

**Is the work clearly and accurately presented and does it cite the current literature?**
Yes

**Is the study design appropriate and is the work technically sound?**
Yes

**Are sufficient details of methods and analysis provided to allow replication by others?**
Yes

**If applicable, is the statistical analysis and its interpretation appropriate?**
Yes

**Are all the source data underlying the results available to ensure full reproducibility?**
Yes

**Are the conclusions drawn adequately supported by the results?**

Yes

***Competing Interests:*** No competing interests were disclosed.

***Reviewer Expertise:*** IoT, Fog Computing, Cloud Computing, ICT4D

**I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.**

## Version 1

Reviewer Report 20 October 2023

https://doi.org/10.5256/f1000research.145775.r211333

? **Nomusa Dlodlo**
Rhodes University, Grahamstown, Eastern Cape, South Africa

Please refer to the attached file.

1. What is the total population of the people who you could pull the participants from and how large is the sample you interviewed. ow did you identify the sample- is it purposive sampling / targetted sampling?

2. What frameworks led to the questionnaire?

3. Be specific on the numbers. How many questionnaires were distributed. ? How many responses did you get back? Are the responses an adequate representative sample of the total population of potential interviewees. How did you choose who to distribute the questionnaire to? Was it intentional or random?

4. The discussion can be approached in sub-sections where you explain the results under each subsection and then give a comparison of the results with other similar researches, e.g., Adoption of cybercrime frameworks, sophistication of threats, technical skills, etc. You already have that. You just need to add the subtopics.

**Is the work clearly and accurately presented and does it cite the current literature?**
Yes

**Is the study design appropriate and is the work technically sound?**
Partly

**Are sufficient details of methods and analysis provided to allow replication by others?**

Yes

**If applicable, is the statistical analysis and its interpretation appropriate?**
Yes

**Are all the source data underlying the results available to ensure full reproducibility?**
No

**Are the conclusions drawn adequately supported by the results?**
Yes

***Competing Interests:*** No competing interests were disclosed.

***Reviewer Expertise:*** IoT, Blockchain, ICT4D, ICT in Education, ICT in Health

**I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.**

Author Response 10 Feb 2024

**Vusumuzi Maphosa**

Population: The study targeted IT experts from the country's financial institutions comprising commercial banks, merchant banks, discount houses, building societies, and finance houses.
Sampling: Convenience sampling was used to recruit participants.
Framework: The top frameworks used are the Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and Related Technologies (COBIT), while a fifth is yet to adopt cybercrime frameworks.

Questionnaire: The study's questionnaire was adapted from the International Organization for Standardization (ISO)/International Electrotechnical Commission (ISOC/IEC) (ISOC/IEC, 2012). ISOC/IEC is a task force responsible for crafting and reviewing industry-wide cybersecurity standards every five years.
Questionnaire: An online questionnaire was used and 76 responses were received. The data set is available to the public. The distribution was random.

Discussion: The discussion is categorised into cybersecurity, security of data, security issues in developing countries, and emerging threats.

A paragraph on frameworks has been added to the discussion section.

Developing countries have rapidly increased access to cyberspace, without corresponding effort to fortify cyberspace and improve security measures. Developing countries face challenges in adopting cybersecurity frameworks and struggle to deter cybercrime (Muller, 2015). The most common cybersecurity frameworks in Zimbabwe are the ITIL and COBIT, while other frameworks like the NIST and ISO 27002 are quickly gaining recognition.

Muller, L. P. (2015). Cyber security capacity building in developing countries: challenges and opportunities Norwegian Institute of International Affairs, Norway.

***Competing Interests:*** No competing interests were disclosed.

Reviewer Report 09 October 2023

https://doi.org/10.5256/f1000research.145775.r211331

?

**William Vambe**
Walter Sisulu University, Mthatha, Eastern Cape, South Africa

The paper present a very important aspect especially with the incoming of 4IR, internet and where everyone now use mobile, online and internet banking daily. I have few issues that I think might improve the paper.

Introduction

- In the context of Zim, is this statement true, "Decreasing data costs... ". Since the paper is about Zimbabwe, I think we need to contextualize why there is a rise in using online, mobile, internet banking.

- In your write up, I propose you present state of cyber security in the context of Europe, Africa, Sadc countries, then Zimbabwe in particular since it is the study area. This gives us a clear view. Then you conclude this section by giving us the aim./ objective of this paper. Last paragraph should be a signpost to inform the reader what to expect in the whole paper.

Literature

- In the literature/related work, I was expecting more focus and discussion to be on Zim not the world in general. Is there government policy, or financial organization policies pertaining to cybersecurity? What are the challenges and implications of implementing them? What does the current/literature say about cybersecurity in Zimbabwe? What are open gaps?

- These discussions will help us to see why there was a need to do this research and will also helps us to link with the results section.

Results

- I propose using graphs rather than tables as graphs show the comparison better.

**Since you are an expert, based on your results, I propose you put a section Possible Solutions/ Significant Recommendations, where you articulate what as a researcher think can be done to address the challenges you got from literature and your results. This can be backed by literature on solutions that have been implemented in other countries almost similar to Zim.

**Is the work clearly and accurately presented and does it cite the current literature?**
Yes

**Is the study design appropriate and is the work technically sound?**
Yes

**Are sufficient details of methods and analysis provided to allow replication by others?**
Yes

**If applicable, is the statistical analysis and its interpretation appropriate?**
Partly

**Are all the source data underlying the results available to ensure full reproducibility?**
Yes

**Are the conclusions drawn adequately supported by the results?**
Yes

***Competing Interests:*** No competing interests were disclosed.

***Reviewer Expertise:*** IoT, Fog Computing, Cloud Computing, ICT4D

**I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.**

Author Response 10 Feb 2024

**Vusumuzi Maphosa**

Developed countries have developed effective cybersecurity frameworks and policies to strengthen operations, raise awareness and support training programmes (Russell et al., 2017). Countries such as the United States of America, Australia, Canada and South Africa use cybersecurity to secure and fortify critical infrastructure which drives socioeconomic development (Catota et al., 2019). Developing countries lag in the adoption of cybersecurity despite the unprecedented adoption of ICTs over the last two decades. Only 11 African countries have cybersecurity policies (Kshetri, 2019). Kabanda (2019) noted that cybersecurity systems in Africa are underdeveloped due to limited infrastructure, lack of funding, inadequate policies and legislation, lack of education and awareness, and limited reporting and data-sharing platforms.

In Zimbabwe, not much has been done in terms of cultivating a culture of cyber security and combating cybercrimes. Zimbabwe has a massive shortage of cybersecurity specialists and this is compounded by the lack of frameworks and policies to drive national implementation programmes. Kabanda (2019) notes in Zimbabwe, cybersecurity is regarded as an afterthought and is not part of the core business strategies and this is worsened by the unprecedented brain drain of skilled cybersecurity personnel. Zimbabwe faces challenges such as a lack of programmes and opportunities to equip the general public with skills, knowledge and awareness to fight cybercrime (Mutunhu et al., 2022). The Cyber Security and Data Protection Bill promulgation is a critical step in fighting cybercrime, but it has been widely criticised and viewed as a tool for the State to obstruct civil society, and the media in the fight against corruption (Transparency International, 2020). There is a need to include non-state actors in the development of the Bill.

Zimbabwe mobile data prices have been decreasing over the past two decades from USD180.00 per giga byte in 2010 to USD15.50 in 2020 (POTRAZ, 2021).

**Recommendations**

More awareness and education are required for cyberspace users. A cybersecurity culture should be developed in the early stages of schooling such as at the primary school level.
There should be a deliberate effort to grow cybersecurity skills which are extremely important to the financial services sector and are in short supply due to brain drain.
The government and the private sector should partner to set up Computer Emergency Response Teams for the financial services sector and other sectors.
The cybersecurity bill should be flexible to allow for continuous review by state and non-state actors and align with the dynamic threat levels.
Tax rebates on cybersecurity equipment are required to ensure that organisations can afford basic cybersecurity equipment.

**Works Cited**

Catota, F.E; Morgan, M.G; Sicker, D.C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. 1–19. DOI:10.1093/cybsec/tyz001
Kabanda, G. (2019). A Bayesian Network Model for a Zimbabwean Cybersecurity System. *Orient. J. Comp. Sci. & Technol., 12*(4), 147-167.
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** Proceedings of the International Conference on Industrial Engineering and Operations Management, Nsukka, Nigeria
Russell, J.D; Weems, C.F; Ahmed, I; Richard III, G. (2017). Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. J Cyber Secur Technol. 1 (3-4), 163-174.
POTRAZ. (2021). Mobile data prices in Zimbabwe. cyber behaviour: https://t3n9sm.c2.acecdn.net/wp-content/uploads/2021/02/POTRAZ-Press-Statement-Mobile-Data-Prices-in-Zim-Final.pdf, Harare, Zimbabwe.
Transparency International. (2020). Zimbabwe: Cyber Security and Data Protection Bill would restrict anti-corruption watchdogs. https://www.transparency.org/en/press/zimbabwe-cyber-security-and-data-protection-bill-would-restrict-anti-corruption-watchdogs-1

***Competing Interests:*** No competing interests were disclosed.