BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

AN ANALYSIS OF THE IMPACTS OF CYBERCRIME ON THE PERFORMANCE OF FINANCIAL INSTITUTIONS DOMICILED IN HARARE

KUDAKWASHE Z MANHANDO

(B223369B)

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE BACHELOR OF COMMERCE HONOURS DEGREE IN FINANCIAL INTELLIGENCE OF BINDURA UNIVERSITY OF SCIENCE EDUCATION. FACULTY OF COMMERCE.

YEAR: JUNE 2026

RELEASE FORM

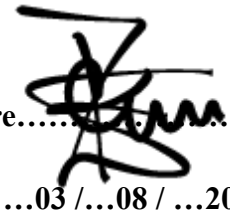
NAME OF AUTHOR: **KUDAKWASHE Z MANHANDO**

STUDENT NUMBER: **B223369B**

DISSERTATION TITLE: AN ANALYSIS OF THE IMPACTS OF CYBERCRIME ON THE PERFORMANCE OF FINANCIAL INSTITUTIONS DOMICILED IN HARARE

DEGREE PROGRAM: **Bachelor of Commerce Honors Degree in financial intelligence**

DECLARATION: The project is my original work and it has not been presented or published for examination in any other university. This project may not be reproduced without approval of Bindura University of Science Education.



Signature…….

Date **…03 /…08 / …2026…….**

KUDAKWASHE Z MANHANDO (B223369B)

Physical Address: 2060 SUNSET LANE ASPINDALE PARK

Cell Phone Number: +263 777 983 517

Email: zaynmanando@gmail.com

APPROVAL FORM

TITLE: **:** AN ANALYSIS OF THE IMPACTS OF CYBERCRIME ON THE PERFORMANCE OF FINANCIAL INSTITUTIONS DOMICILED IN HARARE

1. TO BE COMPLETED BY THE STUDENT:

   I certify that this dissertation meets the preparation guidelines as presented in the Faculty Guide and instructions for typing dissertations.

   …….. …9…../……08../……2026……

   (Signature of Student) (Date)

2. TO BE COMPLETED BY THE SUPERVISOR

   This dissertation is suitable for submission to the Faculty and should be checked for conformity with the Faculty guidelines.

   ……. 09./…08/…2026

   (Signature of Supervisor) (Date)

3. TO BE COMPLETED BY THE CHAIRPERSON OF THE DEPARTMENT

   I certify to the best of my knowledge that the required procedures have been followed and the preparation criterion has been met for this dissertation.

   …… …26…../…….09/……26

(Signature of Chairperson) (Date)

DEDICATION

I would like to dedicate this research study to my mom her unconditional support and unwavering belief in my academic journey made it possible that I was able to finish this study. Not forgetting the almighty God for the wisdom and knowledge that he has given me to undergo this research

ACKNOWLEDGEMENTS

First and foremost, I thank God for his grace, strength and guidance throughout this study. I also want to express my gratitude to my supervisor, Mr. E Maravanyika for his time, effort, patience, and direction in helping me finish this job on time. Although I was the student who put together the research project, I was just a vessel who have his name on the cover page. I am incredibly grateful to everyone who contributed to this shared success. Sincere gratitude to my family and friends for the moral, material, and social support they provided me with while I was conducting my project research.

I am also indebted to the department of intelligence and all the lectures who played part in my academic journey. Their cooperation and assistance was a pinnacle for my success.

Above all, I give praise to God and His word, which is the foundation of all reality and hope.

I'm forever grateful.

ABSTRACT

The rapid digitalisation of Zimbabwe's banking sector, through online banking, mobile banking and other ICT-enabled financial services, has improved efficiency and access to financial services but has also exposed financial-sector institutions to growing cybercrime risk. This study examined the impact of cybercrime on the performance of financial-sector institutions in the Harare Central Business District, with specific objectives to assess the link between ICT adoption and cybercrime risk, identify the most prevalent forms of cybercrime, evaluate their effect on operational and financial performance, and recommend strategies for strengthening cyber security resilience.

A descriptive survey design using a mixed-methods approach was adopted, combining questionnaires and interviews. Data were collected from 15 participants drawn from the ICT, risk-control, accounting and compliance departments of four financial-sector institutions, as well as bank customers, with an 80% response rate. Findings revealed that the overwhelming majority of participants had adopted technology-based banking systems and perceived a strong link between ICT adoption and cybercrime exposure. Phishing and digitally enabled fraud emerged as the most prevalent forms of cybercrime, followed by insider-related threats, while malware attacks were comparatively less common. Monetary loss was identified as the most significant performance impact, alongside reputational damage, reduced operational efficiency and erosion of client trust. Although institutions had adopted cyber security measures such as firewalls, access controls and awareness training, gaps remained in threat detection, staff awareness and consistent monitoring.

The study concludes that technological advancement and cybercrime risk are closely interdependent, and that effective cyber security requires combining technological controls with sustained staff training and regulatory compliance. Recommendations are made for financial institutions, regulators, customers and future researchers to strengthen cyber resilience in Zimbabwe's banking sector.

LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation/Acronym	Meaning
AI	Artificial Intelligence
ATM	Automated Teller Machine
ATMs	Automated Teller Machines
CABS	Central African Building Society
CBD	Central Business District
COVID-19	Coronavirus Disease 2019
ICSPA	International Cyber Security Protection Alliance
ICT	Information and Communication Technology
ICTs	Information and Communication Technologies
IT	Information Technology
KPMG	Klynveld Peat Marwick Goerdeler (KPMG International)
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
RBZ	Reserve Bank of Zimbabwe
SIM	Subscriber Identity Module
TTC	The Training Camp (Source cited in Vishing literature)
ZIPIT	Zimbabwe Instant Payment Interchange Technology
ZOL	Zimbabwe Online

Abbreviation/Acronym	Meaning
ZRP	Zimbabwe Republic Police

Table of Contents

CHAPTER 11
1.0 INTRODUCTION1
1.1 Background of the Study1
1.2 Problem Statement.3
1.3 Aim of the Study4
Specific Objectives:4
1.4 Research Questions4
1.5 Significance of the Study5
To the researcher:5
To Bindura University:5
To the financial sector:5
To policymakers and regulators:5
To customers and the general public5
1.6 Assumptions5
1.7 Delimitations of the Study6
1.8 Limitations of the Study6
1.8.2 Under-reporting of Cybercrime Incidents7
1.8.3 Financial and Resource Constraints7
1.8.4 Institutional Bureaucracy7
1.8.5 Large population and sample size7
1.9 Chapter Summary8
CHAPTER 29
2.0 LITERATURE REVIEW9
2.1 Conceptual Framework9
2.1.1 The Concept of Banking Technology9
2.1.2 Cyberspace10
2.1.3 Forms of Electronic Banking Provided by Financial Institutions10
2.1.3.1 Internet Banking [online banking]10
2.1.3.2 Mobile Banking11
2.1.3.3 Smart Cards11
2.1.3.4 Credit Cards11
2.1.3.5 Debit Cards12
2.1.4 Cybercrime12
2.1.5 The Nature of Cybercrimes13
2.1.5.1 Electronic Card Fraud13
2.1.5.2 Phishing13
2.1.5.3 Vishing14
2.1.5.4 Malware Attacks14

2.1.5.5 Hacking14
2.1.6 Impact of Cybercrime on the Performance of Financial Institutions15
Productivity Loss15
Direct Financial Losses15
Increased IT and Security Costs16
2.1.7 Impact of Technology on Financial Institutions16
Revenue Generation16
Improved Efficiency17
2.2 Theoretical Literature17
2.2.1 Routine Activity Theory17
2.2.2 Space Transition Theory18
2.2.3 Fraud Theory19
2.3 Empirical Review20
Singh and Singh (2019)20
Akinbowale et al. (2020)20
Mugari et al. (2016)20
Boateng et al. (2011)21
Frank and Odunayo (2013)22
2.4 Summary of Previous Studies and Identification of the Research Gap22
2.5 Chapter Summary24
Chapter 325
3.0 Introduction25
3.1 Research Design25
3.1.1 Descriptive Research Design26
3.1.2 Justification of the Research Design26
Limitations of the Design27
3.2 Population of the Study27
3.3 Sample Population27
3.4 Sampling Techniques28
3.4.1 Stratified Random Sampling28
3.4.2 Convenience Sampling28
3.5 Research Instruments28
3.5.1 Questionnaires29
Advantages of Questionnaires29
Disadvantages of Questionnaires29
3.5.2 Interviews30
Advantages of Interviews30
Disadvantages of Interviews30
3.6 Data Collection Procedures30

3.7 Data Presentation and Analysis31
3.7.1 Quantitative Data Analysis31
3.7.2 Qualitative Data Analysis31
3.8 Ethical Considerations31
3.9 Summary31
CHAPTER FOUR32
DATA PRESENTATION, ANALYSIS AND DISCUSSION32
4.0 Introduction32
4.1 Response Rate32
Table 4.1 Questionnaire Response Rate32
4.1.2Demographic Characteristics of Respondents33
4.2 Gender of Respondents33
fig 4.2.1: Gender of Respondents**Error! Bookmark not defined.**
4.2.3Age Group of Respondents33
Table 4.2.3 Age Group of Respondents34
4.3 Level of Education34
fig 4.3: Highest Level of Education**Error! Bookmark not defined.**
4.4 Work experience35
Fig 4.4: Work Experience35
4.5 ICT Adoption and Its Contribution to Cybercrime Risk35
4.5.1 Adoption of Digital Banking Technologies35
Table 4.5.1 Adoption of Digital Banking Technologies36
4.6 Digital Technologies used36
4.7 Link Between ICT Adoption and Cybercrime Risk37
Table 4.7 ICT Adoption Contributes to Cybercrime Risk37
Table 4.7.1 Digital Banking–Cybersecurity Risk Relationship**Error! Bookmark not defined.**
4.8 Prevalent Forms of Cybercrime Affecting Financial Institutions38
Fig 4.8 Prevalence of Cybercrime by Type39
4.9 Interviews40
4.9.1 Impact of Cybercrime on Operational and Financial Performance41
Table 4.9.1 Impact of Cybercrime on Performance Area41
4.10 Impacts of cyber crime41
4.10.1Financial loss41
4.10.2 Institutional reputation41
4.10.3 Operational efficiency42
4.11Cybersecurity Strategies Adopted and Their Effectiveness42
4.11.1 Cybersecurity Awareness Training42
Table 4.11.1: Provision of Cybersecurity Awareness Training42
Table 4.11.2: Cybersecurity Measures42

4.12 Effectiveness of Cybersecurity Measures43
graph 4.12: Effectiveness of Cybersecurity Measures44
4.13 Resource Allocation and Incident Reporting44
Table 4.13: Resource Allocation and Formal Incident Reporting44
4.14 Regulatory Compliance45
4.14.1 Respondents Recommendations for Reducing Cybercrime45
Table 4.14.1: Themes in Respondent Recommendations45
4.15 Discussion of Findings47
4.16 Chapter Summary48
CHAPTER FIVE49
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS49
5.0 Introduction49
5.1 Summary of the Study49
5.2 Conclusions50
5.2.1 ICT Adoption and Cybercrime Risk50
5.2.2 Prevalent Forms of Cybercrime50
5.2.3 Impact of Cybercrime on Institutional Performance50
5.2.4 Cybersecurity Preparedness51
5.3 Recommendations51
5.3.1 Recommendations for Financial Institutions51
5.3.2 Recommendations for Regulatory Authorities51
5.3.3 Recommendations for Customers52
5.3.4 Recommendations for Future Researchers52
5.4 Chapter Summary52

CHAPTER 1

1.0 INTRODUCTION

In today's fast-changing financial services landscape, technology innovation and increasing digital connectivity have become the norm. The adoption of digitally enabled banking systems, banking channels through mobile systems, internet-based payment mechanisms and digital financial services has improved the operational efficiency of the banking sector, made banking more convenient for customers and extended access to formal financial services; although these technological advances have benefited the banking sector, they have also introduced new vulnerabilities that leave financial-sector institutions and clients increasingly vulnerable to cyber threats.

The banking sector in Zimbabwe has undergone significant changes over the last two decades in terms of technology. Digital channels are gaining traction in the financial services sector, particularly among commercial banks, building societies, microfinance organisations and mobile money operators, to enable faster and more convenient financial services. This shift to electronic banking was accelerated when cash was scarce and reinforced by the covid-19 pandemic when remote financial services were even more important.

While digitalisation offers a number of advantages, the increased reliance on ICT systems has also led to an increased vulnerability to cyber related crime. New threats to financial-sector institutions include phishing, ID theft fraud, SIM-swap fraud, hacking, malware-based attacks, unauthorised system access, and electronic funds theft. These cyber threats have caused financial losses, disruption of regular business operations, harm to institutional reputation and lost client confidence in the banking sector.

The present study aimed to assess the influence of cyber-related crime on the performance of the financial-sector institutions in Zimbabwe with a specific focus on financial-sector institutions in the Harare Central Business District (CBD). The background of the study, the problem statement, the research objectives, the research questions, the significance of the study, the underlying assumptions, the scope limitation and the study constraints are presented in this chapter.

1.1 Background of the Study

The compatibility of technology and banking goes back a number of decades. Financial-sector institutions have always been adopting technologies to enhance service delivery, improve efficiency in operations and customer relationship. Within the Zimbabwean setting, the adoption of banking technology developed into more noticeable in the early 1990s when Standard Chartered Bank and the Central African Building Society (CABS) implemented automated teller machines (Atm machines)

in major urban centres. Dube (2009) states that the launch of Atm machines was one of the early significant strides in Zimbabwe's banking technology scene.

The financial sector has since then experienced significant technological change in Zimbabwe. Along with the traditional banking services, financial-sector institutions have gone beyond and have also introduced online banking, mobile banking applications, real-time gross settlement mechanisms, ZIPIT transfers, point-of-sale transactions, biometric verification systems, and digital payment channels. According to Gono (2012), nearly all banks in Zimbabwe have adopted electronic banking technologies as a strategy to stay competitive and enhance service provision.

The economic environment in Zimbabwe has also played a great role in the development of electronic banking. The financial crunch experienced from 2016 to 2020 compelled many consumers and businesses to heavily depend on mobile money platforms and electronic payment systems. The COVID-19 pandemic further contributed to the adoption of digital financial services, as the lockdowns and social distancing measures have increased reliance on online financial transactions, while physical banking operations have been curtailed.

With the growth of electronic banking, the threats related to cyber also increased. Zimbabwe's internet penetration continued its steady growth by 2025, with newer internet networks like Starlink also becoming available, according to the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). Increased Internet connectivity and smartphone usage has opened up a greater arena for cybercriminal activity against financial-sector institutions and clients.

Cyber related crime has therefore emerged as a significant problem in the financial sector in Zimbabwe. Financial-sector institutions are subject to growing threats in the cyber sphere, including phishing fraud, SIM-swap fraud, malware attacks, identity theft fraud, electronic funds theft, and access to banking systems. These cyber risks have contributed to monetary losses, disruption of service, increased spending on cyber security, and reputational harm to institutions in the banking sector.

Cyber related crime has become one of the fastest-growing threats to economic and financial stability internationally. Financial-sector institutions are especially susceptible since they manage sensitive information from their customers and process huge quantities of electronic transactions each day. According to the international cyber security reports, financial-sector institutions are still under attack by cyber activity, both in formulated and developing economies.

There have also been significant increases in cyber incidents impacting the financial industry in other countries throughout Africa, including South Africa, Kenya, Nigeria, and Zimbabwe. In the Zimbabwean context, the Cyber-related crime Unit of the Zimbabwe Republic Police (ZRP) has

indicated that the number of incidents related to phishing, unauthorised access to mobile banking, identity related fraud, and SIM-swap fraud are on the increase.

Victimization of cybercrime isn't just a financial affair. Cyber incidents can cause loss of clients' trust, affect banking processes, escalate the legal and compliance costs of financial institutions, and require financial institutions to invest heavily in cyber security. Economic instability has already put some strain on public confidence in the financial sector in Zimbabwe, and cyber events are likely to further erode confidence in digital financial systems.

To mitigate these threats, the Reserve Bank of Zimbabwe (RBZ) has issued cyber security guidelines and compliance requirements which aim at enhancing the cyber security resilience capacity of financial-sector institutions. While such measures have been put in place, multi-factor authentications, reporting of cyber security incidents, risk-control frameworks and continuous monitoring of the digital mechanisms remain conditions, but the financial sector in Zimbabwe still faces cyber related crime.

With increasing reliance on ICTs, and the increase in cyber-related incidents, there is a need for more research to understand the impact of cyber-related crime on the performance of financial-sector institutions in Zimbabwe. The current investigation aims to evaluate the effects of cyber-related crime on the daily business and earnings of financial institutions and to identify potential actions to mitigate cyber-related risks.

1.2 Problem Statement.

The rapid adoption of digital banking technologies in Zimbabwe has transformed financial institutions through the use of internet banking, mobile banking platforms, electronic payment systems, and real-time digital transactions. While these technological developments have improved efficiency, financial inclusion, and customer convenience, they have also created new opportunities for cybercrime and electronic fraud.

Zimbabwean financial institutions continue to experience increasing cases of phishing attacks, SIM-swap fraud, identity theft, malware attacks, unauthorised access to banking systems, and electronic fund theft. These cyber-related crimes have resulted in financial losses, operational disruptions, reputational damage, increased cybersecurity expenditure, and declining customer confidence in digital banking systems.

Although financial institutions and regulators such as the Reserve Bank of Zimbabwe have introduced cybersecurity frameworks and risk management measures, cybercrime incidents continue to rise within Zimbabwe’s financial sector. Despite the growing prevalence of cybercrime, there is still limited empirical research specifically examining how cybercrime affects the operational and

financial performance of financial institutions in Zimbabwe, particularly within the Harare Central Business District (CBD).

Therefore, the study seeks to assess the impact of cybercrime on the performance of financial institutions in Zimbabwe and to identify strategies that may strengthen cybersecurity resilience within the banking sector.

1.3 Aim of the Study

- The central purpose of this research is to appraise the impact of cyber-related crime on the performance of financial-sector institutions in Zimbabwe..

Specific Objectives:

- To analyse how heightened use of ICT in Zimbabwe's banking industry has played a part in risks linked to cyber offending affecting performance of institutions.
- To identify the most prevalent forms of cybercrime affecting financial institutions.
- To evaluate the impact of cybercrime on the operational and financial performance of financial institutions.
- To recommend strategies for reducing cybercrime in Zimbabwe's financial sector.

1.4 Research Questions

The study aimed to answer the following questions;

- How has ICT development influenced the rise of cybercrime in Zimbabwe's banking sector?
- What are the most common forms of cybercrime affecting financial institutions?
- What impact does cybercrime have on the operational and financial performance of financial institutions?
- What measures can financial-sector institutions and regulatory authorities adopt to reduce cyber-related crime and strengthen cybersecurity resilience in Zimbabwe's banking industry?

1.5 Significance of the Study

To the researcher:

The present study offers an investigative experience in academic research and develops analytical skills, critical thinking and the ability to solve problems. The present research also contributes to the body of knowledge of the investigator on the cyber security challenges in the financial sector in Zimbabwe.

To Bindura University:

- The current research contributes to the existing knowledge base of cyber-related crime and digital finance in Zimbabwe and could be used as a guide for future researchers.
- The evidence also can be helpful to future researchers in their studies concerning cyber security, financial technology, and the performance of the banking sector

To the financial sector:

- The findings from the current research can help financial-sector institutions to enhance cyber security frameworks, aid in the development of risk-control systems, and create more efficient cyber-related crime prevention strategies. The ongoing research could also help organisations to understand the operating and financial consequences of cyber crime.

To policymakers and regulators:

- The findings of the current research can help support the creation of more effective cyber security policies and regulatory action.
- This research findings on the nature and extent of cyber related offences in the Zimbabwean banking sector can provide guidance in developing and fine-tuning the regulatory, supervisory and reporting guidelines for cyber security in the banking sector.

To customers and the general public

The present study can raise awareness on potential threats of cyber-offence to electronic banking channels and can stimulate the users of electronic financial services to enhance the security of electronic financial services.

1.6 Assumptions

The following assumptions were made in conducting this study:

More digitisation in banking is making the sector more vulnerable to cybercrime.

The operational and the financial performance of financial institutions is impacted by cybercrime in a measurable way.

The respondents would give suitable and appropriate information needed to the study.

1.7 Delimitations of the Study

Scope boundaries are the intentional boundaries and scope restrictions set by the investigator to maintain a focused and manageable research.

The present study concentrated on financial institutions in Harare as key operational, compliance and cyber security functions are centralised in these institutions providing better access to relevant data. The focus of the current research was to specifically examine the impact of cyber-related crime on the performance of financial-sector institutions in Harare.

The period of the current research covered 2022 – 2025. The selection of this timeframe was driven not only by a significant rise in both the number of electronic banking transactions being used and the reported incidents of cyber-related banking frauds, but also because it coincided with a period of rapid electronic banking uptake in Zimbabwe, after the onset of the COVID-19 pandemic.

The current research focused on the participants in three departments (IT, compliance, and risk-control) of selected financial-sector institutions. The selected bank clients were also included in the research participants to provide the views on customer experience and the awareness of cyber security.

1.8 Limitations of the Study

There are several limitations of this research, which are admittedly addressed in designing this research. These constraints, which relate to factors beyond the investigator's direct control may affect the depth of the results. It is important to take these restrictions into account when considering the findings from the research.

1.8.1 Confidentiality and Disclosure Constraints

The issue of cyber crime is very delicate for financial-sector institutions. Banks are reluctant to give any granular detail of their protection failures, fraud losses or system vulnerabilities because such details could damage their reputation, lead to regulatory bias and provide intelligence to potential threats. This may have resulted in some participants not providing data, and some institutional data which would have supported the base of the research was not provided. To overcome this, the

investigator ensured that the anonymity and confidentiality of all participants and organisations was guaranteed.

1.8.2 Under-reporting of Cybercrime Incidents

Official statistics underestimate the incidence of cyber-related crime in the world generally is a well-recognised shortcoming of research on cyber-related crime. The under-reporting issue is prevalent in the Zimbabwean context. Few people and organizations voluntarily disclose cyber-related incidents to the authorities, or do so because they lack confidence in the regulatory system, fear reputational damage, lack knowledge about the likelihood of recovery or simply don't know that there are formal mechanisms to help with disclosure. This will imply that official sources of cybercrime data, like the ZRP Cyber-related crime Unit and RBZ, may not be a complete reflection of the actual size of the cybercrime problem. This is recognised in the present research and care is taken in interpreting the official statistics alone.

1.8.3 Financial and Resource Constraints

The investigator was constrained by financial resources to limit the geographical extent of data collection and to limit the amount of primary data to be collected by the investigator. There were issues with transportation costs, printing costs and access to some academic and institutional databases. They were controlled by careful prioritization of data collection activities, with the use of digital collection of data instruments where possible and by tapping into the financial resources of family members. In spite of these limitations, the investigator feels that the information obtained has been adequate for analysis and valid conclusions.

1.8.4 Institutional Bureaucracy

Senior staff who could provide informed responses to the research's queries and have the necessary expertise and authority to do so were hard to come by, due to multiple layers of management control in Zimbabwean banks and related organisations. Sometimes, formal information requests had to be processed multiple times through various approval steps to receive the information; this caused delays in the collection of information process. This difficulty was overcome by the investigator by sending institutional heads formal introductory letters beforehand and by following up with the institutional heads on a consistent basis.

1.8.5 Large population and sample size

Given the relatively large number of financial-sector institutions in the current research population, the investigator had limited time and resources to gather all available information for each of these

institutions. The researcher chose Harare financial sector institutions as a representative sample of selected financial sector institutions to overcome this limitation.

1.9 Chapter Summary

This chapter presented an introduction to the research, beginning with the background of the cyber-related crime in Zimbabwe's financial sector, and the increased linkage of technology-based banking systems and cyber-related threats. The chapter highlighted that technology-enabled transformation has enhanced efficiency, access and access to financial services but brought a greater vulnerability to financial sector institutions in the context of cybercrime.

The problem statement, research aims, research questions, significance of the research, underlying assumptions, scope boundaries and constraints of the research were also outlined in the chapter. The present study aims to evaluate the effects of cyber-related crime on the performance of financial sector institutions in Zimbabwe and identify measures that can enhance the cyber security resiliency of financial institutions in Zimbabwe.

The next chapter summarizes some key literature and theoretical backgrounds on relevant aspects of cyber-related crime, electronic banking and the functioning of financial-sector institutions.

CHAPTER 2

2.0 LITERATURE REVIEW

The literature reviewed in this chapter describes the nature of cybercrime, the effectiveness of financial-sector institutions, and in Zimbabwe the banking sector. It presents conceptual definition, theoretical approaches and empirical research, and then defines gaps which are filled by the current research. Throughout the chapter, the discussion goes beyond merely summarizing the previous research and addresses the conflicting viewpoints in this research, and the meaning of the disagreement to the understanding of cybercrime in Zimbabwe's modern day electronic banking landscape.

2.1 Conceptual Framework

2.1.1 The Concept of Banking Technology

In the banking sector, banking technology is the use of digital and electronic technologies for financial transactions, financial services delivery and financial-sector operations. Innovations like smart cards, mobile banking, telephone banking and online banking revolutionized the way customers interacted with the banks, marking the initial phases of digital banking. These developments led to what is commonly referred to as electronic or online banking which enables the clients to carry out banking transactions without going to the banking halls via secure digital mediums (Aysan, 2014).

In Zimbabwe, the early adoption of digitally facilitated banking systems were hampered by lack of infrastructure, high internet costs and low trust for digital platforms but the banking system has undergone massive transformation over the last 20 years. Between 2016 and 2020, the need for cash was a constant challenge, forcing financial-sector institutions and their clients to adopt electronic payment systems. Mobile money payments in Zimbabwe were more than physical cash payments in terms of volume transactions by 2019, an indication of structural shift in the manner of financial services usage (Reserve Bank of Zimbabwe, 2020).

This was reinforced by the COVID-19 pandemic. This is consistent with the experience in Zimbabwe, where Auer et al (2020) estimated that the pandemic led to three to five years of premature digital financial uptake in developing economies. The attack surface for cybercriminals, though, grew in proportion to the number of payments that were conducted online. This current investigation, then, looks at the intersection of the advantages of banking technology and the dangers of increasing cyber security threats.

2.1.2 Cyberspace

As Gibson (1984) originally describes Cyberspace it is a networked environment of inter connected computers where data is stored, processed and communicated. In the bank setting, cyberspace is the setting in which the information of clients, financial records, electronic payments, and communication systems of the institutions are processed. It's now become the backbone for contemporary banking.

Mobile network infrastructure upgrades and increased smartphone penetration in Zimbabwe have fuelled growth in the country's progressive extension of cyberspace.Improvement in mobile network infrastructure and increased smartphone penetration in Zimbabwe has contributed to its progressive advancement of cyberspace. Mobile data subscription grew significantly in Zimbabwe by mid-2024, indicating a significant improvement in connectivity compared to 2018 data which pointed to opportunities for access to formal financial services, but also exposed individuals to cybercriminal activities (POTRAZ, 2024). The Reserve Bank of Zimbabwe, in its annual report (2024), highlighted that increased digital connectivity has been linked to increased numbers of cyber threats to financial-sector institutions. As mentioned in Chapter 1, the digital penetration in Zimbabwe has been on the rise, with smartphones gaining ground and their use of the internet expanding, which has introduced more cyber-related threats to Zimbabwe.

2.1.3 Forms of Electronic Banking Provided by Financial Institutions

2.1.3.1 Internet Banking [online banking]

Yibin (2003) defines online banking as the delivery of banking products/services via the Internet. In addition, Chang and Hamid (2010) stated that the online banking helps the client to conduct financial transactions electronically without having to go to banks and other financial institutions.

In Zimbabwe, growth in online banking was enabled by the increase in broadband connectivity through providers like NetOne, ZOL and Econet Wireless. By 2025, POTRAZ said that around 63 percent of the target group was internet users, which means there has been a significant user base for online banking service.

Online banking has brought convenience, efficiency and access to formal financial services to most commercial banks in Zimbabwe, but according to recent studies, increased digital connectivity has also increased the cyber security threat to financial-sector institutions. The Reserve Bank of Zimbabwe states that as digital financial services continueto grow, so have the phishing schemes, malware attacks, unauthorised access to systems and online fraud. The consequences of such cyber threats can include disruption of normal activities, financial losses, harm to the reputation of the institution and loss of trust by clients in electronic banking services.

2.1.3.2 Mobile Banking

Mobile banking is defined by Arcand et al. (2017) as a service that allows clients to make banking transactions by mobile devices without the need to visit banks and other banking related organizations. Okiro (2013) also defines mobile banking as the use of mobile phones and internet-enabled devices to provide financial services.

Mobile banking has seen massive growth in Zimbabwe as a result of increased mobile phone penetration and growth of mobile money services. Clients can now make transfers, buy airtime, pay their utility bills and do all sorts of financial transactions from their mobile phones.

In Zimbabwe, POTRAZ noted a significant rise in WhatsApp related cyber related crime and digital impersonation scams involving users of financial services in 2024. This means that the mobile banking option helps to make banking more accessible and convenient, but it also raises cyber security concerns with the potential to impact the institutional credibility and client confidence. According to the Financial Intelligence Unit of Zimbabwe (2023), the number of SIM swaps rose from 2021 to 2023, highlighting the growing cyber security threats associated with mobile banking despite its accessibility and convenience.

2.1.3.3 Smart Cards

In Shuabi's (2010) definition, a smart card is a plastic card that is fitted with an embedded integrated circuit to securely store and process information. Amedu (2005) state that smart cards are used for electronic financial transactions and can be operated as debit or credit cards.

Debit and smart cards, which are widely used through the Zimbabwean network of Zimswitch, are also in the cybercriminal spotlight. Atm skimming and point-of-sale skimming remains a significant cyber security risk (Reserve Bank of Zimbabwe, 2024).

2.1.3.4 Credit Cards

A credit card is a payment card issued by financial-sector institutions, giving users the ability to borrow money for purchases or payments (Deitel et al., 2001). It is also explained by Essinger (1999) that credit cards are the medium by which clients can use banking services electronically through the use of authorised payment systems.

Although credit card use in Zimbabwe is limited, this has also limited the prevalence of some forms of credit card fraud; however, as credit card usage continues to expand, so do the likelihoods of exposures to associated cyber-related frauds like card not present, account takeover, and ID-related frauds. As the banking systems in Zimbabwe become increasingly connected and integrated with the international systems, the users of the cards face a higher risk of falling victim to a cyber network targeting financial card data on a large scale.

2.1.3.5 Debit Cards

According to Shuabi (2010) a debit card is defined as a plastic payment card that gives clients direct electronic access to their bank accounts. According to Nwaolisa and Kasie (2012), debit card transactions immediately take money out of the account of the customer.

The Zimswitch network supports integration between the debit cards issued by various commercial banks, allowing clients to transact on various platforms, although this has provided the convenience, it has also created extra vulnerability. Mugari et al. (2016) found debit card fraud to be one of the most commonly reported categories of cyber-related crimes by the financial-sector institutions in Zimbabwe, with the Reserve Bank of Zimbabwe (2024) indicating that debit card fraud continues to rise even as financial institutions have enhanced their protection measures.

2.1.4 Cybercrime

Cyber-related crime is criminal activity that uses computers, digital mechanisms or internet-based technologies. Sandywell (2010) defines cyber-related crime as 'crime committed through the use of the internet and virtual environments. The Fraud Advisory Panel (2009) also defines cyber related crime as being made through hacking, phishing, using malware, cyber extortion, identity related fraud or illegal access to a computer system.

In Zimbabwe, cybercrime has become a major issue in the financial services sector as banks increasingly rely on digitally facilitated financial transactions and banking systems. Weak technological protection and low level of cyber security awareness initially contributed to vulnerabilities in Zimbabwe's financial sector in relation with cyber related crime (Kabanda, 2012). Although these definitions do not exhaustively describe the complexity of today's cybercrime, they do illustrate the broad scope of such crimes against financial-sector institutions and financial-sector clients, as mentioned in Chapter 1.

The Cyber and Data Protection Act of 2021 was a significant piece of legislation in Zimbabwe that established a legal framework for the prosecution of cyber crimes and the regulation of the protection of financial-sector institutions' personal data. The Reserve Bank of Zimbabwe (2024), noted that the Act provided an improved regulatory environment, but that some institutions lacked capacity in cyber security and also faced difficulties in enforcing the law. The disconnect between the written words of law and what actually occurs when things go wrong is a common pattern in the body of literature on cyber crimes governance in the developing economies.

2.1.5 The Nature of Cybercrimes

2.1.5.1 Electronic Card Fraud

The Reserve Bank of Zimbabwe (2024) identifies electronic card fraud as one of the main categories of cybercrime impacting financial-sector institutions. Card fraud, also known as electronic card fraud, occurs when criminals illegally acquire card information and utilise it for their unauthorised transactions.

Burns and Stanley (2002) define a number of types of card fraud: fake card fraud, lost card fraud, stolen-card card fraud and application-based fraud. Skimming devices and compromised registers are common ways that cybercriminals steal customer card data.

The financial damage caused by electronic card fraud is not just the loss of the value of the unauthorized transactions. For example, according to Akinbowale et al. (2020) the indirect costs of this fraud can often outweigh the direct losses from the fraud itself, making electronic card fraud a significant threat to the performance of institutions. As mentioned in Chapter 1, financial-sector institutions are still suffering losses due to unauthorised transactions and fraud enabled by digital technologies.

2.1.5.2 Phishing

In the book "Phishing: Definition and Technique", by Nielsen et al (2017), phishing is defined as a "cyber-related crime technique that involves the fraudulent acquisition of sensitive information for illegal purposes. Phishing is defined as identity theft, in which a cybercriminal pretends to be a real institution and tricks a target into providing confidential information, according to Baegh (2012).

Phishing attacks are frequently perpetrated through deceptive e-mail, SMS and fake websites that look like financial services organizations. Victim is asked to provide passwords, account information, or one-time passwords. Once they have the data, the cybercriminals access customer accounts illegally.

As digital communication technology and AI tools have evolved, so have phishing schemes. In Zimbabwe's context, the revolution of online and mobile banking channels have increased clients' vulnerability to fraudulent emails, fake websites and deceptive mobile communication. In its report, the Reserve Bank of Zimbabwe noted that the financial-sector institutions remain putting in place cyber security measures and systems to identify fraud to mitigate threats to payment systems and online banking platforms as they increase. In addition to financial losses, phishing schemes can also undermine consumers' trust in digitally based banking systems and create compliance and operational expenses for financial-sector institutions.

2.1.5.3 Vishing

Vishing is a technique used in a cyber-related crime that involves the use of telephone communication or voice messaging systems to make a person reveal confidential financial information, according to TTC (2008). According to Ollman (2007) the word is derived from a mix of two words: "voice" and "phishing.

Impersonating a bank official or client service representative, the cybercriminal might ask for account information, passwords, or verification codes from the unsuspecting target. The Financial Intelligence Unit (FIU) (2023) noted an increased trend of vishing off clients of financial institutions in Zimbabwe, especially old people who might not be aware of cyber security.

2.1.5.4 Malware Attacks

According to the KPMG (2011) definition, malware is any software that harms, hacks or disrupts computer systems. Malware can be viruses, worms, Trojan horses, spyware, and ransomware.

Cybercriminals employ malware attacks to penetrate banking systems, steal client information and disrupt financial activities. Malware can be introduced through infected email attachments, malicious websites and software.

As with the rest of the financial services industry, malware attacks are evolving with the technology and digitalisation. The latest cyber security report reveals that banks and other financial institutions are investing more in building cyber security resilience, fraud identification tools and frameworks for managing cyber incidents in order to reduce disruptions to normal operations caused by its attacks. Despite these efforts, the malware attack is still a significant risk as it can impact the confidential customer data, interfere with payment systems, and undermine the performance of institutions at the cost of recovery and damage to the institutions' reputation. As described in Chapter 1, institutions in the financial sector have had to pour significant amounts of funds into their cyber security systems to reduce these risks to as low a level as possible.

2.1.5.5 Hacking

Hacking is an unlawful entry into the mechanism or database of a computer for an illegal purpose. Mugari et al. (2016) state that hackers target systems to either steal confidential information, alter the systems, or defraud the financial system.

Hacking in Cyber Laws is defined as the act of changing or using computer mechanisms in manner that is not intended. Often the financial sector's institutions have been the targets because they deal with private data of their customers and are responsible for handling a great number of electronic transactions.

There has been a growing trend of hacking activity into the financial-sector institutions and digital payment systems in Zimbabwe. The accidents have led to financial losses, service delays and reputation loss for financial institutions. Hacking currently is divided into categories according to the sophistication and objectives of the actors of the crime. Ibrahim (2022) distinguished between opportunistic hacking (hacking against the weaknesses that are known in the open) and organised attacks by cyber-related crime syndicates (when cyber-related crime syndicates target specific organisations, conduct sustained campaigns and use their resources to exploit weaknesses known to only them). The latter is a significantly more dangerous category as it could allow criminals to steal data or make fraudulent payments over a longer period of time before detection, as specific organisations may not have reported such information publicly, but the Reserve Bank of Zimbabwe (2024) reported an increase in financial-sector-related illegal access attempts from 2022 to 2024, consistent with the findings of the African Union Cyber Security Expert Group (2023) which recorded a rise in such incidents across the continent.

2.1.6 Impact of Cybercrime on the Performance of Financial Institutions

The collective and comprehensive effects on the performance of institutions brought about by cyber-related crime are the best way to understand impact. The literature identifies four main avenues by which a crime involving cyber affects the performance of institutions: productivity loss, direct monetary losses, increased security costs, and damage to the reputation of the institution.

Productivity Loss

Productivity losses are defined by McAfee (2014) as a decrease in organisational effectiveness due to cyber incidents and disruptions. Victim financial-sector institutions frequently spend more on investigations, system recovery and client support as a result of cyber-related crime, limiting the efficiency of the institution.

Cyber-attacks can also cause disruptions in usual banking activities, leading to slow payments, diminished quality of banking services for customers and possible temporary banking system shutdown.

Direct Financial Losses

Data losses that result directly from cyber-related crime involve the loss of money through fraudulent transactions, unauthorised access to the account or manipulation of the system. According to McAfee (2014), the International economy loses billions of dollars each year due to cyber-related crime, and financial sector institutions suffer disproportionately.

The Reserve Bank of Zimbabwe (RBZ) has reported the direct losses suffered by financial-sector institutions as a result of cyber-related crime, among the various annual reports of the same nature. The Reserve Bank (2024) highlighted that frauds involving digital means continued to be one of the largest contributors to unintended monetary losses of commercial banks, though the exact magnitude of the losses is not made public for reasons of supervisory confidentiality. In the Kenyan context, Njeru and Gaitho (2019) found that monetary losses caused by cybercrime could materially impact the returns on assets of the affected banks, and this serves as a helpful regional indicator for assessing the performance impact of cybercrime on Zimbabwean banks.

Increased IT and Security Costs

Financial-sector institutions have to invest more in cyber security infrastructure, system upgrades, risk-control systems, and cyber security staff in order to combat cyber-related crime.

When looking at institutions, McAfee (2014) note that they have extra costs for threat identification, system maintenance, compliance conditions, and recovery processes after cyber incidents.

The Reserve Bank of Zimbabwe (2024) highlighted that the majority of the financial-sector institutions in Zimbabwe had considerably increased their investments in cyber security due to increased cyber security threats and changing regulatory requirements as stipulated by the Cyber and Data Protection Act of 2021; this increased investment is operationally required but represents a direct cost to profitability. In a survey of African banks and related institutions by Deloitte (2023), cyber security now represents between 8 and 15 percent of the IT expenditure plans of African banks and related institutions, twofold higher than the last five years. Smaller Zimbabwean banks with restricted operating budgets are facing an excessive burden due to these expenses.

2.1.7 Impact of Technology on Financial Institutions

As noted in this discussion, much of the attention has been paid to the risks associated with banking technology, but there has also been a significant performance benefit associated with technology for financial-sector institutions. To get a balanced perspective of the relationship between technology and performance of institutions, both sides should be taken into account.

Revenue Generation

Electric banking channels can be used by financial sector institutions to gain more and more customers, to expand transactions and to attain extra income. In Zimbabwe, banks that were quick to embrace the cash shortage mobile and online banking solutions have enjoyed tangible competitive edges over those that took too long to catch up. During this period, the banks that had a well-established mobile-based banking system had better customer acquisition and customer retention,

which meant they had better revenue institutional performance compared to their competitors documented by Njanike (2021). Electronic banking has played a significant role in bringing populations who previously lacked access to formal financial services into the formal financial sector globally, and mobile banking in particular, and has proven operational benefits in times of economic uncertainty and during the Covid-19 pandemic when physical banking operations were limited.

Improved Efficiency

Banking technology allows to enhance the operational efficiency of services by decreasing the manual handling of transactions, transaction delays and channel errors (Karjaluoto et al., 2012).

In the Zimbabwe context, the implementation of instant payment mechanisms such as Real time Gross Settlement (RTGS) and Zimbabwe Inter Bank Payment and Settlement (ZIPIT) has greatly reduced the costs and timeliness of domestic payments, but as Kabanda (2021) noted, the benefits that flow from banking technology are limited unless backed by sufficient investment in cyber security. Organizations that permit cyber security to become an afterthought in their technology uptake could find an efficiency benefit that is undermined by cyber losses and disruptions.

2.2 Theoretical Literature

This present inquiry is primarily informed by the Routine Activity Framework as the main conceptual tool used to analyse the vulnerability to cyber-related crime and impact on institutions. The Space Transition Framework and the Fraud Triangle Theory are also included as additional theories to explain aspects of cyber related crime behaviour that are not covered by the Routine Activity Framework. Each of the three is a complementary and comprehensive conceptual base that is especially suitable for the analysis of cyber-related crime in the Zimbabwe's rapidly changing electronic banking environment.

2.2.1 Routine Activity Theory

Cohen and Felson (1979) created the concept of routine activity theory as an explanation for why crime happens when it does, based on the routine activities and spatial behavior of criminals and victims. The theory suggests that there are three components of committing an offence that need to be present in time and space – a motivated offender, a suitable target and the lack of a capable guardian. Importantly, the framework assumes that criminal motivation is always present in a population; that the rate of offending is not a function of increasing or decreasing motivation in the perpetrators, but instead is a function of increasing or decreasing opportunities for crime and guardianship against crime.

The framework assumes that criminals are rational and seize opportunities when they arise during various day-to-day activities. Routine Activity Framework has been a successful, long-standing, and

useful analytical tool in the study of cyber related crime. The explosive growth of internet and mobile banking in Zimbabwe has created a myriad of viable targets: millions of customers banking online in a variety of platforms that differ significantly in their security levels. There are several levels of understanding the lack of capable guardianship: at the client level (weak passwords, not knowing about cyber security, not paying attention to alerts about protection), at the institutional level (poor cyber security infrastructure, poorly staffed protection teams), at the regulatory level (restrictions to enforcement).

Paternoster (2011) adapted Routine Activity Theory for cyber-related crime, and found that it is just as powerful in cyber settings as in real settings; users who practised more online operations and less protective guardianship behaviour were much more likely to fall victim to cyber-related crime. More recently, Leukfeldt and Yar (2016) conducted a systematic review of the literature on the use of Routine Conduct Theory in the context of cyber-related crime and found that the structure was found to be a good fit for the explanation of victimisation patterns for various types of cyber-related crime, including those most relevant to banking contexts.

The current research adopts the most direct explanation of the relationship between electronic-banking expansion and increase in cyber incidents against financial institutions as its analytical framework: Routine Activity Theory. The framework also underscores the importance of institutional guardianship as a mediating link that has direct implications for the understanding of the effects of cyber security investment decisions on the performance of institutional outcomes.

With the rapid growth of online banking, mobile banking, and digital payments in Zimbabwe, as discussed in Chapter 1, there has been an increase in opportunities for cybercriminal activities. Insufficient cyber security measures, customer knowledge and inadequate digital protection practices can diminish the effectiveness of guardianship and therefore make customers more vulnerable to cyber related crime.

2.2.2 Space Transition Theory

Space Transition Theory has been developed by Jaishankar (2008) to explain criminal behaviour in cyberspace, since the existing criminology theories that were developed before the advent of the internet as a social space have not been able to explain this behaviour. The framework states that users might act differently in virtual space than in real space; the virtual space may provide anonymity, less social oversight and an opportunity for users to avoid real-life regulatory repercussions that might arise from their actions in the virtual space as they might in the real one.

The theory makes several propositions that are relevant to the current research. One, a person who is conforming in real life can become deviant through the use of the internet because this area isn't as

visible socially and held accountable by law. Second, in the modern world, criminals can move from physical to virtual space and back with ease, and can thus operate in a flexible way that is difficult for law enforcement to match. Thirdly, the lack of effective cyber deterrence, especially in countries that lack robust cyber crime laws, further facilitates cyber crime.

Space Transition Theory adds to Routine Activity Theory in the following aspects of the present research: it helps explain why the motivation to commit a cyber-related crime could be greater in digital spaces than in similar situations in the physical world; Routine Activity Theory explains systemic conditions that promote crime, while Space Transition Theory is concerned with the behavioural dynamics that bring offenders into cyber-related crime. The conditions outlined in Space Transition Theory are especially relevant in the Zimbabwean context where the enforcement of the Cyber and Data Protection Act (2021) is still in early stages and cross-border cases of cyber-related crime is difficult to prosecute.

2.2.3 Fraud Theory

Donald Cressey (1953) and then extended by Wells (2011), has developed the Fraud Triangle Theory which states that three things must happen concurrently to enable fraud to occur: Perceived opportunity, Perceived pressure and Rationalisation.

Perceived pressure would be the financial or personal pressures that inspire a person to defraud. Such pressures usually include financial concerns that stem from personal debt, unemployment or economic uncertainty, according to Wells (2011). The pressure of unemployment and financial difficulties in Zimbabwe is high and therefore the incentive to act as a victim may be high for cybercrime. This was confirmed by Rasha and Andrew (2012), who showed that (financial) hardship was an important predictor of financial fraud motivation in developing economy contexts.

Perceived opportunity is the set of circumstances that allows for the possibility of fraud, such as weak internal controls, weak monitoring systems and low cyber security awareness. Kabanda (2021) identified the opportunity conditions for cybercriminal activities occurring in Zimbabwe's financial sector as a result of technological gaps and lack of cyber security practices. The opportunity element of the Fraud Triangle is also supported by the Financial Intelligence Unit of Zimbabwe (2023) findings which indicated that organisations with lower cyber security strength had more incidences of fraud.

Rationalisation is the mechanism in which the fraudster makes sense of his or her actions to himself. Cybercriminals might tell themselves that the financial-sector institutions can withstand the losses, that there's financial injustice that's fair to them, or that there are no victims. The need to design policies with an understanding of rationalisation is heightened because interventions that enhance

perceived social harm from cyber-related crime might also affect its incidence without intervention by law enforcement.

The Fraud Triangle Theory contributes to the theoretical underpinnings of the study by explaining less directly the individual-level motivational factors that bestow a desire to commit cyber-related crime, evidenced in Routine Activity Theory and Space Shift Theory.

2.3 Empirical Review

In this section, previous research on cybercrime and financial institutions' performance is discussed.

Singh and Singh (2019)

Singh and Singh (2019) concluded that technological advancements create greater risks for cyber-related crimes compared to what most organisations can do to protect against them, leading to continued disruptions to business operations as institutions investigate and remediate crimes while maintaining regular business operations. In a study that is close to the current research in Zimbabwe, Mugari et al., 2016, reported significant disruptions to regular operations due to phishing, hacking, malware and identity related fraud in financial sector organizations in Harare. While their study is the most geographically specific in the literature, it is not applicable in the current electronic banking environment, due to its pre-2019 period of study. The International Journal of Computer Application-based (2014) noted that regulatory systems often fall behind technological developments leaving behind a continuing operational vulnerability across the financial sectors around the world.

Akinbowale et al. (2020)

Akinbowale et al. (2020) demonstrated the negative impact of cyber-related crime on banking performance in four dimensions of the Balanced Scorecard namely financial, customer, internal process, learning by showing that there is loss of money to the financial institution before the direct losses. Njeru and Gaitho (2019) reported that Kenya commercial banks faced measurable losses in return on assets after being victims of cyber-related crime, which serves as a regional benchmark on the financial results impact in Zimbabwe. A study by ICSPA (2014) of businesses in Canada revealed that businesses consistently underestimate the total cost of cyber incidents and this could be the reason why some of the institutions in Zimbabwe have not invested enough in cyber security despite the perceived threats.

Mugari et al. (2016)

Mugari et al (2016) conducted a study on cyber related crime in the financial services sector in Zimbabwe, using survey questionnaires and interview sessions from selected financial services institutions in Harare. Their

The most common forms of cyber related crime found in institutions were identified to be phishing, hacking, malware-based attack and identity related fraud. The present study reported on these incidents resulted in significant disruption of regular operations, institutional resources being directed to recovery, and the disruption of service delivery. Mugari et al. found that technological progress in financial-sector institutions has a direct positive effect on their cyber related crimes exposure and suggested that staff's training, cyber security awareness programmes, updates of anti-virus software and installation of firewall could be used as mitigating measures.

But there are some limitations in this context for the research. It has been conducted prior to Zimbabwe's hasty shift to mobile banking during the shortfall of monetary in 2016-2020 and ahead of the systemic adjustments enforced by the Cyber and Data Protection Act of 2021. Its proposals also precede the more modern developments in cyber security, like AI-powered fraud identification and zero-trust security concepts. These limitations make Mugari et al. a valuable starting point, but no longer fully capture Zimbabwe's current electronic banking landscape for the purposes of understanding cyber-related crime.

Boateng et al. (2011)

Boateng et al. (2011) carried out qualitative interview sessions with banking staff, IT experts and police officers to explore the trend of cyber related crimes in Ghana. The result they found is that cyber-related incidents in the financial sector in Ghana were on the increase, largely due to increased internet penetration and increasing digital payment systems. An interesting result was that a significant number of incidents were not reported and organisations were hesitant to publicise breaches for fear of damage to their reputation and loss of confidence if incidents were made public.

The results of the study are applicable to the Zimbabwean context in two ways. First, the under-disclosure nature observed in Ghana is similar to what the Reserve Bank of Zimbabwe (2024) has noted in its initiatives for voluntary disclosure, which are designed to address under-disclosure. Second, like Ghana, Zimbabwe's electronic banking environment is rapidly growing, while its capacity in cyber security has not been able to keep up, making the vulnerabilities identified by Boateng et al. generalizable.

The limitations of the research should be noted, however. It is qualitative and conducted more than 10 years ago, so it is based on a less complex electronic banking environment than is currently available. The forms of cyber-related crime described by Boateng et al. and the vulnerabilities of the institutions have now changed considerably, particularly since the introduction of mobile banking fraud, ransomware and organised transnational cyber-related crime networks, not as prominent in 2011 as they are now.

Frank and Odunayo (2013)

Frank and Odunayo (2013) has studied the problems of Cyber security in organisations in Nigeria with particular emphasis on the significance of insufficient cyber security practice in the vulnerability of institutions coupled with the far-reaching implications that followed the occurrence of cyber incidents. They found that key factors contributing to a high risk of cyber-related crime were poor cyber security awareness, inadequate staff training and poor information protection regimes. More importantly, the study revealed that cyber incidents caused significant damage to institutional reputation which had the potential to impact competitive positioning and client confidence, even when the impact on the client was relatively small for each incident. The current researchers suggested the following priority responses: improving cyber security awareness programmes, regular staff capacity building and protection of the institutional data systems.

The present research is important in its contribution to the current research. This is a disconnect between the view of damage to institutions' reputations surpassing "real" monetary loss as it would be measured by institutions, which is why its findings are so important. This is especially relevant in Zimbabwe's context where the financial-sector institutions' credibility is already low because of the history of economic volatility. Institutions that experience cyber security incidents that are visible will face the loss of their direct victims, but also wider confidence of their clients as Nyamwanza et al (2022) later found in the Zimbabwean banking environment.

This study has identified the following as its limitations: Nigerian focus and being an old study. Although some elements are similar, the regulatory and economic landscape in which Nigeria's banking industry functions is different from Zimbabwe's. Moreover, Frank and Odunayo didn't consider mobile banking fraud, ransomware, and AI-assisted phishing in their analysis, which has shifted significantly since 2013. What they have said on the matters of awareness and governance are still relevant, but their particular suggestions should be updated in the context of the ongoing developments of the cyber-related crime.

A review of the literature.A Literature review.

2.4 Summary of Previous Studies and Identification of the Research Gap

The literature reviewed shows that cyber crime is a significant and increasing problem in both global, regional and national financial-sector institutions. A regular finding of studies by Singh and Singh (2019), Mugari et al. (2016), Akinbowale et al. (2020), and others is that the negative impact of cyber crime on the performance of institutions is fourfold—direct financial losses, disruption to routine operations, reputational loss, and forced rise in security spending.

Despite this knowledge, there are still some key areas of omissions that this research aims to fill. The first one is a time gap. The bulk of the literature on the subject of electronic banking in Zimbabwe prior to 2016, particularly that by Mugari et al. (2016), was conducted before the significant structural shifts that altered the electronic banking environment in Zimbabwe since 2019. The developments encompass the quick expansion of mobile banking in the cash shortage period, the significant rise in digital payments in the COVID-19 era and the enactment of the Cyber and Data Protection Act of 2021. Prior to these changes, research conducted would not do justice to the current cyber security status of financial-sector institutions in Zimbabwe.

The second is a geographical and institutional gap, although Ghanaian (Boateng et al., 2011) and Nigerian (Frank and Odunayo, 2013) studies are useful as background, the economic conditions, regulatory environments and banking industry characteristics of these countries vary significantly from the conditions in Zimbabwe. The high penetration of mobile banking services, the relatively new formal legal structure for cyber-related crime in Zimbabwe and the recent economic instability in the country make an empirical investigation into the situation a priority, rather than an extrapolation from the experience of other countries in Africa.

The third is that there is a methodological gap. Past Zimbabwean studies such as Mugari et al. (2016) had concentrated on identifying and categorising the various forms of cyber related crime in the financial sector institutions and only briefly discussed how the cyber related crime forms relate to measurable impacts on institution performance. Clearly, there is a need for research that explicitly connects specific types of cyber-related crime to the outcomes of the crime, so that financial-sector institutions and regulators can effectively prioritize cyber security investments by the evidence of impact rather than general threat perception.

The fourth is a situation gap; a gap in the context of COVID. In Zimbabwe, electronic banking habits has been significantly changed by the COVID-19 pandemic, with faster adoption rates and emerging new interactions between clients and digital platforms. To the best of the researcher's knowledge, no prior research on the financial sector's cyber-related crime landscape focused specifically on understanding if the period of the pandemic resulted in any permanent change in the nature of cyber-related crime or in the vulnerability landscape in Zimbabwe.

The study aims to fill these gaps by looking at the effects of cyber crime on the day-to-day operations and the financial performance of financial institutions in Harare from 2022 to 2025. This focus provides for a time relevance, geographic specificity and continuity with the post-pandemic and post-legislative environment that is the current electronic banking landscape of Zimbabwe.

2.5 Chapter Summary

The chapter examined various types of electronic banking and some of the main types of cyber-crime that is being perpetrated against financial-sector institutions such as phishing, hacking, malware attacks, vishing and electronic card fraud.

The present study was based on the Routine Conduct Theory, the Space Shift Theory and the Fraud Theory that are all associated with cyber-related crime behaviour and opportunities in digital environments. The empirical review revealed that the level of cyber related crime is on the rise in the world and in the African financial systems. The chapter also revealed significant gaps in the literature regarding the impact of cyber related crime on the day to day operations and financial outcomes of financial institutions in Harare in the electronic banking period after COVID, particularly limited recent studies conducted in Zimbabwe in this area. This chapter discusses the research methodology used in the research.

Chapter 3

3.0 Introduction

In this chapter, the research methodology that was used to guide the research regarding the impact of cyber related crime on performance of financial-sector institutions in Zimbabwe is set.This chapter outlines the research methodology used to guide the study on the impact of cyber related crime on the performance of financial-sector institutions in Zimbabwe. This chapter details the research design, victim population, sample size, sampling procedures, research instruments, data collection methods, statistical data analysis techniques and ethical issues used in the research.

The current study targeted financial-sector institutions in Harare Central Business District (CBD) as they are considered one of the main centres of the banking and financial services industry in Zimbabwe. The area was identified as suitable because the commercial banks, building societies, savings banks and digital financial service providers were all concentrated there. These institutions rely more and more on online banking systems, mobile banking and financial technologies (FinTech). Recent research indicates that the rapid shift in Zimbabwe's banking environment from manual to increasingly technology-driven processes has resulted in increased vulnerability to cyber risks such as phishing, malware attacks, hacking, identity theft and fraud, SIM swap fraud and ransomware attacks.

In the current study, the research approach used was mixed methods research which included both qualitative and quantitative methods. A survey questionnaire was used for quantitative data collection and interview sessions were used for collection of qualitative data. The primary data gathering tools included the survey questionnaire and the interview session, while secondary data was sourced from journal articles, records of the Reserve Bank of Zimbabwe, scholarly publications and previous research conducted in the field of cyber security and banking performance.

3.1 Research Design

Design of research is a plan that is used to collect, analyse and interpret data in a research. Mouton (2001) states that a research design gives the researcher a plan to systematically and effectively answer the research questions.

The present study adopted the descriptive survey design in conducting the inquiry with the aim of appraising the impact of cyber-related crime on the day-to-day functioning of institutions, client trust, service provision and financial stability of banking and related institutions in Zimbabwe. The design

was appropriate as it allowed the researcher to collect detailed data from the participants on cyber related crime experiences, cyber security preparedness, digitally enabled banking systems and fraud management measures.

In other recent cyber security studies in the financial services industry in Zimbabwe, descriptive and quantitative research designs were used to investigate the threats of cyber security in the banking and banking related institutions. (Mhlanga, 2022; RBZ, 2023)

3.1.1 Descriptive Research Design

According to Williams et al (2013), descriptive research design is a method to describe, analyse and interpret existing requirements or relationships in a specific phenomenon. The design facilitated the gathering of data about trends in cybercrime, banking technology, cyber security measures and institutions' performance.

The descriptive design was appropriate because the nature of cyber-related crime in Zimbabwe's financial sector is constantly changing as a result of the advancement of technology, increased penetration of the internet, growth of mobile banking and the advent of digital financial innovation. In Zimbabwe, electronic banking platforms and artificial intelligence systems were increasingly used by banks for fraud identification purposes from 2021 to date, creating new cyber security threats.

The design also allowed for the qualitative and quantitative data to be incorporated, which enhanced the reliability and trustworthiness of the results.

3.1.2 Justification of the Research Design

The researcher used descriptive survey design for the following reasons:

The design was able to facilitate the collection of both qualitative and quantitative data on cyber-related crime and banking performance.

It provided the researcher the opportunity of studying the impact of cybercrime on financial institutions in Zimbabwe.

The design allowed for respondents to give detailed explanations about the cybersecurity challenges and fraud prevention mechanisms.

It allowed the researcher to examine the latest advancements in cyber security in Zimbabwe's banking sector.

The design was appropriate for studying various dynamics of technology – including online banking fraud, phishing schemes, ransomware and cyber enabled financial crimes.

Limitations of the Design

A drawback of the descriptive research design was the requirement for the researchers to have a high level of analytical skills to come to conclusions about the many different responses from the participants who were involved in highly specialised banking and ICT environments. Additionally, the design was contingent on the willingness of the participants to provide correct information on their experiences regarding cyber crimes.

To address this challenge, the investigator examined the latest academic studies and cyber security assessments of electronic banking, fraud-identification systems and cyber resilience capacity of financial-sector institutions in Zimbabwe.

3.2 Population of the Study

According to Wegner (2003), a study population is the entire set of people or groups that have certain characteristics that are being studied. The respondents to this study were financial sector institutions in the Harare CBD and their customers.

The Harare CBD was selected because it is home to the offices of most financial-sector institutions registered by the Reserve Bank of Zimbabwe (RBZ). The organisations were deemed suitable as they utilise ICT infrastructure, digital payment systems, mobile banking applications and online financial services extensively and are therefore vulnerable to cyber-related crime.

3.3 Sample Population

According to Saunders (2005), there are two definitions of a sample; one is a selection made from a larger group of people or things of the same type and the second is a group selected from a larger group of people or things of the same type to represent the views and characteristics of the larger group.

Four financial sector institutions were selected within the Harare CBD from the identified population. The participants were drawn from departments that have direct involvement in managing cyber security, banking operations, risk-control, compliance and information technology.

The sample population comprised of:

- 2 ICT personnel
- 2 risk management officers
- 2 accountants
- 5 compliance officers
- 4 bank customers

This resulted in a total of 15 selected participants. The sample was deemed to represent the population because the participants were chosen directly from among units directly engaged in cyber security operations. Time constraints, accessibility of participants and restriction of confidentiality to cyber information were all factors that affected the sample size.

3.4 Sampling Techniques

Sampling involves taking representative elements from a larger group of elements. Stratified random sampling and convenience sampling were used in the current study.

3.4.1 Stratified Random Sampling

Stratified random sampling is a sampling method in which the target population is segmented into homogeneous groups and then samples are drawn from each group, according to Kothari (2004).

The investigator applied stratified random sampling technique to get representation from different banks and related institutions and departments engaged in cyber security and banking operations. The strata consisted of commercial banking institutions, building societies, savings banks, ICT units, compliance departments, risk-control units and e-banking departments.

This method increased the credibility and validity of the research findings as all essential classes pertaining to Cyber crimes management were included.

3.4.2 Convenience Sampling

Convenience sampling is the use of subjects who are convenient to the investigator. When choosing the clients of the banks, this method was applied since they were more readily available during the research period.

Convenience sampling was done to save time and cut costs, but was subject to potential bias as some respondents may have been overrepresented and others may have been underrepresented.

3.5 Research Instruments

Research instruments are defined as the instruments for gathering data that is relevant to a study (Leedy and Ormrod 2005). This research uses the primary instruments for collecting data in the form of a questionnaire and interview sessions. Secondary sources comprised academic papers, policy papers, cyber security reports, RBZ publications and previous empirical research on cyber related crime and financial sector institutions.

3.5.1 Questionnaires

As defined by Saunders, Lewis and Thornhill (1997), survey questionnaires are a collection of data technique that involves asking a standardized series of questions to respondents.

Survey questionnaires were sent to participants, with both open-ended and closed-ended questions. The survey questionnaires gathered information on:

The prevalence of cybercrime in financial institutions is on the rise.The frequency of cybercrime in financial institutions is increasing.

Digital banking security systems.

Hacking and phishing events are reported.

Increased customer trust in electronic banking.Improved customer confidence in electronic banking.

- Cybersecurity awareness
- Fraud detection technologies

The use of AI and machine learning in fraud prevention and management.Application of artificial intelligence and machine learning for fraud prevention and management.

- Insider threats and the threat from outside sources

Questionnaires were used to collect the standardised responses which were appropriate for quantitative analysis.

Advantages of Questionnaires

- They made it easier for the researcher to gather data from numerous participants in a brief time frame.
- They fostered confidentiality and asked for truthful answers.
- They helped facilitate the statistical analysis and comparisons of responses.

.

Disadvantages of Questionnaires

There was a delay in receipt of completed questionnaires from some respondents.

The cost of data collection went up with the printing and transport costs.

To mitigate the impact of such challenges, some questionnaires of the surveys were sent and received using electronic communication tool like email and WhatsApp.

3.5.2 Interviews

From Kotler (1999), the interview is defined as a formal and systematic conversation (questioning) between an investigator and the participants for obtaining detailed information. Interviews were conducted with the selected officers from the ICT and the risk-control officers and accountants.

Semi-structured interview sessions were employed to gain deeper understanding of the status of cyber-related crime trends, fraud management systems, cyber security preparedness and institutional response to cyber-related threats. Interviews were conducted both face-to-face and virtually via Zoom, Microsoft Teams, etc.

Online communication channels were increasingly used in research and banking activities during 2021-25, given recent technological advancements and trends in technology-driven transformation in the banking sector that have occurred since the onset of COVID-19.

Advantages of Interviews

Interviews allowed the researcher to gain in-depth information from the participants.

They allowed clarification of complex cybersecurity issues.

They produced qualitative data that supplemented the questionnaire data.

.

Disadvantages of Interviews

Some respondents were hesitant to share information in a confidential manner related to cyber security.

- Bias and personal opinions affected some responses.

It was hard to arrange interviews with bankers because of their heavy workloads.

The researcher ensured that the respondents were assured of confidentiality and anonymity in order to overcome these challenges.

3.6 Data Collection Procedures

The investigator first obtained permission from the selected financial-sector institutions before beginning to collect the data. Participants were sent a survey with a questionnaire both in paper and electronic format. Follow-ups were done through email, telephone calls, and WhatsApp messages to ensure promptness in responding.

Interview session guides had been created and distributed to participants prior to the interview session. The interview sessions were conducted on cyber security threats, cyber fraud trends, fraud identification systems, institutional preparedness and the effect of cyber related crimes on the performance of banks.

The data collected were structured, coded and made ready for analysis in Chapter Four.

3.7 Data Presentation and Analysis

Analysis of data was the process of organising and interpreting data gathered from participants which was done to respond to the research aims. Qualitative and quantitative method was applied, qualitative data was analysed by thematic experience while quantitative data was analysed by applying statistical method.

3.7.1 Quantitative Data Analysis

Descriptive numeric techniques like tables, pie chart, figures, percentages were used to analyse the quantitative data. The statistical presentation made the interpretation and comparisons of responses made by the various participants and institutions easier.

3.7.2 Qualitative Data Analysis

Thematic and summative content interpretation of qualitative data received from interview sessions and open-ended questions were analyzed. Answers were broken down into categories that focused on cyber related crime, cyber security measures, risks to electronic banking, clients' trust in the electronic banking system and fraud control.

The qualitative findings supplemented quantitative findings, giving depth to the understanding of the problems of cyber related crime in Zimbabwe's banking sector.

3.8 Ethical Considerations

The research adhered to ethical considerations to achieve credibility and confidentiality and professionalism. There was no pressure for participants to join the study and they were told about the goals of the study before they joined.

The investigator used methods to ensure confidentiality by not asking for the participants' names or sensitive banking information. Information obtained during the research was used strictly for academic purposes

3.9 Summary

This chapter outlined the research methodology taken up in the research. It talked about Research Design, the population, selected group size, sampling techniques, research instruments, procedures for data collection and analysis of data. Professional considerations that were noted during the research process were also emphasized.

The results from the participants on how financial-sector institutions are affected by cyber related crime is outlined, analysed and explained in the next chapter.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 Introduction

This chapter outlines, interprets and discusses the data gathered from the respondents on the effect of cyber-related crime on the efficiency of financial-sector institutions in Harare. The chapter is structured along the four objectives outlined in Chapter One as follows: Assessment of increased risk of cyber related crime due to increased use of ICT; Identification of the most common types of cyber related crime that has affected financial-sector institutions; Evaluation of the impact of cyber related crime on daily business and financial results; and Assessment of the countermeasures that institutions are taking to manage cyber related crime. Both quantitative data collected from the survey instrument and the qualitative data collected from the open-ended survey instrument items and key informant interview sessions are presented in frequency tables with percentage values, and, in the case of the latter, are examined thematically to explain and enrich the findings of the former. The chapter starts with the response rate and the description of the demographics of the participants, before it goes into the substantive results.

4.1 Response Rate

Table 4.1 Questionnaire Response Rate

Category	Frequency	Percentage (%)
Questionnaires distributed	15	100
Questionnaires returned and usable	12	80
Questionnaires not returned	3	20

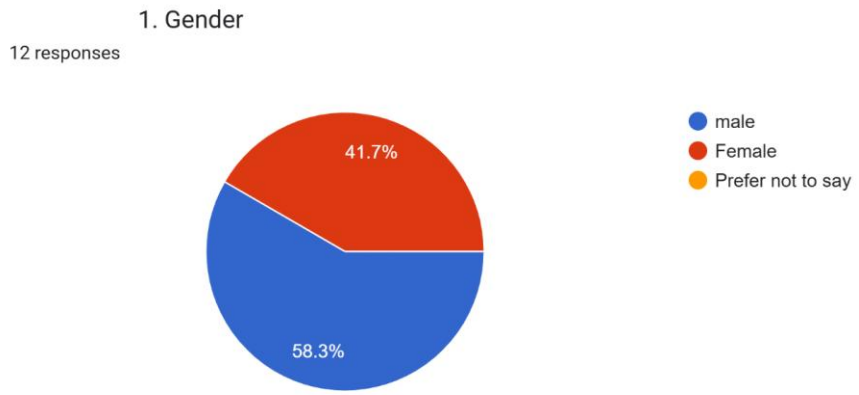
4.1.2Demographic Characteristics of Respondents

The introduction of the participants' background characteristics was important prior to the tackling of the major research goals because it has an effect on the credibility and relevance of the views expressed. Demographic data gathered included gender, age group, years of service channel, level of education, and department/position occupied.

4.2 Gender of Respondents

In Table 4.2, the male respondents outnumbered the female with the percentages of 58.3 and 41.7 respectively. While the sample size is small, there was a reasonably good balance of males and females and the mix is broadly in line with that of the typical ICT, risk and compliance role in Zimbabwe, where males have traditionally outnumbered females. However, the fact that both males and females were included in the sample does not imply that there is only one perspective on cybercrime in the institutions analyzed.

Figure 4.2.1: Gender of Respondents



4.2.3Age Group of Respondents

The majority of respondent, fell within the 31-–40 years age bracket, then followed by 21-30 years bracket and finally 41–50 years bracket. The predominance of middle aged participants aligns with the profile of staff commonly engaged in the mid-level management and risk department, cyber security and electronic banking functions of financial-sector institutions in Zimbabwe, who are

likely to be relatively post graduate and certified students with more scholarship of these cyber crimes.

Table 4.2.3 Age Group of Respondents

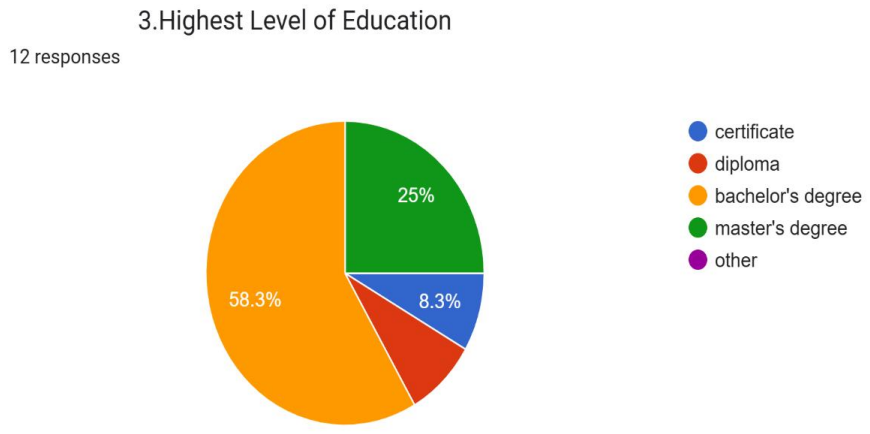
Table 4.2.3 Age Group of Respondents

Age Group	Frequency	Percentage (%)
21–30 years	2	16.7%
31–40 years	9	75%
41-50 years	1	8.3%

4.3 Level of Education

Regarding academic qualifications, most of the participants had a Bachelor's degree and the rest had a Master's extent. Both Diploma and Certificate qualified people made up 8.3 percent of the sample. This suggests that respondents are well educated and more likely to have a good understanding of the specialist questions included in the survey questionnaire, providing a degree of reliability in their answers with regards to use of ICT, classification of cyber related crime and the effectiveness of cyber security controls.

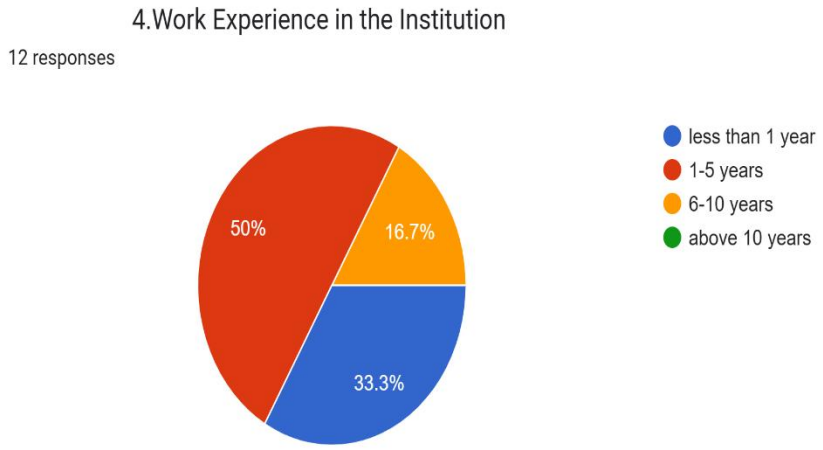
Figure 4.3: Highest Level of Education



4.4 Work experience

The relatively short time that many participants had been in their current organisation did not seem to have affected their capacity to reflect in detail about recent incidents, technologies adopted and security measures implemented, as the following sections of this chapter demonstrate; however, it is acknowledged that this may have been because of limited institutional memory of cyber-related crime trends over a longer period.

Fig 4.4: Work Experience



4.5 ICT Adoption and Its Contribution to Cybercrime Risk

The first aim of the research was to examine the role of increased and enhanced application of ICTs in the banking sector in Zimbabwe on the risks associated with cyber offences on the performance of banks. This section details the technology-based banking systems that the respondent organisations have adopted, how the respondent organisations see this adoption as related to a risk of cyber-related crime and the qualitative perspective regarding this relationship

4.5.1 Adoption of Digital Banking Technologies

The majority of respondents (nearly all the participants) reported that his/her institution had implemented modern banking systems based on technology and only one said he was unsure. No one said he/she did not introduce a totally technology based banking system in his/her institution. This finding aligns with the situation highlighted in Chapter One and Chapter Two, where Zimbabwean financial-sector institutions are on the verge of significantly changing in technology, due to financial crisis, COVID-19 pandemic and market pressures for better service delivery.

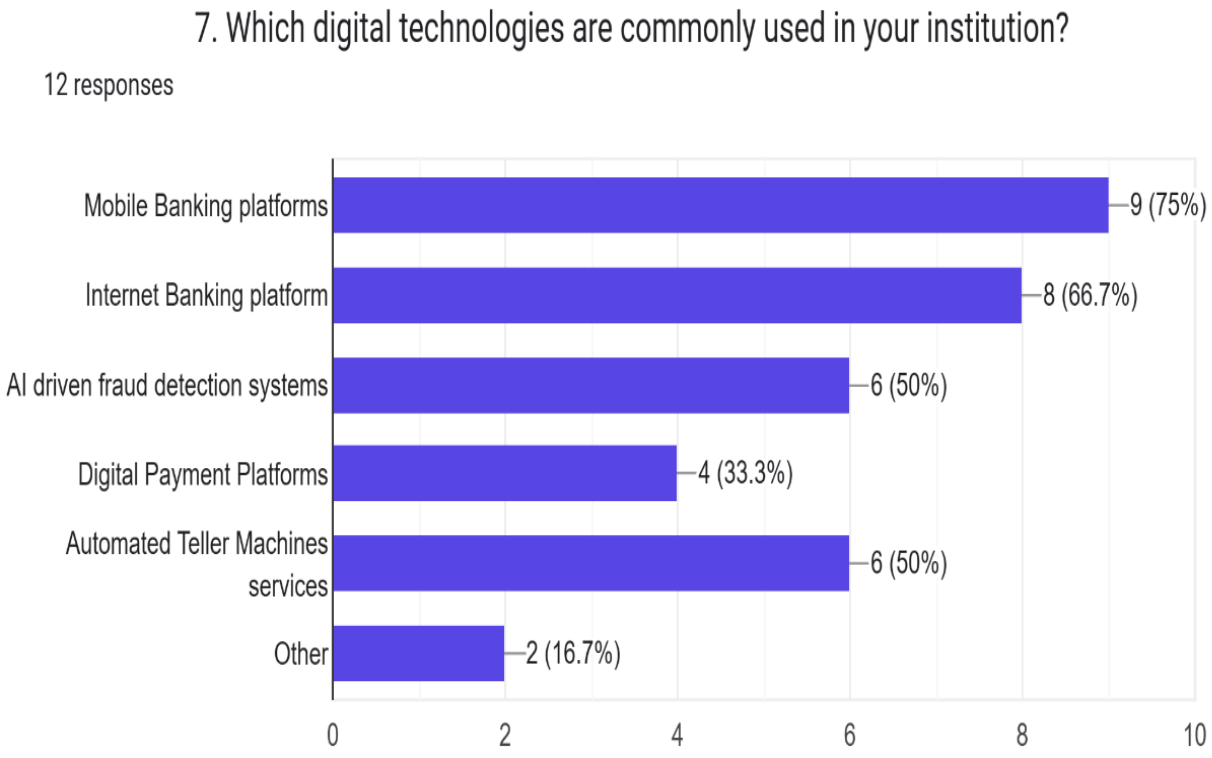
Table 4.5.1 Adoption of Digital Banking Technologies

Response	Frequency	Percentage (%)
Yes	11	91.7
Not Sure	1	8.3
Total	12	100.0

4.6 Digital Technologies used

The participants were also asked to indicate if their organisation had adopted specific technologies, with multiple answers possible – the most popular technologies were mobile-based banking channels, online banking platforms, Artificial intelligence-driven fraud-identification mechanisms and automated teller machine services, with 33.3 percent of them reporting on the use of digital payment channels. A small minority answered that they each used other not specified technologies.

graph4.6 Digital Technologies used



The dominance of mobile and online banking corroborates with literature reviewed in Chapter Two that showed these two banking channels as the main pillars of Zimbabwe's demise from the use of monetary banking medium for payments after 2016 (Reserve Bank of Zimbabwe, 2020). It is important to note that half of the organisations in the sample have already introduced AI-powered fraud-identification systems, indicating that the application of artificial intelligence in fraud management as discussed conceptually in Chapter Two is not doomed to remain just theoretical, but that it is manifesting itself in the Harare banking industry.

4.7 Link Between ICT Adoption and Cybercrime Risk

Participants were asked directly if they felt increased use of ICTs had contributed to risks associated with cyber offending in financial institutions. The answers in Table 4.9 demonstrate a high degree of consensusThe further ICT was progressing, the further so was cyber-related crime. The present study conducted by Singh et al, (2019), had reviewed that technological developments drive the criminals to engage in cybercrime. A study conducted by International Journal of Computer Application, also found that Internet technology has grown tremendously and along with that, the opportunities for cyber-related crime have increased as well.

Table 4.7 ICT Adoption Contributes to Cybercrime Risk

Response	Frequency	Percentage (%)
Strongly Agree	3	25.0
Agree	7	58.3
Neutral	2	16.7
Total	12	100.0

One of the most obvious outcomes of this research is this agreement and it is directly relevant to the first objective. The argument in Chapter Two suggests that although there are benefits of increasing the efficiency and availability of formal financial services to the people in the country due to the expansion of cyberspace and electronic banking, there are also advantages of cybercriminals in the attack surface they use to attack the formal financial system (Gibson, 1984; Reserve Bank of Zimbabwe, 2024). This sentiment was not only shared by participants who hold positions in cyber security and ICT but also those in management, suggesting that it is a shared perception, not limited to technical teams.

Table 4.6.1 Digital Banking-Cybersecurity Risk Relationship

Theme	Frequency
New attack surfaces / more doors for hackers	3
Electronic fraud / account takeover risk	2
Social engineering threats	1
Technology dependency / cloud vulnerabilities	1
General increase in digital risk	1

The key message was the creation of each new digital service provides an additional entry point for criminals. One of the cyber security participants simply put, "With every new digital service that's created it's a new point of entry for hackers to attempt to break through, and another of the participants connected the rise in online payments with increased opportunities for digitally-enabled fraud and account takeover. A senior participant gave a more detailed explanation and said that electronic banking moves big amounts of money electronically, making banking institutions and those classified as fintechs more appealing targets than normal banking because if it is successful, they can see the direct monetary loss. This approach uncovers the argument that has been cited in the literature that can be attributed to the financial sector's cash value aggregation which has been determined to serve as a structural cause of cybercriminal interest (Akinbowale et al., 2020).

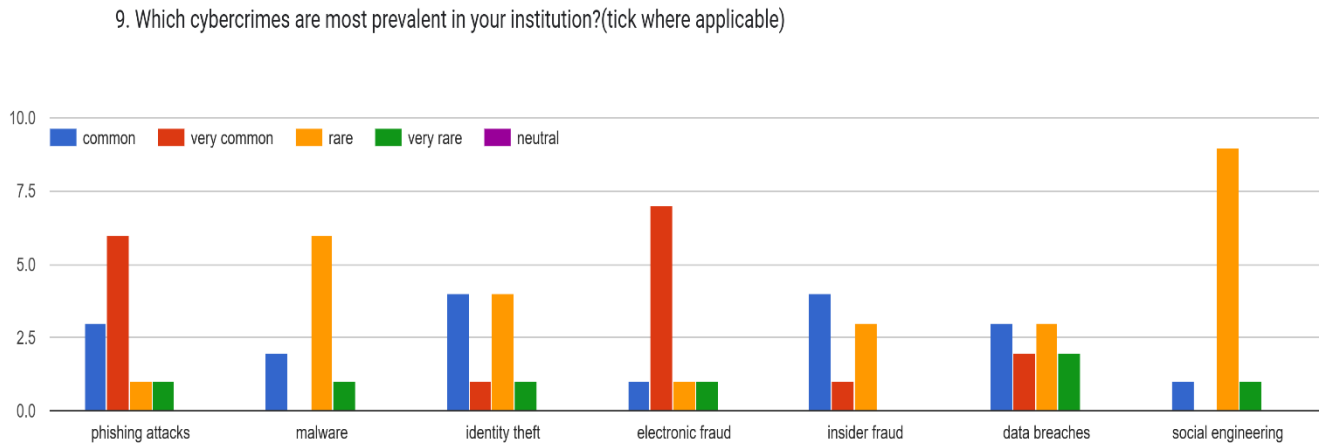
Other participants cited dependency on technology and cloud services as a systemic weakness, and the emergence of manipulative social-engineering tactics that are emerging in tandem with the growth of electronic banking. The quantitative finding that 83.3 percent of the participants consider the use of ICTs as an increase in exposure to cyber related crimes, combined with the qualitative explanations for this perception, provides a strong support for the first objective – with the digitalisation of the banking sector comes an increase in the number of points at which a system can be attacked, the use of ICTs is widely considered as an increase in exposure to cyber related crimes in Zimbabwe's banking industry.

4.8 Prevalent Forms of Cybercrime Affecting Financial Institutions

The second goal was to identify the most common types of cybercrime occurring among financial institutions. The participants rated seven categories of cyber related crime on a 4-point rating scale of Very Common, Frequent, Rare and Very Rare. Average scores were calculated for each class,

for ease of comparison with the other classes, with a lower mean score representing a higher prevalence percentage reported.

Fig 4.8 Prevalence of Cybercrime by Type



The most common fraud crime to occur on the institutions sampled was Digitally enabled fraud as seven of 10 participants said it was very common and nine of 11 participants said it was common, with the lowest mean score, followed closely by Phishing schemes, which nine of 11 participants said was common and seven of 10 said it was very common. These two findings align with the existing literature and with the fact that phishing is often cited as the way in which digitally enabled fraud and account takeover is often achieved (Nieles et al., 2017; Baegh, 2012). Phishing could appear to be the first step in the attack chain going on to downstream financial consequences in digitally enabled fraud – not two unrelated threats like it could be in the organisations studied.

The third major threat was insider cyber-related threats, an issue to be taken up with special interest as it is an issue that moves away from the purely external, tech-driven image of cyber-related crime. The data indicate that there is a real internal risk to financial-sector institutions in Harare, as well as an external risk, and that this might have implications for the distribution of cyber security resources between external and internal defence. The top four categories were those of identity-related fraud and hacking/data breaches, followed by malware and ransomware and manipulative social-engineering, which were reported as the least prevalent of the categories assessed, though it is noted that even these less prevalent categories were still occurring to some degree by all respondents answering the item.

4.9 Interviews

The questions to the interview guide for ICT officers, risk officers and accountants were open ended and directly asked the participants about forms of cyber crime they had noticed in their institution or the broader Zimbabwean financial sector. The answers in the interviews were very similar to the findings of the questionnaire. The risks that interviewees consistently mentioned were phishing, and manipulative social engineering, typically in the context of fraudulent emails and fake websites/impersonation attempts against staff and clients. Other interviewees cited digitally-based fraud and account takeover as the threat that has the greatest impact on the bottom line, as when a phishing or manipulative social-engineering attack is successful, the typical outcome is that money is transferred out of the bank's customer or institutional accounts. The quantitative ranking of the questionnaire and the qualitative interview conducted in this intergation strengthens the confidence in the finding that phishing enabled, digitally enabled fraud is the most immediate cyber related crime threat facing the institutions studied, rather than more technically sophisticated attacks like malware or large-scale hacking.

4.9.1 Impact of Cybercrime on Operational and Financial Performance

The third mission assessed the repercussions of cybercrime on the regular functioning and financial standing of financial institutions. Participants assessed the magnitude of the impact for each of eight dimensions of performance on a scale of Zero to Very High Impact. Again, mean scores were computed to allow a lower score to reflect a higher impact of the occurrence; this was not done for details of the occurrence.

Table 4.9.1 Impact of Cybercrime on Performance Area

Performance Area	Very High	High	Moderate	Low	No Impact	Mean	Rank
Financial losses	5	3	2	1	0	1.91	1
Institutional reputation	2	1	7	2	0	2.75	2
Operational efficiency	1	3	3	3	0	2.80	3
Data security	0	4	5	2	0	2.82	4
Regulatory compliance costs	0	4	5	2	0	2.82	4
Service delivery	1	1	7	2	0	2.91	6
Employee productivity	1	1	6	1	1	3.00	7
Customer trust	1	2	3	4	0	3.00	7

4.10 Impacts of cyber crime

4.10.1Financial loss

the results show that, monetary losses pose the greatest effect in financial instituitions as it was ranked initial on the licket scale.almost every respondent chosen pointed out that cyber crimes have monetary losses risk.similar results were carried out by Global forum crime survey (2011) which also showed that monetary losses has a greater impact on organisational perfomance. Some of those interviewed said that it is unlikely that the crime incidents of cyber crimes are covered up to ensure that investors or clients would not be "alarmed".

4.10.2 Institutional reputation

This was the second, and this indicates that cybercrime can have detrimental impacts on the reputation of financial institutions, especially when data breaches compromise personally identifiable information of customers. When the public image is damaged, this can cause the employees to lose confidence and influence how competitive the institution is.

4.10.3 Operational efficiency

The negative impact of cyber crimes on the working of the organisational processes. These frequently result in system down time, work flow disruptions and increased allocation of resources to prevention.

Data security cyber crimes reported that cyber crimes have considerable energy towards the organisations, since they can lead to data losses, improper service delivery and decrease in productivity of the employees, as shown in the above fig.

4.11Cybersecurity Strategies Adopted and Their Effectiveness

The fourth was to recommend suggestions on how to minimize cyber-related crimes in the financial sector in Zimbabwe, which involved finding out what financial institutions were already putting in place and how effective participants considered these were.

4.11.1 Cybersecurity Awareness Training

The vast majority of the institutions surveyed provide some capacity building for employees on Cyber security awareness. Of those responding, 58.3 per cent reported that training was provided, 33.3 per cent reported sometimes training was provided and 8.3 per cent reported that no training was provided.

Table 4.11.1: Provision of Cybersecurity Awareness Training

Response	Frequency	Percentage (%)
Yes	7	58.3
Sometimes	4	33.3
No	1	8.3
Total	12	100

Table 4.11.2: Cybersecurity Measures

Measure	Frequency	Percentage (%)
Employee Awareness Training	9	75.0
Regular System Audits	9	75.0
Multi-Factor Authentication	7	58.3

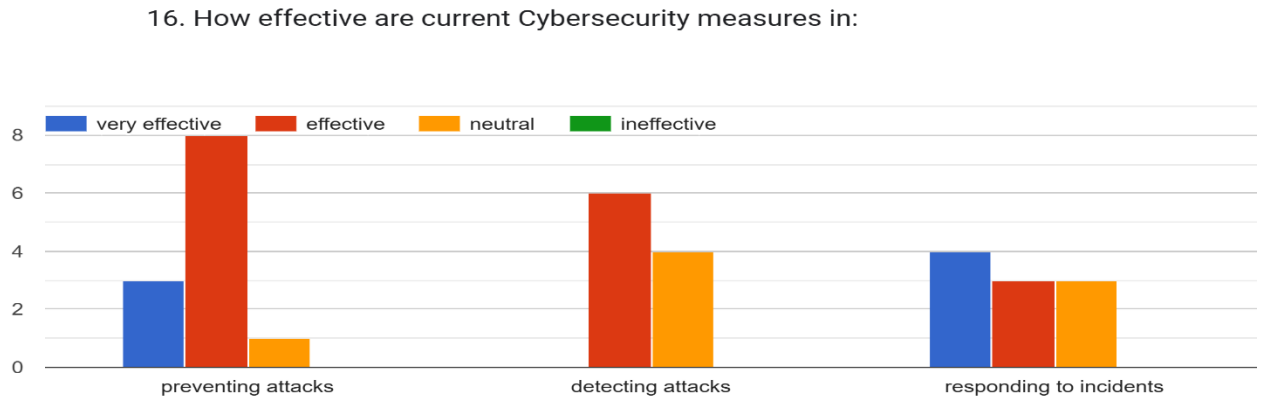
Cybersecurity Policies	6	50.0
Firewalls and Antivirus Systems	5	41.7
Data Encryption	5	41.7

Firewalls and antivirus mechanisms were also the least commonly reported of the six controls noted, along with the data encryption controls – which is somewhat surprising as they are considered the most fundamental layer of cyber defence. This could mean that institutions in the sample have been investment focused on newer, more visible controls like multi-factor authentication and policy frameworks and that they are taking for granted or assuming to be sufficiently addressed by the existing IT infrastructure foundational technical controls – firewalls and data encryption controls.

4.12 Effectiveness of Cybersecurity Measures

In addition to determining which measures were in place, participants provided a rating of the effectiveness of each measure in preventing cyberattacks, detecting them, and reacting to them. The result is shown in Table 4.17.

graph 4.12: Effectiveness of Cybersecurity Measures



The participants rated the effectiveness of cyber security controls of their institutions highest for the prevention element, with all 12 respondents considering this element to be very effective or effective (excluding one that rated it as neutral). Almost as favorably was the rating for incident response. However, the identification capability was not as developed as the other two with none of the participants rating the detection as very effective and four of ten participants rating it as merely neutral.

A difference between strong prevention and response and comparatively weak identification is a significant finding of the research's fourth objective. It indicates that institutions in the sample have been successful in maintaining a risk portfolio of known risks and in managing with confidence known incidents once they are detected, but are less confident in their ability to proactively identify or flag malicious activity already in the system like unusual transactional patterns, and access to accounts by third parties or suspicious activity by insiders. Considering that insider threat was cited in section 4.4 as the third most common type of cyber crime, this lack of detection may be significant because insider activity is typically more difficult to detect using perimeter based prevention controls and is more dependent on monitoring and anomaly detection functions.

4.13 Resource Allocation and Incident Reporting

Three-quarters of participants, confirmed that their institution allocates sufficient resources to cyber security, while the remaining were not sure. Likewise, two thirds of respondents said that they had a formal reporting process within their organisation for cyber incidents, and 33.3 percent said they were not certain whether there is a formal reporting process or not.

Table 4.13: Resource Allocation and Formal Incident Reporting

Item	Yes (%)	No (%)	Not Sure (%)

Sufficient resources allocated to cybersecurity	75.0	0.0	25.0
Cyber incidents formally reported	66.7	0.0	33.3

4.14 Regulatory Compliance

The participants were asked, in an open-ended item, if the organisation was following the rules of cyber security issued by the Reserve Bank of Zimbabwe. Of the nine respondents to this question six responded definitively with a yes, indicating compliance, and two responded with a don't know, with one responding due to being a first year at the institution, and another stating that he/she was not willing to give an opinion.

A few of the participants specifically mentioned the RBZ's Cyber Security Framework and Risk Management Guidelines, one senior respondent saying that most licensed banks in Zimbabwe and financial-sector institutions have a target of complying with these guidelines. This discovery supports the discussion in Chapter Two about the new regulatory environment created by the Cyber and Data Protection Act of 2021 and the new RBZ guidance, and suggests that at least from an institutional staff perspective, there is no option for not being compliant with the regulations, but it is is an expectation. However, the qualitative answers in this research are participants' own perceptions of compliance, not results of the audit, and as such should be interpreted accordingly.

4.14.1 Respondents Recommendations for Reducing Cybercrime

The last question called for participants to suggest other strategies which might help deter cyber related crimes in financial-sector institutions in Zimbabwe. Nine of 12 participants recommended and these recommendations were represented under five major themes,

Table 4.14.1: Themes in Respondent Recommendations

Theme	Frequency
Technology upgrades (e.g. firewalls, MFA)	3
Staff training, awareness and education	2
Ethical hacking / penetration testing	2
Phishing simulations and cyber drills	1
Investment in cybersecurity resources	1

The most common upgrade recommended was technology such as increased deployment of multi-factor authentication and increase in firewalls. Relevant to this was the notion raised by two participants of proactive

testing through ethical hacking and port scanning, suggesting a desire among practitioners to adopt a more offensive testing-based assurance method, in addition to a defensive approach.

4.15 Discussion of Findings

The findings from this chapter directly address the four aims outlined in Chapter One. The data confirm that there is a broad perception that the use of ICT has been associated with cyber-related crimes risk on the first objective, as 91.7 per cent of the participant institutions have introduced technology-based banking systems and 83.3 per cent of the participants agree/strongly agree that the use of ICTs has contributed to the cyber-related crimes risk. This statistic becomes meaningful if it is supported by qualitative statements made by the participants, such as the suggestion that each new digital service opens another avenue by which criminals can operate. This view is consistent with Gibson's (1984) theory of cyberspace, as described in Chapter Two, that with the growth of electronic banking, the opportunities for criminals to attack also grow.

As regards the second objective, the study identified phishing and digitally empowered fraud as the leading types of cyber offences, well followed by insider risks in third position. The ordering is informative for financial-sector institutions that want to focus on limited cyber security resources: it suggests that the most cost-efficient investments in the short term will likely focus on controls that help prevent manipulative social-engineering and account-takeover fraud, as well as those that address internal risk, rather than investments focused exclusively on technically sophisticated risks like malware, which participants indicated were less prevalent.

The most significant finding for the third objective was that monetary loss was identified as the most impacted institutional performance area when it comes to cyber-related crime. This reflects the image commonly found in the literature, in which the monetary impact of cybercrime effect (Akinbowale et al., 2020) is seen as the main shortfall of cyber-based crime. The evidence presented here, from organisations based in Harare, suggests that for the sample organisations, the tangible and visible cost of cyber crime is that time, focus and productivity are lost as a result of managing and recovering from cyber incidents. The impacts on client trust and regulatory compliance costs were also cited as having a significant impact, further confirming the theme from Chapter Two that effects of cybercrime go far beyond the institution's balance sheet to the client and regulatory relationships.

Awareness training and system reviews are prevalent as prevention strategies. While RBZ regulatory compliance seems to be broadly observed, identification capability falls behind prevention and response, data encryption, firewall controls and other newer controls like multi-factor authentication are not used as regularly as they are expected to be, and the correlation between a lack of staff incentives and low staff cyber security awareness indicates that specialist controls are unlikely to overcome human-influence weaknesses identified in the course of this chapter. Recommendations made by the participants, especially the call for more regular and more practically oriented capacity building activities (monthly phishing simulations), suggest a joint specialist and behavioural approach as the best way forward for these organisations in the future.

These results must be taken with due caution. Strict confidentiality of financial-sector institutions and the 80 percent response rate from the 12 organisations, all of whose participants were spread across the relevant departments, means that the findings are representative of the behaviour of participants in the organisations studied and are only indicative of behaviour patterns within the sector as a whole. However, the evidence closely resembles that reported in Chapter One and Chapter Two based on secondary sources like RBZ and POTRAZ records, which lends credibility that the primary data collected here illustrate actual, observable dynamics within the financial-sector institutions in Harare.

4.16 Chapter Summary

This chapter introduced, analysed and discussed the primary data obtained from various participants from the four financial-sector institutions in Harare with 80 percent response rate. The demographic profile indicated that the participants were relatively middle, well educated and were from ICT, Cyber security, Risk and Management roles. Regarding the first objective, the chapter identified that almost all the banks studied are currently using technology for banking services and the participants viewed the use of ICT as a direct link to cyber-related crime risks. In response to the second objective, phishing and digitally enabled fraud were listed as the top two most common types of cyber related crimes, while insider threats also were mentioned, and most institutions reported that they had a high number of cyber incidents rather than a few or none at all. In the third objective, the chapter concluded that monetary loss is the most significant, followed by operational efficiency, and client confidence and regulatory compliance expenses are also significantly impacted by cyber-related crime. Lastly, with respect to the fourth goal, the chapter demonstrated that institutions have adopted an adequate range of cyber security measures and are reasonably compliant with the RBZ's regulatory requirements, but there are still difficulties with the ability to detect these risks and to consistently train staff well, and participants recommended a greater frequency of practical, hands-on training and ongoing investment in technology. The findings presented in the following chapter are summarised and recommendations are made for financial-sector institutions, regulators and future research.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter presents a summary of the major findings of the research, makes conclusions in line with the research purpose and findings presented in Chapter Four and offers recommendations to address cyber related crime and enhance cyber security resilience in financial sector institutions in Zimbabwe. Also discussed in the chapter are future research areas.

5.1 Summary of the Study

The study aimed at investigating the Effects of Cyber Related Crime on the Performance of Financial Sector Institutions in Harare Central Business District (CBD) was carried out. With the growing penetration of technology in banking systems like mobile banking, online banking, electronic payment systems and other ICT based financial services, the present study was triggered by the consequence of the impact of technology on banking operations and the associated threat of cyber crime to the banking organisations.

The current research used a descriptive survey research design and utilised a mixed-methods approach. The study involved the collection of data from employees of the selected financial-sector institutions from the following four departments: ICT, compliance, risk-control and accounting departments, in addition to selected bank clients. Both qualitative and quantitative data were collected using survey questionnaires and interview sessions. When asking the 15 survey questionnaires, 12 were successfully completed and returned, yielding an 80% return rate.

The evidence suggested that presently financial sector institutions operating in Harare are widely using technology based banking systems. Mobile banking and online banking were the most frequently used digital services. The findings of the current study confirmed that the overuse of the ICTs has had a significant role in the risks associated with cyber offences in financial sector institutions. Most participants agreed that the increased availability of electronic banking services has increased the opportunities available for cybercriminals to target technological gaps, which is consistent with arguments put forward by Singh and Singh (2019), and with the propositions of Routine Conduct Theory of Cohen and Felson (2018).

The present study also found that the digitally enabled fraud, phishing schemes, identity-related fraud, hacking, and malware-based attacks and insider-related cyber-related threats are some of the most common types of cyber-related crimes faced by financial-sector institutions. The findings are similar

to those by Mugari et al. (2016), Kabanda (2012) and the Financial Intelligence Unit Zimbabwe (2023) that reported similar cyber related threats in the Zimbabwean financial sector.

In terms of institutions' performance, the findings indicated that financial-sector institutions suffer from negative monetary losses, disruption of normal activities, damage to the reputation of the institutions and loss of trust among their clients as a result of cyber-related crime. The immediate financial impacts were the most sizeable, with damage to institutional reputation and lower levels of operational efficiency coming in next. Participants also reported that the level of cyber-related crime relates to the cost of cyber security infrastructure, fraud management and the regulatory burden.

The current research also revealed that financial institutions have adopted different types of cyber security strategies, such as firewalls, anti-virus technology, access controls, and fraud detection and prevention technology; however, problems exist in the areas of cyber threat identification, employee awareness, and ongoing monitoring. Inadequate cyber security awareness and human error were seen as important factors to institutional vulnerability.

5.2 Conclusions

In the light of the results of the study presented in Chapter Four, the following conclusions were drawn:

5.2.1 ICT Adoption and Cybercrime Risk

The findings of the research indicate that the increasing use of ICT and technology-based banking systems has created a situation whereby all financial-sector institutions in Zimbabwe are facing a huge cyber related crime risk exposure, despite the improvements it has brought to the operational efficiency, delivery of services and access to formal financial services. The evidence shows that technological progress and the development of cyber crimes have been interdependent in the current banking landscape.

5.2.2 Prevalent Forms of Cybercrime

Based on this research, it has been determined that phishing schemes, digitally enabled fraud, hacking, identity related fraud and malicious software are the most prevalent types of cyber related crime perpetrated against financial-sector institutions while insider fraud is not a widespread crime. These cyber-related threats take advantage of both technological and human weaknesses, which means that cyber security challenges go beyond technological mechanisms and behavioral/ organisational issues.

5.2.3 Impact of Cybercrime on Institutional Performance

The findings of the research indicate that the effect of cyber related crime on the performance of financial-sector institutions is quite high. Financial damages caused by fraudulent transactions and

illegal access to banking systems have a close relationship with profitability. Moreover, operational inefficiencies, service disruptions, reputational damage, and loss of client confidence are all factors that can result from cyber incidents. The combined impact of these consequences will undermine the long-term sustainability and competitiveness of financial-sector institutions.

5.2.4 Cybersecurity Preparedness

The finding from the research was that financial-sector institutions have been investing in the cyber security infrastructure and risk-control systems, but not all such controls are adequate to mitigate the new cyber risks. Poor employee awareness, lack of cyber threat identification and ongoing monitoring allows cyber criminals to take advantage of institutional weaknesses. To achieve effective cyber security, technology must go hand-in-hand with the development of staff capabilities and a commitment to organisational security.

5.3 Recommendations

The following recommendations are made based on the findings and conclusions of the study

5.3.1 Recommendations for Financial Institutions

It is essential for financial-sector institutions to regularly enhance their cyber security systems, including through system upgrades or testing for vulnerabilities and investments in modern cyber security technologies. Periodically review current security measures and ensure they continue to be useful in combating new cyber threats.

There should be greater awareness campaigns in financial-sector institutions, for both staff and clients, about cyber security. Staff and client capacity building sessions should be regularly conducted and awareness sessions and simulations of cyber-attacks should be held to enhance the capability of employees and clients to identify and deal with cyber threats including phishing, social engineering and identity theft.

Banks need to improve their internal controls and monitoring to limit the risks arising from internal staff and access to the systems. Access privileges must be reviewed on a regular basis and consistent with employees' job responsibilities.

Financial-sector institutions should boost investment in fraud-identification systems, real-time monitoring technologies and cyber incident response capabilities to aid in the early detection and rapid response to cyber incidents.

5.3.2 Recommendations for Regulatory Authorities

The Reserve Bank of Zimbabwe (RBZ), POTRAZ and other relevant regulatory authorities need to persist with beefing up cyber security regulations and compliance for financial-sector institutions.

There is a need for increased information sharing between financial-sector institutions on new cyber-related threats, fraud trends and cyber security best practices, which should be encouraged by regulatory authorities. This will enhance the joint readiness and facilitate joint efforts in responding to cyber-related crime.

It is important for financial institutions to conduct regular cyber security audits and compliance checks to ensure that they are operating at a secure level and meeting the necessary regulations, including key legislation like the Cyber and Data Protection Act of 2021.

5.3.3 Recommendations for Customers

Clients should be encouraged to follow safe banking procedures online, including using strong passwords and enabling multi factor authentication, and not sharing banking information with anyone via emails or phone calls that they don't know or through online platforms.

Financial-sector institutions should remain educating their customers about threats that are routine to cyber, and how to keep individual financial information safe.

5.3.4 Recommendations for Future Researchers

The research should be expanded to include financial-sector institutions in other provinces of Zimbabwe.

The effectiveness of new technologies in the financial sector to curb cyber-related crimes in Zimbabwe should be analysed further with the aid of artificial intelligence, machine learning and behavioural analysis.

Additionally, future research could explore the relationship between the increased investment in cyber security and organisational performance over time, employing more extensive sample sizes and more sophisticated statistical methods.

5.4 Chapter Summary

This chapter summarised the major findings of the research, the conclusions drawn from the research results and the recommendations to assist in mitigating cyber related crimes and enhancing cyber security resilience in the financial sector institutions in Zimbabwe. The study also confirmed that increased use of the ICT has contributed to an increase in the risks associated with cyber offending; of these, phishing, fraud enabled by ICTs, and identity-related fraud and hacking are most common. The evidence also highlighted that the monetary loss, disruption of normal operations and institutional reputation losses are the negative impacts that cyber related crime has on performance of institutions. The recommendations made include on strengthening cyber security frameworks, awareness raising and improving regulatory oversight and future research on cyber related crime in Zimbabwe's financial sector.

REFERENCES

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020) 'The impact of cybercrime on the banking sector using the Balanced Scorecard approach', Journal of Financial Crime, 27(3), pp. 945–958.

Amedu, S. (2005) 'The impact of automated teller machine on banking operations in Nigeria', Journal of Internet Banking and Commerce, 10(1), pp. 1–8.

Arcand, M., PromTep, S., Brun, I. and Rajaobelina, L. (2017) 'Mobile banking service quality and customer relationships', International Journal of Bank Marketing, 35(7), pp. 1068–1089.

Auer, R., Cornelli, G. and Frost, J. (2020) 'Covid-19, cash, and the future of payments', BIS Bulletin, 3, pp. 1–7.

Aysan, A.F. (2014) 'Banking technology and financial service delivery', International Journal of Finance and Banking Studies, 3(4), pp. 1–10.

Baegh, B. (2012) Phishing and Identity Theft Prevention. New York: McGraw-Hill.

Boateng, R., Longe, O.B., Isabalija, S.R. and Mbarika, V. (2011) 'Cybercrime in Ghana: Causes, effects and prevention', International Journal of Cyber Criminology, 5(1), pp. 1–20.

Burns, P. and Stanley, A. (2002) Card Fraud and Prevention Strategies. London: Financial World Publications.

Chang, Y.T. and Hamid, N.R.A. (2010) 'An analysis of internet banking adoption', Journal of Internet Banking and Commerce, 15(1), pp. 1–12.

Cohen, L.E. and Felson, M. (1979) 'Social change and crime rate trends: A routine activity approach', American Sociological Review, 44(4), pp. 588–608.

Cressey, D.R. (1953) Other People's Money: A Study in the Social Psychology of Embezzlement. Glencoe, IL: Free Press.

Cyber Laws. (2015) Cyber Laws and Information Technology. New Delhi: Universal Law Publishing.

Deitel, H.M., Deitel, P.J. and Steinbuhler, K. (2001) E-business and E-commerce for Managers. Upper Saddle River, NJ: Prentice Hall.

Deloitte. (2023) African Banking Cybersecurity Survey Report 2023. Johannesburg: Deloitte.

Dube, T., Chitura, T. and Runyowa, L. (2009) 'Adoption and use of internet banking in Zimbabwe: An exploratory study', Journal of Internet Banking and Commerce, 14(1), pp. 1–13.

Essinger, J. (1999) The Future of Banking. London: Financial Times Pitman Publishing.

Financial Intelligence Unit Zimbabwe. (2023) Annual Report 2022/2023: Trends in Financial Crime in Zimbabwe. Harare: FIU Zimbabwe.

Fraud Advisory Panel. (2009) Cybercrime: Understanding the Online Threat. London: Fraud Advisory Panel.

Frank, O. and Odunayo, A. (2013) 'Cybersecurity challenges in Nigerian organisations', International Journal of Computer Science and Security, 7(2), pp. 45–57.

Gibson, W. (1984) Neuromancer. New York: Ace Books.

Gono, G. (2012) Zimbabwe's Casino Economy: Extraordinary Measures for Extraordinary Challenges. Harare: Zimbabwe Publishing House.

Ibrahim, A. (2022) Cybercrime and Financial Institutions in Africa. Nairobi: African Security Press.

International Centre for the Study of Cyber Security and Protection Alliance (ICSPA). (2014) Cybercrime and Business: The Economic Impact. London: ICSPA.

Jaishankar, K. (2008) ‘Space transition theory of cybercrimes’, in Schmallager, F. and Pittaro, M. (eds.) Crimes of the Internet. Upper Saddle River, NJ: Prentice Hall, pp. 283–301.

Kabanda, G. (2012) ‘Cybercrime trends in Zimbabwe and strategies to combat it’, International Journal of Advanced Computer Science and Applications, 3(6), pp. 155–161.

Kabanda, G. (2021) Cybersecurity and Digital Banking in Zimbabwe. Harare: University of Zimbabwe Press.

Karjaluoto, H., Koenig-Lewis, N., Palmer, A. and Moll, A. (2012) ‘Banking technology and service efficiency’, International Journal of Bank Marketing, 30(4), pp. 261–281.

Kothari, C.R. (2004) Research Methodology: Methods and Techniques. 2nd edn. New Delhi: New Age International.

Kotler, P. (1999) Marketing Management. 10th edn. Upper Saddle River, NJ: Prentice Hall.

KPMG. (2011) Cybercrime Survey Report. London: KPMG International.

Leedy, P.D. and Ormrod, J.E. (2005) Practical Research: Planning and Design. 8th edn. Upper Saddle River, NJ: Pearson Education.

Leukfeldt, E.R. and Yar, M. (2016) ‘Applying routine activity theory to cybercrime’, European Journal of Criminology, 13(3), pp. 263–280.

McAfee. (2014) Net Losses: Estimating the Global Cost of Cybercrime. Santa Clara, CA: McAfee Center for Strategic and International Studies.

Mhlanga, D. (2022) ‘Cybersecurity challenges in Zimbabwe's financial sector’, Journal of African Business Studies, 8(2), pp. 45–59.

Mouton, J. (2001) How to Succeed in Your Master's and Doctoral Studies. Pretoria: Van Schaik.

Mugari, I., Gona, J. and Maunga, T. (2016) ‘Cybercrime in Zimbabwe's financial sector’, International Journal of Computer Science and Information Security, 14(5), pp. 120–129.

Nieles, M., Dempsey, K. and Pillitteri, V. (2017) An Introduction to Information Security. Gaithersburg, MD: National Institute of Standards and Technology.

Njanike, K. (2021) Digital Banking and Financial Inclusion in Zimbabwe. Harare: Zimbabwe Open University Press.

Njeru, A. and Gaitho, N. (2019) ‘Effects of cybercrime on the financial performance of commercial banks in Kenya’, International Journal of Economics, Commerce and Management, 7(5), pp. 112–128.

Nwaolisa, E.F. and Kasie, E.G. (2012) ‘Electronic banking and customer satisfaction’, Journal of Economics and Sustainable Development, 3(10), pp. 1–8.

Okiro, K. (2013) ‘The impact of mobile banking on financial performance’, International Journal of Research in Management, 2(4), pp. 45–56.

Ollman, G. (2007) The Phishing Guide. London: Security Publications.

Paternoster, R. (2011) ‘Routine activities and cybercrime victimisation’, Criminology and Public Policy, 10(3), pp. 123–140.

Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). (2024) Sector Performance Report 2024. Harare: POTRAZ.

Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). (2025) Sector Performance Report 2025. Harare: POTRAZ.

Rasha, K. and Andrew, M. (2012) ‘Economic pressures and fraud motivation in developing economies’, Journal of Financial Crime, 19(4), pp. 345–358.

Reserve Bank of Zimbabwe (RBZ). (2020) Annual Report 2020. Harare: RBZ.

Reserve Bank of Zimbabwe (RBZ). (2023) Banking Sector Report 2023. Harare: RBZ.

Reserve Bank of Zimbabwe (RBZ). (2024) Banking Sector Report 2024. Harare: RBZ.

Sandywell, B. (2010) Internet and Society. London: Sage Publications.

Saunders, M., Lewis, P. and Thornhill, A. (1997) Research Methods for Business Students. Harlow: Pearson Education.

Saunders, M., Lewis, P. and Thornhill, A. (2005) Research Methods for Business Students. 4th edn. Harlow: Pearson Education.

Shuabi, A. (2010) Electronic Payment Systems and Banking Technology. Lagos: Financial Press.

Singh, K. and Singh, P. (2019) 'Cybercrime and organisational performance in the digital era', International Journal of Information Systems and Management, 5(2), pp. 89–102.

Telecommunication Technology Committee (TTC). (2008) Voice Phishing (Vishing) Security Guidelines. Tokyo: TTC.

Wegner, T. (2003) Applied Business Statistics. Cape Town: Juta.

Wells, J.T. (2011) Corporate Fraud Handbook. 3rd edn. Hoboken, NJ: Wiley.

Williams, C., Onyebuchi, A. and Uzoamaka, E. (2013) 'Descriptive research design in social science studies', International Journal of Social Research Methodology, 6(3), pp. 65–78.

World Bank. (2022) Digital Financial Services in Sub-Saharan Africa. Washington, DC: World Bank.

Yibin, M. (2003) 'Internet banking development and customer adoption', Journal of Banking Technology, 12(2), pp. 45–58.

Zimbabwe Republic Police (ZRP). (2025) Cybercrime Statistics Report. Harare: ZRP.

Appendix

questionnaire

Dear Respondent

I am a student at Bindura University of Science Education pursuing a Bachelor of Commerce Honours Degree in Financial Intelligence. I am conducting a research study entitled: An analysis of the impacts of cybercrime on the perfomance of financial institutions domiciled in harare.

The purpose of this study is to examine the effects of cybercrime on the operational and financial performance of financial institutions in Zimbabwe. Your responses will contribute towards the successful completion of this academic study.This questionnaire is intended for employees involved in ICT, cybersecurity, operations, risk management, compliance, or managerial functions

Please note the following:

- **Participation is voluntary.**
- **Your responses will remain confidential and anonymous.**
- **Information provided will be used strictly for academic purposes only.**

INSTRUCTIONS

- **Please answer all questions honestly.**
- **Tick [□] where appropriate.**
- **Do not write your name or any identifying information.**

SECTION A: DEMOGRAPHIC INFORMATION

1. Gender

- **Male [ ]**
- **Female [ ]**
- **Prefer not to say [ ]**

2. Age Group

- **21–30 years [ ]**
- **31–40 years [ ]**
- **41–50 years [ ]**
- **51 years and above [ ]**

3. Highest Level of Education

- **Certificate [ ]**
- **Diploma [ ]**
- **Bachelor's Degree [ ]**
- **Master's Degree [ ]**
- **Other (Specify) _____**

4. Work Experience in the Institution

- **Less than 1 year [ ]**
- **1–5 years [ ]**
- **6–10 years [ ]**
- **Above 10 years [ ]**

5. Position Held in the Institution

- **Senior Management [ ]**
- **Middle Management [ ]**
- **ICT/Cybersecurity Staff [ ]**
- **Operations Staff [ ]**
- **Other (Specify) _____**

SECTION B: CYBERCRIME IN FINANCIAL INSTITUTIONS

6. Has your institution adopted modern digital banking technologies

- **Yes [ ]**
- **No [ ]**
- **Not Sure [ ]**

7. Which digital technologies are commonly used in your institution? (Tick all that apply)

- **Mobile Banking platforms [ ]**

- **Internet Banking platforms [ ]**
- **AI driven fraud detection systems [ ]**
- **Digital Payment Platforms [ ]**
- **Automated Teller Machines services (ATMs) [ ]**
- **Other (Specify) _____**

8. Do you believe increased ICT usage has contributed to cybercrime risks in financial institutions?

- **Strongly Agree [ ]**
- **Agree [ ]**
- **Neutral [ ]**
- **Disagree [ ]**
- **Strongly Disagree [ ]**

9. Which cybercrimes are most prevalent in your institution? (tick where applicable)

Type of Cybercrime	Common	Very common	rare	Very rare	Neutal
Phishing attacks					
Malware/ Ransomware					
Identity theft					
Electronic fraud					
Insider cyber threats					
ATM/Card fraud					
Hacking/ Data breaches					
Social engineering					

10. During the past 12 months, how often has your institution experienced Cyber related incidents?

- **Very Frequently [ ]**
- **Frequently [ ]**
- **Occasionally [ ]**
- **Rarely [ ]**
- **Never [ ]**

SECTION C: IMPACTS OF CYBERCRIME ON FINANCIAL PERFORMANCE

11. To what extent has cybercrime affected the following areas of institutional performance? (1 = very High Impact, 2 = high Impact, 3 = moderate Impact , 4 =low impact impact 5 = no impact)

Performance Area	1	2	3	4	5
Financial losses					
Customer trust and confidence					
Operational efficiency					
Service delivery					
Institutional reputation					
Data security					
Employee productivity					
Regulatory compliance costs					

12. to what extent has cybercrime negatively affected customer confidence in digital banking services? (tick where applicable)

- **high [ ]**
- **very high [ ]**
- **Not Sure [ ]**
- **low [ ]**
- **very low [ ]**

13In your opinion, what relationship exists between the expansion of digital banking services and cybersecurity risks?

_____
_____
_____
_____

SECTION D: CYBERSECURITY STRATEGIES.

14. Does your institution provide cybersecurity awareness training to employees?

- **Yes [ ]**
- **No [ ]**
- **Sometimes [ ]**

15. Which cybersecurity measures are currently used in your institution? (tick all that applies)

- **Firewalls and Antivirus Systems [ ]**
- **Multi-factor Authentication [ ]**
- **Employee Awareness Training [ ]**
- **Data Encryption [ ]**
- **Regular System Audits [ ]**
- **Cybersecurity Policies [ ]**

- **Incident Response Plans [ ]**
- **not sure [ ]**

16. How effective are current Cybersecurity measures in:

Area	Very Effective	Effective	Neutral	Ineffective	Very Ineffective
Preventing attacks					
Detecting attacks					
Responding to incidents					**NOT**

17.Does your institution allocate sufficient resources to cybersecurity?

- **YES [ ]**
- **NO [ ]**
- **NOT SURE [ ]**

18. Are cyber incidents formally reported within the institution?

- **YES [ ]**
- **NO [ ]**
- **NOT SURE [ ]**

19. In your opinion how knowledgeable are employees regarding cybersecurity threats?

_____

_____

20.Does the institution comply with cybersecurity regulations issued by the Reserve Bank of Zimbabwe?

- **YES [ ]**
- **NO [ ]**
- **NOT SURE [ ]**

21. What additional measures would you recommend to reduce Cybercrime in Zimbabwean financial institutions?

_____

_____

THANK YOU FOR YOUR PARTICIPATION.

N.B Please do not disclose confidential institutional information or information that may identify specific Cyber incidents.

Appendix 2

INTERVIEW GUIDE

- How long have you been employed at this institution, what is your current role, and to what extent are you involved in cybersecurity, ICT, risk management, or operational decision-making?
- To the best of your knowledge, what major technological developments or digital banking innovations has your institution adopted between 2021 and 2025?
- What forms of cybercrime have you observed or become aware of within your institution or the Zimbabwean financial sector?
- To what extent do factors such as increased technology adoption, low employee awareness of cybersecurity practices, weak internal controls, and insider threats contribute to cybercrime incidents?

- How has cybercrime affected the financial performance of your institution?
- How has cybercrime affected customer confidence and trust?
- How has cybercrime affected affected your operational efficiency
- Without disclosing confidential information, are you aware of any significant cyber incidents that have affected your institution or the Zimbabwean banking sector? .
- What role, if any, do employee behaviours play in creating cybersecurity risks within financial institution.
- To what extent do challenges such as budget constraints, shortages of skilled cybersecurity personnel, technology limitations, regulatory compliance requirements, and user behaviour affect your institution's ability to prevent and manage cybercrime?
  What cybersecurity measures has your institution implemented to combat cybercrime, and how effective have these measures been in protecting the institution from cyber threats?

  a)Why do you think some measures perform better than others
  b)which measures have been the most effective?
  c) which measures have been the least effective
- What role do Reserve Bank of Zimbabwe regulations play in strengthening cybersecurity?
- How do technologies such as artificial intelligence affect both cybersecurity risks and cybersecurity protection?
- Based on your experience, how prepared do you believe Zimbabwean financial institutions are to deal with emerging cyber threats.

Appendix 3

turn it in report