

BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES



**EFFECTIVENESS OF MEASURES EMPLOYED BY FINANCIAL INSTITUTIONS TO
COMBAT CYBER THREATS. A SURVEY OF COMMERCIAL BANKS IN HARARE
CBD, ZIMBABWE.**

BY

LLOYD JOSEPH DUCHE

(B221275B)

**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.**

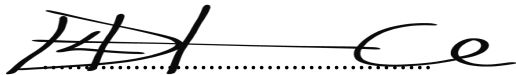
JUNE 2026

Approval form

Title: Effectiveness of measures employed by financial institutions to combat cyber threats. A survey of Commercial banks in Harare CBD, Zimbabwe.

To be completed by the student

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



(Signature of student)

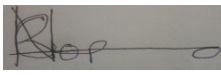
.....30/07/26

Date

To be completed by the supervisor

This dissertation is suitable for submission to the Faculty.

This dissertation has been checked for conformity with the Faculty guidelines.

(Signature of Supervisor).....

Date.....30/07/26

To be completed by the department chairperson

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



(Signature of Chairperson)

.....18...../...8...../..26.....

Date

Release form

NAME OF STUDENT: LLOYD JOSEPH DUCHE

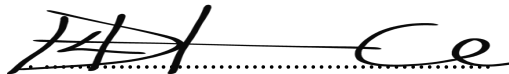
DISSERTATION TITLE: Effectiveness of measures employed by financial institutions to combat cyber threats. A survey of Commercial Banks in Harare CBD, Zimbabwe.

DEGREE TITLE: Bachelor of Commerce (Honours) degree in Financial Intelligence

YEAR GRANTED: 2026

Permission is hereby given to the Bindura University of Science Education Library to produce single copy of this dissertation and to lend or sell such copy for private, scholarly or scientific research purposes. Only the author reserves the other publication rights and; neither the dissertation nor extensive extracts from it may be printed or otherwise reproduced without the author's permission.

SIGNED



PERMANENT ADDRESS:

12012, Nyatsime phase 4

Mashonaland East

Zimbabwe

TELEPHONE:

+263773747373

EMAIL:

lloydduche27@gmail.com

DATE:

30/07/26

Declaration

I, Lloyd Joseph Duche, declare that this dissertation is my own original work and has not been submitted to any other institution for the award of any degree or qualification. All sources used have been duly acknowledged and referenced.

Signature:  Date: 30/07/26

Dedication

This dissertation is dedicated to those whose quiet strength, patience, and belief carried me through every stage of its completion. I am deeply indebted to my parents, Mr. Joseph Duche and Mrs. Magadalena Duche Mapetere, whose sacrifices and unwavering encouragement laid the foundation of my academic journey and shaped the values upon which my aspirations rest. I also extend my heartfelt appreciation to my siblings, Loraine, Liberty, Lawrence, Lisbon, and Lorinet, together with their families, for their constant support and enduring confidence in my efforts. Above all, I dedicate this work to my beloved wife, Vimbai Chokumanyara, whose love, patience, and steadfast encouragement sustained me through the most demanding moments of this journey and gave meaning to its completion.

Acknowledgments

I am profoundly indebted to all those whose support, in one form or another, made the completion of this study possible. My deepest gratitude is due to my parents, Mr. Joseph Duche and Mrs. Magadalena Mapetere, whose sacrifices, guidance, and steadfast belief in my abilities have formed the foundation of my academic journey. I am equally indebted to my siblings, Loraine, Liberty, Lawrence, Lisbon, and Lorinet, together with their families, for their constant encouragement and enduring support throughout this endeavor. My heartfelt appreciation is extended to my wife, Vimbai Chokumanyara together with my best friend Trish Chikawa whose patience, strength, and sustained support carried me through the most demanding stages of this research. Finally, I give thanks to Almighty God for His grace, wisdom, and guidance throughout this academic journey. To Him be all the honor.

Abstract

Cyber threats in Zimbabwe's financial sector continue to threaten the stability, data security, and trust of digital banking systems in commercial banks. The study aimed to evaluate the effectiveness of cybersecurity measures in commercial banks located in Harare CBD. The objectives of the study were to identify the cybersecurity measures currently employed, to determine their effectiveness in combating cyber threats, to explore challenges encountered in implementing these measures, and to recommend strategies for improving cybersecurity effectiveness. The study adopted a pragmatist mixed methods research design, using a sample of 40 bank employees selected through questionnaires and interviews, with data analyzed using SPSS and thematic analysis. Findings revealed that commercial banks employ cybersecurity measures including firewalls, encryption, multi-factor authentication, intrusion detection systems, backups, and staff awareness training, while advanced systems such as Security Information and Event Management (SIEM) remain limited. The study further found that although preventive, detective, and recovery controls are implemented, their effectiveness is constrained by weak system integration and inconsistent application across institutions. Key challenges identified include weak regulatory enforcement, shortage of skilled personnel, outdated systems, financial constraints, and employee non-compliance with cybersecurity policies. It was concluded that the effectiveness of cybersecurity measures depends on the integration of technology, human capacity, and governance frameworks. It is recommended that commercial banks adopt integrated cybersecurity systems and strengthen continuous staff training to enhance cyber threat detection and response.

Keywords: *Cybersecurity, commercial banks, cyber threats, Harare CBD, cybersecurity effectiveness, digital banking.*

TABLE OF CONTENTS

APPROVAL FORM.....	II
RELEASE FORM.....	III
DECLARATION.....	IV
DEDICATION.....	V
ACKNOWLEDGMENTS.....	VI
ABSTRACT.....	VII
TABLE OF CONTENTS.....	VIII
CHAPTER I.....	1
INTRODUCTION.....	1
1.0 INTRODUCTION.....	1
1.1 BACKGROUND OF STUDY.....	1
1.5 Objectives of the Study.....	4
1.6 SIGNIFICANCE OF THE STUDY.....	5
1.6.1 To banks.....	5
1.6.2 To policy makers.....	5
1.6.4 To the Body of Knowledge.....	6
1.6.5 To the University.....	7
1.7 DELIMITATIONS.....	7
1.8 LIMITATIONS OF THE STUDY.....	8
1.8.1 Limited Generalisability.....	8
1.8.2 Data Sensitivity and Response Bias.....	8

1.8.3 Data Access Constraints.....	9
1.8.4 Temporal Scope.....	9
CHAPTER II.....	11
LITERATURE REVIEW.....	11
2.0 INTRODUCTION.....	11
2.1 PURPOSE OF LITERATURE REVIEW.....	11
2.2 CONCEPTUAL FRAMEWORK.....	12
2.2.1 Concept of Cybersecurity.....	12
2.2.2 Cybersecurity Measures and Effectiveness.....	12
2.2.2.1 Preventive Measures.....	12
2.2.2.2 Detective Measures.....	13
2.2.2.3 Corrective Measures.....	14
2.2.2.4 Human and Organisational Measures.....	15
2.2.3 Challenges in Implementing Cybersecurity Measures.....	16
2.3 THEORETICAL LITERATURE.....	17
2.3.2 Technology Acceptance Model (TAM).....	18
2.3.3 Integration of DiD and TAM.....	18
2.4 EMPIRICAL EVIDENCE.....	19
2.4.1 Objective 1 - Measures Employed to Combat Cyber Threats.....	19
2.4.1.1 Mashizha and Kanengoni (2024) – The Adequacy of Cybersecurity in Financial Institutions in Zimbabwe.....	19
2.4.1.2 Mutanda & Chrispen (2023) – Cyber fraud risk management strategies in Zimbabwean commercial banks.....	19
2.4.1.2 Mutanda & Chrispen (2023) – Cyber fraud risk management strategies in Zimbabwean commercial banks.....	20
2.4.1.3 Maphosa, V. (2023) – An overview of cybersecurity in Zimbabwe’s financial services sector.....	20
2.4.1.4 Dzomira (2014) – Electronic fraud risk and internal control	

measures in Zimbabwean banking sector.....	20
2.4.2.5 Chigaro (2017) – E-Banking Security Strategies in Zimbabwe.....	21
2.4.2 Objective 2 - Effectiveness of Cybersecurity Measures.....	21
2.4.2.1 Akinbowale, Klingelhöfer and Zerihun (2024) – Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation.....	21
2.4.2.2 Mutanda and Chrispen (2023) – Towards a Cyber Resilient Banking System: Effectiveness of Cyber Fraud Risk Management Strategies Adopted by Commercial Banks in Zimbabwe.....	22
2.4.2.3 Chigaro (2017) – An Assessment of the Effectiveness of E-banking Security Strategies in Stanbic Bank Zimbabwe.....	22
2.4.2.4 Maphosa, V. (2023) – An overview of cybersecurity in Zimbabwe’s financial services sector.....	23
2.4.3.1 Dzingirai (2022) – Managerial Challenges Under FinTech: Evidence from Zimbabwean Commercial Banks.....	23
2.4.3.2 Mugari et al. (2016) – Cybercrime and Institutional Vulnerabilities in Zimbabwe’s Financial Sector.....	24
2.4.3.3 Maphosa (2023) – Human Factors and Skills Constraints in Cybersecurity Implementation within Financial Institutions.....	24
2.4.3.4 Dzomira (2014) – Institutional and Regulatory Constraints in Managing Electronic Fraud in Zimbabwean Banks.....	24
2.4.3.4 Chikowero and Nyoni (2023) – Resource Constraints and Cybersecurity Investment Challenges in Zimbabwean Financial Institutions.....	24
2.4.4 Objective 4 - Strategies and Recommendations for Improving Cybersecurity.....	25
2.4.4.2 Takavarasha Jr, Van Heerden, Thakur and Jordaan (2023) – Cyber-security in the era of the COVID-19 pandemic: a developing countries’ perspective.....	26
2.4.4.3 Gumbo, Masimba and Zuva (2025) – A Cybersecurity Framework	

for Enhancing Public Sector Digital Resilience in Emerging Economies.....	26
2.4.4.4 Kanyongo and Wadesango (2025) – Cybersecurity and Risk Mitigation Strategies in Commercial Banks.....	27
CHAPTER III.....	30
RESEARCH METHODOLOGY.....	30
3.0 INTRODUCTION.....	30
3.1 RESEARCH PHILOSOPHY.....	30
3.2 RESEARCH DESIGN AND JUSTIFICATION.....	31
3.3 TARGET POPULATION.....	32
3.4 SAMPLING TECHNIQUES.....	33
3.5 SAMPLE SIZE.....	33
3.6 SOURCES OF DATA.....	34
3.6.1 Primary Data.....	34
3.6.2 Secondary Data.....	35
3.7 RESEARCH INSTRUMENTS.....	35
3.7.1 Structured Questionnaires.....	35
3.7.2 Interviews.....	37
3.8 DATA COLLECTION AND APPROPRIATENESS OF PROCEDURES.....	38
3.9 DATA PRESENTATION AND ANALYSIS.....	38
3.10 VALIDITY.....	39
3.11 RELIABILITY.....	39
3.12 ETHICAL CONSIDERATIONS.....	40
3.13 CHAPTER SUMMARY.....	40
CHAPTER IV.....	41
DATA PRESENTATION, INTERPRETATION AND ANALYSIS.....	41
4.0 INTRODUCTION.....	41
4.1 RESPONSE RATE.....	41
4.2 DEMOGRAPHIC PROFILE CATEGORIES.....	43

4.2.1 Gender of Respondents.....	46
4.2.2 Age Distribution of Respondents.....	46
4.2.4 Job Position of Respondents.....	46
4.2.5 Department of Respondents.....	47
4.2.6 Years of Work Experience of Respondents.....	47
4.3 Cybersecurity Measures Currently Employed commercial banks in Harare CBD.....	47
4.3.1 Firewalls.....	49
4.3.2 Multi-Factor Authentication (MFA).....	50
4.3.3 Data Encryption.....	50
4.3.4 Intrusion Detection and Prevention Systems (IDS/IPS).....	51
4.3.6 Patch Management.....	52
4.3.7 Data Backup Systems.....	53
4.3.8 Disaster Recovery Plans.....	54
4.4.9 Staff Cybersecurity Training.....	54
4.4.3 Firewalls.....	57
4.4.4 Data Encryption.....	58
4.4.6 Patch Management.....	59
4.4.7 Disaster Recovery Planning (DRP).....	59
4.5 CHALLENGES FACED IN IMPLEMENTING CYBERSECURITY MEASURES.....	62
4.5.1 Regulatory and Institutional Challenges (Weak regulatory frameworks hinder effective cybersecurity implementation in commercial banks.).....	64
4.5.2 Skills and Human Resource Challenges (Lack of skilled cybersecurity personnel affects implementation of cybersecurity measures in commercial banks).....	64
4.5.3 Technological (Legacy Systems) Challenges (Outdated legacy systems limit the effectiveness of modern cybersecurity tools in commercial banks).....	65
4.5.4 Financial and Resource Constraints (Limited financial resources restrict investment in cybersecurity infrastructure within commercial banks.).....	66

4.6 Recommended Strategies to Enhance the Effectiveness of Cybersecurity Measures in Commercial Banks.....	67
4.6.1 Increase Staff Training.....	69
4.6.2 Regular System Updates.....	70
4.6.3 Strengthen MFA Systems.....	70
4.6.4 Invest in Cyber Technologies.....	71
4.6.5 Conduct Awareness Campaigns.....	72
4.6.6 Improve Incident Response.....	72
4.6.7 Strengthen Stakeholder Collaboration.....	73
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS.....	75
5.0 INTRODUCTION.....	75
5.1 SUMMARY OF THE STUDY.....	75
5.2.1 To identify cybersecurity measures currently employed by commercial banks in Harare CBD.....	76
5.2.2 To determine the effectiveness of cybersecurity measures in combating cyber threats.....	77
5.2.3 To explore the challenges encountered by the commercial banks located in Harare CBD when implementing measures to combat cyber threats.....	77
5.2.4: To recommend strategies for improving the effectiveness of cybersecurity measures in commercial banks.....	78
5.3 CONCLUSION.....	79
5.4 RECOMMENDATIONS.....	79
5.4.2 Strengthen Continuous Cybersecurity Training and Awareness.....	80
5.4.3 Enhance Investment in Advanced Cybersecurity Technologies and Collaboration.....	80
5.5 SUGGESTIONS FOR FUTURE STUDIES.....	80
REFERENCES.....	82

APPENDIX A.....	87
APPENDIX B.....	88
INTERVIEW GUIDE.....	88
APPENDIX C.....	89
RESEARCH QUESTIONNAIRE.....	89

LIST OF TABLES

TABLE 4.1: RESPONSE RATE.....	42
TABLE 4.2: DEMOGRAPHIC PROFILE CATEGORIES OF RESPONDENTS.....	43
TABLE 4.3: CYBERSECURITY MEASURES USED IN COMMERCIAL BANKS (HARARE CBD) (N=32).....	48
TABLE 4.4: CHALLENGES FACED BY COMMERCIAL BANKS IN IMPLEMENTING CYBERSECURITY MEASURES (N = 32).....	62
TABLE 4.5: RECOMMENDED STRATEGIES TO ENHANCE THE EFFECTIVENESS OF CYBERSECURITY MEASURES IN COMMERCIAL BANKS.....	68

LIST OF FIGURES

FIGURE 4.1; EFFECTIVENESS OF CYBERSECURITY MEASURES EMPLOYED IN HARARE CBD.....	56
--	----

CHAPTER I

INTRODUCTION

1.0 Introduction

Cybersecurity has become a critical concern for financial institutions globally due to the escalating frequency, complexity, and financial impact of cyber threats. Banks operating within Harare's Central Business District (CBD) faced increasingly sophisticated cyber risks arising from digital banking platforms, electronic payment systems, and interconnected financial technologies. This study examined the effectiveness of cybersecurity measures employed by banks in Harare's CBD, with the aim of assessing, evaluating, and refining existing defensive mechanisms against cyber threats. By focusing on commercial banks located in Harare's CBD, the study contributed to strengthening cybersecurity resilience within Zimbabwe's financial sector. The chapter outlined the background to the study, the problem statement, research aim, and objectives. It also presented the scope of the study, delimitations, and acknowledged potential limitations and biases to ensure transparency and academic rigor.

1.1 Background of study

The rapid integration of digital technology in global financial sector has led to profound transformation in banking industry thereby resulting in convenience, efficiency, and access to banking services (Vives, 2017). Banks increasingly made use of online platforms, internet banking and mobile banking, electronic

funds transfer and automated payment systems to optimize banking operations and expand financial inclusion (Gozman et al., 2018; Moro et al., 2021). The use of digital technology has expanded the surface of attacks on financial institutions thereby exposing them to various cyber threats.

The financial sector, due to high volume of financial assets and information, is seen as the top target for cyber-attacks globally. There are several financial institutions like JPMorgan Chase, Citigroup and Bank of America that faced large-scale cyber breaches and data exfiltration (Kumar et al., 2022). In total, almost 70% of banks faced at least one cyber-attack and on average costs per attack were around \$18.4 million (Accenture, 2020). The financial sector had incurred the second highest data breach costs in the world due to regulatory fines, operational disruption, loss of information and damage to the reputation of the institutions (IBM, 2022). As financial institutions increasingly rely on third parties and cloud services for various operations and management, vendor and supply chain risks also rose (OMFIF, 2020).

Considering such cyber-attacks, the significance of cybersecurity for financial institutions escalated to an unprecedented level. About 73% of banks around the world acknowledged cybersecurity as a major organizational risk and over 71% of them reported having increased their investment in cybersecurity infrastructure including intrusion detection systems, encrypted systems and ongoing monitoring mechanisms (Deloitte, 2022). Cyber criminals continue to adopt new advanced technologies like ransomware, phishing, malware and social engineering and resulting in financial loss (Kshetri, 2022).

Similarly, cyber security threats to financial institutions have rapidly escalated across Africa, with Interpol reporting that cyber-attacks against financial institutions grew by 15% year-on-year, and banking sector had among the top targets. Around 64% of organizations were hit by at least one cyber attack and almost one in five organizations faced a ransomware attack in 2020 (Kaspersky,

2020; Symantec, 2020). Total annual losses suffered by economies in Africa because of cybercrime were about \$3.5 billion (UNCTAD, 2020) and cost per organization at \$4.35 million (IBM, 2020), underscoring the need to improve capacity across the continent (ITU, 2020).

In the Zimbabwean context, banking institutions in Harare Central Business District were not spared from such threats. The growing reliance on digital channels like internet and mobile banking at financial institutions like ZB Bank, CBZ Bank, Stanbic Bank Zimbabwe, and Standard Chartered Bank Zimbabwe in Harare had exposed the financial sector to various cyber risks. The Reserve Bank of Zimbabwe (RBZ, 2020) had acknowledged cyber threats to be one of the main threats to financial stability in Zimbabwe based on vulnerabilities of the various payment systems, online banking platform, customer data and others. Estimates show about 70% of the Zimbabwean banks faced one or another form of cyber attacks with average costs for each attack ranging up to \$1 million.

One such widely reported case was the ransomware attack on ZB Financial Holdings, orchestrated by a notorious hacker group named "Mad Liberator," which was accused of breaching and leaking sensitive customer data from the bank when the ransomware payment demand was not met (TechZim, 2019; TechZim, 2024). This attack brought into focus the weaknesses inherent in Zimbabwe's financial system including absence of advanced threat detection systems and fragmented security framework. It is estimated that Zimbabwean banks had lost as much as \$1.8 billion on an average in each financial year due to cybercrimes. Most common cyber threats identified by The Reserve Bank of Zimbabwe (2019) were phishing, social engineering and malware attacks.

Against this background, the current study seeks to investigate the effectiveness of cybersecurity measures employed by banks in Harare Central Business District and to inform better cyber security framework design capable of mitigating cyber risk and ensuring continued trust in the digital banking industry.

1.3 Problem Statement

The rapid proliferation of cyber threats within the Zimbabwe financial sector is an issue that could undermine national economic stability, financial security, and public trust in electronic banking. Notwithstanding the rapid adoption of electronic financial services, there was limited empirical evidence to ascertain the efficiency of the cyber security measures used by financial institutions within Zimbabwe. The National Risk Assessment Report (2015) revealed huge economic losses through cybercrime and later studies concluded poor coordination of cyber awareness programmes and organizational readiness (Mutunhu et al., 2022). Given the majority of financial institutions are located within Harare's Central Business District (CBD) and that these are central to the national payment system, an assessment of the efficiency of banking institutions' cyber security measures in this area was necessary. This lacuna of information, arising from a dearth of empirical evidence on the issue, hampered informed policy formulation and decision making at organizational level (RBZ, 2020). The purpose of this study therefore was to fill this lacuna and to make empirically grounded recommendations for improving cyber security.

1.4 Research Aim

The purpose of the study was to assess the impact of the current cybersecurity measures adopted by banks located in Harare Central Business District on the security of their financial systems against cyber-attacks, and to manage cyber-risks in an increasingly complex and rapidly evolving cyber-crime environment. Several research objectives were pursued to help achieve this purpose.

1.5 Objectives of the Study

1. To identify the cybersecurity measures currently employed by Commercial banks in Harare CBD.

2. To determine the effectiveness of the current cybersecurity measures employed by Commercial banks in Harare CBD to combat cyber threats.
3. To explore the challenges encountered by the commercial banks located in Harare CBD when implementing measures to combat cyber threats.
4. To recommend strategies to enhance effectiveness of cybersecurity measures in combating cyber threats in Commercial Banks located in Harare CBD.

1.5 Research Questions

1. What cybersecurity measures are currently being employed by commercial banks?
2. How effective are cybersecurity measures in combating cyber threats?
3. What challenges have commercial banks in Harare CBD encountered in implementing effective cybersecurity strategies?
4. What strategies can be recommended to enhance the effectiveness of cybersecurity measures?

1.6 Significance of the Study

This study holds considerable significance across various domains.

1.6.1 To banks

The study recommended practical solutions for strengthening security within Zimbabwean banks, particularly within the commercial banking industry in Harare, to curb monetary risks and customer information from security threats and assure customer confidence. It deepened awareness on optimal methods to secure financial infrastructure, guide internal control systems and assist banks in meeting internal regulatory needs and global benchmarks, and through it reinforce the institutions, contain risks and retain confidence.

1.6.2 To policy makers

The study results provided policymakers and regulatory bodies like the Reserve Bank of Zimbabwe (RBZ) and the Zimbabwe Financial Intelligence Unit (ZFIU) with the relevant empirical data about the nature of current cyber threats and the extent to which defense mechanisms currently in use are adequate. It helped influence discussions within the regulatory sphere concerning the adequacy and effectiveness of preparedness and response to cybercrime, which fit into the broader initiatives in the modernization of regulation of the financial sector, which was further supported by the state's wider direction toward the adoption of digital technologies and financial depth in the National Development Strategy (NDS) frameworks.

1.6.3 To the nation

The research was therefore relevant at a national level and was part of the process of building a secure and resilient digital economy in Zimbabwe. The assessment of the security measures in banks, for example, contributed to the security of the vital financial infrastructure required to support national economic stability and trust in the security of digital financial transactions. These objectives were consistent with policy imperatives expressed by national strategies. NDS1 stipulated the achievement of an advanced information communication technology-driven and digitally enabled economy; and this strategy advocated for e-government services and a national cyber security infrastructure as measures that could facilitate good service delivery and a reduction in the prevalence of cybercrimes. The successor National Development Strategy 2 emphasized the contribution of science, technology, innovation, and human capital in creating a digitally enabled economy and deepening financial inclusion.

Consistent with these policy objectives, the Government adopted a National Cybersecurity Strategy in 2025 outlining the mechanisms for strengthening

national capacity to prevent, detect, respond to and recover from cyberattacks in all sectors of public and private organizations including financial sector service providers. By framing the research in this policy context, it generated findings with implications for robust implementation of national cyber security initiatives, securing national assets, and achieving the desired objectives set out in the policy documents of the two-five-year national development strategies.

1.6.4 To the Body of Knowledge

The research provided value by making an addition to knowledge in terms of management of financial crime and cybersecurity in developing countries. By selecting banks within the Central Business District of Harare, the research identified a research gap concerning empirical evidence of the cybersecurity situation in the Zimbabwean banking sector. The study enhanced knowledge on how banks in developing countries manage the threat of cyber attacks and critically evaluated the relative importance of alternative ways to manage the threat. It added to literature that explored cyber risk management, information security practices, institutional preparedness and other aspects. The results provide a benchmark for future studies including case studies across different countries or sectors. The information generated from this research can provide valuable insight into curriculum development of topics like finance, information security and digital governance. Thus, it contributes to the development of knowledge in cybersecurity, financial stability and national development.

1.6.5 To the University

The research supplemented the academic resources of the University by giving actual studies on the issue of cybersecurity in the financial sector. The research was an essential guide for students and future researches, facilitating both teaching and learning in the disciplines of finance, information systems and risk management. The study was in conformity to Zimbabwe National Development

Strategies (NDS1 & 2) which aimed at digital transformation of the economy and capacity building which the study contributed positively.

1.7 Delimitations

The research was limited to the Commercial banks that operate in the CBD of Harare, Zimbabwe, as indicated by the research purpose to investigate the efficiency of actions to be taken in order to overcome the threats of cyber security in the banking sector. 2022-2025 was chosen for the time frame of the study to evaluate current cyber security strategies, institution's actions and new threat patterns in a current operating environment. The research covered eight institutions that are CBZ Bank Limited, FBC Bank Limited, Nedbank Zimbabwe Limited, Metbank Zimbabwe Limited, NMB Bank Limited, First Capital Bank Limited, Stanbic Bank Zimbabwe Limited and Steward Bank Limited, these institutions were chosen because they are major financial institutions within the Zimbabwean financial system. The research applied qualitative methodology that was framed by the Defense-in-Depth (DiD) Theory and the Technology Acceptance Model (TAM), which provided for a coherent perspective to understand multiple security controls and acceptance of security technologies within the organization, respectively. The research concentrated on the CBD of Harare due to the reason that it was the Centre of the financial decision-making and operations that facilitated information about top-level actions, strategies and mechanisms for security within the national banking sector.

1.8 Limitations of the Study

Despite its academic contribution, the study encountered several limitations during its execution.

1.8.1 Limited Generalizability

The scope of the study was restricted to commercial banks located in Harare's CBD and no other categories of financial institutions like merchant banks, investment banks, microfinance banks, insurance companies etc. Such limitations were necessary to ensure that the research was kept at an appropriate depth and manageable scale, it however restricts the generalization of the findings beyond the chosen type of bank and location. Therefore, the conclusions on the current state of the cybersecurity practices are derived primarily from the context of urban commercial banks. This could be made broad by including other categories of financial institutions in the other parts of Zimbabwe in future research.

1.8.2 Data Sensitivity and Response Bias

One of the main difficulties faced by the researcher was in the sensitivity of data and the possible biased responses. A major issue was the hesitation on participating in banks in revealing substantial details about their internal cybersecurity systems, internal controls and past cyber incidents. This could be directly related to the confidentiality requirements and the risk to the banks' reputation. Measures were taken by the researcher to ensure data reliability in terms of confidentiality, anonymity and cross-checking through several sources; however, there was a risk that selective reporting and social desirability could still affect the results. This could potentially be overcome in further studies by making use of independent and anonymized third-party audits or, if access were possible, through regulated data.

1.8.3 Data Access Constraints

The access to extensive and detailed cyber-security data was a constraint due to the tight security measures and NDAs within the banking environment. Such

controls prevent further technical investigation into some parts of the research. Instead, other methods like interview and structured questionnaire, alongside public reports, were adopted. However, inability to access in-house systems and internal reports restricted exploration of some mechanisms. There is potential for formal partnerships with regulatory bodies or industrial associations in future investigations to achieve broader data access.

1.8.4 Temporal Scope

The period 2022–2025 for examination of cybersecurity measures and threats was considered appropriate in order to gain insight of recent trends but the approach may not have provided a wider scope of institutional experiences to threats on the longer term, and their past responses prior to the indicated timeframe. Consequently, results are focused on contemporary responses and may not be representative of how cybersecurity has evolved within Zimbabwean banks. A broader timeframe covering the earlier part of this millennium could provide an institutional learning and evolution analysis.

1.9 Assumptions

The following is assumed to be true in this study:

- The use of cyber threats is increasing in the banking sector.
- Respondents are adequately skilled in cybersecurity concepts and are willing to answer truthfully.
- The gathered data can be utilized to recommend measures to improve cybersecurity posture of Zimbabwean banks.

1.10 Chapter Summary

This chapter presented the background of the study by contextualizing cyber security as a prominent issue in today's banking environment of commercial

banks operating within the Harare Central Business District. It provided the background of the study and presented the problem of study which emanates from increasing cyber-attacks while the cyber security measures in banking system in Zimbabwe are under-researched. It identified the aim and objectives of the study and formulated the research questions. Its significance was then examined in terms of key stakeholders, and these are banks, policymakers, country, academia, and university, highlighting the implications for financial stability, policy making, knowledge and so on. Delimitations and limitation were stated in the study to increase the transparency of the research methodology. Lastly, assumptions of the study were presented.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

The provision of cybersecurity is no longer an option but an essential function within modern banking, as banks move towards fully digitalizing the management of financial transactions, customer data and sensitive personal information. With cyber-threats becoming both more pervasive and more sophisticated, the financial industry becomes vulnerable to data losses and breaches as well as financial, and public confidence damage, thus requiring banks to put into place adequate security measures to ensure the integrity, secrecy and availability of data.

2.1 Purpose of Literature Review

This literature review aims to bring together empirical and theoretical studies relating to bank security mechanisms. It further aims to provide a basis upon which the link between the adoption of security measures and their effectiveness is established (Eddington et al., 2019). It aims to highlight gaps in knowledge and compare world best practices in the light of Zimbabwean banks (Farooq et al., 2021). The collection of numerous research articles contributes to establishing the comprehensive theoretical and conceptual framework needed in order to analyze the implementation and success of security measures in banking institutions (Zhang & Zhao, 2018).

2.2 Conceptual Framework

It states that cybersecurity principles and their relation that are foundational to banking are given in conceptual framework. It helps with the evaluation of efficiency of the measures taken. It helps to protect confidential information and to ensure the continuity of business operations (Kizza, 2017).

2.2.1 Concept of Cybersecurity

Cybersecurity can be defined as a collection of technologies, policies, procedures and practices in order to protect a system (including hardware, software and data) from unauthorized access or manipulation and to maintain integrity of system data (Ahmad, 2018). In case of banking sector, security measures to protect confidentiality of data, integrity of transactions and availability of information are called cybersecurity. The banking sector is at higher risk because the data being managed in banks is considered sensitive, therefore banks become targets to many cyber criminals (Reddy, 2021). The risks can be minimized using security preventive, detective measures as well as organization policies. Furthermore, it also relates to rules and regulations like ISO/IEC 27001 for controlling protection of information as well as the security of system, which must be followed by banks, according to rules.

2.2.2 Cybersecurity Measures and Effectiveness

Banks use preventative, detective, corrective, and human-centric methods in their efforts to protect systems and information (Farooq et al., 2021) measures are only as effective as the context in which they are applied, how well they are implemented, and how they are assessed and monitored within institutions (Ahmad, 2018)

2.2.2.1 Preventive Measures

Preventative measures are utilized so that cyber-attacks do not materialize. These involve firewalls, multi-factor authentication and encryption methods (Eddington et al. 2019).

a) Firewall Systems

A firewall is a network security device that examines the traffic on networks and filters according to pre-defined security rules. It works by prohibiting unauthorized access to bank networks and preventing malicious traffic from entering the network (Stallings & Brown, 2015). According to one study, with efficient firewalls many intrusion attempts can be eliminated by banks (Accenture, 2020). In this way, they act as a first line of defense and decrease the possibility of system compromise, helping to secure customer data (Farooq et al., 2021).

b) Multi-Factor Authentication (MFA)

MFA provides better access control by asking the user to authenticate the required information by more than one credential i.e. Passwords, one-time passwords and biometric authentication (Ahmad, 2018). It reduces the possibility of passwords being stolen or guessed. Banks who use MFA have fewer numbers of unauthorized access compared to not using MFA (Eddington et al., 2019). It works very well with on-line banking and mobile banking where phish attacks are frequent (Green, 2019).

c) Data Encryption

By encrypting data, important files become unreadable to anyone not given the right permission, therefore only authorized individuals would be able to use the encrypted data (Zhang & Zhao, 2018). Encryption is also widely used by banks for

the storing and transacting of sensitive information. Based on research, the occurrences of data breaches are minimized due to the implementation of encryption (Accenture, 2020).

2.2.2.2 Detective Measures

Detectives can alert banks to an ongoing or potential security incident by implementing detective measures (Reddy, 2021).

a) Intrusion Detection and Prevention Systems (IDS/IPS)

IDS and IPS work by constantly monitoring network activity to spot malicious behavior, policy breaches or any anomaly (Kizza, 2017). IDS notify administrators and IPS block malicious activity in real time. There are a few studies showing how banks with IDS/IPS detect attacks faster and react to damage them more efficiently (Farooq et al., 2021).

b) Security Information and Event Management (SIEM)

SIEM systems combine information from various sources of security data so that they can identify trends of malicious behavior (ECB, 2020). These systems generate automated alerts and analysis capabilities to detect threats. Evidence has shown that SIEM enhanced banks achieve higher rates of early detection of threats, better digital forensics and increased regulatory compliance (Green, 2019).

2.2.2.3 Corrective Measures

Corrective actions restore the banking system following a security incident and will prevent future incidents from occurring (Zhang & Zhao, 2018).

a) Patch Management

The aim of patch management is to provide software updates which are intended to fix weaknesses (Stallings & Brown, 2015). Banks that practice fixed patch schedules make themselves less susceptible to attack by vulnerability exploit (Farooq et al., 2021). Investigations indicate a reduction in incidents and increase in system reliability with patch management (Eddington et al., 2019).

b) Data Backup and Recovery

Backups are secure copies of sensitive data, used for data recovery, should data loss occur, or in the event of a ransomware attack (Green, 2019). Automated, encrypted backups provide fast data recovery, ensuring continued business operations. Available evidence shows that banks with strong backup strategies can restore up to 95% of data within 48 hours following a breach (Zhang & Zhao, 2018).

c) Disaster Recovery Planning

Disaster recovery planning defines the steps to be taken to recover banking operations after major disasters (Krutz & Vines, 2010). When a bank has had tested DR plans it can mean the restoration of operations is quicker, financial losses will be smaller, and the institution will recover much faster (Farooq et al., 2021). DR plan testing has to be performed regularly to maintain customer confidence and institutional stability (ECB, 2020).

2.2.2.4 Human and Organizational Measures

Human behavior and organizational culture are critical in the effectiveness of cybersecurity measures (Ahmad, 2018). Employee training, awareness campaigns, and management oversight reduce the risk of human error, a leading cause of breaches (Green, 2019). Studies highlight that banks promoting a security-conscious culture achieve better adherence to protocols, improved incident response, and enhanced overall cybersecurity performance (Farooq et al.,

2021).

2.2.2.5 Overall Effectiveness of Cybersecurity Measures

The success of the measures banks are taking to secure their systems depends upon how they are incorporated, strategized, and evaluated within their processes. Research has shown that the successful protection of financial institutions against cyber-attacks relies on a comprehensive, layered security approach including preventative, detective, corrective and human-related measures (Zhang & Zhao, 2018; NIST, 2020). This approach is closely linked to Defense-in-Depth (DiD) strategy. DiD seeks to apply multiple overlapping security controls to protect critical assets from threats by covering vulnerabilities and minimizing the extent of the potential attack (Ahmad, 2018). Preventive measures such as firewalls, multi-factor authentication and encryption, reduce the chances of attacks being successful; whereas detective measures such as IDSs/IPSs and SIEM platforms help detect and address threats at an early stage (Eddington et al., 2019; Farooq et al., 2021). Corrective measures such as patch management, data backups and disaster recovery enable recovery from events, while preventing them from happening again and improving system resilience (Zhang & Zhao, 2018; Green, 2019). Human and organizational factors are an important part of achieving a higher level of cybersecurity effectiveness; where employees' awareness, training programs and an organizational culture aware of security risks will reduce the likelihood of human errors, which still represents a large portion of security incidents in financial institutions (Ahmad, 2018; Farooq et al., 2021). The adoption of a pro-cybersecurity organizational culture enables faster response times and higher compliance with security policies.

Moreover, cyber-attacks are constantly evolving, thus continuous monitoring, evaluating and upgrading of systems are necessary to retain long-term efficiency. Studies have shown that those organizations that assess their cyber security framework and adapt it are best able to deal with new cyber-threats and maintain

integrity (Accenture, 2020; NIST, 2020). Regarding Zimbabwean banks, the integration of international best practices with the local reality have helped the improvement of security within banking systems and the protection of their financial and reputational assets (Farooq et al., 2021; Zhang & Zhao, 2018).

To conclude, the integration and coordinated management of security tools, processes, human beings, and regulations at the organizational level is vital in maximizing the security of banking organizations, mitigating both the likelihood and the impact of cyberattacks while increasing customer trust, operational resiliency and the organization's sustainability.

2.2.3 Challenges in Implementing Cybersecurity Measures

Another significant challenge is that cyber threats are evolving at a rapid rate. Cyber criminals create new methods of attacking systems, such as using Ransomware, Phishing scams or Zero-day attacks that can exploit security gaps in systems (Reddy, 2021). Banks therefore need to update and upgrade their systems continually to protect themselves and this is time-consuming and costly (Farooq et al., 2021). High implementation costs. The initial cost for implementation of systems such as SIEM, IDS/IPS and encryption technologies are very expensive, as is the ongoing maintenance of them (Accenture, 2020).

Human element is another significant threat. Staff may resent new systems and refuse to use them or not follow procedures because they don't have adequate training or they just don't care about them (Ahmad, 2018). Insider threats are a continued problem in the banking environment whether intentional or unintentional (Kizza, 2017). Regulatory and compliance constraints can create significant hurdles to implementation. Banks must comply with a variety of local and international laws which can sometimes be contradictory and require complex monitoring and reporting procedures (Stallings & Brown, 2015). Integration issues: In many cases legacy and modern technology are forced

together, which has a potential to leave security gaps (Zhang & Zhao, 2018).

2.3 Theoretical Literature

The primary frameworks that guide this research are the Defense-in-Depth (DiD) Theory and Technology Acceptance Model (TAM). Some additional relevant constructions were used for theoretical support.

2.3.1 Defense-in-Depth (DiD) Theory

The Defense-in-Depth (DiD) theory is a security approach that uses several layers of defense against cyber threats in systems, networks, and data (Kizza, 2017; NIST, 2020). The main tenet is that "no single control will work alone, instead they will need to be used in combination for preventive, detective, and reactive measures to decrease the overall risk of cyber-attack" (Stallings & Brown, 2015; Krutz & Vines, 2010). Preventive controls, detective controls and responsive controls are discussed and explained as firewalls, antivirus software, access restrictions, intrusion detection system, SIEM (Security Information and Event Management), incident response, and disaster recovery plan (Stallings & Brown, 2015; Krutz & Vines, 2010).

The applicability of this theory to the study is highlighted in the setting of commercial banks within Harare CBD where commercial banks deal with critical financial data and bear cyber threat. The study also found that the implementation of multi-layer security measures is still low in Zimbabwean banks as they still suffer hacking, malware and phishing attempts (Mashizha and Kanengoni 2024). The DiD framework thus presents a model for evaluating the multiple security layers working together to protect the financial sector.

2.3.2 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) created by Davis (1989) proposes that

technology adoption is determined by user's perceived ease of use and perceived usefulness of technology (Ahmad, 2018). In terms of Zimbabwean banks, sophisticated cybersecurity systems would be of little use or would not be used to their full potential by personnel if they have not adopted them or lack the required training and knowledge. According to Maphosa (2024) shortage in staff skills and awareness about cybersecurity issues are key constraints for technology adoption. TAM therefore contributes to understanding how human and organizational factors may make or break a cybersecurity strategy in Harare CBD banks.

2.3.3 Integration of DiD and TAM

DiD combined with TAM will constitute the framework of the current study taking into consideration the technical aspects of security and the behavioral aspect impacting on the adoption of the measures and proper utilization of them. DiD presents the necessary structural and technological safeguards to protect sensitive data, while TAM explains why this framework could either be successful or be not useful based on the attitude, belief and behavior of staff.

2.4 Empirical Evidence

This section will look at empirical research related to effectiveness of measures used by financial institutions to improve the security of information systems (cybersecurity). It will look at research done and arranged into 4 different themes which are: Measures used to deter cyber-attacks; effectiveness of security measures; difficulties that banks face; strategies/ recommendations to enhance security in commercial banks in Harare CBD, Zimbabwe.

2.4.1 Objective 1 - Measures Employed to Combat Cyber Threats

2.4.1.1 Mashizha and Kanengoni (2024) – The Adequacy of Cybersecurity in Financial Institutions in Zimbabwe.

This section of this study will explore the empirical studies undertaken to assess the effectiveness of measures employed by financial institutions to enhance information system security (cybersecurity). The studies conducted and the research findings will be grouped into 4 distinct themes which are: Security measures employed to prevent cyber-attacks; effectiveness of security measures; problems that banks encounter; policies/ recommendations to increase security within commercial banks within Harare CBD, Zimbabwe.

2.4.1.2 Mutanda & Chrispen (2023) – Cyber fraud risk management strategies in Zimbabwean commercial banks

Empirical evidence from Zimbabwean commercial banks shows that cybersecurity measures are built around a combination of technical and procedural controls. Mutanda and Chrispen (2023) found that banks primarily implement safeguards such as firewalls, intrusion detection systems, antivirus and anti-malware software, access control mechanisms, multi-factor authentication, and transaction monitoring systems to prevent cyber fraud and unauthorized access. The study further highlights that these controls are complemented by organizational measures such as employee vetting, cybersecurity awareness training, and internal policies aimed at strengthening overall risk management within banking institutions.

2.4.1.3 Maphosa, V. (2023) – An overview of cybersecurity in Zimbabwe's financial services sector

Maphosa (2023) found that Zimbabwean financial institutions employ a combination of technical, organizational, and governance-based cybersecurity

measures such as firewalls, access control systems, encryption, monitoring tools, and ICT governance frameworks like ITIL and COBIT. However, the study notes that the effectiveness of these measures varies across banks due to differences in technical capacity, resources, and cybersecurity maturity levels.

2.4.1.4 Dzomira (2014) – Electronic fraud risk and internal control measures in Zimbabwean banking sector

Dzomira (2014) found that Zimbabwean banks employ a range of internal control and ICT-based cybersecurity measures including transaction verification procedures, access control mechanisms, fraud detection systems, and structured risk management practices. These measures are designed to reduce exposure to electronic fraud and unauthorised transactions within banking systems, although their effectiveness is constrained by resource limitations and evolving cyber threats.

2.4.2.5 Chigaro (2017) – E-Banking Security Strategies in Zimbabwe

Chigaro (2017) conducted a case study on Stanbic Bank and found that although technical measures such as firewalls and access controls are in place, resource limitations and skill gaps constrain their effectiveness. This suggests that measures, while theoretically sound, face practical challenges in execution.

2.4.2 Objective 2 - Effectiveness of Cybersecurity Measures

2.4.2.1 Akinbowale, Klingelhöfer and Zerihun (2024) – Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation

Akinbowale, Klingelhöfer and Zerihun (2024) examined the effectiveness of anti-fraud technologies in South African commercial banks using survey data from banking professionals involved in fraud risk management. The study established

that cybersecurity tools such as firewalls, encryption systems, intrusion detection systems, digital analytics and continuous auditing play a significant role in enhancing the prevention and detection of cyberfraud, thereby strengthening the security and integrity of banking transactions. However, the study further reveals that the effectiveness of these controls is not inherently guaranteed by their adoption but is largely dependent on the degree of system integration, frequency of updates and the level of employee technical competence within banking institutions. This demonstrates that cybersecurity effectiveness is multidimensional, extending beyond technological deployment to include organisational readiness and operational efficiency, implying that weaknesses in implementation can significantly undermine otherwise robust cybersecurity infrastructures.

2.4.2.2 Mutanda and Chrispen (2023) – Towards a Cyber Resilient Banking System: Effectiveness of Cyber Fraud Risk Management Strategies Adopted by Commercial Banks in Zimbabwe

Mutanda and Chrispen (2023) examined the effectiveness of cyber fraud risk management strategies adopted by commercial banks in Zimbabwe using quantitative survey data from banking professionals. The study found that cybersecurity and fraud prevention measures were only partially effective in mitigating cyber risks, as banks continued to experience persistent cyber threats. The study attributed this limited effectiveness to factors such as inadequate technological systems, low cybersecurity awareness among clients, insufficient employee expertise, and the rapidly evolving nature of cybercrime.

2.4.2.3 Chigaro (2017) – An Assessment of the Effectiveness of E-banking Security Strategies in Stanbic Bank Zimbabwe

Chigaro (2017) examined the effectiveness of e-banking security strategies at Stanbic Bank Zimbabwe using a qualitative case study approach supported by

interviews with key banking personnel. The study found that security measures such as secure login authentication, encryption of sensitive data, and customer verification mechanisms significantly enhanced the protection of electronic banking services and strengthened customer trust in digital platforms. However, the study further revealed that the effectiveness of these measures was not absolute, as system vulnerabilities, implementation challenges, and user-related behaviors such as poor password practices reduced overall security performance. The study concluded that sustained effectiveness depends on continuous system updates, staff training, and strong alignment between technological controls and user compliance within the banking environment.

2.4.2.4 Maphosa, V. (2023) – An overview of cybersecurity in Zimbabwe’s financial services sector

Maphosa (2023) conducted a quantitative study on cybersecurity in Zimbabwe’s financial services sector using survey data collected from ICT professionals across financial institutions. The study found that although banks and financial institutions have implemented various cybersecurity measures such as encryption systems, firewalls, access controls and monitoring tools, cyber threats continue to persist due to gaps in technical capacity, limited cybersecurity skills and insufficient organisational preparedness. The study further established that the effectiveness of cybersecurity controls is strongly influenced by institutional capability, staff competence and continuous system strengthening, rather than the mere existence of technological safeguards, highlighting the need for integrated and well-managed cybersecurity frameworks within financial institutions.

2.4.3 Objective 3 - Challenges Faced by Financial Institutions in Combating Cyber Threats

2.4.3.1 Dzingirai (2022) – Managerial Challenges Under FinTech: Evidence from Zimbabwean Commercial Banks

Dzingirai (2022) investigated the challenges associated with digital transformation and FinTech adoption in Zimbabwean commercial banks. The study identified cyber-attacks, technology risk, regulatory compliance requirements, system downtimes, and shortages of skilled ICT personnel as major challenges affecting banking institutions. The findings further revealed that increasing technological complexity and inadequate technical expertise constrained the ability of banks to effectively manage emerging cyber threats, thereby exposing institutions to heightened cybersecurity risks.

2.4.3.2 Mugari et al. (2016) – Cybercrime and Institutional Vulnerabilities in Zimbabwe's Financial Sector

Mugari et al. (2016) found that Zimbabwe's financial institutions face persistent cyber threats driven by increasingly sophisticated attacks, weak coordination between banks and law enforcement, and inadequate cybersecurity infrastructure. The study also noted poor information-sharing systems and limited real-time threat intelligence as major constraints in combating cybercrime.

2.4.3.3 Maphosa (2023) – Human Factors and Skills Constraints in Cybersecurity Implementation within Financial Institutions

Maphosa (2023) identified shortages of skilled cybersecurity professionals, limited technical capacity, and low staff awareness as major human-related challenges in Zimbabwean financial institutions. The study further noted that inadequate training and budget constraints reduce cybersecurity preparedness and increase vulnerability to phishing and social engineering attacks.

2.4.3.4 Dzomira (2014) – Institutional and Regulatory Constraints in Managing

Electronic Fraud in Zimbabwean Banks

Dzomira (2014) highlighted weak regulatory enforcement, outdated legal frameworks, and slow judicial processes as key institutional challenges limiting effective cyber fraud management. The study also pointed out inconsistent cybersecurity standards across financial institutions, which undermines coordinated responses to electronic fraud.

2.4.3.4 Chikowero and Nyoni (2023) – Resource Constraints and Cybersecurity Investment Challenges in Zimbabwean Financial Institutions

Chikowero and Nyoni (2023) investigated financial and infrastructural challenges affecting cybersecurity implementation and found that constrained budgets limited banks' ability to invest in advanced security technologies. Competing organizational priorities often resulted in cybersecurity being treated as a secondary concern rather than a strategic necessity. The study further noted that economic instability exacerbated these challenges by restricting access to updated software, hardware, and external cybersecurity expertise. Consequently, financial institutions struggled to maintain effective and sustainable cybersecurity measures.

2.4.4 Objective 4 - Strategies and Recommendations for Improving Cybersecurity

This subsection reviewed empirical studies that proposed practical strategies and policy recommendations aimed at strengthening cybersecurity within financial institutions. The literature emphasized that effective cyber threat mitigation in banks required a combination of technological investment, human capacity development, governance reforms, and regulatory collaboration, particularly within high-risk urban banking environments such as Harare CBD.

2.4.4.1 Poshai, L., Chilunjika, A., & Intauno, K. (2023) – Examining the institutional and legislative frameworks for enforcing cybersecurity in Zimbabwe

Poshai, Chilunjika and Intauno (2023) examined the institutional and legislative frameworks for enforcing cybersecurity in Zimbabwe and found that weaknesses in coordination among key cybersecurity stakeholders reduce the effectiveness of enforcement mechanisms. The study recommends the development of a more integrated and harmonized institutional structure involving regulators, law enforcement agencies and ICT governance bodies to improve coordination and response to cyber threats. It further highlights the need for stronger and consistent enforcement of the Cyber and Data Protection Act (2021) to enhance prosecution of cybercrime and close existing legal loopholes. The authors also recommend strengthening institutional capacity through specialized training in cybercrime investigation and digital forensics, as well as improving investment in cybersecurity infrastructure such as forensic tools and dedicated cybercrime units. In addition, the study emphasizes the importance of public–private sector collaboration and increased public awareness initiatives to improve cybersecurity compliance and resilience.

2.4.4.2 Takavarasha Jr, Van Heerden, Thakur and Jordaan (2023) – Cyber-security in the era of the COVID-19 pandemic: a developing countries' perspective

Takavarasha Jr et al. (2023) recommend that developing countries strengthen cybersecurity resilience by developing and implementing robust cybersecurity policies that respond effectively to the increased digital risks experienced during the COVID-19 pandemic. The study further emphasizes the importance of continuous cybersecurity awareness and training programmes aimed at reducing human-related vulnerabilities such as phishing attacks and social engineering,

which became more prevalent during periods of remote work. The authors also recommend strengthening institutional capacity through investment in modern cybersecurity infrastructure, improved technical systems, and the development of skilled cybersecurity professionals capable of responding to emerging threats. In addition, the study highlights the need for stronger collaboration between government institutions, private sector organizations', and critical infrastructure operators through information sharing and coordinated cybersecurity response mechanisms to improve overall national cyber resilience.

2.4.4.3 Gumbo, Masimba and Zuva (2025) – A Cybersecurity Framework for Enhancing Public Sector Digital Resilience in Emerging Economies

Gumbo, Masimba and Zuva (2025) propose a comprehensive cybersecurity framework aimed at strengthening digital resilience within public sector institutions in emerging economies. The study recommends a multi-layered approach that integrates cybersecurity awareness, infrastructure modernisation, policy reform, and capacity building as key pillars for improving institutional resistance to cyber threats. The authors further emphasise the need for enhanced coordination among stakeholders to address institutional fragmentation, which often weakens cybersecurity implementation in public sector environments. In addition, the study highlights the importance of investing in skilled cybersecurity personnel and modern security technologies to improve threat detection, prevention, and response capabilities. Overall, the framework advocates for a shift from reactive to proactive cybersecurity management to ensure sustainable digital transformation in the public sector.

2.4.4.4 Kanyongo and Wadesango (2025) – Cybersecurity and Risk Mitigation Strategies in Commercial Banks

Kanyongo and Wadesango (2025) argue that cybersecurity is a critical component of effective risk mitigation strategies in commercial banks within

emerging markets, particularly as digital banking increases exposure to operational and compliance risks. The study highlights that weaknesses in internal control systems, especially in relation to employee access to sensitive customer information, significantly heighten the risk of cyber breaches, and therefore recommends strengthened internal monitoring mechanisms to regulate access rights and detect suspicious activities. The authors further emphasize that cybersecurity effectiveness requires more than policy formulation, stressing the importance of continuous assurance practices such as regular cybersecurity audits and vulnerability assessments to maintain system integrity. In addition, they recommend the adoption of layered technical controls, including multi-factor authentication, automated session management, and advanced firewall systems, to enhance protection against unauthorized access. The study also underscores the role of user awareness in cybersecurity effectiveness, noting that human behaviour remains a major vulnerability, and therefore calls for ongoing customer education to reduce security breaches linked to user error.

2.5 Gap Analysis

The literature shows that financial institutions in Zimbabwe and other emerging markets have put in place a wide range of cybersecurity measures such as firewalls, encryption systems, intrusion detection tools, multi-factor authentication, transaction monitoring systems, and access control mechanisms (Mutanda and Chrispen, 2023; Maphosa, 2023; Mashizha and Kanengoni, 2024; Dzomira, 2014). Alongside these technical tools, banks also use organisational measures like staff training, internal policies, and governance frameworks to strengthen their overall security posture. However, despite all these efforts, cyber threats continue to occur, suggesting that having these systems in place does not always translate into effective protection. A common issue across literature is that cybersecurity measures are often studied separately rather than as a connected system. For example, technical tools are discussed on their own, while

governance and human factors are treated separately, even though in reality they all work together. Because of this, there is still limited understanding of how these different components interact to influence the overall effectiveness of cybersecurity in banks. Although some studies have looked at how effective cybersecurity measures are, most of them mainly focus on whether these tools exist or are being used, rather than how well they actually work in practice to prevent or reduce cyber incidents. This means effectiveness is often assumed instead of being properly tested or measured in real banking environments.

The literature also shows that banks face several challenges such as limited skills, weak enforcement of regulations, lack of resources, and poor infrastructure (Dzingirai, 2022; Chikowero and Nyoni, 2023; Mugari et al., 2016; Dzomira, 2014). However, these challenges are usually discussed on their own, without clearly showing how they directly affect the performance of cybersecurity measures. Another gap is that most studies look at cybersecurity at a national or general level, with very few focusing specifically on high-risk urban banking environments such as commercial banks in Harare Central Business District. This is important because such areas experience high volumes of digital transactions and are more exposed to cyber threats.

Lastly, while many studies suggest solutions such as improving governance, training staff, strengthening regulations, and investing in technology (Poshai et al., 2023; Takavarasha et al., 2023; Gumbo et al., 2025; Kanyongo and Wadesango, 2025), there is still limited evidence showing how effectively these recommendations are being implemented in real banking operations. Therefore, this study fills these gaps by examining how effective the cybersecurity measures used by commercial banks in Harare CBD really are, considering technical systems, human behaviour, and organisational governance together.

2.6 Chapter Summary

This chapter reviewed conceptual, theoretical, and empirical literature on cybersecurity in commercial banks, highlighting its increasing importance due to digitalisation and the growing sophistication of cyber threats. It examined key cybersecurity measures and established that their effectiveness depends on proper integration of technical, organisational, and human factors, as well as continuous evaluation and alignment with institutional processes. The study was grounded in Defence-in-Depth theory and the Technology Acceptance Model, which together explain the need for layered security controls and the role of user behaviour in the effective adoption of cybersecurity measures. Empirical evidence showed that although Zimbabwean banks have implemented various cybersecurity controls, their effectiveness is constrained by challenges such as limited resources, skills shortages, weak regulatory enforcement, and legacy systems. The review also considered recommended strategies for improving cybersecurity, including stronger governance, capacity building, and advanced technological systems, but noted limited empirical evidence on their practical effectiveness in the Zimbabwean banking context. The chapter concluded by identifying key gaps, particularly the lack of comprehensive evaluation of cybersecurity effectiveness, insufficient integration of human and technical dimensions, and limited focus on Harare CBD banks, thereby justifying the need for the present study.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

This chapter details the research methodology employed to investigate the extent of the implementation of cybersecurity measures in financial institutions to prevent attacks, focusing on commercial banks within the Central Business District (CBD) in Harare, Zimbabwe. It discusses and gives rationale to the research philosophy, research design, target population, sampling techniques, sample size, instruments and procedures employed for data collection. This was done to align the methodology with the objectives, research questions and the theory addressed in previous chapters and as such ensuring the rigor, creditability and the coherence of the study.

3.1 Research Philosophy

Research philosophy refers to the stance which research assumes on the nature of reality and the ways in which knowledge is produced and interpreted (Creswell & Creswell, 2018; Saunders, Lewis, & Thornhill, 2019). The research was based on the pragmatist research philosophy which allows the researcher to use both

qualitative and quantitative methods in answering a research problem (Tashakkori & Teddlie, 2010). This study adopted a pragmatist approach because it was concerned with investigating the effectiveness of security measures among the selected commercial banks in Zimbabwe through the use of both qualitative and quantitative methods. Both methods of data collection were adopted since there was need to collect quantifiable data through the questionnaires and in-depth knowledge of participants' perceptions through the use of the semi-structured interview questions. The pragmatist research philosophy enabled the integration of numbers and stories so that the researcher could come to an informed decision (Creswell & Plano Clark, 2018). This helped the researcher to explore the problem holistically as the effectiveness of security measures was looked at as both a technical and organisational issue that could be explained through various factors ranging from employee behavior, institutional policies and procedures as well as government regulations. The pragmatist philosophy was conducive to the approach of mixed methods and it fit in well with the theories of Defence-in-Depth (DiD) and the Technology Acceptance Model (TAM).

3.2 Research Design and Justification

Mixed methods research design was utilized in this study as it seeks to assess the efficacy of the implemented cybersecurity measures by commercial banks within the Central Business District of Harare, Zimbabwe. The reason behind utilizing mixed methods design was because it will aid in acquiring both quantitative and qualitative data, hence providing an in-depth understanding of the entire spectrum of the usage and efficacy of the implemented cybersecurity measures and the response from the banks. A mixed methods design was said to be advantageous because it would not only acquire and integrate data from quantitative as well as qualitative measures but also provides a more thorough as well as balanced inquiry into the problem being addressed. The quantitative

design allowed for measurement using questionnaires, to gather measurable information about how implemented cybersecurity measures were being used, and the level of effectiveness being attained. Whereas the qualitative design provided deeper insight through interviews into how participants viewed and managed cybersecurity, their work experiences and professional judgment of the effectiveness of such measures (Creswell & Plano Clark, 2018). This would ensure that statistical trends and qualitative reasoning of the level of cybersecurity effectiveness could be captured. Cybersecurity, within the banking context, is a multifarious concept which is subject to various forces such as, technology-oriented security measures, Organizational culture and the general attitude of the staff, employee's security awareness and management commitment as well as regulatory compliance (Von Solms & Van Niekerk, 2013). Mixed methods design would be suitable since both human and technological components could be addressed in the study. According to Saunders et al. (2019) the integration of qualitative and quantitative approaches makes the research finding more valid. This research design also adhered to the pragmatic research philosophy where both quantitative and qualitative data would be useful in resolving the research problem (Tashakkori & Teddlie, 2010). Moreover, it was aligned with Defence-in-Depth (DiD) Theory and the Technology Acceptance Model (TAM) because both recognize the role that technology and behavioral factors (among other organizational factors) play in successful use and operation. Therefore, mixed method research design was the appropriate and effective design to be used.

3.3 Target Population

A population is "a totality of the information obtained in a study, where information collected is expected to apply" (Lind, Marchal & Wathen, 2017). This population "consists of all the elements that possess a characteristic of interest in the study" (Kotler & Keller, 2021). There is also the difference between the

target population (the actual desired group) and the accessible population (those people or subjects you are able to get to). The target population is the collection of all commercial banks licensed by Reserve Bank of Zimbabwe (RBZ) which have offices in the CBD of Harare (CBZ Bank Limited, FBC Bank Limited, Stanbic Bank Zimbabwe Limited, Standard Chartered Bank Zimbabwe Limited, Nedbank Zimbabwe Limited, NMB Bank Limited, First Capital Bank Zimbabwe Limited, Steward Bank Limited, ZB Bank Limited, Ecobank Zimbabwe Limited, Metbank Limited, Access Bank Zimbabwe Limited, AFC Commercial Bank of Zimbabwe) the information in the research would then target key people within these organizations in relation to information systems and cybersecurity (IT managers, information system officers, risk & compliance officers, internal auditors, digital banking managers and operations managers).

3.4 Sampling Techniques

Sampling is defined as those methods and procedures used to select a subset of elements from a larger population for the purposes of data collection and analysis in the expectation that this subset would be representative of the whole and would enable generalizations about the population to be made and conclusions to be reached within specified parameters of error (Bryman, 2016; Leedy & Ormrod, 2019). Sampling is an important part of research design as it affects the validity, reliability and generalizability of the results. Methods of sampling are grouped into two major categories: probability sampling where each element of a population has an equal probability of selection enabling generalization to the whole population on a statistical basis (Saunders, Lewis, & Thornhill, 2019), and non-probability sampling where there is an unequal or unknown probability of selection and results in more in-depth but non-generalizable data (Bryman, 2016). For the purpose of this study a mixed sampling strategy was employed in accordance with a mixed methods design (Creswell & Plano Clark, 2018) which involved the use of purposive sampling for

the qualitative part to ensure that respondents selected had practical expertise and experience in performing cybersecurity related activities within commercial banks, and simple random sampling for the quantitative part where all respondents who fit the eligibility criteria had an equal probability of being selected. This combined approach served to broaden and deepen data for study.

3.5 Sample Size

Sampling is the method and procedures adopted in order to draw a sample of items or entities from the larger universe for data collection and analysis and in the assumption that the sample would represent the universe, so that conclusions can be drawn from the sample on the whole within acceptable limits of error (Bryman, 2016; Leedy & Ormrod, 2019). Sampling is one crucial part of research design as it effects the validity, reliability and the generalizability of the study findings. Sampling methods are divided into two major categories: Probability sampling where each element of a universe is equally likely to be selected, allowing generalization of the sample to the entire universe on a statistical level (Saunders, Lewis, & Thornhill, 2019) and non-probability sampling where selection is not equally likely, with the results providing in-depth non-generalizable data (Bryman, 2016). For the purpose of this study a mixed sampling strategy was applied as part of a mixed methods design (Creswell & Plano Clark, 2018), which included the use of purposive sampling for the qualitative section of the study to ensure that all participants had practical knowledge and experience in carrying out cybersecurity related functions in commercial banks and simple random sampling for the quantitative section where each eligible participant had an equal opportunity to be chosen. Combining these two approaches enabled broader and more profound data to be collected for study.

3.6 Sources of data

Data has been defined as a fact which can be used for analysis, interpretation and to formulate conclusions in research (Hair, Page and Brunsveld, 2022). The sources for data are of two types, that are, primary data and secondary data based on the methodology employed to obtain them, and their applicability for the research work (Bell, Bryman, and Harley, 2022). These two sources of data were used to achieve a thorough understanding of the practices of cybersecurity within the commercial banks functioning in the Central Business District of Harare (CBD).

3.6.1 Primary Data

Primary data defined as 'information collected firsthand by the researcher to address the research objectives of the specific research' (Saunders, Lewis and Thornhill, 2019) is perceived as being highly relevant, as it is specific to the context and gives an up-to-date, targeted, insight into the research problem. For this research primary data was gathered from selected commercial bank employees who work within cybersecurity and information systems functions- this included IT managers, security officers, risk and compliance officers, internal auditors, digital banking managers, and operations managers, with data collected via questionnaires and semi-structured interviews in order to secure qualitative and quantitative evidence.

3.6.2 Secondary Data

Secondary data is information that has already been gathered and published for different reasons other than for the current study and helps to supplement and complement the data used in the study (Johnston, 2021). Sources include academic literature, journal articles, business reports, textbooks, legal instruments and journals. In this study secondary data was collected from

academic literature, Reserve Bank of Zimbabwe, the different security frameworks and banking sector reports. It was employed to support the theoretical framework of the study and support the interpretation of primary data findings. Both primary and secondary data increased the breadth, accuracy and academic soundness of the study (Bell, Bryman and Harley, 2022).

3.7 Research instruments

Research instruments include devices or techniques employed to gather data in a systematic way. These include a wide range of devices and procedures that may be used to measure, gather, classify and analyze data relevant to the research problem. These research instruments are important for validity and reliability of data and in solving a research problem. In this study the primary instruments were structured questionnaires and semi-structured interviews. Secondary data was gathered from various literature sources like academic books, articles, and reports of institutions as well as policy documents.

3.7.1 Structured Questionnaires

Structured questionnaires, a type of instrument for the collection of quantitative data, refers to fixed sets of standardized questions seeking uniform answers from many people (De Vaus, 2021). These types of questionnaires were increasingly utilized in survey research because of their ease in comparison, reliability, and the ease of analysis in statistical means. Standardized questionnaires need to be explicit, simple and unambiguous in nature so that unbiased responses are obtained, according to Creswell and Creswell (2021). In this study, both hard copies and soft copies of the structured questionnaires were distributed to individuals to achieve more effective distribution and response rates. Majority of the questionnaires comprised of closed-ended Likert scale questions followed by only a few open-ended questions to allow for a fuller explanation of specific issues. These questionnaires were distributed to

employees in respective departments, such as Information technology, cybersecurity, risk & compliance, operations and digital banking in order to find out the effectiveness of cybersecurity and institutional controls and knowledge of cyber risks.

a) Advantages of structured questionnaires

- Inexpensive, suitable for large samples
- Provides consistency by asking the same questions to all respondents
- Data collection and statistical analysis are quick and simple
- Encourages honest answers due to the promise of anonymity
- Can be administered to remote respondents.

) Disadvantages of structured questionnaires

- Limited flexibility once administered
- Does not capture non-verbal cues such as tone and body language
- Risk of misinterpretation of questions without clarification
- Possible low response rates without follow-up strategies.

A pilot study was undertaken before the main data collection, in order to check the questionnaire's comprehensibility, organisation and reliability and to highlight any relevant constraints. Accordingly, adjustments were made to increase the validity of the questionnaire. Furthermore, questionnaires were complemented by interviews in order to gain greater contextual understanding and validity of the quantitative data.

3.7.2 Interviews

Interviews provide a way to collect qualitative data that entails "an interaction in which the researcher is trying to gather more in-depth information on a specific topic from their respondents" (Saunders, Lewis & Thornhill, 2023). Interviews are helpful in research, as they allow a subject to explain their experiences, perspectives, attitudes and opinions in much detail. In this particular research semi-structured interviews were used to gather in-depth data from both employees and management of selected commercial banks within the Harare CBD about the success of measures that banks employ to fight cyber threats. Use of interviews also help researchers to clarify issue about security systems and the problems they face from threats of computer viruses (Creswell and Creswell, 2022).

a) **Advantages of interviews**

- They provided detailed information relevant to the study
- They allowed clarification through follow-up questions
- They encouraged participants to freely express their views

b) **Disadvantages of interviews**

- They were time-consuming
- Some participants were unwilling to share sensitive information

To prevent these difficulties the researcher pre-scheduled the interviews and informed interviewees that any information provided would be anonymous and used solely for academic research.

3.8 Data Collection and Appropriateness of Procedures

This research utilized a mixed methods approach which was underpinned by the philosophy of pragmatism. The philosophy views research from the position that a variety of methods are needed in order to best explore and understand complex, real-world issues. The philosophy recommends combining both quantitative and qualitative methods to attain applicable and comprehensive results (Creswell and Creswell, 2022). Given the nature of this study investigating cybersecurity in the banks within the Harare Central Business District, it was concluded that both qualitative and quantitative methods were necessary to draw accurate, generalizable trends, but also achieve depth in understanding the issues. The combination of both methods enhanced the triangulation of results, and hence contributed to improving the validity, reliability, and depth of the results. A questionnaire was distributed to the staff at the banking institutions, and this was used to obtain the quantitative data concerning their awareness on cybersecurity measures in place at their banks, implementation procedures and perceived level of effectiveness of the implemented security systems. This allowed data to be collected from a large number of respondents in a relatively short period and with relative ease and was suitable to identify the commonalities and disparities in cyber security among institutions. Semi-structured interviews were carried out with some members of the IT, risk management and compliance department within a few selected banking institutions. The objective was to gain qualitative insights into the various procedures, issues and operations within institutions concerning cybersecurity at the workplace. This also allowed for comparison between policy and practice thus enhancing validity. This gave first-hand contextual understanding of how policy is implemented within the daily operations of the banking institutions without interfering with the daily work.

3.9 Data Presentation and Analysis

Following the collection of data, they were systematically collated and checked for their accuracy, completeness and consistency within the qualitative and quantitative data sets through checking for missed answer boxes and the consistency of transcribed replies. As can be observed the quantitative questionnaire data were analyzed using descriptive statistical tools that measure the frequencies and percentages of respondents' opinion on cybersecurity methods, the findings of which are displayed through use of tables, bar charts and pie charts (Saunders, Lewis and Thornhill, 2023). The qualitative responses to the interview were analyzed by thematic analysis where responses were carefully coded and categorized under specific themes identifying their experiences, perceptions and institution's actions (Braun & Clarke, 2006). These were all then merged under the interpretative process of using the statistics to support and explain the results using quotes and excerpts.

3.10 Validity

Validity is the degree to which a research instrument measures exactly what it is supposed to measure (Creswell and Creswell, 2022). Validity is necessary within research because it ensures that findings are accurate, applicable and appropriate. Validity is defined by Saunders, Lewis and Thornhill (2023) as "the extent to which research instruments deal appropriately with the study objectives and gather relevant data". The interview questions and the questionnaire were drawn up with a great amount of thought and reviewed prior to any data collection to ascertain whether the relevant information under investigation was covered.

3.11 Reliability

Reliability means consistency of research instruments in achieving steady and

reliable results when used under the same conditions (Fowler, 2020; Bell, Bryman and Harley, 2022). This means the outcomes are not due to chance but the true reflection of what is under study. In this research, the questionnaires were formulated to be clear-cut, and the interview schedule was structured and directed by research objectives. The instruments were tested before the actual data collection so as to obtain consistency, clarity and consistency in perception among selected bank respondents in Harare CBD.

3.12 Ethical considerations

These were noticed throughout the duration of data collection. Participants were explained the aims of the study, that their responses would be kept confidential, and that it was completely voluntary to participate. All data was stored securely and was only used for academic study.

3.13 Chapter Summary

This chapter described the research approach used in this study that is based on pragmatist philosophy with the use of mixed methods. The study approach explained the research design, data collection, data analysis techniques, sampling and methods used for collecting data from the Harare Central Business District Banks. This also explains the validity and reliability of the research, ethical issues and the process to use when analyzing and presenting data. Generally, it explains the process used when collecting data, how data will be analyzed and then how the collected data will be presented in Chapter Four.

CHAPTER IV

DATA PRESENTATION, INTERPRETATION AND ANALYSIS

4.0 Introduction

This chapter analyses, presents and discusses the results of a study carried out on the measures used by financial institutions to combat cyberattacks in banks in Harare CBD, Zimbabwe. A mixed methods approach under the pragmatism philosophy was used and questionnaires and interviews were the tools used to gather data from a sample of 40 participants. Quantitative data were analyzed through use of frequencies, percentages, means and standard deviations while qualitative data were analyzed using the thematic method. The results are displayed according to the objectives of the study and interpretations based on the Defence-in-Depth Theory and Technology Acceptance Model (TAM) are done.

4.1 Response Rate

A total sample size of 45 employees from the surveyed banks in Harare CBD was chosen for the purpose of a study of measures employed by financial institutions against cyber threats. There were 35 questionnaires administered to junior and senior level employees in the banks to gather quantitative data; 32 of which were successfully completed and returned. Interviews with 10 participants were conducted to gather qualitative data; 8 of which were completed and analyzed by

theme.

Table 4.1: response rate

Questionnaires Distributed	Questionnaires Returned	Response Rate	Non-response rate
35	32	91.4%	8.6%
Interviews scheduled	Interviews conducted		
10	8	80%	20%

Source: Primary data (2026)

The response rate for the questionnaire can be observed in table 4.1 above, at 91.4% (n=32 completed questionnaires out of 35 sent). This has increased the reliability and generalizability of the quantitative data; by decreasing the chance of a non-response bias occurring, the data quality has been enhanced leading to greater statistical inference. Survey research recently conducted suggests that higher response rates tend to correlate highly with questionnaire validity and greater validity of the results from quantitative studies on organization, (Dillman, Smyth, and Christian, 2020).

Further, it was planned to have 10 interview questions for selected banking personnel, out of which 8 were interviewed so that the interview response rate was 80.0%. Such response rate is deemed acceptable in the field of qualitative research, where quality and richness of data take precedence over the quantity of data collected. Guidance of qualitative research states that the required

participation would be reached if collected data is rich enough to provide adequate themes and the same may not involve comprehensive data from all selected respondents (Braun & Clarke, 2021).

4.2 Demographic profile categories

In this section the details on the demographic profile of the 32 respondents participating in the study are outlined. The respondents were all employees working at the commercial banks located at Harare CBD. The profile details the age of respondents, gender of respondents, their educational level, their job title and department and years of working. The information is given on the table below:

Table 4.2: Demographic profile categories of respondents

Variable	Category	Frequency	Percentage (%)
Gender	Male	18	56.3
	Female	14	43.7
	Total	32	100
Age distribution	20–29	8	25.0
	30–39	14	43.7
	40–49	7	21.9

	50+	3	9.4
	Total	32	100
Education Level	Higher Diploma	5	15.6
	Bachelor's Degree	18	56.3
	Master's Degree	7	21.9
	Doctorate	2	6.2
	Total	32	100
Department of Respondents	IT	10	31.3
	Compliance/ Risk	6	18.8
	Finance and Accounting	6	18.8
	Operations	5	15.6
	Internal Audit	3	9.4
	Customer Service	2	6.1

	Total	32	100
Job positions of Respondents	Customer Service Officers	10	31.3
	Tellers	8	25.0
	Credit officers	6	18.8
	ICT/Security officers	5	15.6
	Branch managers	3	9.4
	Total	32	100
Years of Working Experience	1-3years	7	21.9
	4-6 years	12	37.5
	7-10 years	9	28.1
	10+ years	4	12.5
	Total	32	100

Source: Primary data (2026)

4.2.1 Gender of Respondents

The above table displays the gender breakdown of the respondents; 18 of them (56.3%) were males and 14 (43.7%) were female. Thus, we have almost equal representation of males and females among the commercial banks in Harare CBD with a majority of males. Due to such even spread of both gender the interpretation of findings would not lean too heavily on the views of either one sex.

4.2.2 Age Distribution of Respondents

Regarding the ages of the respondents, 14 respondents (43.7%) were in the 30–39-year age group, followed by 8 respondents (25.0%) aged between 20-29 years, 7 respondents (21.9%) were in the 40–49-year age group, while 3 respondents (9.4%) were over 50 years of age. This observation indicates that a considerable proportion of the respondents falls within an age group that is often financially active and has extensive.

4.2.3 Level of Education of Respondents

The education level of respondents indicates that 18 (56.3%), have a bachelor's degree, 7 (21.9%) have a master's degree, 5 (15.6%) have a Higher Diploma and 2 (6.2%) have a Doctorate. Because of this, respondents were well-educated. Most respondents have a minimum qualification of bachelor's degree. The response pattern suggests that most employees possess relevant knowledge to contribute to cyber security issues and business operations in commercial banks of Harare CBD.

4.2.4 Job Position of Respondents

Table 4.2: Respondents by Job Position

Job Position	Number of Respondents	Percentage (%)
Customer Service Officer	10	31.3
Teller	8	25.0
Credit Officer	6	

18.8 ICT/Security Officer 5 15.6 Branch Manager 3 9.3 Total 32 100 Table 2 shows the distribution of the respondents by job position. From the result, 10 (31.3%) were Customer Service Officers, 8 (25.0%) were Tellers, 6 (18.8%) were Credit Officers, 5 (15.6%) were ICT/Security Officers and 3 (9.3%) were Branch Managers. This implies that the sample includes both operational staff and management staff working within commercial banks in Harare CBD. The inclusion of staff from different functional roles also guaranteed that different viewpoints of operational controls and information security measures in the banking sector were considered.

4.2.5 Department of Respondents

Regarding departmental distribution of the respondents, there were 10 (31.3%) of Information Technology, 6 (18.8%) of Compliance/Risk management, 6 (18.8%) of Finance/Accounting, 5 (15.6%) of Operations, 3 (9.4%) of Internal Audit and 2 (6.1%) of Customer Service. The above confirms that there were respondents from main functional areas within the commercial banks in Harare CBD. Including both the technical and operational departments helped to collect both the technical and operational views.

4.2.6 Years of Work Experience of Respondents

Out of the 32 respondents that completed the survey, 12 respondents (37.5%) have been working as professionals for 4-6 years. The 9 respondents (28.1%) have 7-10 years of experience, and 7 respondents (21.9%) have 1-3 years of experience. The final 4 respondents (12.5%) have more than 10 years of experience. It can be concluded from the data presented above that respondents most likely to participate are to have average to a lot of work experience within commercial banks in Harare CBD. The presence of both younger (less experienced) employees as well as experienced employees in this sample provided a mixture of perceptions and experiences.

4.3 Cybersecurity Measures Currently Employed commercial banks in Harare CBD

This part presents the results regarding the various security measures being utilized by commercial banks in Harare CBD. The results are both quantitative and qualitative, derived from 32 questionnaires which were administered to various banking officials and supplemented by the results of 8 interviews held with the staff of commercial banks. The quantitative results are depicted below in Table 4.3 in the form of frequencies, percentages, mean score and standard deviation to measure the extent to which the measures are being utilized. The qualitative findings complement the statistical data by adding explanatory evidence of the respondents' accounts and therefore enhance the statistical analysis in this part.

Table 4.3: Cybersecurity Measures Used in Commercial Banks (Harare CBD)
(n=32)

Measure	Strongly agree		Agree		Disagree		Strongly disagree		Descriptive statistics	
	Freq	%	Freq	%	Freq	%	Freq	%	Mean	St dev
Firewalls	16	50.0	12	37.5	3	9.4	1	3.1	3.34	0.74
Multifactor Authentication	17	53.1	11	34.4	3	9.4	1	3.1	3.38	0.72

Data Encryption	15	46.9	13	40.6	3	9.4	1	3.1	3.31	0.73
Intrusion Detection/Prevention Systems (IDS/IPS)	12	37.5	14	43.8	4	12.5	2	6.2	3.13	0.86
Security Information and Event Management (SIEM) Systems	10	31.3	13	40.6	6	18.8	3	9.4	2.94	0.91
Patch Management	14	43.8	12	37.5	4	12.5	2	6.2	3.19	0.82
Data backup Systems	18	56.3	11	34.4	2	6.2	1	3.1	3.44	0.68
Disaster Recovery Plan	13	40.6	13	40.6	4	12.5	2	6.2	3.16	0.84
Staff Cybersecurity Training	16	50.0	10	31.3	4	12.5	2	6.2	3.25	0.81

Source: Primary data (2026)

4.3.1 Firewalls

The findings as illustrated by table 4.3 above indicated that firewalls are strongly implemented in commercial banks in Harare CBD, as shown by 87.5% of respondents who strongly agreed (50.0%) and agreed (37.5%) that firewall

systems are actively used. The mean score of 3.34 and standard deviation of 0.74 indicated a high and consistent level of implementation across institutions. This suggests that firewalls are widely used as a primary preventive control to monitor and filter network traffic, thereby restricting unauthorized access to banking systems.

The interview results support this, as the interviewee stated, *'firewalls are the initial defensive measure against unwanted access into bank systems'*. This result is in line with Stallings and Brown (2015) who reiterated that firewalls should be used as perimeter defense mechanisms at the lowest layer in the enterprise security architecture. It also concurs with Mutanda and Maireva (2023) who established that commercial banks in Zimbabwe rely heavily on firewalls and access controls to deter unauthorized access and protect customer data

4.3.2 Multi-Factor Authentication (MFA)

It is apparent that MFA is highly implemented; 87.5% of respondents agreed (53.1%) and strongly agreed (34.4%) that it is implemented in the banking systems. This is evident in the calculated mean value 3.38 and a standard deviation of 0.72 which demonstrates strong agreement among respondents. This may indicate that the banks are reinforcing security on their systems through better authentication mechanisms to mitigate the risks resulting from unauthorized system access and password theft. This is evident in the interviews where respondents noted *that "multi-factor authentication has cut down cases of unauthorized access significantly"*. This aligns with Mutanda and Chrispen (2023), who found that Zimbabwean banks widely use access control mechanisms and multi-factor authentication as part of their cybersecurity controls to prevent unauthorized access and cyber fraud. Similarly, Maphosa (2023) notes that access control systems are a key component of ICT governance frameworks in financial institutions, although their effectiveness depends on institutional capacity and implementation quality. Note that effectiveness depends on proper

enforcement and consistent use across systems.

4.3.3 Data Encryption

All, except those that strongly disagreed (25%) were able to identify encryption as a technology used to secure sensitive banking information (Strongly agree: 46.9%; Agree: 40.6%). Both the mean value of 3.31 and the standard deviation of 0.73 demonstrate that this is implemented consistently in banks, in both data at rest and data in transit to remain protected from unauthorized access and interception. This is supported in the interview responses where it is stated *that customer transaction data is encrypted to secure it from being intercepted.*. It is also supported by Dzomira (2014), who said fraud detection systems and structured internal controls as key mechanisms used to reduce electronic fraud in banking systems. This is supported by ENISA (2020), which highlights encryption as a critical safeguard for protecting sensitive financial and transactional data. This aligns with Mutanda and Chrispen (2023), who reiterated that Zimbabwean banks use transaction monitoring systems as part of broader fraud prevention and cybersecurity controls to detect and prevent unauthorized activities. Similarly, Maphosa (2023) explained in his study that ICT-based monitoring tools are widely adopted in financial institutions, although their effectiveness depends on institutional capacity, system integration, and consistent implementation.

4.3.4 Intrusion Detection and Prevention Systems (IDS/IPS)

The findings on table 4.3, showed that IDS/IPS systems are also being implemented, with 81.3% comprising of respondents agreeing (43.8%) and strongly agreeing (37.5%) that these systems are in use. The mean score of 3.13 and standard deviation of 0.86 indicate moderate agreement with variation. This suggests that while IDS/IPS systems are present, their deployment may not be fully uniform across all banks. Interview findings support this, with respondents

noting that *"alerts are generated, but response depends on the availability of technical staff"*. This aligns with Dzomira (2014), who identified fraud detection systems and internal control mechanisms as key tools used by Zimbabwean banks to reduce electronic fraud, although their effectiveness is constrained by resource limitations and evolving cyber threats. According to ENISA (2020), IDS/IPS systems are essential for early detection of network anomalies and cyber intrusion attempts. It is also supported by Mutanda and Chrispen (2023), who found that intrusion detection systems and transaction monitoring tools are widely used as part of integrated cybersecurity controls to enable real-time detection and prevention of cyber fraud. Similarly, Maphosa (2023) notes that ICT security tools differ in sophistication across financial institutions, with their effectiveness largely dependent on system integration, institutional capacity, and implementation quality.

4.3.5 Security Information and Event Manage (SIEM) Systems

According to the results 71.9% of respondents (31.3% strongly agreed and 40.6% agreed) reported that SIEM system is used in commercial banks. It shows that the Mean (2.94) and SD (0.91) are moderate and diverse among different respondents. These findings were confirmed by interview responses where respondents said, *"most of monitoring is manual rather than with full integrated SIEM dashboard"*. Similar findings were reported by Chigaro (2017) about resource and skill constraints impacting the deployment of highly integrated cybersecurity systems in banks. As also revealed by Splunk (2020), SIEM systems expedite the detection time and shorten the response time, while processing events and alarms in real-time. Likewise, Mashizha and Kanengoni (2024) noted that aging systems, coupled with poor cybersecurity frameworks render institutions vulnerable to security threats. From these results, it is concluded that a majority of commercial banks are likely still utilizing a disparate, rather than a wholly integrated and real-time security monitoring solution.

Consequently, threat detection is likely largely based on human oversight, raising the risk of slower response times to advanced threats such as APTs and concerted phishing attacks. Furthermore, it is possible that many institutions have a reactive rather than a proactive security approach whereby security events are reported after they have already occurred and caused some system damage. IBM Security (2024) highlights that organizations without an integrated security analytics platform will face a higher risk of longer threat detection and response times thus increasing overall vulnerability.

4.3.6 Patch Management

The result showed that 81.3% agree consists of 43.8% of the respondents strongly agreed and 37.5% agreed that the patch management is practiced regularly in commercial banks in Harare CBD; this indicates an institutional strong practice to maintain systems and vulnerabilities. An average score 3.19 also showed a moderate to strong adoption in system patching and software updates in which most respondents believe that updating the system with latest security updates and patches is a routine task performed within their institutions and the system is kept up to date, addressing vulnerabilities in their systems and making it difficult for intruders such as malware to penetrate into their system and unauthorized access to information. However, this operation isn't always running smoothly on all the institutions. Findings from interviews showed that the operation aspect of patch management is the following: *“system updates are done regularly although at times delayed because of operation constraints and the need to minimize system downtime during business hours”*; this indicates that formal patch management policies exist but there are occasions when they can be influenced by operational requirements.

This is consistent with Chigora (2018), where banks used internal security policies and system controls as essential measures in protecting their systems. The results also concur with Maphosa (2023) who emphasized that periodic

system assessment is an important way to develop cyber resilience and prevent the exposure of the system to threats but still mentioned that unpatched systems create major access ways for attackers on financial institution's systems.

4.3.7 Data Backup Systems

Results indicate that 90.7% of the respondents which covers Strongly agree (56.3%) and Agree (34.4%) have stated that data backup systems are installed in commercial banks. The mean score of 3.44 indicates that recovery is strongly emphasized in the banking industry. Responses from interview also reinforce the statement, *"daily backups are performed for recovery purposes in case of a system failure or cyber-attack"*. This is supported by Chigora (2017) who emphasized the importance of strong data backup systems to prevent sensitive banking data from being compromised, erased or damaged by cyber-attacks.

Strong emphasis placed on backup systems may also indicate the importance for commercial banks located in Harare CBD to have very fast restoration of service after any catastrophic events caused by cyber-attacks thereby minimizing operation interruptions and loss of service to customers. Practically in Harare CBD the data backup systems installed will ensure critical financial data is recoverable within short duration to reduce operation downtime and losses due to system failures or attacks. It is supported by IBM Security (2021) that organizations using automated and tested backup system recovers much faster after a ransomware attack.

4.3.8 Disaster Recovery Plans

Results showed that 80.6% of respondents both strongly agree and agree (40.6% respectively) that disaster recovery planning is undertaken in commercial banks within the CBD of Harare, with a mean score of 3.16 indicating that is widely adopted. It can be interpreted that a large proportion of these institutions have

put in place official procedures which are required to regain services following a cyber-attack or disruption and a more formal strategy for business continuity is being put in place within the sector. This was supported by interview results which state *"disaster recovery plans are tested periodically to ensure continuity"*. This is further supported by the view of Dzomira (2014) where it is noted that structured recovery planning is considered part of the cyber risk management framework in order to reduce operational disruptions and provide continuity in critical banking services and this is also a key element for business continuity management plans within financial institutions according to ISO 22301 (2020), given their high dependency on system availability and potential high risks.

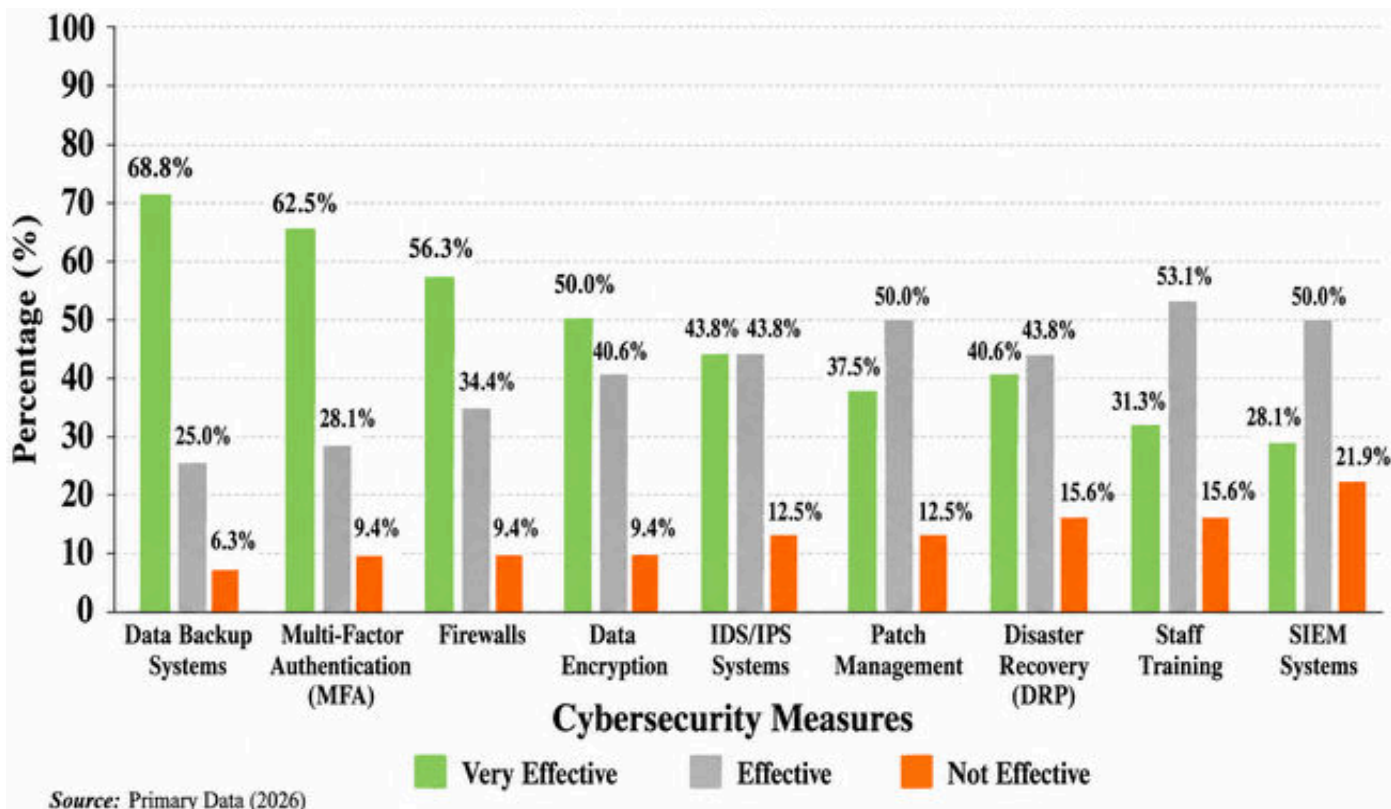
4.4.9 Staff Cybersecurity Training

There was an 81.3 % implementation, consisting of 50.0 % strongly agree and 31.3 % agree responses, and had a mean of 3.25, meaning most commercial banks in the CBD of Harare had carried out staff awareness on the security training programs. This means most institutions felt the need to have employees to be aware of the security measures as a key factor to mitigate some human error associated risks. The findings were also supported by interviewee responses where they reported that *"staff are regularly trained on phishing awareness and cyber threats."* This aligns with Dzomira (2014), who identified that human error and weak compliance with internal controls significantly contribute to electronic fraud in Zimbabwean banks, highlighting the need for improved user discipline within cybersecurity systems. It is also supported by Mutanda and Chrispen (2023), who found that cybersecurity awareness training and employee vetting are essential organizational controls used to reduce cyber fraud and strengthen institutional security. Similarly, Maphosa (2023) notes that limited staff skills and low cybersecurity awareness remain major weaknesses in financial institutions, and that continuous training is critical for improving overall cybersecurity effectiveness.

4.4 Effectiveness of Current Cybersecurity Measures in Combating Cyber Threats.

In this chapter data concerning Objective II of the study which was to examine the extent to which existing cybersecurity strategies adopted by commercial banks in Harare CBD could combat cyber threats was presented. Figure 4.1 below displays responses to questions on perceptions of various cybersecurity measures in percentage. This data was then supplemented by answers given by sampled bank employees interviewed and by descriptive statistics including mean and standard deviation values.

Figure 4.1; Effectiveness of Cybersecurity Measures Employed in Harare CBD



4.4.1 Data Backup Systems

For data backup systems, 68.8% considered them to be very effective and 25.0% as effective, leading to a total of 93.3% respondents who perceive data backup systems as an effective cybersecurity tool in commercial banks in Harare CBD. These findings indicate that data backup systems play an essential role in restoring data and business continuity in case of a cyber incident such as a ransomware attack, system failure or accidental data deletion. This was further affirmed in the interviews conducted, as the following response from an interview participant shows; *'backups are fundamental in quick data recovery after any form of system failure or cyber-attack.'* This aligns with Chigaro (2017), who found that e-banking security strategies in Zimbabwean banks include system recovery and restoration mechanisms that help maintain service continuity after cyber incidents, although their effectiveness depends on system reliability and consistent implementation. These findings were consistent with Kim and Park (2021), who said that reliable backup systems enhanced organisational resilience by ensuring continuous availability of data and services even after system compromise.

4.4.2 Multi-Factor Authentication (MFA)

Findings showed that 28.1% of respondents rated MFA as effective, while 62.5% indicated that it was very effective, resulting in a combined 90.6% of respondents who perceived MFA as an effective cybersecurity control within commercial banks in Harare CBD. The results suggested that MFA strengthened identity verification by requiring multiple authentication factors, thereby reducing unauthorised access even when credentials were compromised. The descriptive

statistics showed a mean score of 3.38 and a standard deviation of 0.71, indicating consistent responses. This was supported during interviews, where one respondent stated that: *"Multi-Factor Authentication has greatly reduced unauthorised access because even when passwords are stolen, access is still blocked by secondary verification."* These findings concur with Mutanda and Chrispen (2023), who reiterated that access control mechanisms and multi-factor authentication are widely used in Zimbabwean banks as part of integrated cybersecurity controls to reduce unauthorised access and cyber fraud. Similarly, Maphosa (2023) notes that authentication-based controls form a key component of ICT security frameworks in financial institutions, although their effectiveness depends on institutional capacity, system integration, and proper implementation.

4.4.3 Firewalls

In firewalls, the study revealed that 34.4% had classified them as an effective control while 56.3% as very effective hence an average of 90.7% users of firewalls rated them as a very effective control in commercial banks located in Harare CBD. This indicates that firewalls acted as first line defense by blocking malicious attacks and controlling access to computer systems within an organization. These responses were affirmed with descriptive statistics having mean 3.44 and SD 0.72, indicating quite similar views from respondents. This view was reiterated by interviews, in which one interviewee clearly articulated: *"Firewalls are very important in blocking any unauthorized access and it is the first layer of defense that our organization has"*.

The results agree with Chigora (2017) that basic controls such as firewalls play a significant role in preventing unauthorized access in Zimbabwean banks. These findings align with Mutanda and Chrispen (2023), who found that firewalls are widely used in Zimbabwean banks to prevent unauthorized access and cyber fraud, although their effectiveness depends on proper implementation and system integration.

4.4.4 Data Encryption

Encryption was rated by 40.6% and 50% of the respondents as useful and very useful, thus giving a total of 90.6% which considered encryption as a useful cybersecurity measure. It seemed that sensitive banking data was protected with encryption as it transforms data to a format which cannot be understood by those who intercept it, regardless of whether the data is being transmitted or stored. The mean obtained was 3.38 and it has a standard deviation of 0.71 which indicated relatively similar responses. This was found in interviews as one respondent claimed: *"Encryption is important, if data were to be intercepted it can't be read."* These findings are in line with Ali et al (2020) where encryption helped to prevent data interception attacks against financial systems. Maphosa (2023), found that encryption systems are widely used in Zimbabwean financial institutions as part of core cybersecurity controls; however, their effectiveness depends on institutional capacity, system strength, and continuous improvement of security frameworks.

4.4.5 Intrusion Detection and Prevention Systems (IDS/IPS)

As presented on figure 4.1 above, 43.8% perceived the use of IDS/IPS as effective and 43.8% as very effective for a total of 87.6% who perceive it as important to the security of cyber technologies within the commercial banks in the CBD of Harare. IDS/IPS is perceived as very important as they are useful in monitoring networks, detecting malicious activities, and preventing the intrusion of networks into bank systems. The mean was 3.28 and the standard deviation was 0.73. This confirms the positive perception of IDS/IPS as a critical security measure and highlights low variation across banks. This indicates that IDS/IPS systems is very helpful in early detection of threat to network and strengthening it to avoid cyber intrusions. During interviews one interviewee responded that *"IDS/IPS systems is useful as it detects unusual network activity early"*. This aligns with Akinbowale, Klingelhöfer and Zerihun (2024), who found that continuous auditing and

monitoring tools significantly enhance the detection and prevention of cyberfraud in banking systems, although their effectiveness depends on system integration, update frequency, and staff technical competence.

4.4.6 Patch Management

It was found that 50.0% of the respondents rated it effective and 37.5% rated patch management as very effective, so 87.5% thought that patch management was effective in protecting commercial banks in Harare CBD from cyber threats. Patch management was said to minimize system vulnerabilities because it dealt with known software flaws that could be used to attack systems by cyber criminals especially through out-of-date Operating Systems and applications. The average score was 3.22 and the standard deviation 0.66 implying general positive view with consistency in application varying across institutions as confirmed by one interview *response "timely patching prevented the known weaknesses to be exploited because attackers will mostly use up-to-date systems"*. These findings align with Maphosa (2023), who found that continuous system strengthening and regular updates are essential for improving cybersecurity effectiveness in financial institutions, as outdated systems increase vulnerability to cyber threats despite the presence of security tools.

4.4.7 Disaster Recovery Planning (DRP)

It was found that 43.8% and 40.6% respectively regarded Disaster Recovery Planning as effective and very effective for an accumulated 84.4% of respondents who regarded DRP as an essential business continuity and security control within commercial banks operating in the Harare CBD. The finding also implied that DRP was considered as a significant control to ensure that normal banking activities resume as quickly as possible when faced with computer based or other events. The calculated mean was 3.19 while standard deviation was 0.82, suggesting relatively positive opinions about the use of DRP with some

variation, especially with respect to institutions testing frequency. The finding also implies that testing and integration into an overall risk management strategy were essential for the effectiveness of DRP. This was evident from an interview, where one interview respondent said, *"Disaster recovery plans guarantee that the business processes continue, but effectiveness would only be realized with frequent tests"*. These findings concur with Maphosa (2023, emphasized DRP reduces downtime and improves operational continuity when supported by regular testing, simulation exercises, and integration into business continuity planning.

4.4.8 Staff Cybersecurity Training

From figure 4.1 above, it is evident that 53.1% of respondents considered staff cyber security training to be effective while 31.3% indicated that it was very effective giving a total of 84.4% who regarded staff cyber security training as an essential measure of developing cyber security capabilities in commercial banks in Harare CBD. These results revealed that training staff equipped personnel is better to understand, identify, and manage cyber threats like phishing, social engineering and vulnerable system usage therefore increasing staff's risk mitigation capacity and minimizing human-related security risks. These outcomes have a mean of 3.09 with standard deviation of 0.78 indicating overall positive assessment with relatively little spread among institutions. These results are pointed toward the human element remaining important in cyber security, and that effective training can help reduce preventable compromises.

These results also corresponded with the results obtained from interviews where one respondent said, *"The repeated training in cyber security has assisted staff to recognize the attacks in their earliest stage, to thus avoid risky procedures"*. These findings align with Chigaro (2017), who noted that system effectiveness in banking environments improves when staff are adequately trained to correctly use cybersecurity controls, as user-related errors such as weak passwords can

compromise otherwise strong systems. It is also supported by Mutanda and Chrispen (2023), who found that low cybersecurity awareness among employees and clients significantly reduces the effectiveness of cybersecurity measures, despite their technical availability

4.4.9 Security Information and Event Management (SIEM) Systems

Respondents revealed that 50% thought SIEM systems to be effective, and 28.1% thought it to be very effective (combined 78.1% response deemed SIEM to be important to security monitoring in a commercial bank in Harare CBD). The findings therefore proposed that SIEM systems played an important part in aggregating and analyzing security logs across many systems, hence enhancing the detection of malicious activity, and enabling rapid response to incidents. The mean was 2.97 and the standard deviation 1.00; this indicates moderate system effectiveness, though with high variation in responses, suggesting that differences in system usage, integration, and in institutional IT expertise affect perceptions.

The results are an indication that the effectiveness of SIEM depends greatly on its depth of implementation, and on its level of use within organizations, something also confirmed during qualitative interviews where one respondent asserted, *"SIEM systems help us track and analyses logs from different systems to detect suspicious activity early."* These findings align with Akinbowale, Klingelhöfer and Zerihun (2024), who found that centralized monitoring tools such as continuous auditing and real-time analytics improve threat detection in banking systems, although their effectiveness depends on system integration and staff technical competence. Similarly, Mutanda and Chrispen (2023) highlight that weak system configuration, limited ICT skills, and inadequate organizational preparedness reduce the effectiveness of cybersecurity monitoring mechanisms in Zimbabwean banks, despite their widespread use.

4.5 Challenges Faced in Implementing Cybersecurity Measures

This section reports and interprets on the difficulties commercial banks in Harare CBD face when trying to implement cybersecurity to combat cyber-attacks. Based on Table 4.4 this section has utilized the frequency, percentage, mean and standard deviation statistics to interpret the degree of agreement among the respondents. The interpretation has been organized by statement as shown in Table 4.4 and each statement corresponds to a class of problems. The regulatory challenges and weak regulations statement have been reported under regulatory and institutional challenges, inadequate skilled personnel under skills and human resource challenges, obsolete systems under technological challenges, financial constraints under financial resources and employees' non-compliance under human and behavioral challenges. Each has been reported based on respondent agreement levels, statistical measures, impact of cyber security implementation on operation and supported with interview-based responses and relevant empirical research.

Table 4.4: Challenges Faced by Commercial Banks in Implementing Cybersecurity Measures (n = 32)

Question	Strongly Agree		Agree		Disagree		Strongly disagree		Descriptive statistics	
	Fre q	%	Fre q	%	Fr eq	%	Fre q	%	Mean	St Dev
Weak regulatory frameworks	12	37.5	14	43.8	4	12.5	2	6.3	3.13	0.89

hinder cybersecurity implementation										
Lack of skilled cybersecurity personnel affects implementation	13	40.6	12	37.5	5	15.6	2	6.3	3.12	0.88
Legacy systems limit modern cybersecurity effectiveness	15	46.9	11	34.4	4	12.5	2	6.3	3.22	0.81
Limited financial resources restrict cybersecurity investment	16	50.0	10	31.3	4	12.5	2	6.3	3.25	0.83
Employee non-compliance increases cyber risk	14	43.8	12	37.5	4	12.5	2	6.3	3.18	0.85

Source: Primary data (2026)

4.5.1 Regulatory and Institutional Challenges (Weak regulatory frameworks hinder effective cybersecurity implementation in commercial banks.)

Weak regulatory framework impedes effective cybersecurity implementation in commercial banks. Looking at Table 4.5, 37.5% strongly agreed with the statement and 43.8% agreed, thus the total level of agreement among respondent was 81.3%. The statement achieved the following result: Mean 3.13 and SD 0.89, which can be interpreted as strong agreement with a relative consistency in respondent's perception. The question item belongs to regulatory and institutional challenges that concern legal, institutional, enforcement and governance capacity. Results showed that weak regulatory framework negatively impacts the effectiveness of cybersecurity. Lack of strictness of regulation, slow resolution of cybercrime, limited enforcement capacity contributes negatively to implementation of security measures. Such conditions breed the creation of loopholes that could be exploited by attackers and also create weak deterrence effect toward perpetrators of cybercrime. In the interview, one respondent argued, *"Cybersecurity enforcement is still weak because regulations are not strict enough and cybercrime cases take too long to be resolved."* this conforms with the work of Dzomira (2014), whose study indicates that, Weak regulatory framework, the slow resolution of judicial cases, lack of enforcement capacity severely negatively impact upon effective cybersecurity implementation in Zimbabwean banks.

4.5.2 Skills and Human Resource Challenges (Lack of skilled cybersecurity personnel affects implementation of cybersecurity measures in commercial banks)

Shortage of skilled cybersecurity personnel impacted on the deployment of security measures by commercial banks. From table 4.4, 40.6% strongly agreed

and 37.5% agreed to this statement, therefore 78.1% agreed to the statement. The item scored 3.12 for the mean and 0.88 for the standard deviation. This showed a higher agreement among participants with relatively consistent answers. This statement belongs to the skills and human resource challenges category because it refers to the lack of cybersecurity personnel and technical know-how in banks. This shortage of expert cybersecurity professionals hindered banks from efficiently installing and managing their cybersecurity systems. Therefore, delayed threat detection, inefficient configuration of systems and dependence on a small pool of technical experts caused a rise in organizational vulnerability to cyber-attack, and this also weakened overall organizational security strength. During an interview, a respondent commented: *"We do not have enough specialist personnel that know security, so at times, the systems are not monitored as properly as possible."* This supports the findings of Maphosa (2023) that lack of skilled professional cyber security employees, low level awareness, among staffs were great challenges to deployment of cyber security among financial institutions in Zimbabwe.

4.5.3 Technological (Legacy Systems) Challenges (Outdated legacy systems limit the effectiveness of modern cybersecurity tools in commercial banks)

This issue, the presence of old legacy system making the use of modern cybersecurity tools difficult in commercial banks was agreed by the majority. From Table 4.4 46.9% of the respondents strongly agreed and 34.4% agreed with the item, giving a majority agreement of 81.3%. The mean was 3.22 with standard deviation of 0.81 thus indicating a fairly high degree of agreement and minimal spread across respondents. The problem belongs to technological challenges because the system is based on infrastructure and system integration.

It implied that the usage of old legacy systems prevents banks from fully utilizing modern cybersecurity tools such as advanced threat detection and real time response. This makes the banks vulnerable, hinders efficiency of operations and

inability to counter emerging threats since the current technology infrastructure is obsolete. According to one *respondent* "Some of our systems are old and do not easily support new cybersecurity tools, making it more difficult for us to implement some of the new tools and security measures and consequently increases the risk of attacks". This aligns with Dzingirai (2022), who found that system downtimes, increasing technological complexity, and inadequate technical expertise are major operational challenges in Zimbabwean banks, which hinder effective management of emerging cyber threats.

4.5.4 Financial and Resource Constraints (Limited financial resources restrict investment in cybersecurity infrastructure within commercial banks.)

Limited financial resources constrained the acquisition of cybersecurity infrastructure by commercial banks. Out of the 50% that strongly agreed and 31.3% agreed to this item based on table 4.4, it shows that overall 81.3% of the respondents agreed with this statement, item recorded a mean of 3.25 and a standard deviation of 0.83 indicating that most of the respondents strongly agree with the statement and also the responses are relatively consistent. This issue is categorized under financial and resource constraints since the item refers to limitations due to budget constraints which in turn affect ability to buy/ upgrade or maintain security tools.

This item indicated that there is a lack of allocation of finances for cybersecurity which limited the banks' capability to afford up to date security solutions/ technologies, and also systems upgrade and purchase of outside security experts which will significantly decrease the bank's ability to prevent and handle cyber-attacks, especially with regard to new and emergent attacks in the banking sector. One respondent said during an interview; *"cybersecurity tools and upgrades cost money and often we prioritise other operational activities against security updates and upgrades."* This concurs with Dzingirai (2022), who found that resource constraints and system limitations in Zimbabwean commercial

banks, including technological risk and operational inefficiencies, reduce the ability of institutions to effectively manage and implement cybersecurity measures against emerging threats.

4.5.5 Employee Non-Compliance Challenges (Employee non-compliance with cybersecurity policies increases cyber risk in commercial banks.)

Employees fail to adhere to the cybersecurity policies. This fact would increase cyber risk within commercial banks. According to Table 4.4, 43.8% respondents "strongly agree" and 37.5% "agree" with the item (sum: 81.3% of respondents). The item has a mean score of 3.18 and a standard deviation of 0.85. The result shows respondents had high agreement with the item and moderately consensus with the response. The challenge falls under human and behavioral challenges category, since it refers to whether employees follow the security policies and procedures, or have safe digital behaviors.

According to the finding, lack of adherence to cybersecurity policies by employees can expose the banks to unnecessary risks, such as phishing attacks, poor password security management, unauthorized system access and so forth. This would undermine the effectiveness of robust cybersecurity system, since human behavior becomes an important part in overall cybersecurity system and could be the critical vulnerability point. A respondent had said that: *"Even though we have strong security systems in place, some employees do not follow the procedures strictly, thereby making them a source of vulnerability"*. This aligns with Mugari et al. (2016), who found that weak coordination between banks and law enforcement, along with inadequate cybersecurity infrastructure and poor information-sharing systems, significantly constrain effective cybercrime prevention in Zimbabwe's financial sector.

4.6 Recommended Strategies to Enhance the Effectiveness of Cybersecurity Measures in Commercial Banks

This section provided the responses of respondents in relation to strategies recommended for the enhancement of the effectiveness of the cybersecurity measures within the commercial banks in the Harare Central Business District (CBD). This section analyzed respondents' opinion on what measure can improve cybersecurity readiness, increase detection and response, improve the awareness of personnel, and alleviate the present technological and operational challenges that impact on the effectiveness of the implementation of the cybersecurity measures. The section also analyzed the priority areas for cybersecurity governance and strengthening the institutional capacities for cybersecurity implementation in banks as identified by the respondents and examined both human-centric and technology-based solutions as critical element of mitigating the security threats and strengthening system defenses. These results were tabulated through frequencies, percentages, mean values and standard deviations (shown in table 4.5) using descriptive statistics.

Table 4.5: Recommended Strategies to Enhance the Effectiveness of Cybersecurity Measures in Commercial Banks

Recommendations strategy	Strongly Agree		Agree		Disagree		Strongly disagree		Descriptive Statistics	
	Freq	%	Freq	%	Freq	%	Freq	%	Mean	Std dev
Increase Staff training	17	53.1	12	37.5	2	6.3	1	3.1	3.38	0.82

Regular System Updates	19	59.4	8	25.0	3	9.4	2	6.3	3.38	0.80
Strengthen MFA systems	18	56.3	10	31.3	1	3.1	3	9.4	3.34	0.80
Invest in Cyber technologies	19	59.4	10	31.3	2	6.3	1	3.1	3.47	0.75
Conduct Awareness campaigns	20	62.5	8	25.0	1	3.1	3	9.4	3.41	0.81
Improve Incident response	15	46.9	15	46.9	1	3.1	1	3.1	3.38	0.61
Strengthen Stakeholder collaboration	17	53.1	13	40.6	1	3.1	1	3.1	3.44	0.63

Source: Primary data (2026)

4.6.1 Increase Staff Training

Results concerning the recommendation to increase staff training showed a highly positive response, with 90.6% of all respondents (consisting of 53.1% strongly agreed and 37.5% agreed) stating that staff training was important for improving cybersecurity in commercial banks in Harare CBD. Also, results yielded a mean score of 3.38 with a standard deviation of 0.82 thus showing that it was

ranked moderately high by most people though with slight variations. During the interviews the participants said *that "the continuity of staff cybersecurity awareness programs is crucial as a lack of staff awareness has led to people falling victims to phishing attacks and intrusion of systems."*

This showed that increasing staff training was rated as very important recommendation due to employee knowledge enhancement to detect cyber-attacks, human error minimization, and an increased level of cyber security culture within the organization. These findings implied that increasing staff training was strongly endorsed as a key cybersecurity recommendation because it strengthened employees' ability to identify cyber threats, reduced human error, and improved overall organizational cybersecurity culture. This aligns with Takavarasha Jr et al. (2023), who recommend continuous cybersecurity awareness and training programmes to reduce human-related vulnerabilities such as phishing and social engineering, which became more prevalent in digital banking environments. It is also supported by Kanyongo and Wadesango (2025), who emphasize that human behavior remains a major cybersecurity vulnerability in commercial banks and therefore call for ongoing customer education and awareness initiatives to reduce security breaches linked to user error.

4.6.2 Regular System Updates

Regular system update results had very strong consensus as 84.4% respondents that consist of 59.4% strongly agreed and 25.0% agreed confirmed that regular system updates were necessary for enhancement of the cybersecurity in commercial banks of Harare CBD. The result gave a mean score of 3.38 and standard deviation of 0.80 implying that this strategy was viewed favorably by respondents and opinions were very close to one another.

These results concluded that regular system updates were strongly recommended as a cybersecurity measure as they help to protect system from

any security vulnerabilities, system performance are improved and system is less exposed to new cybersecurity threats. This point was heavily supported during interview session as one respondent mentioned that *"failure to update banking system on time will make institutions susceptible to malware attack and unauthorized access attempts"*. This strong endorsement of regular system updates aligns with Chigora and Sibanda (2020), who highlighted that weak system maintenance created cybersecurity gaps in financial institutions. This aligns with Kanyongo and Wadesango (2025), who recommend continuous cybersecurity assurance practices such as regular system audits and vulnerability assessments to reduce exposure to system weaknesses and maintain security integrity in banking environments.

4.6.3 Strengthen MFA Systems

For strengthening multi-factor authentication systems there was found to be a very high agreement with this recommendation as the results show that 87.5% of the respondents were comprised of 56.3% of strong agreement and 31.3% of agreement thus confirming the importance of strengthening multi-factor authentication systems as a security recommendation to protect against cyber-attacks in commercial banks in Harare CBD. This strategy had a mean score of 3.34 and standard deviation of 0.80 which proves that it was ranked high by respondents with there being close similar perceptions between them. Through interviews respondents noted that, *"multi-factor authentication had significantly reduced cases of unauthorized access"* and furthermore *"added layers of authentication to control banking system logins and discourage intrusions."* These findings implied that strengthening MFA systems was strongly endorsed as a key cybersecurity recommendation because it enhanced user authentication, reduced unauthorized access risks, and added an additional security layer against identity based cyberattacks. This aligns with Poshai, Chilunjika and Intauno (2023), who recommend strengthening institutional capacity and

improving cybersecurity infrastructure to enhance the detection and prevention of cyber threats in financial systems

4.6.4 Invest in Cyber Technologies

The result in relation to investment in cyber technologies received very strong endorsement with 90.7% of respondents, which is composed of 59.4% who strongly agreed and 31.3% who agreed that "continuous investment on advanced cyber technologies are very important in building up the cybersecurity of the commercial banks within Harare CBD. The result also yielded a mean of 3.47 and a standard deviation of 0.75 indicating that the strategy has a high endorsement from the respondents and their responses are quite close to each other. Participants interviewed strongly believe that enhancing current systems are key; with one respondent stating that *"AI driven threat detection, next generation firewalls, SIEM, XDR and ZTA are vital to real time detection and response of modern cyber threats."*

These results signify that investing in cyber technologies received an overwhelming endorsement as the top cybersecurity recommendation, because of its effectiveness in promoting proactive threat detection, enabling faster response times, and enhancing systems resistance against diverse cyber threats. The endorsement is in line with Chikoto (2022) who advocates for consistent investment in technological solutions coupled with robust ICT governance for effective management of cyber threats among financial institutions. The findings also corroborate with the extant literature that AI-driven analytics, Zero Trust framework and unified security platforms like XDR and SIEM play a key role in modern banking security in achieving cyber threat detection and response (ENISA, 2022).

4.6.5 Conduct Awareness Campaigns

From results on having a cybersecurity awareness campaign, it was very highly supported, 87.5% of which composed of 62.5% who strongly agree and 25.0% who agree supported that an awareness campaign is important for a stronger cybersecurity. It produced a mean score of 3.41 and a standard deviation of 0.81; this indicates strong support. Based on the interviews conducted, respondents stated *that "continuous awareness campaign enhances employees to detect phish email and risky practice with the system"*

This concurs with Takavarasha Jr et al. (2023), who emphasized continuous cybersecurity awareness and training programmes to reduce human-related vulnerabilities such as phishing and social engineering in digital environments. It is also supported by Poshai, Chilunjika and Intauno (2023), who recommend strengthening public awareness initiatives and institutional capacity to improve cybersecurity compliance and response to cyber threats. Additionally, Gumbo, Masimba and Zuva (2025) indicated the importance of integrating cybersecurity awareness within a broader multi-layered framework that combines human, technical, and governance measures to enhance overall digital resilience.

4.6.6 Improve Incident Response

Improving incident response' findings had a very high level of support with 93.8% of respondents (46.9% strongly agreed and 46.9% agreed) noting that strengthening incident response is critical for commercial banks in Harare CBD's cybersecurity profile. The results obtained gave a mean value of 3.38 with a standard deviation of 0.61, this gave an indication that participants responded at a high level and that their response was relatively tightly clustered together. Interview respondents made recommendations in relation to having speedy and integrated response mechanisms and *that "incident response systems should quickly isolate infected systems so as to contain the spread of cyber threat"*,

while another respondent was quoted to say that *"there is need for improved escalation procedures so that there is prompt response to cyber incident"*.

The implication is that improving incident response is highly supported as it leads to faster identification, containment, eradication and recovery of cyber-attack, thus ensuring operational efficiency and a reduced disruption of services. This supported the recommendation by Chikoto (2022) which suggests the establishment of integrated ICT governance structure and standardized incident response frameworks as way of improving cyber-threat management in banks.

4.6.7 Strengthen Stakeholder Collaboration

From the recommendations on strengthening stakeholder collaboration, there was very strong support for this recommendation with 93.7 % of respondents which includes 53.1% who agreed strongly and 40.6% who agreed to the statement that stakeholder collaboration should be increased for cybersecurity in commercial banks in Harare CBD. The responses recorded a mean score of 3.44 and a standard deviation of 0.63 which suggests that the scores were high and were not spread out very widely. In the interviews held, stakeholders highlighted that collaboration between the banks, regulators and ICT service providers are crucial, a respondent clearly states that *"effective cyber security requires banks and regulators to share information in order to quickly address any emerging threats."*

These findings implied that strengthening stakeholder collaboration was strongly endorsed as it improved information sharing, coordinated response to cyber threats, and enhanced overall sector wide cybersecurity resilience. This aligns with Gumbo, Masimba and Zuva (2025), who recommend enhanced coordination among stakeholders as a core pillar of improving cybersecurity preparedness and response capabilities within digital environments.

4.8 Chapter Summary

This chapter highlighted and examined the information about measures being taken by commercial banks in the Harare CBD to protect against the threats of cybercrime. The results show that measures like integrated cyber security systems, training of staff on regular basis, multi factor authentication, real time monitoring and ICT governance are very important for enhancing cyber security, by making the financial institutions to better prevent, detect and respond to cybercrime attacks. Generally, the study found that cyber security effectiveness of commercial banks is based on combined strategy of technical, human and governance controls.

CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

The chapter summarizes the final phase of the study that is the application of measures by financial institutions in fighting against cyberattacks where commercial banks in Harare CBD, Zimbabwe are the focus. This chapter summarizes the whole study, the main findings that are linked to research objectives, conclusion reached and recommendations made. This chapter depends on empirical findings presented in Chapter four.

5.1 Summary of the Study

Cyber threats in Zimbabwe's financial sector continue to threaten the stability, data security, and trust of digital banking systems in commercial banks. This study evaluated the effectiveness of cybersecurity measures employed by commercial banks in Harare Central Business District (CBD). Specifically, the study sought to identify the cybersecurity measures currently employed, determine their effectiveness in combating cyber threats, examine challenges encountered in their implementation, and recommend strategies for improving cybersecurity effectiveness. The study adopted a pragmatist mixed methods approach and utilized a descriptive research design. Data was collected using questionnaires and interviews from a sample of 40 bank employees drawn from selected commercial banks in Harare CBD. Quantitative data were analyzed using

SPSS, while qualitative data were analyzed using thematic analysis.

The findings revealed that commercial banks employ cybersecurity measures such as firewalls, encryption, multi-factor authentication, intrusion detection systems, data backup systems, and staff cybersecurity awareness training, although the adoption of advanced technologies such as Security Information and Event Management (SIEM) systems remains limited. The study found that these measures were generally effective in mitigating cyber threats and enhancing the security of banking operations. Key challenges including weak regulatory enforcement, shortage of skilled cybersecurity personnel, outdated systems, financial constraints, and employee non-compliance with cybersecurity policies affected their effectiveness. The study concluded that effective cybersecurity in commercial banks depends on the integration of cybersecurity technologies, staff competencies, and institutional coordination within the financial sector. It is recommended that commercial banks adopt integrated cybersecurity systems and strengthen continuous staff training to enhance cyber threat detection and response.

5.2 Summary of Major Findings

The major findings of the study are presented according to the following research objectives:

1. To identify the cybersecurity measures currently employed by Commercial banks in Harare CBD.
2. To determine the effectiveness of the current cybersecurity measures employed by Commercial banks in Harare CBD to combat cyber threats.
3. To explore the challenges encountered by the commercial banks located in Harare CBD when implementing measures to combat cyber threats.
4. To recommend strategies to enhance effectiveness of cybersecurity measures in combating cyber threats in Commercial Banks located in

Harare CBD.

5.2.1 To identify cybersecurity measures currently employed by commercial banks in Harare CBD

The study established that a variety of cybersecurity controls have been implemented by banks in Harare CBD to safeguard the banking systems and customer data, with generally high levels of adoption among the critical controls. Controls such as firewalls, multi-factor authentication, encryption, data backup (90.7%), staff cybersecurity training, intrusion detection and prevention systems (81.3%), patch management (81.3%) and disaster recovery (80.6%) had a strong implementation as these are largely preventive and recovery controls where most banks institutionally endeavor to secure their systems and operations. The application of Security Information and Event Management (SIEM) was found to have lower adoption level (71.9%).

5.2.2 To determine the effectiveness of cybersecurity measures in combating cyber threats

The research concluded that the cybersecurity controls utilized by the selected commercial banks in Harare CBD were largely effective in preventing cyber threats with a particularly strong performance in preventive and recovery controls. Effective levels of above 90 percent were identified with data backup systems (93.3%), firewalls (90.7%), multi-factor authentication (90.6%) and data encryption (90.6%) indicating that the banks had a strong defense against unauthorized Access to sensitive information. Other measures like intrusion detection and prevention systems (87.6%), patch management (87.5%), disaster recovery plan (84.4%) and staff cybersecurity training (84.4%) also proved effective in monitoring, enhancing system resilience and building human awareness. Security Information and Event Management (SIEM) systems were found to be the least effective at 78.1 percent.

5.2.3 To explore the challenges encountered by the commercial banks located in Harare CBD when implementing measures to combat cyber threats.

It was concluded that several interrelated issues made the implementation of cybersecurity practices difficult in commercial banks in Harare CBD. A limitation to effective implementation of cybersecurity measures was weak regulatory and institutional frameworks as 81.3% of respondents stated that poor enforcement capacity hindered collaborative efforts in security management and made organizations less accountable. Skills and human resource limitations were also a concern as 78.1% agreed that shortages of IT personnel and skilled security professionals undermined the effectiveness of system monitoring and rapid response to attacks. Technological constraints were also found to be a problem because 81.3% stated that use of obsolete systems limited the installation of modern security technologies. Financial constraints were a major problem as 81.3% reported that inadequate capital undermined security investments. Non-compliance with cybersecurity policies was a behavioral problem as 81.3% agreed that it exposed organizations to threats.

5.2.4: To recommend strategies for improving the effectiveness of cybersecurity measures in commercial banks

This revealed that effective cyber security enhancement of the commercial banks within the CBD of Harare would be best enhanced if an integrated package of the institutional co-ordination of Cyber Security, adoption of technology, human resource capacity development and a highly regarded incident response strategy were implemented. Incident response strategy recorded the highest level of support at 93.8%, indicating that the ability to detect, contain and recover from cyber-attacks is of primary concern to operational continuity in a risk-filled digital banking environment. Almost on par with this, stakeholder co-operation recorded 93.7%, emphasizing the fact that strong cybersecurity resilience in banking is largely dependent on the co-ordination of information exchange between banks

and regulatory bodies to develop timely threats intelligence and a unified approach to threats.

While investment on Cyber technology recorded 90.7%, institutions are now investing in sophisticated security systems that can improve threats detection and systems security using intelligent real-time systems. Support for multi-factor authentication system, recording 87.5%, demonstrated the increased need for robust identity management, while support for cybersecurity staff training at 87.5% and cyber security awareness program at 84.4% revealed the lingering challenge that the human factor has presented in the pursuit of strong cyber security, thereby underlining the necessity of continuous human resource capacity building. In addition, system updating recorded support at 84.4%, emphasizing the fact that a constant system update is necessary in enhancing cyber security through mitigating its underlying vulnerabilities. Combined, these revealed that Cyber security can only be best achieved with a synergy of technology, the human element, and institutional cooperation working together to provide a comprehensive layer of protection.

5.3 Conclusion

From the outcome of the study, it was concluded that a set of comprehensive cyber security measures which include preventive, detective, and recovery controls have been applied by the commercial banks in Harare CBD thus fulfilling the objective that of identifying cyber security strategies that have been applied. It was concluded that cyber security measures has been reasonably effective in strengthening the security of the system especially those related to foundational controls like firewalls, encryption, multi-factor authentication, data backup, and so forth, but less effective in sophisticated monitoring systems like SIEM due to poor system integration, inadequate technical capability, thereby fulfilling the objective on effectiveness. It was concluded that the major cyber security

implementation challenges were legacy system limitation, shortage of technical staff, financial limitation, lack of strict regulatory enforcement, and personnel non-compliance, thus fulfilling the objective on challenges in the implementation of the various cyber security strategies. Lastly, it was concluded that for greater effectiveness, all these cyber security systems must be better integrated and technically upgraded, effective response mechanism, better regulated, and continuous awareness is created among all employees, thus fulfilling the last objective on recommended measures of improvement for cyber security in commercial banks in Harare CBD.

5.4 Recommendations

In consideration of the findings, the following recommendations are put forward to enhance cybersecurity effectiveness within commercial banks in Harare CBD:

5.4.1 Improve Integration of Cybersecurity Systems

It is recommended that the commercial banks within Harare CBD must upgrade and merge their security systems, to enhance their cybersecurity defenses. It was realized that the security systems of commercial banks within Harare CBD are disjointed systems, which rely heavily on obsolete legacy systems. Hence real-time monitoring and concerted response are hindered. Nonetheless, the enhancement of the connectivity between prevention systems, detection systems, and response systems will surely be the most useful approach.

5.4.2 Strengthen Continuous Cybersecurity Training and Awareness

Furthermore, banks are advised to enhance continuous and real security training to all employees. The study proved that human factors (lack of awareness, non-adherence to security policies and lack of practical exposure) are able to neutralize robust technical security measures. Hands-on and real training in specific threat environments would enable the organization's personnel to better

detect threats such as phish attacks and reduce operational errors in which a system can be compromised.

5.4.3 Enhance Investment in Advanced Cybersecurity Technologies and Collaboration

Additionally, it is proposed that commercial banks and regulators invest more in modern cyber security technologies and coordination mechanisms in the financial sector. The results indicated a low rate of use of modern technologies such as comprehensive security monitoring tools which affected early detection of security threats. Improvement in coordination, information sharing and automated security tools would strengthen the ability of commercial banks to prevent security threats, facilitate swift responses and promote overall cybersecurity.

5.5 Suggestions for Future Studies

Future research must include:

1. Evaluation of AI/ML in detecting and preventing threats in the banks.
2. The effect of behavior and culture on cybersecurity.
3. Evaluation of the cyber security regulations in banks in Zimbabwe.

REFERENCES

- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024). Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation. *Journal of Financial Crime*, 31(1), 201–225. <https://doi.org/10.1108/JFC-02-2023-0025>
- Bell, E., Bryman, A., & Harley, B. (2022). Business research methods (6th ed.). Oxford University Press.
- Bhandari, S., Panihar, R., Naval, S., Laxmi, V., Zemmari, A., & Gaur, M. S. (2018). SWORD: Semantic aware Android malware detector. *Journal of Information Security and Applications*, 42, 46–56. <https://doi.org/10.1016/j.jisa.2018.07.003>
- Chigaro, M. (2017). An assessment of the effectiveness of e-banking security strategies in Zimbabwe: The case of Stanbic Bank Zimbabwe (master's thesis, University of Zimbabwe).
- Chigaro, M. (2017). An evaluation of the effectiveness of e-banking security strategies in Zimbabwe: A case study of Zimbabwean commercial banks. *Journal of Internet Banking and Commerce*, 22(3).
- Creswell, J. W., & Creswell, J. D. (2021). Research design: Qualitative, quantitative, and mixed methods approach (6th ed.). Sage.
- Creswell, J. W., & Creswell, J. D. (2022). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). Sage.
- Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). Sage.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.

De Vaus, D. A. (2021). *Surveys in social research* (6th ed.). Routledge.

Deloitte. (2022). *Global financial services cybersecurity survey: Managing systemic risks in banking*. Deloitte Insights.

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry Zimbabwe. *Risk Governance and Control: Financial Markets & Institutions*, 4(2), 17–27.

Dzomira, S. (2014). Electronic fraud (e-fraud) in the Zimbabwean banking sector. *International Journal of Economics, Commerce and Management*, 2(10), 1–16.

Farooq, M., Khan, A., & Zhao, L. (2021). Cybersecurity practices in emerging banking ecosystems: A comparative analysis of technical and organizational frameworks. *International Journal of Information Management*, 57, Article 102281. <https://doi.org/10.1016/j.ijinfomgt.2020.102281>

Flick, U. (2022). *An introduction to qualitative research* (7th ed.). Sage.

Gozman, D., Liebenau, J., & Mangan, J. (2018). On the innovation mechanisms of fintech start-ups: Insights from Swift's Innotribe competition. *Journal of Management Information Systems*, 35(1), 145–179.

Gumbo, F., Masimba, F., & Zuva, T. (2025). A cybersecurity framework for enhancing public sector digital resilience in emerging economies. In *Proceedings of the 5th International Multidisciplinary Information Technology and Engineering Conference (IMITEC 2025)*. <https://doi.org/10.1109/IMITEC67386.2025.11410479>

Hair, J. F., Page, M., & Brunsveld, N. (2022). *Essentials of business research methods* (5th ed.). Routledge.

IBM Security. (2022). *Cost of a data breach report 2022*. IBM Security.

Interpol. (2020). African cyberthreat assessment report. Interpol Cybercrime Directorate.

International Telecommunication Union. (2020). Global cybersecurity index 2020. ITU Publications.

Jain, N., & Agarwal, R. (2026, February 20). Digital transformation in banking: Navigating the fintech revolution, cybersecurity imperatives, and regulatory frontiers in the global digital economy. SSRN. <https://ssrn.com/abstract=6562779>

Johnston, M. P. (2021). Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Research Methods*, 5(1), 619–626.

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

Kizza, J. M. (2017). Guide to computer network security (4th ed.). Springer.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, 8(6), 898.

Krutz, R. L., & Vines, R. D. (2010). The CISSP prep guide: Mastering the ten domains of computer security (2nd ed.). John Wiley & Sons.

Leedy, P. D., & Ormrod, J. E. (2019). Practical research: Planning and design (12th ed.). Pearson.

Maphosa, V. (2024). An overview of cybersecurity in Zimbabwe's financial services sector (Version 2). *F1000Research*, 12, 1251. <https://doi.org/10.12688/f1000research.132823.2>

Moro, A., Wisniewski, T. P., & Mantovani, G. (2021). Does digital transformation mitigate or amplify operational risk in commercial banking? *Journal of Financial Stability*, 54, Article 100882. <https://doi.org/10.1016/j.jfs.2021.100882>

Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime: The emerging threat to the financial services sector in Zimbabwe. *Mediterranean Journal of Social Sciences*, 7(3 Suppl. 1), 135–143. <https://doi.org/10.5901/mjss.2016.v7n3s1p135>

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce.

Office of National Risk Assessment. (2015). National risk assessment report on money laundering and cybercrime threats. Government Printer.

Poshai, L., Chilunjika, A., & Intauno, K. (2023). Examining the institutional and legislative frameworks for enforcing cybersecurity in Zimbabwe. *International Cybersecurity Law Review*, 4(4), 431–449.

Reddy, K. H. (2021). Digital payment vulnerabilities and technical measures for secure transaction routing. *Journal of Financial Engineering*, 28(2), 145–163.

Reserve Bank of Zimbabwe. (2019). Financial stability report 2019. Reserve Bank of Zimbabwe.

Reserve Bank of Zimbabwe. (2020). Bank supervision annual report 2020. Reserve Bank of Zimbabwe.

Saunders, M., Lewis, P., & Thornhill, A. (2023). Research methods for business students (9th ed.). Pearson.

Stallings, W., & Brown, L. (2015). Computer security: Principles and practice (3rd ed.). Pearson.

Takavarasha, S., Jr., Van Heerden, R., Thakur, S. C., & Jordaan, A. (2023). Cyber-security in the era of the COVID-19 pandemic: A developing countries' perspective. *International Journal of Industrial Engineering and Operations Management*, 5(2), 77–85. <https://doi.org/10.1108/IJIEOM-02-2023-0026>

Tashakkori, A., & Teddlie, C. (2010). SAGE handbook of mixed methods in social and behavioral research (2nd ed.). Sage Publications.

United Nations Conference on Trade and Development. (2020). The economic cost of cybercrime to digital economies in Africa. United Nations Publications.

Vives, X. (2017). The impact of fintech on banking market structure and financial stability. *Oxford Review of Economic Policy*, 33(2), 179–200.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.

Whitman, M. E., & Mattord, H. J. (2017). Principles of information security (6th ed.). Cengage Learning.

Appendix A

Bindura University of Science Education

P Bag 1020

Bindura

Dear Respondent

I am an undergraduate student at the above mentioned institution undertaking a Bachelor of Commerce (Honours) Degree in Financial Intelligence. I am carrying out a research study on the topic titled: "Effectiveness of Measures Employed to Combat Cyber Threats: A Survey of Commercial Banks in Harare CBD, Zimbabwe." In order for this research to be successful in obtaining relevant information, I kindly appeal to you to assist by completing the attached questionnaire. The information you provide will be treated with strict confidentiality and will be used solely for academic purposes. Disclosure of personal information such as your name, physical address, phone number, or any other identifying details is not required. Participation in this study is voluntary and you are free to withdraw at any stage without any penalty.

Your cooperation and honest responses will be greatly appreciated as they will contribute significantly to the success of this study.

For further information regarding this study, please feel free to contact the undersigned:

Researcher: Lloyd Joseph Duche

Contact Number: +263 773747373

Appendix B

Interview Guide

Dissertation Title:

“Effectiveness of Measures Employed to Combat Cyber Threats: A Survey of Commercial Banks in Harare CBD, Zimbabwe”

Position/Role: _____

Bank Name (optional code e.g., Bank A, Bank B, Bank C): _____

1. What cybersecurity measures are currently employed by your bank to combat cyber threats?
2. How effective are the current cybersecurity measures in preventing or reducing cyber threats within the bank?
3. What challenges does your bank encounter when implementing cybersecurity measures?
4. How do employee awareness, technology, and financial resources affect cybersecurity effectiveness in your bank?
5. What strategies would you recommend to improve the effectiveness of cybersecurity measures in commercial banks?

6. What role should regulators and other stakeholders play in strengthening cybersecurity in the banking sector?

7. Is there anything else you would like to share regarding cybersecurity practices in your bank?

Appendix C

RESEARCH QUESTIONNAIRE

SECTION A: DEMOGRAPHIC INFORMATION

Please tick (✓) the appropriate option.

1. Gender

☐ Male

☐ Female

2. Age Group

☐ 20–29 years

☐ 30–39 years

☐ 40–49 years

☐ 50 years and above

3. Highest Educational Qualification

☐ Higher Diploma

☐ Bachelor's Degree

☐ Master's Degree

☐ Doctorate

4. Department

- ☐ IT Department
- ☐ Compliance / Risk Management
- ☐ Finance and Accounting
- ☐ Operations
- ☐ Internal Audit
- ☐ Customer Service

5. Job Position

- ☐ Customer Service Officer
- ☐ Teller
- ☐ Credit Officer
- ☐ ICT / Security Officer
- ☐ Branch Manager

6. Years of Experience in Banking

- ☐ Less than 2 years
- ☐ 2–5 years
- ☐ 6–10 years
- ☐ Above 10 years

SECTION B: CYBERSECURITY MEASURES IN USE

Indicate the extent to which your bank uses the following cybersecurity measures.

Scale: SA = Strongly Agree A = Agree D = Disagree SD = Strongly Disagree

Cybersecurity Measure	SA	A	D	SD
Firewall systems	☐	☐	☐	☐
Multi-Factor Authentication (MFA)	☐	☐	☐	☐
Data encryption systems	☐	☐	☐	☐
Intrusion Detection Systems (IDS)	☐	☐	☐	☐
Security Information and Event Management (SIEM)	☐	☐	☐	☐
Patch management systems	☐	☐	☐	☐
Data backup systems	☐	☐	☐	☐
Disaster recovery planning	☐	☐	☐	☐
Employee cybersecurity training	☐	☐	☐	☐

SECTION C: EFFECTIVENESS OF CYBERSECURITY MEASURES

Rate the effectiveness of the following measures in combating cyber threats within your bank.

Scale:

VE = Very Effective E = Effective I = Ineffective VI = Very Ineffective

Cybersecurity Measure	VE	E	I	VI
Data backup systems	☐	☐	☐	☐

Multi-Factor Authentication (MFA)	☐ ☐ ☐ ☐
Firewall system s	☐ ☐ ☐ ☐
Encryption systems	☐ ☐ ☐ ☐
Staff awareness and training	☐ ☐ ☐ ☐
Intrusion Detection Systems (IDS)	☐ ☐ ☐ ☐

SECTION D: CHALLENGES FACED IN COMBATING CYBER THREATS

Indicate your level of agreement with the following challenges experienced by your bank.

Scale: SA = Strongly Agree A = Agree D = Disagree SD = Strongly Disagree

Challenge	SA	A	D	SD
Weak regulatory and legal frameworks	☐	☐	☐	☐
Shortage of skilled cybersecurity personnel	☐	☐	☐	☐
Outdated legacy banking systems	☐	☐	☐	☐
Limited financial resources for cybersecurity	☐	☐	☐	☐
Employee non-compliance with security policies	☐	☐	☐	☐

SECTION E: STRATEGIES FOR IMPROVING CYBERSECURITY EFFECTIVENESS

Indicate your level of agreement with the following strategies.

Scale: SA = Strongly Agree A = Agree D = Disagree SD = Strongly Disagree

Recommended Strategy | SA | A | D | SD

Increase staff cybersecurity training | ☐ | ☐ | ☐ | ☐

Conduct regular system and software updates | ☐ | ☐ | ☐ | ☐

Strengthen MFA systems using biometrics | ☐ | ☐ | ☐ | ☐

Increase investment in modern cybersecurity technologies | ☐ | ☐ | ☐ | ☐

Conduct continuous cybersecurity awareness programmes | ☐ | ☐ | ☐ | ☐

Improve incident response mechanisms | ☐ | ☐ | ☐ | ☐

Strengthen collaboration with regulators and ICT providers | ☐ | ☐ | ☐ | ☐

SECTION F: OPEN-ENDED QUESTIONS

1. What do you consider to be the most serious cyber threat currently facing commercial banks in Harare CBD?

.....

.....

2. Suggest any measures that could improve cybersecurity effectiveness in your institution.

.....

.....

THANK YOU FOR YOUR PARTICIPATION

Lloyd Joseph Duche

Chapter 1-5

FI DISSERTATION PLAGIARISM CHECK

Document Details

Submission ID

trn:oid:::2945:394337975

Submission Date

Jun 19, 2026, 4:49 PM GMT+2

Download Date

Jun 19, 2026, 5:28 PM GMT+2

File Name

Chapter 1-5.docx

File Size

430.9 KB

90 Pages

21,114 Words

128,312 Characters



Page 1 of 105 - Cover Page

Submission ID trn:oid:::2945:394337975



Page 2 of 105 - Integrity Overview

Submission ID trn:oid:::2945:394337975

14% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- 258 Not Cited or Quoted 12%**
Matches with neither in-text citation nor quotation marks
- 51 Missing Quotations 2%**
Matches that are still very similar to source material
- 1 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 9% Internet sources
- 3% Publications
- 12% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

PLAGIARISM REPORT

AI report

Lloyd Joseph Duche

LLOYD J. DUCHE DISSERTATION CHAPTER 1-5

 FI DISSERTATION PLAGIARISM CHECK

Document Details

Submission ID

tm:oid:::2945:394522664

Submission Date

Jun 21, 2026, 2:52 PM GMT+2

Download Date

Jun 21, 2026, 3:53 PM GMT+2

File Name

LLOYD J. DUCHE DISSERTATION CHAPTER 1-5.docx

File Size

545.6 KB

87 Pages

21,929 Words

130,984 Characters



Page 1 of 89 - Cover Page

Submission ID tm:oid:::2945:394522664



Page 2 of 89 - AI Writing Overview

Submission ID tm:oid:::2945:394522664

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (i.e., our AI models may produce either false positive results or false negative results), so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.