

**BINDURA UNIVERSITY OF SCIENCE EDUCATION**

**FACULTY OF COMMERCE**

**DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES**



**THE EFFICACY OF CYBERCRIME DETECTION AND PREVENTION STRATEGIES  
EMPLOYED BY RETAILERS IN ZIMBABWE. A CASE STUDY OF BINDURA CBD.**

**BY**

**CHAPFUWA TIRIVASHE GODFREY**

**(B223869B)**

**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 of dissertation: The efficacy of cybercrime detection and prevention strategies employed by retailers in Zimbabwe. Case study of Bindura CBD.

1. To be completed by student:

I certify that this dissertation meets the preparation guidelines as presented in the Faculty guide and instruction for preparing dissertations.



22/06/2026

(Signature of student) (Date)

2. To be completed by the Supervisor:

This dissertation is suitable for presentation to the faculty. It has been checked for conformity with the faculty guideline.



30/07/2026

(Signature of Supervisor) (Date)

3. To be completed by Chairman of the department.

I certify to the best of my knowledge that the required procedures have been fulfilled and the preparation criteria was met in the dissertation.



17/08/2026

(Signature of Chairperson) (Date)

## RELEASE FORM

STUDENT NUMBER :B223869B

TITLE OF PROJECT :The efficacy of cybercrime detection and prevention strategies employed  
by retailers in Zimbabwe.Case study of Bindura CBD.

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

Permission is hereby granted to Bindura University of Science Education library to produce  
copies of this dissertation for scholarly and research only. The rights and neither the project nor  
extensive extracts from it may be printed or otherwise reproduced without the author's approval.

SIGNED .....

(Author's signature )

PERMANENT ADDRESS: Chirorwe Primary School

Post Office Box 220

Nyika

TELEPHONE: +263772908877

EMAIL: [chapfuwatirivashe@gmail.com](mailto:chapfuwatirivashe@gmail.com)

DATE: ...22...../.....06...../.....2022.....

## **DEDICATION**

I dedicate this project to my siblings and parents, Mr and Mrs Chapfuwa for their unwavering support and sacrifice throughout my academic journey.

## **ABSTRACT**

The rapid adoption of digital payment systems in Zimbabwe's retail sector has outpaced the development of adequate cybercrime defences, leaving small retailers in secondary urban centres increasingly exposed to financial losses and operational disruptions. This study evaluated the efficacy of cybercrime detection and prevention strategies employed by retailers in Bindura Central Business District. Specifically, the study sought to identify the cybercrime detection and prevention strategies currently in use, to evaluate their efficacy in mitigating financial losses and protecting daily operations, to identify the challenges hindering their implementation, and to recommend strategies to strengthen cybersecurity within the retail sector. A mixed-methods research design was adopted, combining structured questionnaires administered to 25 respondents across five retail categories with semi-structured interviews conducted with 7 purposively selected key informants. The study was underpinned by Routine Activity Theory, Rational Choice Theory, and the Theory of Technology-Enabled Crime. Findings revealed that Point of Sale system protection and employee cybersecurity awareness training were the most widely adopted strategies, while password management and mobile money transaction verification remained the least consistently applied due to shared credentials and queue pressure during peak trading. Employee training and POS protection were rated most effective in reducing fraud incidents, whereas password management and mobile money verification were rated ineffective by the majority of respondents. The key challenges identified were the high cost of security technology, unreliable internet connectivity and load shedding, a shortage of skilled ICT personnel, and the absence of formal written security policies. The study concludes that the dominant failure mode in Bindura retailers is not the absence of cybersecurity tools but the collapse of consistent human guardianship under operational pressure a pattern corroborated by all three theoretical frameworks. It is recommended that the Government of Zimbabwe introduce subsidised cybersecurity support for small retailers under the Cyber and Data Protection Act, that Bindura University of Science Education and the Bindura Business Chamber collaborate to deliver structured annual cybersecurity capacity-building programmes, and that retailers formalise written cybersecurity policies and embed transaction verification as a non-negotiable point-of-sale step.

**Keywords:** *Cybercrime, cybersecurity, retailers, detection strategies, prevention strategies, Bindura CBD, Zimbabwe, mixed methods, Routine Activity Theory, Rational Choice Theory*

## **ACKNOWLEDGEMENT**

This journey would not have been possible without the guidance and patience of my supervisor, Mr Mirirai, whose direction kept this project on course from its earliest stages. Your willingness to challenge my thinking and push me toward greater clarity made this a far better piece of work than it would otherwise have been. I am deeply grateful.

To my family, your support has been the quiet foundation behind everything I have accomplished. The sacrifices you made and the encouragement you offered during the most demanding periods of this programme did not go unnoticed. This achievement belongs to you as much as it does to me.

To my friends and colleagues, thank you for the conversations, the shared frustrations, and the moments of laughter that made this process bearable. Your brotherhood and sisterhood turned many difficult days into manageable ones, and I carry your support with genuine gratitude.

## Table of Contents

|                                     |     |
|-------------------------------------|-----|
| Approval form.....                  | i   |
| RELEASE FORM.....                   | ii  |
| DEDICATION.....                     | iii |
| ABSTRACT.....                       | iv  |
| ACKNOWLEDGEMENT.....                | vi  |
| Table of Contents.....              | 1   |
| List of Tables.....                 | 8   |
| List of Figures.....                | 9   |
| LIST OF ABBREVIATIONS.....          | 10  |
| CHAPTER ONE.....                    | 11  |
| INTRODUCTION.....                   | 11  |
| 1.0 Introduction.....               | 11  |
| 1.1 Background of the Study.....    | 11  |
| 1.2 Statement of the Problem.....   | 13  |
| 1.3 Research Aim.....               | 13  |
| 1.4 Research Objectives.....        | 13  |
| 1.5 Research Questions.....         | 14  |
| 1.6 Significance of the Study.....  | 14  |
| 1.6.1 To the Student.....           | 14  |
| 1.6.2 To the Retailers.....         | 14  |
| 1.6.3 To the Customers.....         | 15  |
| 1.6.4 To the University.....        | 15  |
| 1.7 Assumptions of the Study.....   | 15  |
| 1.8 Delimitations of the Study..... | 15  |

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| 1.8.1 Geographic Scope.....                                               | 15 |
| 1.8.2 Time Period.....                                                    | 16 |
| 1.8.3 Sector Focus.....                                                   | 16 |
| 1.8.4 Strategy Focus.....                                                 | 16 |
| 1.8.5 Theoretical Delimitations.....                                      | 16 |
| 1.8.6 Research Design.....                                                | 16 |
| 1.9 Limitations of the Study.....                                         | 16 |
| 1.10 Organisation of the Study.....                                       | 17 |
| Table 1.1 Organisation of study.....                                      | 17 |
| 1.11 Chapter Summary.....                                                 | 17 |
| CHAPTER TWO.....                                                          | 18 |
| LITERATURE REVIEW.....                                                    | 18 |
| 2.0 Introduction.....                                                     | 18 |
| 2.1 Conceptual Framework.....                                             | 18 |
| 2.2 The Concept of Cybercrime.....                                        | 18 |
| 2.3 Forms of Cybercrime.....                                              | 18 |
| 2.3.1 Phishing.....                                                       | 18 |
| 2.3.2 Card Fraud.....                                                     | 19 |
| 2.3.3 Identity Theft.....                                                 | 19 |
| 2.3.4 Hacking.....                                                        | 19 |
| 2.3.5 Ransomware.....                                                     | 20 |
| 2.4 Cybercrime Prevention and Detection Strategies Used by Retailers..... | 20 |
| 2.4.1 Firewalls and Antivirus Software.....                               | 20 |
| 2.4.2 Strong Password Policies and Multi-Factor Authentication (MFA)..... | 20 |
| 2.4.3 Regular Software Updates and Patch Management.....                  | 21 |

|                                                                                                      |    |
|------------------------------------------------------------------------------------------------------|----|
| 2.4.4 Employee Cybersecurity Training.....                                                           | 21 |
| 2.4.5 Backup and Disaster Recovery Systems.....                                                      | 21 |
| 2.4.6 Point of Sale (POS) System Protection.....                                                     | 21 |
| 2.4.7 Mobile Money Transaction Verification.....                                                     | 22 |
| 2.5 Challenges Faced in Implementing Detection and Prevention Strategies.....                        | 22 |
| 2.5.1 Skills Shortage.....                                                                           | 22 |
| 2.5.2 High Implementation Costs.....                                                                 | 22 |
| 2.5.3 Rapid Evolution of Cybercrime Threats.....                                                     | 23 |
| 2.5.4 Lack of Clear Roles and Responsibilities.....                                                  | 23 |
| 2.5.5 Lack of Management Support.....                                                                | 23 |
| 2.5.6 Integration Barriers with existing Retail Systems.....                                         | 23 |
| 2.5.7 Lack of Employee Awareness and Training.....                                                   | 24 |
| 2.5.8 Unreliable Internet Connectivity and Infrastructure Constraints.....                           | 24 |
| 2.6 Theoretical Framework.....                                                                       | 24 |
| 2.6.1 The Theory of Technology-Enabled Crime.....                                                    | 25 |
| 2.6.2 Routine Activity Theory.....                                                                   | 25 |
| 2.6.3 Rational Choice Theory.....                                                                    | 25 |
| 2.7 Empirical Evidence.....                                                                          | 26 |
| 2.7.1 To Identify Cybercrime Detection and Prevention Strategies Adopted by Retailers.....           | 26 |
| 2.7.2 To Evaluate the Efficacy of Cybercrime Detection and Prevention Strategies.....                | 27 |
| 2.7.3 To Identify the Challenges in Implementing Cybercrime Detection and Prevention Strategies..... | 28 |
| 2.7.4 To Recommend Strategies to Strengthen Cybercrime Detection and Prevention.....                 | 29 |
| 2.8 Summary of Literature and Justification for the Study.....                                       | 31 |
| 2.9 Chapter Summary.....                                                                             | 32 |

|                                            |    |
|--------------------------------------------|----|
| CHAPTER THREE.....                         | 33 |
| RESEARCH METHODOLOGY.....                  | 33 |
| 3.0 Introduction.....                      | 33 |
| 3.1 Research Philosophy.....               | 33 |
| 3.2 Research Approach.....                 | 33 |
| 3.3 Research Design.....                   | 34 |
| 3.4 Sampling Strategy.....                 | 34 |
| 3.5 Target Population.....                 | 34 |
| 3.6 Sample Size.....                       | 35 |
| Table 2.0 Sample Size.....                 | 35 |
| 3.7 Sampling Techniques.....               | 35 |
| 3.7.1 Stratified Random Sampling.....      | 35 |
| 3.7.2 Purposive Sampling.....              | 36 |
| 3.8 Research Instruments.....              | 36 |
| 3.9 Questionnaire.....                     | 36 |
| 3.9.1 Advantages of Questionnaires.....    | 36 |
| 3.9.2 Disadvantages of Questionnaires..... | 37 |
| 3.10 Interview Guide.....                  | 37 |
| 3.10.1 Advantages of Interviews.....       | 37 |
| 3.10.2 Disadvantages of Interviews.....    | 37 |
| 3.11 Data Collection Procedures.....       | 38 |
| 3.12 Validity.....                         | 38 |
| 3.13 Reliability.....                      | 38 |
| 3.14 Data Presentation and Analysis.....   | 39 |
| 3.15 Ethical Considerations.....           | 39 |

|                                                                                                   |    |
|---------------------------------------------------------------------------------------------------|----|
| 3.16 Chapter Summary.....                                                                         | 39 |
| CHAPTER FOUR.....                                                                                 | 40 |
| DATA PRESENTATION, ANALYSIS AND DISCUSSION.....                                                   | 40 |
| 4.0 Introduction.....                                                                             | 40 |
| 4.1 Response rate.....                                                                            | 40 |
| Table 3 .1: Questionnaire Response Rate.....                                                      | 40 |
| 4.1.2 Interview response rate.....                                                                | 41 |
| Table 3.2: Interview response rate.....                                                           | 41 |
| 4.2 Demographic characteristics of respondents.....                                               | 41 |
| Table 3.3: Demographic characteristics of respondents (N=25).....                                 | 41 |
| 4.3 Objective One: Cybercrime detection and prevention strategy currently used by retailers.....  | 45 |
| Table 3.4: Cybercrime Detection and Prevention Strategies Currently Used by Retailers (N=25)..... | 45 |
| 4.3.2 Point of Sale (POS) system protection.....                                                  | 45 |
| 4.3.3 Antivirus and anti-malware software.....                                                    | 46 |
| 4.3.4 Password management and access control.....                                                 | 46 |
| 4.3.5 Employee cybersecurity awareness training.....                                              | 46 |
| 4.3.6 Mobile money transaction verification.....                                                  | 47 |
| 4.4 Objective two: Effectiveness of cybercrime detection and prevention strategies.....           | 48 |
| Fig 4.1 The effectiveness of cybercrime detection and prevention strategies.....                  | 48 |
| 4.4.2 Effectiveness of point of sale system protection.....                                       | 48 |
| 4.4.3 Effectiveness of antivirus and anti-malware software.....                                   | 49 |
| 4.4.4 Effectiveness of password management and access control.....                                | 49 |
| 4.4.5 Effectiveness of employee cybersecurity awareness training.....                             | 49 |
| 4.4.6 Effectiveness of mobile money transaction verification.....                                 | 50 |
| Objective 3 : Challenges faced in implementing cybercrime detection and prevention                |    |

|                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------|----|
| strategies.....                                                                                     | 51 |
| Table 3.5 Challenges faced in implementing cybercrime detection and prevention                      |    |
| strategies(N=25).....                                                                               | 51 |
| 4.5.1 High cost of security technology.....                                                         | 51 |
| 4.5.2 Unreliable internet connectivity.....                                                         | 52 |
| 4.5.3 Lack of skilled Information and Communication Technology (ICT) personnel....                  | 52 |
| 4.5.4 Rapidly Evolving Cyber Threats and Absence of Formal Policies.....                            | 52 |
| 4.6 Objective Four: Recommended strategies to strengthen cybercrime detection and prevention.....   | 53 |
| Fig 4.2 : Recommended strategies to strengthen cybercrime detection and prevention strategies53     |    |
| 4.6.1 Adoption of Affordable Machine Learning and AI-Based Detection Tools.....                     | 53 |
| 4.6.2 Structured and Continuous Employee Cybersecurity Training.....                                | 54 |
| 4.6.3 Government Support and Infrastructure Investment.....                                         | 54 |
| 4.6.4 Regular Software Updates and Automated Patch Management.....                                  | 54 |
| 4.7 Chapter Summary.....                                                                            | 55 |
| CHAPTER FIVE.....                                                                                   | 56 |
| SUMMARY, CONCLUSION AND RECOMMENDATIONS.....                                                        | 56 |
| 5.0 Introduction.....                                                                               | 56 |
| 5.1 Summary of the Study.....                                                                       | 56 |
| 5.2 Summary of Research Findings.....                                                               | 57 |
| 5.2.1 What Cybercrime Detection and Prevention Strategies Are Currently Used?.....                  | 57 |
| 5.2.2 How Effective Are the Strategies in Mitigating Financial Losses?.....                         | 57 |
| 5.2.3 What Challenges Do Retailers Encounter When Implementing Cybercrime Prevention Measures?..... | 58 |
| 5.2.4 What Strategies Can Strengthen Cybercrime Detection and Prevention?.....                      | 58 |
| 5.3 Conclusion.....                                                                                 | 58 |
| 5.4 Recommendations.....                                                                            | 60 |

|                                                                                                                                 |    |
|---------------------------------------------------------------------------------------------------------------------------------|----|
| 5.4.1 Retailers Should Formalise Written Internal Cybersecurity Policies.....                                                   | 60 |
| 5.4.2 Retailers Should Embed Transaction Verification as a Non-Negotiable Point-of-Sale Step.....                               | 60 |
| 5.4.3 The Government of Zimbabwe Should Introduce Subsidised Cybersecurity Support Under the Cyber and Data Protection Act..... | 60 |
| 5.4.4 BUSE and the Bindura Business Chamber Should Collaborate to Deliver Annual Cybersecurity Capacity Building.....           | 60 |
| 5.4.5 Law Enforcement Should Strengthen Cybercrime Reporting Mechanisms for Retailers.....                                      | 61 |
| 5.5 Recommendations for Further Research.....                                                                                   | 61 |
| REFERENCES.....                                                                                                                 | 62 |
| Research Authorization letter.....                                                                                              | 70 |
| Appendix 2.....                                                                                                                 | 71 |
| Questionnaire for Bindura CBD Retailers.....                                                                                    | 71 |

## **List of Tables**

|                                                                                                         |    |
|---------------------------------------------------------------------------------------------------------|----|
| Table 1.1 Organisation of study.....                                                                    | 17 |
| Table 2.0 Sample Size.....                                                                              | 35 |
| Table 3 .1: Questionnaire Response Rate.....                                                            | 40 |
| Table 3.2: Interview response rate.....                                                                 | 41 |
| Table 3.3: Demographic characteristics of respondents (N=25).....                                       | 41 |
| Table 3.4: Cybercrime Detection and Prevention Strategies Currently Used by Retailers<br>(N=25).....    | 45 |
| Table 3.5 Challenges faced in implementing cybercrime detection and prevention<br>strategies(N=25)..... | 51 |

## **List of Figures**

|                                                                                                    |    |
|----------------------------------------------------------------------------------------------------|----|
| Fig 4.1 The effectiveness of cybercrime detection and prevention strategies.....                   | 48 |
| Fig 4.2 : Recommended strategies to strengthen cybercrime detection and prevention strategies..... | 53 |

## **LIST OF ABBREVIATIONS**

|              |                                          |
|--------------|------------------------------------------|
| <b>AI</b>    | Artificial Intelligence                  |
| <b>BUSE</b>  | Bindura University of Science Education  |
| <b>CBD</b>   | Central Business District                |
| <b>CDPA</b>  | Cyber and Data Protection Act            |
| <b>ICT</b>   | Information and Communication Technology |
| <b>MFA</b>   | Multi-Factor Authentication              |
| <b>POS</b>   | Point of Sale                            |
| <b>RAT</b>   | Routine Activity Theory                  |
| <b>RCT</b>   | Rational Choice Theory                   |
| <b>SADC</b>  | Southern African Development Community   |
| <b>TTEC</b>  | Theory of Technology-Enabled Crime       |
| <b>USD</b>   | United States Dollar                     |
| <b>VPN</b>   | Virtual Private Network                  |
| <b>ZIMRA</b> | Zimbabwe Revenue Authority               |

## **CHAPTER ONE**

### **INTRODUCTION**

#### **1.0 Introduction**

This chapter introduces the study on the efficacy of cybercrime detection and prevention strategies employed by retailers in Bindura Central Business District. It situates the study within its broader digital and economic context, establishing why cybercrime poses a growing threat to retailers operating in a resource-constrained environment. The chapter covers the background of the study, problem statement, research objectives, research questions, significance of the study, assumptions, delimitations and limitations.

#### **1.1 Background of the Study**

The past two decades have seen technology reshape how retail businesses operate, with computers, mobile phones and internet connectivity fundamentally altering how transactions are processed and how businesses communicate (Holt & Bossler, 2016). Yet this digital growth has carried a serious cost the retail sector has become one of the primary targets of cybercrime globally. INTERPOL's Operation HAECHI IV recorded nearly 3,500 arrests and USD 300 million in seized assets across 34 countries within just six months (INTERPOL, 2023). Chaudhary (2025) found that traditional security systems in United States retail organisations are increasingly inadequate against evolving threats, while Bressler (2009) confirmed that fewer than half of small businesses employ any meaningful cybersecurity measures. Manchikanti (2025) added that most small retailers lack the financial capacity to deploy adequate detection systems, a gap reflected by the fact that only 54% of UN Member States had procedural powers to secure electronic evidence as of December 2025 (Council of Europe, 2026).

Africa has felt these pressures acutely. Vassilakos and Martin (2023) documented that South Africa, Nigeria, Kenya, Egypt and Zimbabwe consistently rank among the continent's most cyber-attacked nations, with losses estimated at around USD 895 million annually consistent with INTERPOL's recorded continental losses exceeding USD 3 billion between 2019 and 2025 (INTERPOL, 2025). Over two-thirds of African countries surveyed reported cybercrime accounting for a medium to high share of all offences, exceeding 30% of reported crimes in both

Western and Eastern Africa (INTERPOL, 2025). Okeke (2015) found that up to 70% of identity theft in African retail organisations is carried out by internal staff, a threat that remains severely underestimated.

At the regional level, Zimbabwe and fellow SADC member states score poorly on the National Cyber Security Index, reflecting weak and fragmented cybersecurity policy across the region (Vassilakos & Martin, 2023). Zimbabwe ranks 134th globally with an NCSI score of just 18.33 out of 100, recording zero across cyber incident response, crisis management and threat awareness (eGA NCSI, 2026). Though 96% of African states have initiated cybercrime legislation reform, implementation remains uneven, with many laws adopted without the regulatory capacity to enforce them (Council of Europe, 2026).

Within Zimbabwe's urban business districts, this vulnerability has already produced measurable harm. Kudanga et al. (2022) documented widespread fraud in Bulawayo CBD EcoCash scams, card cloning, electronic banking fraud and employee-facilitated theft with complainants losing approximately USD 100 million through mobile money fraud in 2021 alone. Where technology was applied systematically through transaction monitoring and proper documentation, detection rates improved substantially (Kudanga et al., 2022).

Bindura CBD mirrors these vulnerabilities closely. The town serves mining operations, border trade and a large agricultural population, processing high daily volumes of EcoCash, ZIPIT and point-of-sale transactions through retailers that mostly operate without dedicated ICT staff or formal security policies. The threat is real and documented in February 2021, three fraudsters were arrested after defrauding Bindura victims of between USD 4,100 and USD 12,000 each through fake WhatsApp RTGS payment confirmations (Pindula News, 2021). The ZRP Cybercrime Unit under the Commercial Crimes Division remains the only institutional line of defence retailers can rely on, within a national environment scoring zero in cyber incident response and threat awareness (eGA NCSI, 2026; ZRP, 2024). Digital payment adoption has accelerated sharply since 2019, driven by cash shortages, pulling retailers deeper into financial systems they are ill-equipped to protect (Chingoriwo, 2022). It is against this background that this study evaluates the efficacy of the cybercrime detection and prevention strategies employed by retailers in Bindura CBD

## **1.2 Statement of the Problem**

Despite the rapid adoption of digital payment systems in Bindura CBD, effective cybercrime detection and prevention strategies among retailers remain largely absent, leaving businesses exposed to financial losses and operational disruptions they are ill-equipped to address. Retailers in the town process high daily volumes of EcoCash, ZIPIT and point-of-sale transactions through outlets that largely operate without dedicated ICT staff, formal security policies or reliable internet infrastructure. In February 2021, three fraudsters defrauded Bindura victims of between USD 4,100 and USD 12,000 each through fake WhatsApp RTGS payment confirmations, confirming that cyber-enabled fraud is an active threat in this town (Pindula News, 2021). Zimbabwe's zero score in cyber incident response and threat awareness (eGA NCSI, 2026) compounds this further, with the ZRP Cybercrime Unit remaining the only institutional defence available to retailers (ZRP, 2024), operating within a regulatory environment that Chingoriwo (2022) describes as ill-equipped to protect businesses embedded in rapidly digitalising financial systems.

## **1.3 Research Aim**

This study aims to evaluate the efficacy of the cybercrime detection and prevention strategies currently employed within the retail sector of Bindura CBD, assess whether those measures are adequate against the digital threats retailers face, identify the challenges hindering their implementation, and recommend practical strategies to strengthen cybersecurity within this context.

## **1.4 Research Objectives**

**1.4.1** To identify the cybercrime prevention strategies currently utilised by retailers in Bindura CBD.

**1.4.2** To evaluate the efficacy of the detection and prevention strategies in mitigating financial losses and protecting the operational integrity of retail businesses in Bindura CBD.

**1.4.3** To identify the challenges encountered by retailers in Bindura CBD when implementing cybercrime detection and prevention measures.

**1.4.4** To recommend strategies to strengthen the cybersecurity of the retail sector in Bindura against evolving cyber threats.

## **1.5 Research Questions**

**1.5.1** What cybercrime detection and prevention strategies are currently being used by retail shops in Bindura CBD?

**1.5.2** How effective are these detection and prevention strategies in reducing financial losses and protecting the daily operations of retail businesses in Bindura CBD?

**1.5.3** What challenges do retailers in Bindura CBD face when trying to put cybersecurity measures in place?

**1.5.4** What practical strategies can be recommended to strengthen Bindura CBD retailers against new and changing digital threats?

## **1.6 Significance of the Study**

The rapid adoption of digital payment systems in Bindura has outpaced the development of any meaningful cybersecurity guidance for small retail businesses. In the absence of a national framework addressing this gap, shop owners, employees, and customers all bear the consequences of inadequate protection.

### **1.6.1 To the Student**

This study fulfils a core academic requirement of the Financial Intelligence degree programme and provides the researcher with direct experience in conducting field-based investigation. The process of designing instruments, collecting data, and analysing findings builds competencies in critical thinking, data interpretation and professional report writing central to the Financial Intelligence programme.

### **1.6.2 To the Retailers**

This study maps the strategies currently in use, assesses whether those strategies are actually working, and identifies where protection is weakest, giving retailers an evidence-based

foundation on which to make more informed decisions about where to direct limited security resources.

### **1.6.3 To the Customers**

Customers in Bindura increasingly rely on EcoCash, point-of-sale machines and bank cards for everyday purchases, meaning their personal and financial data passes through retail systems that may be poorly secured. This study contributes to improvement in how retailers handle and protect customer data by providing the evidence needed to prompt meaningful change.

### **1.6.4 To the University**

This study contributes original, locally grounded data to an under-researched area, enriching teaching in Financial Intelligence and related programmes. Future students can draw on this work as a foundation for further investigation, and the university strengthens its contribution to addressing practical business challenges in the communities it serves.

## **1.7 Assumptions of the Study**

**1.7.1** The cyber threat environment and retail operating conditions remained stable throughout the data collection period, allowing for consistent and comparable responses.

**1.7.2** The cybersecurity strategies reported by respondents had been consistently implemented for a sufficient period to permit a fair assessment of their effectiveness.

**1.7.3** Participants provided honest and accurate information during data collection, particularly given the confidentiality assurances offered by the researcher.

**1.7.4** Retailers and staff in Bindura possess at least a basic awareness of the cybersecurity threats relevant to their daily operations.

## **1.8 Delimitations of the Study**

### **1.8.1 Geographic Scope**

The study was restricted to retail businesses operating within Bindura Central Business District to allow a focused and in-depth examination of cybercrime challenges within a single resource-constrained urban environment.

### **1.8.2 Time Period**

The study concentrated on the period between 2021 and 2025, capturing the most significant phase of post-pandemic digital payment expansion in Zimbabwe, during which mobile money and point-of-sale usage surged and new cyber risks emerged alongside that growth.

### **1.8.3 Sector Focus**

The study targeted the retail sector specifically, as retailers are more directly and frequently exposed to financial data theft and payment fraud than many other sectors.

### **1.8.4 Strategy Focus**

Rather than examining prosecution or legislation, the study focused exclusively on detection and prevention strategies at the business level, directly addressing the most actionable dimension of the cybercrime problem facing Bindura retailers.

### **1.8.5 Theoretical Delimitations**

The study was guided by the Theory of Technology-Enabled Crime, Routine Activity Theory, and Rational Choice Theory. These three frameworks were selected because together they account for how environmental changes, the absence of capable guardians, and offender decision-making interact in digital crime against retailers.

### **1.8.6 Research Design**

A mixed-methods design using questionnaires and semi-structured interviews was adopted to allow detailed, locally grounded data collection within the time and financial constraints of the project, while enabling triangulation of quantitative and qualitative findings.

## **1.9 Limitations of the Study**

The most significant constraint was limited accessibility of respondents, as restricted operational hours and the demands of running an active retail business made scheduling interviews difficult. This was managed through flexibility in appointment times and persistent follow-up. Financial and time constraints limited the scale of data collection, which the researcher addressed through careful planning and disciplined resource management. Several respondents were initially reluctant to share details about security practices out of concern that competitors or fraudsters could exploit the information. This was addressed by assuring all participants of anonymity,

assigning pseudonyms and codes in place of real identities, and making clear that the research was voluntary and conducted exclusively for academic purposes.

### 1.10 Organisation of the Study

*Table 1.1 Organisation of study*

| Chapter | Title                                          | Summary of Content                                                                      |
|---------|------------------------------------------------|-----------------------------------------------------------------------------------------|
| I       | Introduction                                   | Background, research problem, objectives, questions and significance.                   |
| II      | Literature Review                              | Crime theories and empirical studies to highlight existing research gaps.               |
| III     | Research Methodology                           | Research design, target population, sampling, instruments and ethical considerations.   |
| IV      | Data Presentation, Analysis and Interpretation | Field data presented using tables and figures, interpreted against research objectives. |
| V       | Conclusion and Recommendations                 | Key findings, conclusions on strategy efficacy, and practical recommendations.          |

### 1.11 Chapter Summary

This chapter established the foundation of the study by presenting the background to the cybercrime problem facing retailers in Bindura CBD, the statement of the problem, and the research objectives and questions that guide the investigation. The significance of the study was discussed in relation to multiple stakeholders, and the assumptions, delimitations and limitations shaping the research were outlined.

## **CHAPTER TWO**

### **LITERATURE REVIEW**

#### **2.0 Introduction**

This chapter examines existing literature on cybercrime detection and prevention strategies within the retail sector, building the theoretical and empirical foundation for the study. The conceptual framework, theoretical underpinnings and empirical evidence relevant to the cybercrime threats facing retailers in Bindura CBD are presented and discussed in turn.

#### **2.1 Conceptual Framework**

A conceptual framework provides a structured guide for understanding the relationships between variables and explains how different factors interact to produce an observed outcome. It directs data collection, analysis, and interpretation toward the key questions the study seeks to answer. In this study, the framework connects cybercrime threats, the detection and prevention strategies employed by retailers, and the environmental conditions affecting their implementation.

#### **2.2 The Concept of Cybercrime**

Cybercrime is broadly defined as a combination of technologies and processes used to exploit information systems and networks through unauthorised access (Kabanda & Chingoriwo, 2022). Alternatively, it refers to any criminal activity where a computer system is either the primary target or a critical tool used to facilitate the offence, encompassing both computer-assisted crimes and computer-focused crimes (Chingoriwo, 2022). Common to all definitions is the deliberate misuse of computer network systems to cause harm or theft.

#### **2.3 Forms of Cybercrime**

##### **2.3.1 Phishing**

Phishing occurs when attackers use deceptive emails, fake websites and manipulated digital platforms to trick individuals into surrendering sensitive information such as login credentials and banking details (Sari, 2025). It works entirely through deception the victim believes they are

dealing with a legitimate institution and willingly hands over information that is then used against them. Attackers craft URLs and web pages to closely mimic legitimate sites through misspelled domain names, inserted punctuation and character substitution, and incidents have risen significantly in environments where digital literacy is weak and legal frameworks do not recognise phishing as a standalone offence (Zieni, Massari and Calzarossa, 2023).

### **2.3.2 Card Fraud**

Identity theft occurs when criminals use stolen personal information to impersonate someone, typically for financial gain (Oloyede et al., 2023). Once enough identifying details are obtained, offenders can open bank accounts, access existing funds and apply for credit entirely in another person's name. This information is commonly sourced through data breaches and phishing campaigns, with stolen names, addresses and card numbers frequently traded on dark web marketplaces using cryptocurrency to preserve anonymity (Jabeen et al., 2024).

### **2.3.3 Identity Theft**

Identity theft occurs when criminals use stolen personal information to impersonate a legitimate individual, typically for financial gain (Oloyede et al., 2023). Unlike crimes that target devices or systems, identity theft targets the person once a criminal has enough identifying information, they can open bank accounts, access existing funds, apply for credit, and conduct transactions entirely in someone else's name without ever being physically present. The information needed to do this is commonly obtained through data breaches or phishing campaigns and is associated with a wide range of related offences including credit card fraud and internet scams (Oloyede et al., 2023). Stolen data typically includes names, home addresses, credit card numbers, and other identifying details, which are then traded through dark web marketplaces using cryptocurrency to maintain anonymity (Jabeen et al., 2025).

### **2.3.4 Hacking**

Hacking is the unauthorised intrusion into computer systems or networks, typically achieved by exploiting unpatched software, misconfigured systems or weak passwords (Marelino, 2022). Once inside, an attacker can steal data, alter records, install malicious software or use the compromised system to target other connected systems often without the organisation ever noticing. In retail environments where point-of-sale systems are frequently left unpatched due to

cost constraints, attackers can move through the network layer by layer until the entire infrastructure is compromised (Eyeleko and Feng, 2023).

### **2.3.5 Ransomware**

Ransomware is malicious software that encrypts a victim's files and locks them out of their own systems until a ransom typically demanded in cryptocurrency is paid in exchange for a decryption key (Badgular, 2020). It most commonly enters a network through phishing emails or infected downloads, meaning a single employee clicking the wrong link can halt an entire business within minutes. Once activated, the victim must choose between paying with no guarantee of recovery, restoring from backup, or accepting the loss. Retailers are particularly vulnerable, as ransomware can be used to extort money, disrupt operations during critical trading periods or cause lasting damage (Benmalek et al., 2024).

## **2.4 Cybercrime Prevention and Detection Strategies Used by Retailers**

### **2.4.1 Firewalls and Antivirus Software**

A firewall monitors traffic between a retailer's internal network and the wider internet, blocking unauthorised connections before they reach sensitive systems, while antivirus software scans files and active processes for known malware, isolating threats before they cause disruption (Phillips et al., 2023). Together, these tools offer small retailers a practical and affordable layer of protection against common attacks (Saadi, 2024). However, firewalls alone are insufficient and must be integrated with intrusion detection systems and data encryption to form a comprehensive defence (Putra, Dafid and Syafi'i, 2025).

### **2.4.2 Strong Password Policies and Multi-Factor Authentication (MFA)**

Password-based login alone is increasingly insufficient as cybercriminals obtain credentials through phishing, data breaches or brute-force tools (Saadi, 2024). Strong password policies require employees to use complex, regularly rotated passwords, while MFA adds a second verification layer that protects accounts even after a password has been compromised (Amosu et al., 2024). Despite its proven effectiveness, many smaller retailers across developing markets have yet to adopt MFA, often citing cost and technical capacity as barriers.

### **2.4.3 Regular Software Updates and Patch Management**

Cybercriminals routinely scan networks for systems running outdated software, targeting known vulnerabilities for which exploit code is already publicly available (Beretas, 2024). Regular patching closes these weaknesses systematically, while intrusion detection systems working alongside updated software can flag exploitation attempts in real time (Phillips et al., 2023). For retailers with minimal technical staff, enabling automatic updates on all networked devices represents a low-cost, high-impact measure (Beretas, 2024).

### **2.4.4 Employee Cybersecurity Training**

Human error remains one of the leading causes of cybersecurity breaches in the retail sector, making staff training one of the most direct and accessible defences available (Fagbule, 2022). Rather than conducting isolated once-off compliance sessions, retailers need to build a security-aware culture where awareness becomes part of how staff approach daily operations (Fagbule, 2022). Training programmes that incorporate interactive formats, simulated threat scenarios and sustained leadership endorsement produce measurably stronger engagement and retention of security knowledge among employees than passive compliance-driven approaches (Shan-A-Alahi et al., 2024).

### **2.4.5 Backup and Disaster Recovery Systems**

Regular data backups, stored both on-site and in secure off-site or cloud-based locations, allow a retailer to restore critical information following a ransomware attack or data corruption event without paying criminal demands or suffering extended downtime (Ray, Chowdhury & Hasan, 2024). Mohd Saleh et al. (2026) found that retailers who maintained offline backup copies and documented incident response procedures resumed operations significantly faster and sustained substantially lower financial losses following ransomware incidents.

### **2.4.6 Point of Sale (POS) System Protection**

Point of sale terminals process card details and mobile money transactions at high volume, making them a primary target for payment fraud, and protecting them requires hardware-based encryption and tokenisation so that raw payment data is never stored on the retailer's network (Badgujar, 2020). Vaka (2025) found that hardware-based POS malware protection substantially

outperformed software-only alternatives in real retail deployments, confirming that technical controls at the point of transaction represent one of the most effective defences available to small retailers.

#### **2.4.7 Mobile Money Transaction Verification**

Mobile money fraud in Zimbabwean retail most commonly involves fake payment confirmation screenshots, where customers present edited images to deceive till operators into releasing goods before a genuine transaction has occurred (Kudanga et al., 2022). Das et al. (2025) confirm that independently verifying payment notifications on a separate registered device significantly reduces successful fraud attempts, though the protective value of this measure depends entirely on consistent application by frontline staff.

### **2.5 Challenges Faced in Implementing Detection and Prevention Strategies**

#### **2.5.1 Skills Shortage**

Retail organisations frequently struggle to recruit staff with sufficient technical knowledge to deploy and maintain modern detection systems (Razzaq and Shah, 2024). In Bindura, where dedicated ICT staff are rare and security responsibilities fall to general employees, tools may be purchased but incorrectly configured. Even where some technical awareness exists, the absence of formal training means staff cannot distinguish a genuine security alert from normal system activity, leaving threats undetected until damage has already occurred (Navandar, 2023).

#### **2.5.2 High Implementation Costs**

Implementing machine learning-based detection and prevention systems requires substantial upfront expenditure across software licensing, compatible hardware and staff training, placing these solutions beyond what most small retailers can absorb (Razzaq & Shah, 2024). The challenge is compounded by the fact that even basic cybersecurity tools carry recurring costs through subscription renewals, software updates and maintenance requirements that accumulate over time (Fianyi, 2015).

### **2.5.3 Rapid Evolution of Cybercrime Threats**

Razzaq and Shah (2024) observed that attackers systematically target weaknesses across people, processes and technologies, exploiting the anonymity and speed of digital channels to conduct attacks that are difficult to trace and harder to prevent in real time. When a new fraud technique emerges, retailers relying on static, infrequently updated tools find themselves exposed before their defences can be adjusted. The challenge is that criminal methods do not stand still as retailers become familiar with one type of attack, perpetrators adapt their approaches, and the tools available to them grow more accessible and sophisticated over time (Ganguli, 2022).

### **2.5.4 Lack of Clear Roles and Responsibilities**

Razzaq and Shah (2024) identified the absence of clearly defined security roles as a significant challenge, noting that without role clarity, organisations default to a shared but unowned approach where everyone assumes someone else is handling a given security function. Schwartz (2008) further argued that fragmented security accountability consistently undermines the overall effectiveness of detection and prevention strategies.

### **2.5.5 Lack of Management Support**

Chaudhary (2025) found that retail managers frequently underestimate the severity of evolving fraud threats, treating cybersecurity as a background concern rather than an active management responsibility. A particularly damaging assumption is the belief that existing tools are sufficient and require no further review, when in practice cybersecurity effectiveness depends on consistent monitoring, regular auditing, and willingness to update systems as threats change.

### **2.5.6 Integration Barriers with existing Retail Systems**

Even when a retailer acquires a new security solution, integrating it with existing legacy systems often requires specialist configuration that most small businesses cannot access (Razzaq and Shah, 2024). Small and medium enterprises in developing economies frequently find that newer technologies cannot be meaningfully deployed without the supporting infrastructure and technical capacity their environments lack, leaving them caught between outdated systems they cannot secure and modern tools they cannot fully use (Akpan et al., 2021).

### **2.5.7 Lack of Employee Awareness and Training**

Human users frequently represent the weakest link in cybersecurity, as criminals exploit predictable habits and social engineering rather than targeting technical systems directly (Azzani, Purwantoro and Almubarak, 2024). The challenge is not simply initial training but sustained behavioural change employees who receive a single security briefing tend to revert to familiar habits over time, particularly in busy retail environments where serving customers quickly takes priority over security vigilance (Shan-A-Alahi et al., 2024).

### **2.5.8 Unreliable Internet Connectivity and Infrastructure Constraints**

Unreliable internet connectivity and recurring electricity outages represent a structural constraint that is largely absent from mainstream cybersecurity literature but is central to the operating reality of retailers in developing economies (Vaka, 2025). Cloud-based security tools, real-time fraud detection systems, automated antivirus updates and off-site backup processes all depend on consistent connectivity to function as designed. When the internet fails or load shedding interrupts power, these protections are suspended simultaneously and at unpredictable intervals, leaving retailers exposed at precisely the moments when automated defences are most needed (Ardhaninggar and Ramil, 2024). Wagle (2024) documented that infrastructure disruptions in similar developing-economy retail contexts force businesses to either invest in costly redundancy infrastructure such as uninterrupted power supply units and mobile data backup connections, or accept prolonged periods of operating without active cybersecurity protection. In the Zimbabwean context, where power outages and internet failures are routine, these disruptions do not represent occasional edge cases but a persistent operating condition that fundamentally undermines the reliability of any strategy dependent on network connectivity (Chingoriwo, 2022).

## **2.6 Theoretical Framework**

A theoretical framework provides the conceptual lens through which a researcher interprets findings, shaping what to look for, how data is gathered and how results are explained. This study draws on three theories: the Theory of Technology-Enabled Crime, Routine Activity Theory, and Rational Choice Theory.

### **2.6.1 The Theory of Technology-Enabled Crime**

The Theory of Technology-Enabled Crime examines how advances in computer and telecommunications systems have created new opportunities for criminal activity (McQuade, 2006). As digital tools become more embedded in everyday life, they open pathways for offences that traditional law enforcement struggles to detect, largely because criminals exploit the speed and anonymity of the internet to bypass physical security boundaries (McQuade, 2006). Holt and Bossler (2016) built on this by showing that technology fundamentally changes how offenders identify and reach targets, particularly where protective measures such as firewalls are absent. Jaishankar (2011) adds through Space Transition Theory that internet anonymity lowers the perceived risk of criminal behaviour, causing individuals to commit offences online they would never attempt in person. For this study, the theory frames how detection and prevention strategies among Bindura CBD retailers are evaluated, recognising that as criminal methods evolve, defensive responses must equally adapt (McQuade, 2006).

### **2.6.2 Routine Activity Theory**

Routine Activity Theory, developed by Cohen and Felson (1979), holds that crime occurs when three conditions converge a motivated offender, a suitable target and the absence of a capable guardian. Hindelang et al. (1978) complemented this by showing that everyday operational choices directly determine an organisation's exposure to offenders, meaning a retail business can either reduce or amplify its own vulnerability. In Bindura CBD, the rapid expansion of mobile money and cloud-based payment systems has made retail data payment credentials, customer records an attractive target that can be reached remotely without the physical risk of conventional theft (Cohen and Felson, 1979). Where guardianship is absent and targets remain exposed, cybercrime thrives. The theory is central to this study because it explains the structural conditions enabling retail cybercrime in Bindura and frames prevention strategies as mechanisms for strengthening guardianship and reducing target vulnerability (Clarke and Eck, 2003).

### **2.6.3 Rational Choice Theory**

Rational Choice Theory, formulated by Cornish and Clarke (1986), proposes that offenders weigh perceived gains against the likelihood of detection and severity of consequences before committing a crime. Wright (2010) extended this into virtual spaces, arguing that cyberspace removes the physical risks of traditional crime confrontation, being seen, getting caught

meaning even minor rewards can outweigh a heavily diluted risk of detection. Bachmann (2010) confirmed this empirically, showing that hackers carefully analyse system vulnerabilities and calculate the probability of being traced before acting. In the Bindura CBD retail context, the ability to attack remotely, low identification risk and potential for immediate financial gain create conditions that make cybercrime an attractive proposition where protective measures remain underdeveloped. The theory is therefore central to this study because it frames prevention not as a purely technical exercise but as a deliberate effort to make attacks appear more costly and less rewarding to potential offenders (Cornish and Clarke, 1986).

## **2.7 Empirical Evidence**

### **2.7.1 To Identify Cybercrime Detection and Prevention Strategies Adopted by Retailers**

The literature on cybercrime detection and prevention strategies in the retail sector reveals both convergence and significant gaps across different research contexts. Writing from a Nigerian perspective, Chinedu et al. (2021) established through a systematic comparative analysis of intelligent, traditional, and hybrid detection systems that no single approach is sufficient on its own. Their key finding was that hybrid solutions combining rule-based logic with machine learning achieved substantially higher detection accuracy than either method in isolation, and they concluded that cybercrime demands a multi-dimensional response spanning technology, legislation, and social intervention. This establishes an important starting point: effective cybercrime prevention is a layered problem that cannot be resolved through technical measures alone.

Building on this in a more advanced market context, Vaka (2025) examined real-time fraud detection systems across major retail chains in the United States and Europe and found that retailers who integrated machine learning into transaction verification achieved fraud detection rates that far outperformed manual monitoring. Crucially, Vaka also identified that point-of-sale malware protection built around hardware-based verification was substantially more effective than software-only alternatives. Taken together, the findings of Chinedu et al. and Vaka suggest that while sophisticated technological tools exist and perform well in well-resourced environments, the conditions enabling their success are largely absent in contexts like Bindura, where hardware investment is limited and technical support is scarce.

This concern becomes sharper when the focus shifts to the African retail context specifically. Okeke (2015) found that up to 70% of identity theft crimes in African retail organisations are perpetrated by internal staff rather than external hackers, through methods such as copying customer records, colluding with outside criminals, and manipulating colleagues using social engineering. The implication is significant: even where technical defences are in place, they may be largely irrelevant if the threat originates from within the organisation itself. Okeke concluded that internal identity theft is a severely underestimated threat in African retail settings and recommended that formal employee monitoring systems be introduced alongside standardised industry frameworks for detecting and reporting insider fraud. This finding directly shapes the present study's attention to both technical and human-centred prevention strategies among Bindura retailers, reinforcing the argument that technology and people must be addressed simultaneously.

### **2.7.2 To Evaluate the Efficacy of Cybercrime Detection and Prevention Strategies**

Assessing how well cybercrime prevention strategies actually perform in practice reveals a sharp divide between technologically advanced markets and resource-limited environments. The most quantitatively detailed evidence comes from Chaudhary (2025), whose evaluation of AI-powered fraud detection across multiple retail organisations in the United States found that these systems increased detection accuracy by 82.4%, reduced fraud investigation time by 63.7%, and delivered an average financial loss reduction of 37%, with implementation costs recovered within 6 to 8 months. These figures are compelling, but Chaudhary was equally clear that current investment requirements place such systems firmly beyond the reach of most small and medium-sized retailers, and recommended cloud-based subscription models as a more accessible entry point pending support from government and financial institutions.

Mohd Saleh et al. (2026) approached efficacy from a risk management perspective in Malaysia and produced findings more directly applicable to the Bindura context. Phishing and social engineering remained the dominant entry points for retail cyber incidents, yet relatively accessible interventions such as multi-factor authentication, staff awareness training, and continuous monitoring substantially reduced their success rate. Equally significant for resource-constrained retailers, offline backups and documented incident response plans were found to effectively minimise downtime and financial losses when ransomware attacks did succeed.

Where Chaudhary focused on high-cost AI tools, Mohd Saleh et al. demonstrated that lower-cost, process-driven strategies can achieve meaningful protection when consistently applied.

Ardhaninggar and Ramil (2024) and Manchikanti (2025) add two further dimensions that bear directly on the Bindura context. Ardhaninggar and Ramil, examining the retail sector in Depok, Indonesia, found that tools which are implemented but not actively monitored deliver little meaningful protection regardless of their technical specification, a finding particularly relevant where ICT staffing is absent. Manchikanti's systematic review of Artificial Intelligence enabled loss prevention in the United States confirmed that machine learning and automated monitoring substantially outperform manual surveillance but are practically accessible only through a phased deployment model that most small retailers cannot fund without external assistance. Across these studies a consistent pattern emerges: the efficacy of any strategy depends not merely on whether it is adopted, but on whether the operational conditions exist to implement and sustain it correctly, an insight that is central to understanding why strategy adoption in Bindura does not automatically translate into effective protection.

### **2.7.3 To Identify the Challenges in Implementing Cybercrime Detection and Prevention Strategies**

Even where retailers are aware of cybersecurity risks and willing to address them, implementation is rarely straightforward. Graham (2023) drew on a qualitative review of cybercrime prevention literature across small retail businesses in developing economies and identified financial constraint as the dominant barrier, arguing that the cost of acquiring, maintaining, and updating cybersecurity systems places them out of reach for most small business owners. Graham also noted that affordable local technical support is rarely available, meaning even retailers who can afford basic tools often cannot install or maintain them correctly. The result, Graham warned, is a pattern where partial or misconfigured security measures create a false sense of protection without meaningfully reducing risk, a situation potentially more dangerous than having no system at all. The parallels with Bindura are difficult to ignore, as small retailers there operate within similarly tight financial margins, often relying on whoever in the business is most comfortable with technology rather than a dedicated IT professional, and the risk of superficial compliance masking genuine vulnerability is real.

Mohd Saleh et al. (2026) examined implementation challenges across retail businesses in Malaysia and found that phishing and social engineering remained the dominant attack vectors precisely because they exploited human vulnerabilities that technical systems were not designed to address. Their study found that many retailers had invested in firewalls and antivirus software yet continued to experience breaches because their staff lacked the knowledge to recognise manipulation attempts. Mohd Saleh et al. concluded that technical defences and human awareness cannot be treated as alternatives and that organisations failing to invest in both simultaneously will remain exposed regardless of how sophisticated their software is. This finding sits alongside the internal threat patterns documented by Okeke (2015) in the African context, and together they point to a consistent pattern across very different national settings: the human dimension of cybersecurity is persistently underfunded and underestimated.

Wagle (2024) approached the challenge from a different angle, using longitudinal observation and interviews with small retailer owners in South Asia to examine why cybersecurity practices are difficult to sustain over time even after initial implementation. Wagle found that operational pressures, particularly the demands of running a business with a small staff and tight margins, caused owners and managers to deprioritise security maintenance once the immediate threat that prompted action had passed. Wagle concluded that sustainability of cybersecurity practice is as important as initial adoption and recommended that interventions be designed with the operational realities of small businesses in mind, favouring automated, low-maintenance solutions over those requiring regular manual attention. Small retailers in Bindura face these same pressures in intensified form, contending not only with limited staff but also with unreliable electricity and internet connectivity that can interrupt even automated systems, meaning strategies built around consistent human discipline rather than automated processes may face steeper sustainability challenges in this context than Wagle's findings alone would suggest.

#### **2.7.4 To Recommend Strategies to Strengthen Cybercrime Detection and Prevention**

The fourth objective is concerned with what can realistically be done to improve the cybersecurity posture of retail businesses, particularly in resource-constrained environments. Vassilakos and Martin (2023), writing from a Southern African Development Community perspective and drawing on comparative analysis of cybersecurity readiness across SADC member states using the National Cyber Security Index, argued that the most urgent need across

the region is not for more sophisticated technology but for basic cybersecurity infrastructure including functional antivirus protection, regular software updates, and simple password policies. They found that across the SADC region the gap between digital development and cybersecurity readiness is negative for most member states, meaning that countries are adopting digital systems faster than they are building defences to protect them. Vassilakos and Martin recommended that governments and private sector bodies work together to develop accessible, affordable cybersecurity frameworks tailored to small and medium enterprises in the region, and emphasised that awareness campaigns need to reach street-level businesses and not only large corporations. Zimbabwe is among the SADC member states covered by this analysis, and the structural weaknesses identified at the regional level are visible at the ground level in towns like Bindura, where the pace of digital payment adoption has similarly outrun the development of any formal guidance or support for securing those systems.

Aprilia et al. (2026), drawing on a qualitative historical review of cybercrime across five global sectors including retail and covering incidents primarily in the United States, Europe, and Asia, found that the organisations recovering fastest and most effectively from cyber incidents were those that had invested in basic but consistent practices: regular data backups, clear incident response procedures, and staff training. Aprilia et al. concluded that resilience, meaning the ability to detect, respond to, and recover from an attack, matters as much as prevention itself, and that meaningful resilience can be built through low-cost practices without waiting for access to enterprise-grade tools. The lesson here extends to Bindura retailers, not in the sense that their situation mirrors that of a large multinational organisation, but in the more fundamental sense that preparedness and recovery planning can reduce damage even when prevention has failed, and that these preparations do not require significant financial outlay to be meaningful.

Chinedu et al. (2021), in their Nigerian comparative analysis discussed under the first objective, further recommended that cybercrime prevention frameworks for developing contexts should prioritise scalability and simplicity, building detection and response capacity in stages rather than attempting to implement comprehensive systems all at once. They specifically highlighted the value of hybrid approaches that combine basic rule-based detection with human oversight, arguing that even without machine learning infrastructure, trained staff following structured monitoring procedures can catch a significant proportion of fraudulent activity before it causes

serious harm. Mohd Saleh et al. (2026) echoed this in their Malaysian context, recommending layered security that begins with affordable basics and grows as resources allow. What emerges from these studies collectively is a coherent picture of what strengthening cybercrime prevention looks like for retailers who cannot access the tools that dominate the academic literature: for businesses in Bindura, the path forward is not to replicate the enterprise security models of wealthier markets but to build consistent, affordable, human-aware practices that address the specific vulnerabilities of small retail operations in a digitally transitioning economy.

## **2.8 Summary of Literature and Justification for the Study**

The reviewed literature establishes a solid foundation regarding global cybersecurity tools, theoretical frameworks, and empirical evidence on retail cybercrime. However, several contextual and technical gaps persist that specifically necessitate this investigation into the Bindura retail sector.

Most existing research, including the work of Okeke (2015) and Chaudhary (2025), is conducted within developed economies or large-scale online retail environments where stable infrastructure, trained IT personnel, and regulatory support are assumed. There is a significant absence of empirical data on small-scale retail sectors in developing nations like Zimbabwe, particularly in smaller urban centres outside the capital. Unlike the stable operating environments studied by Chaudhary (2025) in the United States, retailers in Bindura contend with frequent power outages, unreliable internet connectivity, and a complete absence of grassroots technical guidance, conditions that fundamentally alter how any cybersecurity strategy performs in practice and that remain largely unexplored in current literature.

While studies such as Murungu et al. (2026) examine cybersecurity within the Zimbabwean context, their focus remains primarily on the banking sector in Harare. The retail sector in smaller towns like Bindura, which serves as a transit point for mining and border trade activity, introduces specific risks associated with transient customer populations and informal cash-equivalent payment systems that are not addressed in existing urban-focused studies. This geographic and sectoral gap means that findings from Harare-based research cannot be straightforwardly applied to the Bindura context without significant adaptation.

A further gap exists in how the literature treats strategy assessment and performance evaluation as separate concerns. Vaka (2025) and Ardhaninggar and Ramil (2024) focus on either the cost of security frameworks or the technical existence of tools without testing their actual efficacy within real-world, resource-constrained retail settings. Additionally, while theories such as Routine Activity Theory and Rational Choice Theory are widely applied to explain why cybercrime occurs, they are rarely used to evaluate whether specific prevention measures such as multi-factor authentication or mobile money verification actually reduce risk in informal retail environments, limiting the practical usefulness of existing work for practitioners in contexts like Bindura.

This research is therefore justified by its intent to bridge these gaps through a multi-theoretical approach combining Routine Activity Theory, Rational Choice Theory, and the Theory of Technology-Enabled Crime, applied directly to the operational realities of small retailers in Bindura CBD. By addressing the unique environmental challenges, infrastructural constraints, and human capacity limitations of this specific context, the study provides practical and cost-effective recommendations that directly respond to the research questions regarding strategy efficacy and local implementation. The findings will contribute original evidence to a geography and sector that existing literature has largely overlooked.

## **2.9 Chapter Summary**

This chapter reviewed theoretical and empirical literature relevant to the study's four objectives. The concept of cybercrime was defined and its main forms examined, followed by a discussion of the detection and prevention strategies available to retailers and the challenges that limit their implementation. Three theoretical frameworks were presented and linked to the retail cybersecurity context. Empirical evidence was reviewed against each objective, and the gaps in existing research that justify this study were identified and explained.

## **CHAPTER THREE**

### **RESEARCH METHODOLOGY**

#### **3.0 Introduction**

This chapter describes the methodological choices made for this study, the reasoning behind each decision, and their respective limitations. The sections that follow outline the research philosophy, approach, design, population, sampling strategy, data collection instruments, analytical procedures, and ethical considerations applied in investigating the efficacy of cybercrime detection and prevention strategies among retailers in Bindura CBD.

#### **3.1 Research Philosophy**

A research philosophy is the theoretical foundation that guides how a researcher interprets data and examines the methodological aspects of their work (Khatri, 2020). This study is guided by pragmatism, which serves as the philosophical base for a mixed-methods approach. Pragmatism focuses on what works to address the research problem, allowing the researcher to value both objective data and subjective human experiences, and enabling the study to utilise quantitative measures to test strategy efficacy alongside qualitative insights to understand the environmental challenges faced by retailers in Bindura.

#### **3.2 Research Approach**

This study adopts a deductive research approach, beginning with established theories and hypotheses regarding cybercrime prevention to test their validity within the retail environment. According to Patel and Patel (2019), a deductive approach is followed when a researcher starts with a specific set of assumptions that need to be confirmed or rejected through the research process. By employing this approach, the study evaluates how existing cybersecurity frameworks and strategies perform in the practical, resource-constrained setting of Bindura.

### **3.3 Research Design**

This study adopted a mixed-methods design, combining quantitative and qualitative approaches to produce a more complete picture of the cybercrime challenges facing Bindura retailers than either method alone could offer (Kothari, 2019). Quantitative methods were used to measure the types of cybercrime prevention and detection strategies in use and assess their perceived effectiveness in reducing financial losses. Qualitative methods were used to explore the reasoning behind those practices, the challenges retailers encounter in sustaining them, and the practical recommendations that emerge from lived experience (Creswell & Creswell, 2018). Combining the two approaches enables triangulation, where numerical findings are supported and explained by participants' real experiences, producing conclusions that are both statistically grounded and practically meaningful (Kothari, 2019).

### **3.4 Sampling Strategy**

This study utilises stratified sampling to divide the retail population in Bindura into distinct groups based on business type, ensuring that each sub-sector is proportionally represented. Additionally, purposive sampling was employed to specifically select respondents with direct experience in digital payment systems and cybersecurity management, ensuring that the information gathered is relevant and authoritative (Patel & Patel, 2019).

### **3.5 Target Population**

The population comprises all retailers operating within Bindura CBD in May 2026 who actively use digital payment platforms including EcoCash, One Money and point-of-sale card machines, covering shop owners, shop managers, till operators, ICT experts and other staff directly responsible for handling digital transactions or system administration. The figure of 30 participants was established through a physical walk-through of Bindura CBD conducted by the researcher in May 2026, during which seven qualifying outlets were identified across five retail categories. Van de Schoot and Miocevic (2020) acknowledge that in cases where the target population is limited in size, a census is the most appropriate and rigorous approach.

### 3.6 Sample Size

Given the small, clearly defined population of 30 respondents across five categories in Bindura CBD, a census approach was adopted, incorporating all identified participants rather than drawing a subset. This approach was appropriate because the population was sufficiently small and accessible to permit total enumeration, eliminating sampling error and ensuring that the findings reflect the full range of cybercrime experiences within the study setting. Table 2.0 illustrates the distribution of participants.

*Table 2.0 Sample Size*

| Category | Owners | Shop<br>Managers | Till<br>Operators /<br>ICT Experts<br>/ Others | Total |
|----------|--------|------------------|------------------------------------------------|-------|
| Total    | 11     | 8                | 11                                             | 30    |

*Table 3.1: Participants of the Research (Source: Primary data, 2026)*

The table above presents the initial population distribution across three primary position categories. In practice, five position types were identified during data collection, with the Till Operators column encompassing till operators, ICT experts and other staff with direct responsibility for system administration and digital transaction oversight.

### 3.7 Sampling Techniques

#### 3.7.1 Stratified Random Sampling

Stratified random sampling works by grouping the population into separate categories based on key attributes before drawing a random sample from each category (Hossan et al., 2023). Respondents were grouped based on their business category and operational scale, identifying small-scale, medium-scale and large-scale retail enterprises. This ensured that all segments were

represented and that each respondent had an equal opportunity to participate, strengthening the accuracy of the findings.

### **3.7.2 Purposive Sampling**

While the broader study distributed questionnaires to managers and owners across retail outlets, 7 individuals were purposely selected for in-depth interviews due to their direct role in implementing and overseeing digital transaction security (Ahmad & Wilkins, 2024). These key informants ensured that the qualitative data accurately reflects the actual cybercrime threats and prevention practices currently in place within the Bindura retail environment.

## **3.8 Research Instruments**

In this study, questionnaires and interviews were the primary tools used to gather data from shop owners, managers and till operators, while supplementary information was drawn from academic journals and theses (Hossan et al., 2023).

### **3.9 Questionnaire**

The research utilises a structured questionnaire as the primary quantitative tool (Ahmad & Wilkins, 2024). A structured format was chosen over a semi-structured questionnaire because the study's quantitative objective required standardised, comparable responses across all participants a level of consistency that open-ended quantitative items would have undermined. The instrument is structured into four sections: Section A captures demographic and business profile data; Section B identifies current cybercrime detection and prevention strategies; Section C assesses the efficacy of these tools in reducing financial losses and protecting daily operations; and Section D addresses both the environmental and operational challenges facing retailers such as power instability and limited technical skills, and solicits respondent views on strategies to strengthen cybersecurity.(Ahmed, 2024).

#### **3.9.1 Advantages of Questionnaires**

Questionnaires were cost-effective and required minimal effort, as only the researcher and the instruments were involved in the data collection process. Bias was minimised since participants completed questionnaires privately without direct influence from the researcher. Anonymity

promoted honest responses to sensitive issues such as local cybercrime vulnerabilities, and the instruments were simple to disseminate across the CBD, with responses generally received promptly.

### **3.9.2 Disadvantages of Questionnaires**

The fixed structure offered limited flexibility and prevented retailers from providing nuanced responses beyond the given options. This was mitigated by supplementing questionnaires with semi-structured interviews. A risk of low response rates was addressed by delivering questionnaires in person and following up directly throughout the five-day collection window. A pilot test conducted with five participants before main data collection identified unclear wording and allowed revisions to be made.

## **3.10 Interview Guide**

Approval was obtained from retail management to interview representatives, who were purposively selected as a subset of the total 30 respondents from seven outlets in Bindura. Both semi-structured and unstructured formats were used to allow open-ended dialogue, giving participants sufficient time and freedom to share their perspectives (Kothari, 2019). To protect participants, interviews were conducted privately and all information gathered was kept confidential.

### **3.10.1 Advantages of Interviews**

Interviews allowed detailed and contextual information to be obtained that would not be captured through structured questionnaires alone. Direct interaction enabled ambiguous responses regarding technical strategies to be clarified immediately, reducing the risk of misunderstanding. Participants were able to elaborate on sensitive topics such as security lapses in a confidential setting, and the flexible format permitted the sequence and wording of questions to be adjusted based on the respondent's flow of conversation.

### **3.10.2 Disadvantages of Interviews**

The interview process required extensive time for scheduling, conducting and transcribing each session, limiting the qualitative sample to seven participants. The presence of the interviewer may have led some respondents to provide socially acceptable answers, which was mitigated by

emphasising confidentiality and using open-ended questions. Possible inconsistency across interviews was managed by maintaining a consistent interview guide while allowing flexibility within it.

### **3.11 Data Collection Procedures**

Before any data was gathered, the researcher obtained permission from Bindura University of Science Education and from the management of each participating retail outlet. Ethical clearance was obtained and each participant was provided with an informed consent form. Questionnaires were self-administered and delivered in person, with respondents given five days to complete them. Seven participants were then purposively selected for semi-structured interviews conducted at each participant's business premises in a private setting, audio-recorded with explicit consent and subsequently transcribed verbatim.

### **3.12 Validity**

Content validity was ensured by developing the questionnaire through an extensive review of existing literature on cybercrime threats and digital security protocols. Construct validity was maintained by aligning questionnaire items with established theoretical frameworks of cybercrime prevention and detection. Internal validity was addressed through standardised administration of instruments across all participants (Hossan et al., 2023).

### **3.13 Reliability**

To address potential reliability issues, the questionnaire was carefully designed and pre-tested with a pilot group of five individuals separate from the final study sample. The pilot test helped identify unclear items and detect sampling-related challenges (Ahmad & Wilkins, 2024). Administration was standardised across all participants to minimise procedural bias. Interview responses were transcribed verbatim and cross-checked against field notes to maintain accuracy, and the tools were reviewed by peers and supervisors to confirm they captured the necessary information.

### **3.14 Data Presentation and Analysis**

Quantitative data were processed using Microsoft Excel to generate descriptive statistics, including frequency tables, percentages and graphical representations. Qualitative data were analysed using Braun and Clarke's (2006) six-phase thematic analysis framework, chosen because it is flexible and fits well with the practical, real-world focus of this study. Unlike content analysis, thematic analysis is concerned with meaning and experience understanding why retailers adopt or abandon strategies rather than counting how often certain words appear. The analytical process moved from reading and becoming familiar with the data, through coding, developing themes and writing a final report tied to the research objectives. Prior to main data collection, a pilot test with five participants led to two questions being reworded for clarity and one response scale adjusted from three to four points. Together, these approaches supported triangulation, ensuring that statistical trends were confirmed and deepened by qualitative insights.

### **3.15 Ethical Considerations**

Voluntary informed consent was obtained from all participants before data collection began. Confidentiality and anonymity were strictly maintained by replacing real names with pseudonyms and alphanumeric codes such as Manager A or Shop 1 throughout data recording and reporting. The principle of beneficence guided the study throughout, ensuring that participation did not expose any respondent to harm or undue risk. Debriefing was conducted at the conclusion of each interview, giving participants the opportunity to ask questions and withdraw any responses they were not comfortable including (Kothari, 2019).

### **3.16 Chapter Summary**

The chapter outlined the methodological framework guiding this study, covering the pragmatist philosophy, deductive approach and mixed-methods design. The target population, census-based sample and sampling techniques were detailed alongside the data collection instruments and procedures for ensuring validity and reliability. Ethical considerations governing confidentiality, informed consent and participant protection were observed throughout.

## CHAPTER FOUR

### DATA PRESENTATION, ANALYSIS AND DISCUSSION

#### 4.0 Introduction

This chapter presents, analyses and discusses the findings of the study on the efficacy of cybercrime detection and prevention strategies employed by retailers in Bindura CBD. Response rates, demographic characteristics and detailed findings for each objective are presented using tables, figures, and narrative descriptions.

#### 4.1 Response rate

*Table 3 .1: Questionnaire Response Rate*

| Total        | Questionnaires Issued | Questionnaires Returned | Response Rate |
|--------------|-----------------------|-------------------------|---------------|
| <b>Total</b> | <b>30</b>             | <b>25</b>               | <b>83.33%</b> |

*(Source: Primary data, 2026)*

Thirty questionnaires were distributed across five retail categories in Bindura CBD. Twenty-five were returned and fully completed, yielding an overall response rate of 83.33%. According to Creswell (2014), a response rate exceeding 50% is considered sufficient for acquiring unbiased results, and the 83.33% achieved in this study therefore strongly supports the validity and reliability of the findings.

#### 4.1.2 Interview response rate

*Table 3.2: Interview response rate*

| Total        | Scheduled Interviews | Conducted Interviews | Response Rate |
|--------------|----------------------|----------------------|---------------|
| <b>Total</b> | <b>7</b>             | <b>7</b>             | <b>100%</b>   |

*(Source: Primary data, 2026)*

All seven planned interviews were successfully conducted, resulting in a 100% interview response rate. This was made possible through the purposive selection of key informants who had direct knowledge of cybercrime detection and prevention practices in their respective businesses.

#### 4.2 Demographic characteristics of respondents

*Table 3.3: Demographic characteristics of respondents (N=25)*

| Demographic Category | Demographic Variable | Frequency | Percentage (%) |
|----------------------|----------------------|-----------|----------------|
| Gender               | Male                 | 15        | 60             |
|                      | Female               | 10        | 40             |
|                      | <b>Total</b>         | <b>25</b> | <b>100</b>     |
| Age Distribution     | Below 25 years       | 4         | 16             |
|                      | 25–29 years          | 10        | 40             |
|                      | 30–34 years          | 6         | 24             |

|                         |                    |    |     |
|-------------------------|--------------------|----|-----|
|                         | 35 years and above | 5  | 20  |
|                         | <b>Total</b>       | 25 | 100 |
| Academic Qualifications | O & A Level        | 4  | 16  |
|                         | Certificate        | 4  | 16  |
|                         | Diploma            | 7  | 28  |
|                         | Undergraduate      | 6  | 24  |
|                         | Postgraduate       | 4  | 16  |
|                         | <b>Total</b>       | 25 | 100 |
| Position Held           | Owners             | 4  | 16  |
|                         | Shop Managers      | 4  | 16  |
|                         | Till Operators     | 8  | 32  |
|                         | ICT Experts        | 5  | 20  |
|                         | Others             | 4  | 16  |
|                         | <b>Total</b>       | 25 | 100 |
| Work Experience         | Less than 1 year   | 5  | 20  |
|                         | 1–3 years          | 4  | 16  |
|                         | 4–6 years          | 10 | 40  |

|                   |                          |    |     |
|-------------------|--------------------------|----|-----|
|                   | 6 years and above        | 6  | 24  |
|                   | <b>Total</b>             | 25 | 100 |
| Types of Business | Grocery stores           | 6  | 24  |
|                   | Clothing stores          | 5  | 20  |
|                   | Electronic & Accessories | 4  | 16  |
|                   | Hardware stores          | 5  | 20  |
|                   | Furniture stores         | 5  | 20  |
|                   | <b>Total</b>             | 25 | 100 |

*(Source: Primary data, 2026)*

The 25-29 years age interval recorded the highest frequency in the age distribution at 40%, followed by the 30-34 years category at 24%, those aged 35 and above at 20%, and those below 25 years at 16%. This age distribution suggests that the study was predominantly informed by young and middle-aged professionals who are more likely to engage with digital payment systems in their daily retail operations.

Diploma holders formed the largest academic group at 28%, followed by undergraduates at 24%, while Ordinary and Advanced Level holders, certificate holders, and postgraduate holders each accounted for 16%. This distribution implies that a substantial proportion of respondents possessed sufficient educational grounding to engage meaningfully with matters relating to cybercrime threats and digital security.

Till operators constituted the largest occupational group at 32%, reflecting their direct and daily exposure to payment transactions and cybercrime risk. ICT experts followed at 20%, while shop owners, shop managers and respondents in other roles each accounted for 16%. The most common experience bracket was four to six years at 40%, followed by those with over six years

at 24%, indicating that most respondents were well acquainted with the operational environment of their businesses. Grocery stores had the highest representation at 24%, with clothing stores, hardware stores and furniture stores at 20% each, and electronics and accessories shops at 16%.

These demographic characteristics carry direct analytical implications for interpreting the findings that follow. The dominance of till operators at 32% means the study is heavily weighted toward frontline workers most directly exposed to payment fraud the same individuals whose behaviour under queue pressure determines whether mobile money verification is applied consistently. Their responses on strategy effectiveness therefore reflect lived operational reality rather than managerial aspiration. The 25–29 age cohort comprising 40% of respondents suggests a digitally literate workforce, which makes the low adoption of password management and mobile money verification less a matter of unfamiliarity with technology and more a product of operational incentives and absent enforcement. The concentration of respondents in the four-to-six-year experience bracket indicates that most participants have encountered enough fraud incidents to form informed views, but may not have observed the structural evolution of cybercrime methods that longer-serving staff would recall which may partly explain why rapidly evolving threats ranked as the least universally agreed-upon challenge in Objective Three.

### 4.3 Objective One: Cybercrime detection and prevention strategy currently used by retailers.

Table 3.4: Cybercrime Detection and Prevention Strategies Currently Used by Retailers (N=25)

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

| Strategy                                  | SA (%) | A (%) | D (%) | SD (%) | Total |
|-------------------------------------------|--------|-------|-------|--------|-------|
| Point of Sale System Protection           | 36%    | 40%   | 16%   | 8%     | 100%  |
| Antivirus and Anti-malware Software       | 32%    | 40%   | 20%   | 8%     | 100%  |
| Password Management and Access Control    | 16%    | 28%   | 36%   | 20%    | 100%  |
| Employee Cybersecurity Awareness Training | 40%    | 36%   | 16%   | 8%     | 100%  |
| Mobile Money Transaction Verification     | 20%    | 24%   | 32%   | 24%    | 100%  |

(Source: Primary data, 2026)

#### 4.3.2 Point of Sale (POS) system protection

Point of Sale system protection was the most widely adopted cybersecurity measure, with 76% of retailers confirming its use (36% strongly agreeing, 40% agreeing). The high uptake reflects the volume of card-based transactions processed daily and the direct financial losses retailers have experienced from payment fraud. A grocery shop manager stated, “*We installed POS protection after a card fraud incident two years ago and have had no major payment breaches since.*” This is supported by Badgujar (2020), who confirms that encryption and tokenisation are

the most effective defences for POS environments and that retailers implementing PCI DSS compliance experience significantly fewer payment data breaches.

#### **4.3.3 Antivirus and anti-malware software**

32% of retailers strongly agreed and 40% agreed that they use antivirus and anti-malware software, making it the second most widely confirmed strategy. Its prevalence is largely explained by the accessibility of free and pre-installed solutions that eliminate the financial barrier for small businesses operating on constrained margins. A clothing shop manager stated, *"We use Windows Defender because it is free and already installed."* This concurs with Wagle (2024), who confirms that even baseline free solutions offer meaningful protection against the most common attack types, though premium tools with active threat intelligence deliver substantially stronger defence, meaning retailers relying solely on pre-installed software remain partially exposed to advanced persistent threats.

#### **4.3.4 Password management and access control**

Password management and access control was the least adopted strategy, with 56% of retailers disagreeing or strongly disagreeing that they use it, citing the impracticality of enforcing formal access restrictions in small operations where multiple staff share devices. A hardware shop owner stated, *"Our staff all know the system password because it is easier than resetting access every time someone is on duty, so the whole concept of access control does not really apply to us."* This differs from Al Naim and Ghouri (2023), who said that protective value collapses entirely when staff share credentials or bypass access restrictions regardless of how well the system is configured. Viewed through Routine Activity Theory, shared credentials effectively remove the capable guardian a system that should restrict access becomes universally accessible, turning every employee into a potential entry point for an insider threat or external attacker who obtains a single password (Cohen & Felson, 1979).

#### **4.3.5 Employee cybersecurity awareness training**

Employee cybersecurity awareness training was jointly the most widely adopted strategy, with 76% of retailers confirming its use (40% strongly agreeing, 36% agreeing). Retailers attributed this to the direct and visible impact that staff behaviour has on fraud outcomes, particularly in an environment where fake payment confirmations represent the most commonly encountered threat.

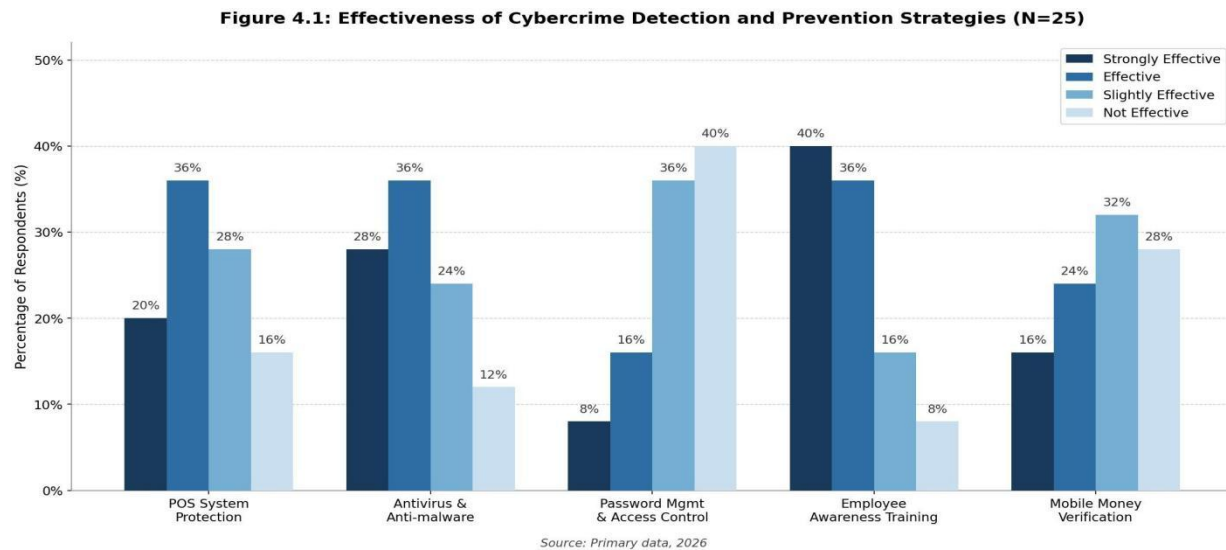
A grocery shop manager stated, *“After regular security reminders with real fraud examples, staff became much more careful about verifying payments and we had far fewer incidents of staff accepting fake EcoCash screenshots.”* This is supported by Fagbule (2022), who argues that training grounded in the real daily experiences of retail workers produces lasting and measurable behaviour change.

#### **4.3.6 Mobile money transaction verification**

Mobile money transaction verification was the least widely adopted strategy, with 56% of retailers disagreeing or strongly disagreeing that they apply it consistently. The majority attributed non-adoption to the operational pressure of busy trading hours, where verification steps create queue delays and customer friction. A clothing shop manager stated, *“When there is a queue of ten customers, stopping to check every payment on a separate phone creates conflict and customers leave, so staff end up skipping it.”* This concurs with Das et al. (2025), who confirmed that transaction verification failures represent the primary vulnerability in mobile payment fraud, and that the protective value of manual verification is entirely contingent on consistent application by staff. Viewed through Routine Activity Theory, every time a till operator skips verification under queue pressure the capable guardian withdraws and the transaction becomes an unguarded target (Cohen & Felson, 1979).

## 4.4 Objective two: Effectiveness of cybercrime detection and prevention strategies

Fig 4.1 The effectiveness of cybercrime detection and prevention strategies



(Source: Primary data, 2026)

### 4.4.2 Effectiveness of point of sale system protection

Point of Sale system protection was rated effective by 56% of respondents (20% strongly effective, 36% effective), with retailers attributing its success to the automated and continuous nature of detection a system that does not depend on staff remembering to act. A grocery shop manager stated, *“Our POS protection has caught several suspicious transaction attempts we would never have noticed manually”*. This concurs with Badgujar (2020), who confirms that proper implementation of POS security incorporating encryption and tokenisation significantly reduces payment data theft in retail environments, and that automated detection closes the critical gap that staff vigilance alone cannot consistently fill during peak trading hours. The finding aligns with Routine Activity Theory: unlike human guardians who withdraw under operational pressure, automated POS protection maintains consistent guardianship regardless of how busy the trading floor becomes (Cohen & Felson, 1979).

#### **4.4.3 Effectiveness of antivirus and anti-malware software**

Antivirus and anti-malware software were rated effective by the majority, with 28% strongly agreeing and 36% agreeing that it had delivered tangible protection. Retailers attributed this to the visible feedback they receive through quarantine notifications and weekly security reports. A clothing shop manager stated, *“Our antivirus has quarantined several threats and without it we would have had no idea those programmes were trying to access our data”*. This is in line with Wagle (2024), who confirms that antivirus programmes reliably detect and neutralise known malware, ransomware and spyware threats, while cautioning that retailers should select solutions with efficient resource allocation to minimise performance trade-offs during daily operations.

#### **4.4.4 Effectiveness of password management and access control**

Password management and access control received the weakest effectiveness rating, with 76% of respondents rating it either not effective or only slightly effective. Many retailers acknowledged that staff routinely share or forget passwords, undermining any system that exists on paper. A grocery shop manager stated, *“Staff keep forgetting passwords or sharing them, which reduces the effectiveness of the whole system”*. This differs from the position of Al Naim and Ghouri (2023), who confirm that inconsistent enforcement of access control policies significantly reduces protective impact regardless of how well the system was originally configured. The pattern here is significant beyond the technical failure: Rational Choice Theory (Cornish & Clarke, 1986) would suggest that an offender including an internal one who observes that shared passwords go unaddressed will rationally conclude that the cost of exploitation is low. The vulnerability is therefore not primarily technical but disciplinary, and it will persist regardless of how the software is upgraded until the underlying credential-sharing behaviour is addressed through policy and accountability.

#### **4.4.5 Effectiveness of employee cybersecurity awareness training**

Employee cybersecurity awareness training received the highest effectiveness rating, with 76% of respondents rating it effective or strongly effective. Retailers attributed this to observable change in staff behaviour and direct reductions in fraud incidents over time. A grocery shop manager stated, *“One staff member stopped a fraudulent EcoCash transaction because she recognised the pattern from our training, and that one incident alone justified the entire programme”*. This is supported by Kamara (2025), who confirms that effective training

programmes significantly reduce successful phishing and social engineering attacks in retail environments. It also raises the perceived cost of attack from the offender's perspective a workforce that recognises fake payment confirmations makes the Rational Choice calculus less favourable for fraudsters who rely on untrained staff (Clarke, 1995).

#### **4.4.6 Effectiveness of mobile money transaction verification**

Mobile money transaction verification was rated the least effective strategy, with 60% of respondents rating it ineffective or slightly effective, reflecting the inconsistent application documented in Objective One. Retailers attributed poor effectiveness directly to the same operational pressures that suppressed adoption queue management demands mean verification is skipped precisely during the busiest and highest-risk trading periods. A clothing shop manager stated, *"We try to verify but when it is busy it just does not happen consistently, and that is exactly when the fake screenshots come in."* This concurs with Das et al. (2025), who confirm that the protective value of manual transaction verification is entirely contingent on consistent application, and that intermittent use delivers outcomes no better than having no verification procedure at all.

### Objective 3 : Challenges faced in implementing cybercrime detection and prevention strategies

*Table 3.5 Challenges faced in implementing cybercrime detection and prevention strategies(N=25)*

| Challenge                            | SA (%) | A (%) | D (%) | SD (%) | Total |
|--------------------------------------|--------|-------|-------|--------|-------|
| High Cost of Security Technology     | 60%    | 40%   | 0%    | 0%     | 100%  |
| Unreliable Internet & Infrastructure | 48%    | 40%   | 8%    | 4%     | 100%  |
| Lack of Skilled ICT Personnel        | 40%    | 40%   | 16%   | 4%     | 100%  |
| Evolving Threats & Absent Policies   | 20%    | 28%   | 32%   | 20%    | 100%  |

*(Source: Primary data, 2026)*

#### 4.5.1 High cost of security technology

The high cost of security technology was confirmed by every respondent, with 100% agreeing that it is the most prohibitive barrier to implementation. Comprehensive cybersecurity packages cost between USD 2,000 and USD 5,000 annually, yet many retailers in Bindura earn less than that figure in annual profit. A grocery shop owner stated, *“I cannot spend USD 3,000 on software when my monthly profit is only USD 900, staff salaries must come first”*. This concurs with Ardhaninggar and Ramil (2024), who confirm that high initial investment costs are the primary structural reason small retailers defer security investment indefinitely.

#### **4.5.2 Unreliable internet connectivity**

Unreliable internet connectivity was confirmed as a significant challenge by 88% of retailers (48% strongly agreeing, 40% agreeing). Daily outages and load shedding disable cloud-based security systems, prevent antivirus updates, and interrupt backup processes at precisely the moments when consistency matters most. A grocery shop manager stated, *“When the internet drops our antivirus cannot update, our backup cannot run, and we are completely exposed”*. This is supported by Vaka (2025), who documents that real-time fraud detection requires consistent connectivity to deliver automated responses, conditions that intermittent infrastructure makes structurally impossible to meet.

#### **4.5.3 Lack of skilled Information and Communication Technology (ICT) personnel**

40% strongly agreed and 40% agreed that the lack of skilled ICT personnel is a significant challenge. Without personnel who can configure, maintain and troubleshoot security systems, even well-resourced retailers find that their tools remain unused or incorrectly set up. A clothing shop owner stated, *“We bought security software but it gave error messages we could not understand and after trying YouTube fixes we gave up, it has been unused for six months”*. This concurs with Ardhaninggar and Ramil (2024), who document that without skilled cybersecurity workers retailers cannot properly configure security systems or keep pace with evolving threats, and who recommend that retailers prioritise training at least one staff member with basic cybersecurity competencies as the most cost-effective first step.

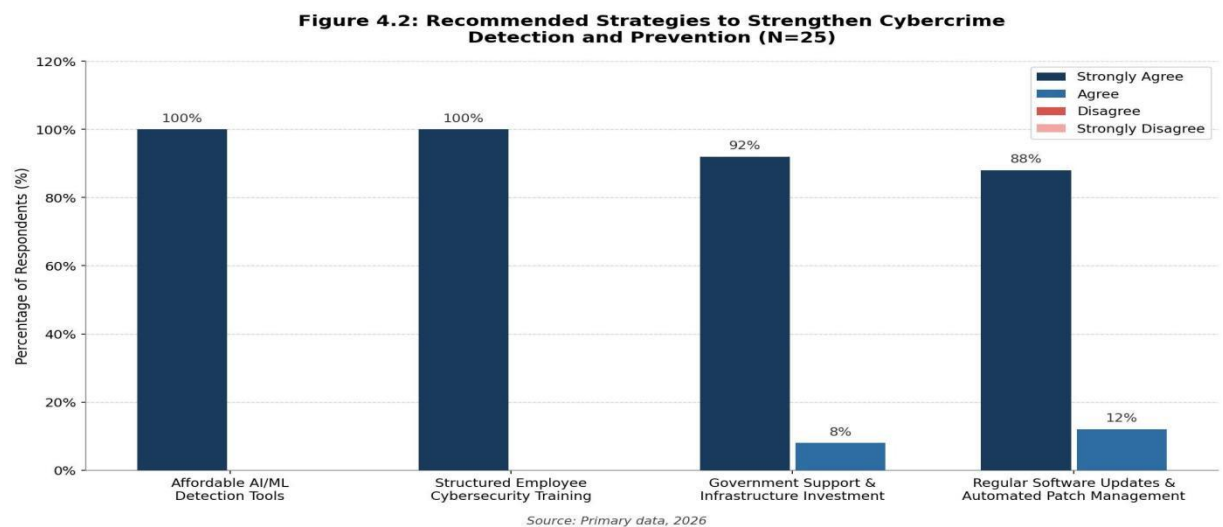
#### **4.5.4 Rapidly Evolving Cyber Threats and Absence of Formal Policies**

Rapidly evolving cyber threats and the absence of formal policies was the least confirmed challenge in the study, with 52% of retailers disagreeing or strongly disagreeing that it posed a significant barrier. Retailers attributed this to their familiarity with the dominant local fraud types, particularly fake EcoCash screenshots and card-related fraud, which they felt sufficiently equipped to recognise and manage. A grocery shop owner stated, *“The fraud we see here is always the same fake EcoCash screenshots and stolen cards so we know what to look for.”* However, Liu et al. (2022) caution that this confidence is itself a vulnerability, as businesses whose awareness is shaped exclusively by past experience remain structurally unprepared when criminal methods shift. McQuade’s (2006) Theory of Technology-Enabled Crime is directly

relevant here criminal techniques evolve continuously through online networks, and a retailer calibrated only to yesterday’s fraud patterns is already behind.

**4.6 Objective Four: Recommended strategies to strengthen cybercrime detection and prevention**

*Fig 4.2 : Recommended strategies to strengthen cybercrime detection and prevention strategies*



*(Source: Primary data, 2026)*

**4.6.1 Adoption of Affordable Machine Learning and AI-Based Detection Tools**

All 100% of retailers agreed that government and financial institutions should facilitate access to affordable AI-based fraud detection tools, producing one of two unanimous recommendations in the study. Retailers identified automated detection as the most transformative capability gap they currently face, particularly for flagging suspicious mobile money transactions before goods are released. A grocery shop manager stated, “An affordable AI system that automatically flags suspicious mobile money transactions before we release goods would transform our security”. Chaudhary (2025) agrees, documenting that AI-powered fraud detection increased detection accuracy by 82.4% and delivered average financial loss reductions of 37% in retail environments.

#### **4.6.2 Structured and Continuous Employee Cybersecurity Training**

All 100% of retailers strongly agreed that formal structured cybersecurity training programmes should be established as an urgent priority. Retailers were unambiguous that training must be continuous and specific to local fraud types rather than generic in content. A clothing shop owner stated, *‘Training should cover the exact types of fraud we see in Bindura with real examples, not generic internet content that does not help staff recognise local fraud tactics’*. This concurs with Murungu et al. (2026), who found that continuous training is essential because human error causes most security breaches and that regular training enables workers to identify and stop new threats before they cause harm.

#### **4.6.3 Government Support and Infrastructure Investment**

Ninety-two percent of retailers strongly agreed that affordable cloud-based subscription models should replace expensive upfront security packages as the primary pathway to improved protection. Retailers consistently distinguished between the unaffordable cost of comprehensive security suites and the potential accessibility of subscription-based tools that spread costs monthly and update automatically. A grocery shop owner stated, *‘We cannot pay USD 2,000 upfront for security software but if there was a monthly subscription we could afford, we would use it immediately.’* This concurs with Saeed et al. (2023), who confirmed that cloud-based subscription security tools are significantly more accessible for small businesses operating on thin margins and that automatic updates remove the skills burden of manual patch management.

#### **4.6.4 Regular Software Updates and Automated Patch Management**

Automated patch management drew the second-highest level of support among the four recommended strategies, with 88% of retailers strongly agreeing and a further 12% agreeing that it should be made standard practice. Retailers explained that updates to their existing antivirus and anti-malware software were applied irregularly, if at all, leaving systems running on outdated definitions long after newer fraud techniques had emerged. A hardware shop owner stated, *‘Our antivirus has not been updated in months because no one knows how to do it and there is no reminder system in place it is running but it is not protecting us properly.’* This concurs with Chingoriwo (2022), who established that outdated software and missed security patches are among the most exploited vulnerabilities in Zimbabwean business environments, and

that automated update scheduling is one of the lowest-cost improvements available to resource-constrained retailers.

#### **4.7 Chapter Summary**

This chapter presented findings on the efficacy of cybercrime detection and prevention strategies employed by retailers in Bindura CBD, supported throughout by empirical evidence from academic sources. The findings confirmed that retailers rely predominantly on basic manual detection strategies, and that their effectiveness varies considerably depending on whether the measures are consistently applied and supported by adequate human capacity and infrastructure.

## **CHAPTER FIVE**

### **SUMMARY, CONCLUSION AND RECOMMENDATIONS**

#### **5.0 Introduction**

This chapter brings together the key findings of the study and draws conclusions that speak directly to the four research objectives. It presents a summary of what was found across all chapters, offers conclusions grounded in both the empirical evidence and the theoretical frameworks, and makes targeted recommendations for retailers, government and relevant institutions. Areas warranting further research are also identified. The chapter is the culmination of a study that set out to evaluate whether the cybercrime detection and prevention strategies currently employed by retailers in Bindura CBD are adequate to the threats they face in an increasingly digital trading environment.

#### **5.1 Summary of the Study**

The study assessed the efficacy of cybercrime detection and prevention strategies employed by retailers in Bindura Central Business District. Chapter One established the problem of the study that the rapid adoption of digital payment systems in Bindura CBD has not been matched by the development of effective cybercrime defences, leaving retailers exposed to financial losses and operational disruptions they are ill-equipped to manage. The chapter situated this problem within the national context of Zimbabwe's fragmented cybersecurity governance framework and the specific vulnerabilities of a secondary urban trading centre operating under conditions of load shedding, poor connectivity and limited institutional support.

Chapter Two reviewed the theoretical and empirical literature on cybercrime detection and prevention in the retail sector. Three theoretical frameworks guided the study Routine Activity Theory, the Theory of Technology-Enabled Crime and Rational Choice Theory each offering a distinct explanation for why cybercrime occurs and what conditions are necessary to suppress it. The empirical review confirmed that the challenges facing Bindura retailers are consistent with those documented in comparable developing economy contexts, while also identifying a gap in research specifically addressing small retailers in secondary Zimbabwean towns.

Chapter Three outlined the research design, adopting a mixed-methods design combining structured questionnaires distributed to 30 respondents and semi-structured interviews with 7 key informants drawn from five retail categories in Bindura CBD. Chapter Four presented, analysed and discussed the findings against the four research objectives, drawing on both quantitative data and interview evidence to explain not just what retailers do but why they do it, and why some strategies succeed while others fail.

## **5.2 Summary of Research Findings**

### **5.2.1 What Cybercrime Detection and Prevention Strategies Are Currently Used?**

Point of Sale system protection and employee cybersecurity awareness training were the most widely adopted strategies, both recording combined agreement rates above 76%. Antivirus and anti-malware software followed closely, largely because free and pre-installed solutions remove the financial barrier for constrained businesses. Password management and access control and mobile money transaction verification were the least adopted, rejected by the majority of retailers the former undermined by shared credentials and the absence of formal access policies, the latter by operational pressure during busy trading periods that causes staff to skip verification steps entirely. The overall pattern of adoption is reactive rather than systematic, driven by past fraud experience rather than deliberate security planning.

### **5.2.2 How Effective Are the Strategies in Mitigating Financial Losses?**

Employee cybersecurity awareness training was rated the most effective strategy, with 76% of respondents confirming it produced measurable reductions in fraud incidents. Antivirus and anti-malware software was the second most effective, rated effective or strongly effective by 64% of respondents, ahead of POS system protection at 56%, which retailers nonetheless valued for the automated and continuous nature of its detection. Password management and access control was rated ineffective by 76% of respondents, with effectiveness collapsing wherever shared credentials and informal access norms persisted. Mobile money transaction verification was rated the least effective strategy overall, with 60% rating it ineffective or slightly effective a direct consequence of the inconsistent application documented under Objective One, where queue pressure causes verification to be abandoned at precisely the moments of highest risk.

### **5.2.3 What Challenges Do Retailers Encounter When Implementing Cybercrime Prevention Measures?**

The high cost of security technology was the most unambiguous barrier, confirmed unanimously by all respondents. Unreliable internet connectivity and load shedding were confirmed by 88% as directly disabling cloud-based tools and interrupting backup systems. The shortage of skilled ICT personnel was confirmed by 80% as leaving purchased tools misconfigured and unmonitored. Rapidly evolving threats and the absence of formal policies was the least confirmed challenge, with 52% disagreeing that it posed a significant problem a finding the study identifies not as reassurance but as itself a vulnerability, since confidence rooted in familiarity with current fraud types leaves retailers structurally unprepared for the next generation of attacks.

### **5.2.4 What Strategies Can Strengthen Cybercrime Detection and Prevention?**

Affordable AI and machine learning-based fraud detection tools and structured employee cybersecurity training each received unanimous endorsement from all respondents. Ninety-two percent strongly agreed that affordable cloud-based subscription models should replace expensive upfront security packages as the primary pathway to improved protection. Automated patch management received the next-highest level of support, with 88% strongly agreeing and 12% agreeing that it should be made standard practice, reflecting the irregular update habits retailers reported for their existing antivirus and anti-malware software.

## **5.3 Conclusion**

Regarding Objective One identifying the detection and prevention strategies currently in use the study concludes that five strategies are actively employed: POS system protection, antivirus and anti-malware software, password management and access control, employee cybersecurity awareness training, and mobile money transaction verification. Adoption is uneven. POS protection and employee training are widely used and their adoption is purposeful. Password management and mobile money verification are rejected by the majority, not because of cost but because of behavioural and operational failures that no software solution alone can address. The pattern of adoption is largely reactive, shaped by past fraud experience rather than forward-looking security planning.

Regarding Objective Two assessing the effectiveness of these strategies the study concludes that employee training and POS protection deliver genuine protection where consistently applied. Password management and mobile money verification are rated ineffective by the majority, not because they are poorly designed but because the conditions for consistent human implementation do not exist. The primary determinant of effectiveness across all five strategies is not the tool itself but whether the organisational conditions exist for its sustained and disciplined application.

Regarding Objective Three identifying implementation challenges cost, infrastructure failure and skills shortage constitute structural barriers that individual retailers cannot overcome in isolation. The finding that 52% of retailers do not perceive evolving threats as a significant challenge is the most analytically consequential result in this objective. It does not indicate that the threat is manageable it indicates that awareness has not kept pace with the threat, and that the absence of formal policies means there is no institutional mechanism to force that update.

Regarding Objective Four recommending strengthening strategies the study concludes that the recommendations endorsed by respondents and developed from the evidence point consistently toward two requirements: external structural support from government and institutions to address cost and infrastructure barriers, and internal behavioural change grounded in sustained training and formalised security procedures to address the human failures that currently undermine even the strategies that are in place.

The findings taken together point to a single overarching conclusion the three theoretical frameworks collectively predicted. The dominant failure mode in Bindura is not the absence of cybersecurity tools but the collapse of consistent human guardianship under operational pressure. Routine Activity Theory explains why each lapse matters whenever a till operator skips verification or a staff member shares a password, the capable guardian withdraws and the target becomes exposed. The Theory of Technology-Enabled Crime explains why majority complacency about familiar local threats is structurally dangerous criminal methods evolve continuously through online networks, and a retailer calibrated only to yesterday's fraud patterns is already behind. Rational Choice Theory explains what must change to deter offenders the perceived cost of attacking a Bindura retailer must be raised through consistent enforcement of verification procedures, access controls and visible staff awareness, not merely through the

presence of software on a device. This theoretical convergence gives the study's recommendations their coherence: each one targets a specific point at which guardianship currently fails, threat awareness stalls, or the offender's cost-benefit calculation favours attack.

## **5.4 Recommendations**

### **5.4.1 Retailers Should Formalise Written Internal Cybersecurity Policies**

Retailers should put written cybersecurity policies in place covering password protocols, device access and verification procedures. This would turn good practice into an enforceable standard instead of something staff apply at their own discretion.

### **5.4.2 Retailers Should Embed Transaction Verification as a Non-Negotiable Point-of-Sale Step**

Independent verification of mobile money payments should be made a fixed step at every till, supported by a clearly displayed procedure. Retailers should rotate staff during busy periods so verification is not skipped under queue pressure.

### **5.4.3 The Government of Zimbabwe Should Introduce Subsidised Cybersecurity Support Under the Cyber and Data Protection Act**

The Government of Zimbabwe should introduce subsidised cybersecurity support for small retailers under the Cyber and Data Protection Act, prioritising affordable cloud-based tools that update automatically. This would help close the gap between the cost of comprehensive security packages and what small retailers can actually afford.

### **5.4.4 BUSE and the Bindura Business Chamber Should Collaborate to Deliver Annual Cybersecurity Capacity Building**

Bindura University of Science Education and the Bindura Business Chamber should partner to deliver an annual cybersecurity training programme for the retail sector. This should include training at least one cybersecurity champion per outlet and producing a yearly local threat report.

#### **5.4.5 Law Enforcement Should Strengthen Cybercrime Reporting Mechanisms for Retailers**

The Zimbabwe Republic Police should set up a dedicated, accessible channel for retailers to report cybercrime, staffed by officers trained in digital evidence. A functional reporting system would raise the risk for offenders and supply the data needed to inform future training and policy.

#### **5.5 Recommendations for Further Research**

A comparative study across other Zimbabwean towns is recommended to establish whether the challenges identified in Bindura are unique to the town or representative of small retailers nationally. Further research quantifying the actual financial losses retailers suffer from mobile money fraud and card-related crime is recommended to guide proportionate investment in cybersecurity.

## REFERENCES

- Ahmad, M., & Wilkins, S. (2024). Purposive sampling in qualitative research: A framework for the entire journey. *Quality & Quantity*, 59(2), 1461–1479. <https://doi.org/10.1007/s11135-024-02022-5>
- Akpan, I. J., Udoh, P., & Adebisi, B. (2021). Small business awareness and adoption of state-of-the-art technologies in emerging and developing markets, and lessons from the COVID-19 pandemic. *Journal of Small Business & Entrepreneurship*, 34(2). <https://doi.org/10.1080/08276331.2020.1820185>
- Al Naim, A. F., & Ghouri, A. M. (2023). Exploring the role of cyber security measures (encryption, firewalls, and authentication protocols) in preventing cyber-attacks on e-commerce platforms. *International Journal of eBusiness and eGovernment Studies*, 15(1), 444–469. <https://ssrn.com/abstract=4626041>
- Amosu, O. R., Kumar, P., Ogunsuji, Y. M., Adelaja, A., Faworaja, O., & Adetula, K. (2024). Enhanced cybersecurity measures: Protect customer data in e-commerce and retail industry. *World Journal of Advanced Research and Reviews*, 23(2), 890–900. <https://doi.org/10.30574/wjarr.2024.23.2.2408>
- Antipova, T., & Riurean, S. (2025). Bytes and battles in AI era: Safeguarding consumers' digital world. In T. Antipova (Ed.), *Digital technology platforms and deployment* (pp. 201–207). Springer. [https://doi.org/10.1007/978-3-031-86547-3\\_16](https://doi.org/10.1007/978-3-031-86547-3_16)
- Aprilia, C., Gebrewold, R. A., Bamiduro, M. D., Borisova, N., & Mengdigali, A. (2026). The evolution of cybercrime and its impact on various sectors. *Data Science: Journal of Computing and Applied Informatics*, 10(1), 11–35. <https://doi.org/10.32734/jocai.v10.i1-24471>
- Ardhaninggar, E. A., & Ramil, K. (2024). A review of cybersecurity framework implementation for retail industry: Challenges and recommendations. *ARRUS Journal of Engineering and Technology*, 4(2), 211–219.

- Azzani, I. K., Purwantoro, S. A., & Almubarak, H. Z. (2024). Enhancing awareness of cyber crime: A crucial element in confronting the challenges of hybrid warfare in Indonesia. *Defense and Security Studies*, 5, 1–9. <https://doi.org/10.37868/dss.v5.id255>
- Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, 4(1&2), 643–656.
- Badgajar, P. (2020). *Securing customer data and best practices for retail point-of-sale systems* [Unpublished manuscript].
- Benmalek, M., et al. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*, 4, 186–202. <https://doi.org/10.1016/j.iotcps.2023.12.001>
- Beretas, C. P. (2024). Information systems security, detection and recovery from cyber attacks. *Universal Library of Engineering Technology*, 1(1), 27–40. <https://share.google/muuwAvJBSkwLggHBZ>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Bressler, M. (2009). Insuring big losses due to security breaches. *Entrepreneurial Executive*, 14, 23–36. <https://doi.org/10.1109/HICSS.2007.280>
- Chaudhary, S. (2025). AI in retail: Advanced technologies for fraud and loss prevention. *International Journal on Science and Technology*, 16(1). <https://www.ijst.org>
- Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime detection and prevention efforts in the last decade: An overview of the possibilities of machine learning models. *Review of International Geographical Education*, 11(7), 950–974. <https://doi.org/10.48047/rigeo.11.07.92>
- Chingoriwo, T. (2022). Cybersecurity challenges and needs in the context of digital development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies: Engineering and Technology*, 3(2), 77–104. <https://doi.org/10.37745/bjmas.2022.0046>

- Clarke, R. V. (1995). Situational crime prevention. In M. Tonry & D. P. Farrington (Eds.), *Building a safer society: Strategic approaches to crime prevention* (Crime and Justice: A Review of Research, Vol. 19, pp. 91–150). University of Chicago Press.  
<https://www.jstor.org/stable/1147596>
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>
- Cornish, D. B., & Clarke, R. V. (1986). Understanding crime displacement: An application of rational choice theory. In D. B. Cornish & R. V. Clarke (Eds.), *The reasoning criminal: Rational choice perspectives on offending* (pp. 1–16). Springer-Verlag.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
- Das, G., Ali, Y. A., Singh, B., & Nag, K. (2025). Digital forensics in e-commerce: Investigating online payment fraud and data breaches. *International Journal of Innovations in Science Engineering and Management*, 4(1), 262–268. <https://doi.org/10.69968/ijisem.2025v4i1262-268>
- Clarke, R. V., & Eck, J. E. (2003). *Become a problem-solving crime analyst*. Jill Dando Institute of Crime Science, University College London.  
<https://www.researchgate.net/publication/32894308>
- Eyaleko, A. H., & Feng, T. (2023). A critical overview of Industrial Internet of Things security and privacy issues using a layer-based hacking scenario. *IEEE Internet of Things Journal*, 10(24), 21917–21943. <https://doi.org/10.1109/JIOT.2023.3308195>
- Fagbule, O. (2022). *Cyber security training in small to medium-sized enterprises (SMEs): Exploring organisation culture and employee training needs* [Doctoral dissertation, Bournemouth University]. Bournemouth University Research Online.  
<https://eprints.bournemouth.ac.uk/39148/>

Fianyi, I. D. (2015). Curbing cyber-crime and enhancing e-commerce security with digital forensics. *IJCSI International Journal of Computer Science Issues*, 12(6), 78–85.

Ganguli, P. (2022). The rise of cybercrime-as-a-service: Implications and countermeasures. In P. Kulshrestha, A. Singh, & R. Gautam (Eds.), *Cyber crime, regulation and security: Contemporary issues and challenges* (pp. 1–14). Libertatem Media Private Limited.

Graham, A. O. (2023). *Cybercrime: Traditional problems and modern solutions* [Master of Laws thesis, Victoria University of Wellington].  
[https://openaccess.wgtn.ac.nz/articles/thesis/Cybercrime\\_Traditional\\_Problems\\_and\\_Modern\\_Solutions/22300909](https://openaccess.wgtn.ac.nz/articles/thesis/Cybercrime_Traditional_Problems_and_Modern_Solutions/22300909)

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Ballinger.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Hossan, D., Dato Mansor, Z., & Jaharuddin, N. S. (2023). Research population and sampling in quantitative study. *International Journal of Business and Technopreneurship*, 13(3), 209–222.  
<https://doi.org/10.58915/ijbt.v13i3.263>

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity theft and data breaches: How stolen data circulates on the dark web: A systematic approach. *Spectrum of Engineering Sciences*, 3(1), 143–161.

Jaishankar, K. (Ed.). (2011). *Cyber criminology: Exploring internet crimes and criminal behavior*. CRC Press. <https://www.routledge.com/Cyber-Criminology-Exploring-Internet-Crimes-and-Criminal-Behavior/Jaishankar/p/book/9781439829493>

Kabanda, G., & Chingoriwo, T. (2022). A cybersecurity culture framework for grassroots levels in Zimbabwe. *Oriental Journal of Computer Science and Technology*, 14(010203), 17–34.  
<https://doi.org/10.13005/ojcs14.010203.03>

Kamara, M. M. (2025). *Use of policies to prevent data breaches among information security managers at large retail organizations* [Doctoral dissertation, Walden University].

- Khatri, K. K. (2020). Research paradigm: A philosophy of educational research. *International Journal of English Literature and Social Sciences*, 5(5), 1435–1440. <https://doi.org/10.22161/ijels.55.15>
- Kothari, C. R., & Garg, G. (2019). *Research methodology: Methods and techniques* (4th ed.). New Age International.
- Kudanga, D., Mthombeni, A., Chinongwa, E., Singende, M., Tshuma, E., & Tembo, E. B. (2022). The role of technology in evidence gathering for cases of fraud: Case of Bulawayo Central Business District, Zimbabwe. *Lighthouse: The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy*, 1(1&2), 5–23. <https://cris.library.msu.ac.zw/handle/11408/6074>
- Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, 13, 927398. <https://doi.org/10.3389/fpsyg.2022.927398>
- Manchikanti, D. R. (2025). AI-enabled retail loss prevention: A framework for enhanced security and operational efficiency. *International Journal of Advances in Engineering and Management*, 7(2), 165–172. <https://doi.org/10.35629/5252-0702165172>
- Marelino, A. (2022). Understanding the types of cyber crime and its prevention. *Mathematical Statistician and Engineering Applications*, 71(1), 108–112. <https://doi.org/10.17762/msea.v71i1.50>
- McQuade, S. C. (2006). *Understanding and managing cybercrime*. Pearson/Allyn and Bacon.
- Mienye, I. D., & Jere, N. (2024). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. *IEEE Access*, 12, 96893–96910. <https://doi.org/10.1109/ACCESS.2024.3426955>
- Mohd Saleh, N. H., Hussin, N. A. A., Suthursan Kumar, M., & Zolkipli, M. F. (2026). Cybersecurity risk management for digital retail: Strategies, frameworks and implementation. *Journal of Advanced Computing and Information Technology*, 1(1), 33–48. <https://doi.org/10.67131/jacoit.v1i1.6>

Murungu, C. N., Kupfuwa, M., & Nyazema, M. (2026). Cybersecurity strategies as enablers of digital transformation in commercial banks: Evidence from Zimbabwe. *International Journal of Research and Innovation in Social Science*, 10(2), 4386–4396. <https://doi.org/10.47772/IJRISS.2026.10200321>

Navandar, P. (2023). The impact of artificial intelligence on retail cybersecurity: Driving transformation in the industry. *Journal of Scientific and Engineering Research*, 10(11), 177–181.

Okeke, R. I. (2015). *The prevention of internal identity theft-related crimes: A case study research of the UK online retail companies* [Doctoral dissertation, University of Central Lancashire]. <https://knowledge.lancashire.ac.uk/id/eprint/12124/>

Oloyede, A., Ajibade, I., Obunadike, C., Phillips, A., Shittu, O., Taiwo, E., & Kizor-Akaraiwe, S. (2023). A review of cybersecurity as an effective tool for fighting identity theft across the United States. *International Journal on Cybernetics & Informatics*, 12(5), 31–42. <https://doi.org/10.5121/ijci.2023.120504>

Patel, M., & Patel, N. (2019). Exploring research methodology: Review article. *International Journal of Research and Review*, 6(3), 48–55. [www.ijrrjournal.com](http://www.ijrrjournal.com)

Phillips, A., Ojelade, I., Taiwo, E., Obunadike, C., & Oloyede, K. (2023). Cyber-security tactics in mitigating cyber-crimes: A review and proposal. *International Journal on Cryptography and Information Security*, 13(2/3), 1–20. <https://share.google/C9oqZJKirro2ueNng>

Putra, F. P. E., Dafid, M., & Syafi'i, I. (2025). Firewall implementation as a computer network security strategy for data protection. *Brilliance Research of Artificial Intelligence*, 5(1), 291–297. <https://doi.org/10.47709/brilliance.v5i1.6162>

Ray, R. K., Chowdhury, F. R., & Hasan, M. R. (2024). Employee performance prediction: An integrated approach of business analytics and machine learning. *Journal of Business and Management Studies*, 6(1). <https://doi.org/10.32996/jbms.2024.6.1.14>

Razzaq, K., & Shah, M. (2024). Challenges, risks, and barriers to adopting machine learning techniques in online retail security. In *Proceedings of the 9th IEEE International Conference on Engineering Technologies and Applied Sciences*. <https://share.google/KIsVgfaLw4RnAy5BG>

- Saadi, I. (2024). The role of cyber security in protecting e-commerce from cybercrimes. *Journal for Strategic Studies and Political Research*, 3(2), 104–120. <https://search.emarefa.net/detail/BIM-1645030>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 6666. <https://doi.org/10.3390/s23156666>
- Sari, R. M. P. (2025). Criminal responsibility in cybercrime: An analysis of phishing crimes in Indonesia. *Jurnal Hukum dan Keadilan*, 2(5), 49–55. <https://doi.org/10.61942/jhk.v2i5.418>
- Schwartz, A. (2008). *Toward objective global privacy standards* [Presentation slides]. National Institute of Standards and Technology.
- Shan-A-Alahi, A., Mustafizur, M., Hossan, K. M. R., & Al Zaiem, A. (2024). Cybersecurity training and its influence on employee behavior in business environments. *Computer Fraud & Security*, 2024(12), 506–515. <https://doi.org/10.52710/cfs.689>
- Vaka, P. R. (2025). Cyber security in the retail industry. *International Research Journal of Modernization in Engineering Technology and Science*, 7(2), 939–946. <https://doi.org/10.56726/IRJMETs67237>
- van de Schoot, R., & Miočević, M. (Eds.). (2020). *Small sample size solutions: A guide for applied researchers and practitioners*. Routledge. <https://doi.org/10.4324/9780429273872>
- Vassilakos, A., & Martin, R. (2023). Understanding the challenge of cybersecurity in Africa: A holistic analysis of Southern African Development Community (SADC) and foundation for future research. *Holistica Journal of Business and Public Administration*, 14(1), 162–172. <https://doi.org/10.2478/hjbpa-2023-0009>
- Wagle, P. (2024). *Investigation and evaluation of the impact of antivirus protection on the performance of a personal computer* [Master's thesis, Vilnius Gediminas Technical University].
- Wright, C. S. (2010). *Criminal specialization as a corollary of rational choice* [Working paper]. SSRN.

Zieni, R., Massari, L., & Calzarossa, M. C. (2023). Phishing or not phishing? A survey on the detection of phishing websites. *IEEE Access*, 11, 18499–18519. <https://doi.org/10.1109/access.2023.3247135>

Council of Europe, Cybercrime Programme Office (C-PROC). (2026). The global state of cybercrime legislation 2013–2025: A cursory overview. <https://www.coe.int/en/web/cybercrime>

e-Governance Academy Foundation (eGA). (2026). National Cyber Security Index: Zimbabwe. <https://ncsi.ega.ee/country/zw/>

INTERPOL. (2023, December 19). USD 300 million seized and 3,500 suspects arrested in international financial crime operation. <https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation>

INTERPOL. (2025). Africa Cyberthreat Assessment Report 2025 (4th ed.). [https://www.interpol.int/content/download/23094/file/INTERPOL\\_Africa\\_Cyberthreat\\_Assessment\\_Report\\_2025.pdf](https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf)

INTERPOL. (2025, September 26). 260 suspected scammers arrested in pan-African cybercrime operation. <https://www.interpol.int/en/News-and-Events/News/2025/260-suspected-scammers-arrested-in-pan-African-cybercrime-operation>

Pindula News. (2021, March 25). Police arrest 3 notorious Bindura fraudsters. <https://www.pindula.co.zw/2021/03/25/police-arrest-3-notorious-bindura-fraudsters/>

Zimbabwe Republic Police (ZRP). (2024). Criminal Investigation Department. <https://www.zrp.gov.zw/index.php/departments/criminal-investigations-department>



**BINDURA UNIVERSITY OF SCIENCE EDUCATION**

Private Bag 1020  
BINDURA, Zimbabwe  
Tel: 0271 – 7531-6, 7615  
Fax: 263 –271 – 7534

**INTELLIGENCE AND SECURITY STUDIES DEPARTMENT**

22 May 2026

Bindura CBD retailers

**RE: REQUEST FOR DATA COLLECTION**

Please may you assist our student Tirivashe G Chapfuwa (B223869B) to carry his research in your organization on his topic on **“The efficacy of cyber crime detection and prevention strategies in the retail sector . A case study of Bindura CBD. ”**. He is our final year student at Bindura University of Science Education in the Intelligence and Security Studies Department.

Your assistance to our student will be greatly appreciated.

Regards

Ms L Chinyoka  
Chairperson



## **Appendix 2 :**

### **Questionnaire for Bindura CBD Retailers**

#### **BINDURA UNIVERSITY OF SCIENCE EDUCATION**

##### **Department of Intelligence and Security Studies**

**Research Title:** The Efficacy of Cybercrime Detection and Prevention Strategies Employed by Retailers in Zimbabwe. A Case Study of Bindura CBD.

This questionnaire is administered to shop owners, managers, till operators and ICT staff in Bindura CBD. All responses are confidential and will be used for academic purposes only. Please tick [ ] or fill in where applicable.

#### **SECTION A: DEMOGRAPHIC DATA**

##### **1. Gender**

Male [ ]      Female [ ]

##### **2. Age**

Below 25 [ ]    25–29 [ ]    30–34 [ ]    35 and above [ ]

##### **3. How long have you worked in your current organisation?**

Less than 1 year [ ]    1–3 years [ ]    4–6 years [ ]    Above 6 years [ ]

##### **4. What is your academic qualification?**

O & A Level [ ]    Certificate [ ]    Diploma [ ]    Undergraduate [ ]

Postgraduate [ ]

##### **5. What is your position?**

Shop Owner [ ]    Shop Manager [ ]    Till Operator [ ]    ICT Specialist [ ]

Other [ ]

6. Type of business

Grocery shop [ ]    Clothing shop [ ]    Electronics & Accessories [ ]

Hardware [ ]    Furniture [ ]

**SECTION B: CYBERCRIME DETECTION AND PREVENTION STRATEGIES IN USE**

7. Which of the following cybersecurity measures does your organisation currently use? Please indicate.

| Strategy                                  | SA  | A   | D   | SD  |
|-------------------------------------------|-----|-----|-----|-----|
| Point of Sale (POS) System Protection     | [ ] | [ ] | [ ] | [ ] |
| Antivirus and Anti-malware Software       | [ ] | [ ] | [ ] | [ ] |
| Password Management and Access Control    | [ ] | [ ] | [ ] | [ ] |
| Employee Cybersecurity Awareness Training | [ ] | [ ] | [ ] | [ ] |
| Mobile Money Transaction Verification     | [ ] | [ ] | [ ] | [ ] |

8. Are there any other cybersecurity measures in place at your organisation not listed above?

.....  
.....

**SECTION C: EFFICACY OF CYBERCRIME DETECTION AND PREVENTION STRATEGIES**

9. How effective have the following strategies been in reducing cybercrime incidents and financial losses at your organisation?

(SA = Strongly Agree A = Agree D = Disagree SD = Strongly Disagree)

| Strategy              | SA  | A   | D   | SD  |
|-----------------------|-----|-----|-----|-----|
| POS System Protection | [ ] | [ ] | [ ] | [ ] |

|                                           |                          |                          |                          |                          |
|-------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Antivirus and Anti-malware Software       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Password Management and Access Control    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Employee Cybersecurity Awareness Training | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Mobile Money Transaction Verification     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

10. Has your organisation experienced any of the following as a result of cybercrime?

| Impact                            | Yes                      | No                       |
|-----------------------------------|--------------------------|--------------------------|
| Direct financial loss             | <input type="checkbox"/> | <input type="checkbox"/> |
| Additional network security costs | <input type="checkbox"/> | <input type="checkbox"/> |
| Loss of sensitive customer data   | <input type="checkbox"/> | <input type="checkbox"/> |
| Reputational damage               | <input type="checkbox"/> | <input type="checkbox"/> |
| Operational disruption            | <input type="checkbox"/> | <input type="checkbox"/> |

#### **SECTION D: CHALLENGES IN IMPLEMENTING CYBERSECURITY MEASURES**

11. How much do the following challenges affect your organisation's ability to implement cybersecurity measures?

(SA = Strongly Agree A = Agree D = Disagree SD = Strongly Disagree)

| Challenge                             | SA                       | A                        | D                        | SD                       |
|---------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| High cost of security technology      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Unreliable internet and load shedding | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Lack of skilled ICT personnel         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Rapidly evolving cyber threats        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

12. What measures do you suggest could strengthen cybersecurity in your organisation or sector?

.....

.....

.....

.....

13. In your view, what role should the government play in helping retailers combat cybercrime?

.....

.....

.....

.....

End of Questionnaire. Thank you for your participation.

### **Appendix 3 : Interview Guide**

**Research Title:** The Efficacy of Cybercrime Detection and Prevention Strategies Employed by Retailers in Zimbabwe. A Case Study of Bindura CBD.

The following questions guide semi-structured interviews with purposively selected key informants. Questions may be reordered or supplemented based on the flow of each interview. All responses are confidential.

#### **SECTION A: CYBERCRIME DETECTION AND PREVENTION STRATEGIES IN USE**

1. What cybercrime threats has your business encountered, and how frequently do they occur?
2. What detection and prevention measures does your organisation currently have in place to deal with cybercrime?
3. How were these measures introduced was it after experiencing a cybercrime incident, through advice from others, or proactively?

#### **SECTION B: EFFICACY OF CYBERCRIME DETECTION AND PREVENTION STRATEGIES**

4. In your experience, how effective have your current cybersecurity measures been in reducing financial losses and protecting your daily operations?
5. Can you describe a specific incident where your security measures either successfully prevented an attack or failed to do so?
6. Which of your current measures do you consider most effective, and why?

#### **SECTION C: CHALLENGES IN IMPLEMENTING CYBERSECURITY MEASURES**

7. What challenges does your business face when trying to put cybersecurity measures in place?
8. How do issues such as load shedding, unreliable internet connectivity and the cost of software affect your ability to maintain consistent protection?

**9.** Do you feel your staff are adequately trained to recognise and respond to cybercrime threats such as fake payment confirmations or phishing attempts?

#### **SECTION D: RECOMMENDATIONS**

**10.** What practical steps do you believe would most meaningfully improve cybersecurity in your business given your current resources?

**11.** What support, if any, would you want from the government, banks or industry bodies to strengthen your defences against cybercrime?

**12.** Is there anything else relating to cybercrime risks or security practices at your business that you would like to share?

End of Interview Guide. Thank you for your time and cooperation.

# Tirivashe Godfrey Chapfuwa

## chapfuwa tirivashe B223869B final

 FI DISSERTATION PLAGIARISM CHECK

### Document Details

Submission ID

trn:oid::2945:394528954

Submission Date

Jun 21, 2026, 4:00 PM GMT+2

Download Date

Jun 21, 2026, 4:11 PM GMT+2

File Name

chapfuwa tirivashe B223869B final .docx

File Size

329.6 KB

44 Pages

14,844 Words

83,697 Characters



Page 1 of 48 - Cover Page

Submission ID trn:oid::2945:394528954



Page 2 of 48 - Integrity Overview

Submission ID trn:oid::2945:394528954

## 9% Overall Similarity

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

### Filtered from the Report

- Bibliography
- Quoted Text

### Match Groups

-  **18 Not Cited or Quoted 6%**  
Matches with neither in-text citation nor quotation marks
-  **10 Missing Quotations 3%**  
Matches that are still very similar to source material
-  **0 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

- 6%  Internet sources
- 1%  Publications
- 7%  Submitted works (Student Papers)

# Tirivashe Godfrey Chapfuwa

## chapfuwa tirivashe B223869B final

 FI DISSERTATION PLAGIARISM CHECK

### Document Details

Submission ID

trn:oid::2945:394528954

Submission Date

Jun 21, 2026, 4:00 PM GMT+2

Download Date

Jun 21, 2026, 11:19 PM GMT+2

File Name

chapfuwa tirivashe B223869B final .docx

File Size

329.6 KB

44 Pages

14,844 Words

83,697 Characters



Page 1 of 46 - Cover Page

Submission ID trn:oid::2945:394528954



Page 2 of 46 - AI Writing Overview

Submission ID trn:oid::2945:394528954

### \*% 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.