BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

EFFECTIVENESS OF CYBERSECURITY MEASURES EMPLOYED BY RETAILERS TO CURB CYBERTHREATS. A CASE STUDY OF SUPERMARKETS IN BINDURA CBD, ZIMBABWE.

BY

Esther Nhopi.

(B212635B)

A DISSERTATION SUBMITTED IN PARTIAL FUFILMENT OF THE REQUIREMENTS FOR THE FINANCIAL INTELLIGENCE OF BINDURA UNIVERSITY OF SCIENCE EDUCATION. FACULTY OF COMMERCE

JUNE 2025

APPROVAL FORM

Title: Effectiveness of cybersecurity measures employed by retailers. A case study of Bindura CBD.

To be completed by the student

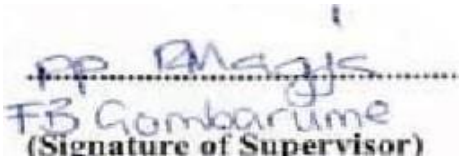
I certify that this dissertation meets the preparation guidelines as presented in the faculty guideline and instructions for typing dissertations.

(Signature of student) **Date**

To be completed by the supervisor

This dissertation is suitable for submission to the Faculty.

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



08/09/25

To be completed by the department chairperson

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

..... 16/9/25

(Signature of chairperson)

RELEASE FORM

NAME OF STUDENT: **ESTHER NHOPI**

DISSERTATION TITLE: **Effectiveness of cybersecurity measures employed by retailers. A case of Bindura retailers.**

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

YEAR GRANTED: **2025**

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

SIGNED **.....**

PERMANENT ADDRESS: **Ndanga Residential**

Stand number 154

Masvingo

TELEPHONE: **+263778437834**

EMAIL: **esthernhopi@icloud.com**

DATE: **...../……../.....**

DEDICATION FORM

This work is lovingly dedicated to my parents, Mom and Dad, whose unwavering support, sacrifices and love have been the cornerstone of my journey. To my brothers, Tinofara and Munyaradzi, thank you for your encouragement, belief in me and constant motivation. To my niece Tendai, and my nephews Michael and Denzel may this achievement inspire you to always dream big and work hard toward your goals. You are all a vital part of my strength and I share this accomplishment with each of you.

ABSTRACT

The rapid digitization of retail operations has exposed supermarkets in Zimbabwe's Bindura Central Business District (CBD) to growing cybersecurity threats. This study investigates the effectiveness of cybersecurity measures implemented by supermarkets in Bindura CBD to mitigate cybercrime. Guided by the Technology Acceptance Model, Routine Activity Theory, and Social Learning Theory, the study adopts a case study approach using both qualitative and quantitative methods. Data were collected through structured questionnaires and interviews from a purposive sample of 60 respondents including till operators, branch managers, and IT professionals. Findings indicate that while employee awareness of cyber threats such as phishing, malware, and hacking is high, existing cybersecurity measures such as antivirus software, firewalls, training programs, and incident response plans vary in effectiveness. Employee training was found to be the most impactful, while incident response planning remains underdeveloped. The study concludes that while basic cybersecurity practices are in place, a more integrated and proactive approach is needed. Recommendations include regular staff training, more robust incident response frameworks, and enhanced use of advanced cybersecurity tools. The study contributes to local cybersecurity knowledge and offers practical guidance for retailers, policymakers, and IT professionals in Zimbabwe's retail sector.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to God Almighty for granting me the strength, guidance, and perseverance to complete this dissertation. I am sincerely thankful to my supervisor, Mr Kunambura for their unwavering support, expert guidance and invaluable feedback throughout the course of this research. Your encouragement and constructive critique helped me stay focused and improve the quality of my work.

I extend my heartfelt appreciation to the management and staff of the supermarkets in Bindura CBD who participated in this study. Your willingness to share your experiences and insights on such a sensitive topic as cybersecurity was essential to the success of this research. Special thanks also go to the Ministry of Higher and Tertiary Education and the Zimbabwean academic community at large, for creating an environment conducive to research and intellectual growth. To my family and friends, thank you for your continuous support, prayers and encouragement during this challenging journey. Your belief in me was a source of constant motivation.

Finally, I acknowledge all the scholars and authors whose work laid the foundation for this study. Your research contributed significantly to the formulation of my ideas and the enrichment of this dissertation.

TABLE OF CONTENTS

List of Figures

List of Tables

CHAPTER ONE

INTRODUCTION

1.0 Introduction

This chapter provides the foundational framework for this research by introducing the study's context, problem statement, objectives, and significance. It establishes the growing vulnerability of supermarkets in Bindura CBD to cyber threats as they increasingly adopt digital technologies, while highlighting the critical gap in understanding the effectiveness of their cybersecurity measures. The chapter outlines the research questions guiding the investigation, defines key terms essential for comprehending the study, and sets boundaries for the research scope while acknowledging inherent limitations. Through this structured introduction, the chapter creates a roadmap for examining how local retailers are responding to cybersecurity challenges within Zimbabwe's unique socioeconomic environment.

1.1 Background of the study

The world has experienced a major technology boom like never before, especially after COVID-19, during which transactions were primarily conducted online. This shift significantly influenced the retail sector, prompting the adoption of new technological strategies and continuous improvements in how the internet is utilized by both individuals and businesses (Donthu & Gustafsson, 2020). Over the past decade, the sharp increase in internet and computer usage has encouraged many businesses to adopt online platforms for their daily transactions—a trend known as electronic commerce or e-commerce (Laudon & Traver, 2022). This transition enables retailers to connect with a broader customer base, extending their market reach beyond physical boundaries across the globe (Statista, 2023). However, despite the wide-ranging benefits of this digital transformation, the rise in internet usage has also been accompanied by a surge in illegal online activities, commonly referred to as cybercrime (Interpol, 2023).

The digital transformation of retail operations globally has created unprecedented cybersecurity challenges for the sector. The retail industry experienced a 43% increase in cyberattacks between 2021 and 2023, with an average data breach costing retailers $3.28 million (Trustwave, 2024). 76% of global retailers have experienced at least one significant cyber incident in the past two years, with point-of-sale (POS) systems and customer databases being primary targets (World Economic Forum, 2024). The COVID-19 pandemic accelerated digital adoption in retail, with e-commerce transactions increasing by 27% globally, further expanding the attack surface for cybercriminals (Retainr, 2023).

Regionally, the African continent has also been deeply affected by cybercrime. The Symantec report (2012) reveals that the number of targeted cyber-attacks in Africa increased by 42%, of which 31% of these attacks, categorized as cyber espionage, and have been said to have affected both large and small businesses. A 2011 Deloitte Touché survey found that financial institutions in Kenya, Rwanda, Uganda, the United Republic of Tanzania and Zambia recorded massive losses of up to $245 million due to cyber fraud (Quarshie & Martin-Odoom, 2012). The study by the International Data Group Connect estimates that, annually cybercrimes cost the South African economy $573 million, the Nigerian economy $200 million, and the Kenyan economy $36 million.

Locally, the Zimbabwean economy has also not been spared in matters regarding cybercrime. The impact seems to be more pronounced within the retail sector, with Nicholas (2014), noting the limited capability of Zimbabwe to deal with cybercrime. According to Reserve Bank of Zimbabwe (RBZ, 2015), Zimbabwe has lost an estimated US$1.8 billion due to cyber related breaches. The study by Mugari et al (2016) and Mugari (2017) have indicated the following forms of cybercrimes as prevalent in the retail sector: card fraud, hacking and/ unauthorized access, viruses and worms, malware, denial-of-service (DOS) attacks and smart phones and mobile application threats. With this background, it is thus imperative to investigate on the effectiveness of the measures that are employed by retailers in Bindura CBD to curb cyberthreats in the retail sector especially in light of the economic challenges in the Zimbabwean economy.

1.2 Statement of the problem

The growing dependence on digital systems and e-commerce platforms within Zimbabwe's retail sector, particularly in supermarkets, has significantly increased the exposure of these businesses

to cybersecurity threats. As supermarket operations become more digitized — from point-of-sale systems to online ordering platforms — they are increasingly targeted by cybercriminals. A study by Mpofu and Maronga (2020) revealed that while many supermarkets in Zimbabwe have implemented basic cybersecurity protocols, these measures are often outdated, underfunded, or poorly enforced, leaving critical systems vulnerable. The impact of these threats is far-reaching, with consequences that include financial losses, operational disruptions, reputational damage, and erosion of customer trust. For instance, a 2021 report by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) noted a 31% increase in reported cybersecurity incidents across commercial sectors, with retail businesses being among the hardest hit. In a context where supermarkets are central to food distribution and employment in urban centers such as Bindura, weak cybersecurity systems pose a threat not only to individual businesses but to local economic stability. Despite these risks, there remains a significant gap in the evaluation of current cybersecurity practices in Zimbabwe's supermarket industry. This study seeks to address that gap by conducting an in-depth assessment of the cybersecurity measures in place within supermarkets operating in Bindura's Central Business District (CBD), with a focus on their effectiveness in mitigating cyber threats and identifying potential areas for strategic improvement.

1.3 Aim of the study

The main aim of this study is to examine the effectiveness of the cybersecurity measures employed by supermarkets in the Bindura CBD, Zimbabwe, in curbing cyberthreats.

1.4 Specific objectives

The specific objectives of this study are:

1. To identify the cybersecurity threats faced by supermarkets in the Bindura CBD, Zimbabwe.
2. To document the cybersecurity measures implemented by supermarkets in the Bindura CBD to mitigate these threats.
3. To evaluate the effectiveness of the cybersecurity measures employed by supermarkets in the Bindura CBD in curbing cyber threats.

4. To recommend strategies to enhance cybersecurity systems of supermarkets in the Bindura CBD, Zimbabwe

1.5 Main research questions

The main research questions guiding this study are:

1. What are the cybersecurity threats faced by supermarkets in the Bindura CBD, Zimbabwe?
2. What cybersecurity measures have supermarkets in the Bindura CBD implemented to mitigate these threats?
3. How effective are the cybersecurity measures employed by supermarkets in the Bindura CBD in curbing cyberthreats?
4. What recommendations can be made to enhance cybersecurity systems of supermarkets in the Bindura CBD, Zimbabwe? Adjust these in line with the comments above

1.6 Significance of the Study

This study holds significant importance for several key stakeholders:

1.6.1 Theory development

The study will contribute to the body of knowledge in the field of cybersecurity and its application in the retail sector. The findings can be used by universities to develop more relevant and practical curricula, ensuring that students are equipped with the necessary skills and knowledge to address the cybersecurity challenges faced by the retail industry.

1.6.2 Policy makers

The study's recommendations can inform policymakers in Zimbabwe, particularly those responsible for developing and implementing cybersecurity regulations and guidelines. This information can help to enhance the country's overall cybersecurity posture and provide a framework for businesses, including supermarkets, to better protect their digital assets and customer data.

1.6.3 To Retailers

The study's findings will be of great interest to supermarket owners, managers, and other stakeholders in the retail industry. The insights gained can help these stakeholders to better understand the cybersecurity threats they face, evaluate the effectiveness of their current measures, and make informed decisions to strengthen their cybersecurity posture and protect their businesses from the devastating consequences of successful cyber-attacks.

1.7 Study Assumptions

This study is based on the following assumptions:

1. Supermarkets in the Bindura CBD, Zimbabwe, have implemented various cybersecurity measures to protect their digital assets and customer data.
2. The cybersecurity measures employed by supermarkets in the Bindura CBD are less effective
3. Participants provide accurate and truthful information about the cybersecurity measures and challenges faced by their oganisations.

1.8 Delimitations of the study

The study was mainly focusing on identifying the cybersecurity measures and also analyzing the effectiveness of cybersecurity measures in the retail industry. It was only restricted to Bindura CBD. The researcher only worked with 60 people who responded to the survey and this includes, till operators, branch managers and also computer engineers. The study period of this research was from June 2024 to the present. Include theoretical and methodological delimitations here as well as time.

1.9 Limitations of the study

it was hard for the researcher to obtain quality information she required due to privacy and confidentiality. It was not easy to research more factual data in the fear of company's privacy policy and confidentiality however; the researcher anonymized all identifying information she used real data without compromising privacy. . The companies were not able to release some of the confidential information on how they deal with cyberattacks in the fear of being giving out information which might also be used by the attackers to get into their computers. To overcame this the researcher highlighted how the participation may help the companies to improve their own

cybersecurity by contributing to broader knowledge. Another limitation the researcher faced was absence of transparency which limits the depth of qualitative analysis and to overcame this the researcher conducted interviews under non-disclosure agreements.

1.10 Organisation of the study

The research will be as follows, the first chapter involves introduction, background of the study, problem statement, objectives, research questions, significance of the study, assumptions, delimitations and limitations of the study. Chapter two focuses on literature review and chapter three is all about research methodology. Chapter four is going to consist of data presentation, analysis and discussion. Finally, chapter five will cover the summary of the research as well as the conclusion and recommendations.

1.11Chapter summary

This chapter dwelt much on the background of the study, statement of the problem, research objectives, research questions, assumptions, delimitations and limitations of the study. Chapter 2 is going to focus on theoretical and conceptual frameworks as well as empirical evidence and gap analysis.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter reviews literature on cybersecurity measures in retail, with a focus on supermarkets. It establishes a theoretical and empirical basis for studying cybersecurity effectiveness in Bindura CBD, Zimbabwe. Key terms are defined, followed by analysis of theoretical and conceptual frameworks. An empirical review adopts a funnel approach, covering global to national perspectives. Research gaps are identified and linked to the current study's focus. The review situates the study within existing scholarship and highlights its unique contribution.

2.1 Conceptual framework

2.1.1 Conceptualization Cybersecurity

Cybersecurity in the retail context refers to the practices, technologies, and processes designed to protect digital systems, networks, and data from unauthorized access, attacks, and damage (Nalini and Sheela, 2022). According to Gao et al. (2020), cybersecurity encompasses measures to ensure the confidentiality, integrity, and availability of information systems and data, particularly those containing sensitive customer and transaction information commonly found in retail environments. Khan et al. (2021) expand this definition to include organizational policies, technical controls, and human-centered approaches aimed at protecting retail digital infrastructure from increasingly sophisticated cyber threats.

In the supermarket context specifically, Kara and Karabiyik (2022) define cybersecurity as the protection of point-of-sale systems, inventory management software, customer databases, and digital payment mechanisms from malicious actors seeking to exploit vulnerabilities. This definition recognizes the unique digital ecosystem of supermarkets that combines multiple technologies with varying security requirements. As noted by Srivastava and Gupta (2023),

effective cybersecurity in retail environments must balance robust protection with operational efficiency, ensuring that security measures do not impede business functions or customer experience.

2.1.2 Cyber threats

Cyber threats refer to potential or actual malicious activities aimed at compromising digital systems, stealing data, or disrupting operations (Sharma et al., 2022). In the retail context, cyber threats have evolved from simplistic attacks to sophisticated, targeted operations often conducted by well-organized criminal groups. According to Marufu and Sanyamuwera (2023), retail-specific cyber threats include point-of-sale malware, payment card skimming, supply chain attacks, ransomware, and social engineering attacks targeting employees. Tsakalidis et al. (2022) categorize retail cyber threats into external threats (from outside attackers), internal threats (from employees or contractors), and hybrid threats combining both vectors. Their framework emphasizes the multi-dimensional nature of threats facing retailers. For supermarkets specifically, Ibrahim et al. (2021) identify priority threats as those targeting payment systems, customer personal information, and operational technology that could disrupt business continuity. This aligns with findings by Ncube and Sibanda (2021) who note that Zimbabwean retailers face threats particularly focused on payment fraud and data theft, reflecting the specific socioeconomic context.

2.1.3 Retail/Retailers

Retailers are businesses that sell goods directly to consumers through various channels including physical stores, online platforms, or a combination of both (Roggeveen and Sethuraman, 2020). Within this broader category, supermarkets represent a specific retail format characterized by self-service, wide product selection, and increasingly digitized operations (Mukwevho and Jacobs, 2022). According to Chinyoka and Vutete (2023), modern supermarkets in Zimbabwe have evolved from traditional grocery stores to complex operations incorporating various digital technologies including point-of-sale systems, inventory management software, surveillance systems, and electronic payment processing. Dhliwayo and Makiwa (2022) further distinguish supermarkets in the Zimbabwean context as formal retail establishments with computerized operations that process significant volumes of transactions and customer data, creating unique cybersecurity requirements compared to informal or traditional retail formats. This distinction is

important for understanding the specific cybersecurity challenges and requirements of supermarkets in Bindura CBD.

2.2 Cybercrimes prevalent in the retail sector

2.2.1 Mobile payment fraud

Mobile payment services enable transactions via mobile devices, with specific apps developed to allow users to pay for goods and services directly through smartphones (FinCoNet, 2016). These services—such as mobile commerce and mobile business—have simplified financial transactions, providing vital support to Zimbabweans amid ongoing liquidity challenges by allowing them to transact without relying on banks (Kufandirimbwa et al., 2013). Examples of such systems include EcoCash, Cellcard, eMali, Textacash, Cybercash, Mobile Banking, One Wallet, Skwama, and Mobile Moola (ibid., p. 93). However, around 63% of these platforms reportedly lack adequate security software to protect users' devices (Mugari, 2016). According to the 2018 Mobile Payments and Fraud Report, inconsistent security standards among providers have introduced significant risks for customers, particularly when proper safeguards are not implemented.

2.2.2 Card fraud

The expansion of digital payment systems in the retail sector has led to a significant rise in card fraud involving debit cards, credit cards, VISA, and stored-value cards. While these systems offer various advantages, their effectiveness in developing countries hinges on the establishment of proper network infrastructure, regulatory frameworks, consumer awareness, and local competition (Kathirvel, 2013). Card fraud, a form of identity theft (Gilsinan et al., 2008), involves using stolen banking information to obtain goods or services under the cardholder's identity (Gottschalk, 2009). This may involve forging new cards with stolen data, physically stealing cards, retrieving unsecured card details, or using skimming devices. In some cases, insiders with access to sensitive information may sell it to fraudsters. Chaudhary, Yadav, and Mallick (2012) classify card fraud into offline fraud, which uses stolen physical cards, and online fraud, conducted through digital channels without the cardholder present. Barker et al. (2008) also highlight counterfeit card production, where fraudsters create fake cards using account data, often aided by employees who help extract magnetic strip or chip information.

2.2.3 Hacking

Wiggins (2002) describes a hacker as an individual with the technical skills to access secure computer systems, typically driven by curiosity and the desire to test their abilities. However, when such access is gained without permission, it becomes unauthorized intrusion (Payne, 2013). While the internet offers a global platform for commerce and connectivity to law-abiding users, it also provides criminals with opportunities to exploit systems with relatively low risk, thereby encouraging cybercrime (Laudon, 2009:271). Closely related to hacking is cracking, which involves deliberately breaching systems to cause damage or disruption (Wiggins, 2002). According to Sinrod and Reilly (2000), crackers can be categorized into external attackers, who seek to sabotage networks for personal gratification, and internal attackers—often disgruntled employees—who misuse their insider knowledge to harm the organization.

2.2.4 Phishing

Isaac, Chiong, and Jacob (2006) describe phishing as the practice of sending deceptive emails or creating fake websites designed to trick individuals into unknowingly providing personal information, which can then be used for identity theft—fraudulently using someone else's identity for financial gain. The primary aim of phishing is to acquire sensitive personal data, particularly financial details, by first gaining the victim's trust. This is typically done by making the communication appear to come from a legitimate source, prompting recipients to click on malicious links that redirect them to counterfeit websites. There, they are misled into sharing personal information such as names, addresses, and banking credentials.

2.3 Impacts of cybercrime on businesses

2.3.1 Loss of intellectual property leading to a reduction in competitive edge

Cybercrime and data breaches significantly disrupt business operations in the market. When intellectual property such as business strategies, marketing plans, or expansion initiatives are compromised through hacking, it leads to a loss of competitive advantage (Clickatell, 2018), as confidential strategies may be exposed to competitors or other market threats. Such breaches can render business plans ineffective, and if sensitive information falls into the hands of rivals, it can cause substantial harm to a company's growth and revenue potential.

2.3.2 Financial losses

Despite increased security awareness, crime can leave a company in severe financial distress (Paganini, 2012). Cybercriminals often pursue high-value targets, resulting in significant losses for businesses. These may include the loss of funds or assets (including intangible assets like goodwill), theft of devices containing sensitive company data, and repair or recovery expenses (ICSPA, 2013). While cybercriminals may gain substantial profit from such attacks, the affected businesses endure considerable financial setbacks.

2.3.3 Reputational damage

Wright (2015) states that cyberattacks can severely damage a company's reputation due to the exposure of sensitive commercial information, the high costs of responding to data breaches, and the potential for legal penalties, such as fines. Customers are unlikely to engage with a business that has a tarnished reputation, especially if it has failed to protect consumer data and confidentiality. According to Laudon (2009), for consumers to trust and feel confident purchasing from a retailer, strong security measures must be in place, including verification of the seller's legitimacy, data privacy, confidentiality, non-repudiation, and a solid reputation. As Mugari (2016) notes, negative reviews and comments circulating on social media can further erode the company's public image.

2.3.4 Increased costs

Due to IT security expenditures, the businesses will experience an increase in their total costs. According to McAfee (2013), IT costs encompass the additional expenditures associated with securing a company's information technology infrastructure. These include the implementation and maintenance of cybersecurity tools such as firewalls, antivirus software, intrusion detection systems, data encryption, and regular security audits. Furthermore, businesses may incur costs for cyber insurance policies, which provide financial protection against losses resulting from data breaches or system compromises. In the aftermath of a cyberattack, recovery costs can be substantial covering data restoration, system repairs, forensic investigations, legal consultations, regulatory compliance measures, and even public relations efforts to repair reputational damage. These growing IT expenses highlight the importance of proactive cyber defense strategies in today's digitally driven business environment.

2.4 Measures to mitigate cybercrime in the retail sector

2.4.1 Employee training

When employees have a clear understanding of the nature of cybercrime, how it is carried out, and its potential consequences, they are more likely to avoid participating in such activities (Bamfield, 1998). Regular workshops and training sessions help to provide staff with essential knowledge and awareness related to criminal behavior.

2.4.2 Deployment of Antivirus Software and Firewalls

According to Meade (2019), antivirus software serves as a key cybersecurity tool commonly utilized by individuals and organizations to detect, scan, and block potentially harmful files or programs from infiltrating computer systems. Firewalls, as described by McAfee, can be either software-based or hardware devices (such as routers) that monitor and control incoming internet traffic during browsing. They function by filtering data, allowing only the requested and legitimate information to pass through while eliminating any potentially harmful or irrelevant content that could pose risks to users online (Laudon, 2009).

2.4.3 Data Encryption

Data encryption refers to the process of converting information into a coded format to ensure its confidentiality (Kahn, 1967). This involves transforming readable data, or plain text, into an unreadable format known as cipher text, which can only be interpreted by the intended sender and recipient (Laudon, 2009). By encrypting data transmitted over the internet, unauthorized third parties are prevented from accessing the information, thereby securing communication and protecting data across all endpoints, while allowing access solely to the intended users (Symantec, 2015).

2.4.4 Use of a Two-Step verification method

According to Clickatell (2018), the two-step verification method offers an extra layer of protection, that which does not only require the use of a password and a username only, but also does require another one-time pin (OTP). An OTP is such one that is sent on either the mobile phone or email mailbox of the authentic user of the account after inputting user credentials, which changes or expires over a period of at least one hour. Therefore, in order for the cyber criminals to access the

account, they must have within their reach the original user's credentials and the authorized user mobile phone or address book for full access, which in most cases is very rare.

2.5 Effectiveness of the measures to mitigate cybercrime in the retail sector

2.5.1 Employee Training

Training employees is one of the best ways to fight cybercrime in the retail industry. When workers learn about cyber threats, how they happen and the problems they can cause they are less likely to become victims or take part in these activities (Bamfield, 1998). Knowledgeable staff are more capable of spotting phishing attempts, social engineering tricks and strange online behaviors that might signal a security issue (Hadnagy, 2018). Regular training sessions and awareness programs help employees make safe choices in their daily tasks and improve their ability to follow cybersecurity rules. This is especially important for frontline employees who manage customer data and financial transactions, as they gain valuable skills in identifying and reporting suspicious activities (Verizon, 2023). However, the success of this training relies heavily on how often and how well it is conducted. If the training is not updated regularly to address new threats, employees may forget what they learned and revert to unsafe practices. Therefore, ongoing engagement and regular evaluations are crucial to keep the training effective over time (ENISA, 2021).

2.5.2 Installing Antivirus Software and Firewalls

Installing antivirus software and firewalls is a crucial step in defending against cybercrime in the retail sector. Antivirus programs play a fundamental role in identifying, scanning and eliminating malicious software, including viruses, ransomware, spyware, and trojans that may attempt to compromise organizational systems (Meade, 2019). These programs are particularly effective in automatically detecting known threats and preventing them from executing harmful actions. Firewalls, whether software-based or hardware-based serve as gatekeepers that monitor and control the flow of incoming and outgoing network traffic. They achieve this by enforcing predefined security rules, blocking unauthorized access and filtering suspicious content from reaching internal systems (Laudon & Laudon, 2009; McAfee, 2023). However, their effectiveness is not absolute. Advanced persistent threats and zero-day attacks can sometimes bypass these defenses (Symantec, 2015). Moreover, poorly configured firewalls may

inadvertently allow malicious traffic, making regular updates and proper management critical. Therefore, while antivirus software and firewalls are vital, they should be used in combination with other measures such as employee training, encryption, and multi-factor authentication to establish a comprehensive and resilient cybersecurity posture.

2.5.3 Data Encryption

Data encryption is a highly effective method for protecting sensitive information in the retail industry. This process involves converting readable data (plaintext) into an unreadable format (ciphertext) using cryptographic algorithms, ensuring that only authorized individuals with the correct decryption key can access the original information (Kahn, 1967). Encryption is especially critical for securing customer personal details, payment information, and confidential business communications, both when transmitted across networks and when stored in databases (Laudon & Laudon, 2009). Even if cybercriminals intercept encrypted data, it remains indecipherable without the appropriate keys, thereby reducing the risk of data leakage or exploitation (Symantec, 2015). However, the overall effectiveness of encryption depends heavily on the secure management of encryption keys. If keys are lost, mishandled, or compromised, the encrypted data may become either inaccessible or vulnerable (NIST, 2020). Furthermore, encryption processes can demand significant computing resources, which may impact system performance if not properly optimized. Despite these challenges, encryption remains a cornerstone of data protection strategies in modern retail operations.

2.5.4 Implementing a Two-Step Verification Process

Using a two-step verification process, also known as two-factor authentication (2FA), significantly strengthens security measures by requiring more than just a username and password. This method typically involves an additional authentication factor, such as a one-time pin (OTP) sent to a registered mobile device or email address. This extra layer of security greatly reduces the likelihood of unauthorized access, as cybercriminals would need not only the login credentials but also access to the second authentication factor, which is generally beyond their reach (Clickatell, 2018). This makes 2FA an effective safeguard against common threats such as credential stuffing, phishing attacks, and brute-force login attempts (Microsoft, 2019). Despite its benefits, two-step verification is not without limitations. Sophisticated attacks such as SIM swapping or phishing for OTPs can still compromise accounts if users are not vigilant (Krebs,

2020). Additionally, the extra step may be viewed as inconvenient by some users, which could hinder widespread adoption unless the process is user-friendly and streamlined. Nonetheless, when properly implemented, 2FA remains a vital component of a modern, multi-layered cybersecurity strategy.

2.6 Theories in cybercrime

2.6.1 Routine Active Theory

Routine Activity Theory, created by Cohen and Felson in 1979, highlights that crime happens when three things come together at the same time and place a motivated offender, a suitable target and the lack of a capable guardian. In retail cybersecurity, "motivated offenders" refer to cybercriminals looking to make money, while "suitable targets" are customer information, credit card details and e-commerce sites. The "capable guardian" includes protective tools such as antivirus software, firewalls, encryption, and alert employees (Reyns, 2013). Retail businesses that depend on online transactions or digital customer interactions face a higher risk of attacks. For instance, retail workers who manage payment systems or online accounts can act as guardians, but if they lack training, they can also create weaknesses. Eck's (2003, 2010) crime triangle supports this idea by stressing the importance of looking at the offender, target, and environment. Poor system setups, inadequate employee training, or old software can make it easier for crimes to happen. Recognizing these patterns allows retailers to create effective cybersecurity strategies that stop the three crime elements from coming together

2.6.2 Social Learning Theory

Social Learning Theory, introduced by Edwin Sutherland, posits that behavior is acquired through interaction with one's environment via observational learning, as behavior and environment are interrelated (Edinyang, 2016). Nabavi (2014) explains that learning takes place within social contexts by observing and imitating the actions and outcomes of others. Ackers (1985; 1991) further notes that early, frequent, and prolonged associations have a stronger influence on shaping behavior. When individuals associate with those who engage in criminal activities, they are more likely to adopt similar behaviors through social interaction (Hansen, 2009), potentially forming cybercriminal networks that target individuals, organizations, and vulnerable institutions. Rational Choice Theory (RCT) proposes that cybercrime happens when

individuals make deliberate choices after considering the risks and benefits involved (Wittek, 2003). People, whether they are insiders or outside hackers, act as rational beings who compare the advantages of accessing sensitive information or disrupting services with the potential consequences, such as legal punishment, losing a job or damaging their reputation (Paternoster & Simpson, 1996; Ogu, 2013). In the realm of retail cybersecurity, this theory helps explain why measures like access monitoring, surveillance and legal repercussions can effectively deter threats. For instance, using two-step verification or conducting regular system audits increases the perceived costs of attacking a system. Employees who are thinking about unethical actions might reconsider if they believe detection is likely or that the penalties would be significant. Likewise, external attackers may choose to bypass well-protected systems in favor of easier targets.

2.6.3 Technology Acceptance Model (TAM)

Technology Acceptance Model (TAM) was created by Davis in 1989; TAM suggests that the main reasons people accept technology are how useful they think it is and how easy it is to use. For cybersecurity to work well in retail, tools like encryption software, two-factor authentication and antivirus programs need to function effectively and also be seen as practical and easy to use by both employees and managers. If retail workers find these technologies too complicated or bothersome, they might avoid using them, which can weaken overall security (Venkatesh & Davis, 2000). On the other hand, when users see that security tools make their jobs easier and protect important information without causing much disruption, they are more likely to use them. TAM also highlights the importance of ongoing cybersecurity training, suggesting that continuous education can boost users' confidence in using these tools. This helps create a stronger security culture, encourages better online practices and decreases human errors, which are often the weakest part of cybersecurity

2.7 Empirical Evidence

Cybersecurity threats in the retail sector have grown significantly with the widespread adoption of information and communication technologies (ICTs). Mugari (2016), in his study on Eastgate Mall in Harare, found that Zimbabwean retail businesses were heavily reliant on mobile payment systems, which exposed them to cyber threats. Common threats included virus infections, hacking and network breaches, while denial of service (DoS) attacks and card fraud were less

prevalent. Mawunge (2017) similarly identified phishing and the spread of computer viruses as major cyber threats affecting retail businesses in Harare CBD. In the financial sector Mugari, Gona, Maunga, and Chiyambiro (2016) noted unauthorized access and identity theft as common threats, with 75% of respondents indicating that unauthorized access occurred within their institutions. Globally, studies echo similar patterns.

The International Cyber Security Protection Alliance (ICSPA, 2014) reported that 69% of Canadian businesses experienced cyber-attacks, with malicious code, phishing, and social engineering being the most common. Balan et al. (2017) in the United States found a high prevalence of cyber-attacks due to low awareness among employees, while Das et al. (2013) reported that spear phishing and frequent website attacks were widespread in India and other countries. These findings collectively demonstrate that supermarkets in Bindura are likely vulnerable to a range of cybersecurity threats, particularly malware, phishing, hacking, and identity theft, given similar trends in urban centers across Zimbabwe and internationally.

Mugari (2016) observed that Zimbabwean retailers were unprepared to handle cyber risks, leading to increased vulnerability. This unpreparedness has financial implications, as shown in Mawunge's (2017) study, which found that cybercrime had caused substantial monetary losses to Harare-based retail businesses. International research confirms these concerns. Balan et al. (2017) noted that American businesses incurred considerable financial losses due to cyber-attacks. Similarly, Paoli et al. (2017) reported that Belgian businesses faced income losses resulting from unauthorized IT system access.

KPMG (2015) revealed that approximately 80% of cyber breaches in small UK businesses were due to ignorance, often damaging business reputation and customer trust. In Ghana, Duah and Kwabena (2015) highlighted that cybercrime hindered the development of electronic business by creating fear and reducing adoption. Boateng et al. (2011) also found that many cybercrime incidents remained undetected, affecting both operational efficiency and public confidence. These studies indicate that supermarkets in Bindura CBD are at risk of experiencing similar operational disruptions, financial losses, and reputational damage if cyber threats are not effectively managed.

Mugari et al. (2016) reported that Zimbabwean financial institutions rely on basic cybersecurity measures such as firewalls, frequent software updates, and employee training. Similarly, Mugari

and Olutola (2021) recommended internal control mechanisms such as employee lifestyle audits, job rotation, and close supervision to curb card-related fraud in Zimbabwe's retail sector. Mawunge (2017) noted that antivirus software was the most widely used defensive tool among retail businesses in Harare CBD.

However, the effectiveness of these basic measures remains questionable in the face of evolving cyber threats. Globally, organizations have implemented a broader array of strategies. Balan et al. (2017) and ICSPA (2014) advocated for data encryption and secure login systems, including password protections. KPMG (2015) emphasized the importance of using unique passwords, providing cybersecurity training, and ensuring encryption on all devices. Frank and Odunayo (2013) recommended promoting cyber ethics, educating staff, and forming IT forums to raise awareness and improve cybersecurity culture. While many of these strategies are yet to be widely adopted in Zimbabwe's supermarket sector, they provide a valuable blueprint for improving local practices.

Mugari and Olutola (2021) stressed the need for robust internal controls, including employee vetting and enhanced supervision. ICSPA (2014) and KPMG (2015) recommended awareness programs, regular training, and the use of advanced tools such as encryption software and intrusion detection systems. Frank and Odunayo (2013) highlighted the role of cyber ethics and education in shaping proactive organizational behavior. The successful adoption of these strategies in Bindura supermarkets would require context-specific adaptation, considering resource constraints and staff capacity. However, the empirical evidence strongly suggests that improved employee training, investment in security technologies, and a strong organizational culture around cybersecurity can significantly reduce vulnerability.

2.7.1 Gap analysis

The previous literature review highlights several important gaps that this study aims to fill. While existing research from Zimbabwe, including works by Mugari (2016), Mugari et al. (2016), and Mawunge (2017), provides valuable insights into cybersecurity in the retail and financial sectors, it mainly concentrates on larger cities like Harare. There is a significant lack of studies focusing on smaller towns like Bindura CBD. This limitation in geography and context reduces the relevance of current findings for this particular area, which may have unique economic and technological factors at play.

Moreover, much of the reviewed literature looks at the broader retail or financial sectors but pays little attention to supermarkets a distinct sub-sector that heavily depends on digital tools such as point-of-sale systems, mobile payments and inventory management software. As a result, the specific cybersecurity challenges faced by supermarkets have not been thoroughly examined. Additionally, many local studies were conducted before the COVID-19 pandemic. With the rapid increase in digitization during and after this period, including more widespread use of mobile payments and e-commerce, today's cybersecurity issues in supermarkets may have changed significantly and are not reflected in earlier research.

Furthermore, while many studies suggest solutions like antivirus software, firewalls, and employee training programs, they often do not critically assess how effective these measures are in real-world settings with limited resources like those found in Bindura. There is also a lack of emphasis on how organizational culture, employee behavior, and cyber ethics play a role factor that international research by Frank and Odunayo (2013) and KPMG (2015) has identified as crucial for maintaining cybersecurity resilience. This gap represents a theoretical shortcoming in understanding how behavioral and cultural elements contribute to cybersecurity vulnerabilities.

Most of the existing literature focuses on traditional cyber threats like viruses, phishing, and credit card fraud. It pays little attention to new dangers such as ransomware, insider attacks, and threats driven by artificial intelligence. These newer threats might already be affecting supermarket operations but often go unreported because people are not aware of them or fail to report them. As a result, there is not enough information available for supermarkets to prepare for and respond to these challenges effectively. This study aims to fill these gaps by looking into cybersecurity threats and ways to counter them specifically in supermarkets located in Bindura CBD. By doing this, it will provide relevant and updated insights that are important for the industry.

2.8 Summary of the previous studies

The above studies included those taken from developed countries (United States of America, Belgium) and developing countries (Zimbabwe, Zambia, Nigeria). Those conducted by Ishmael Mugari affirmed liquidity crisis stimulated the prevalence of cybercrime in many developing countries. In support to the above, Duah and Kwabena (2015) indicated that the challenges faced on eradicating it and its progression with time makes it more complex to curb. Shilpa Balan, Joseph Otto, Edgar Minasian and Arun Aryal (2017), together with that of KPMG (2015) also highlighted

a lack of knowledge, ignorance and negligence as major contributors to cybercrime. Almost all of these studies affirmed that all businesses in every location are at greater risk of cybercrimes. However, studies of those like Shilpa Balan, Joseph Otto, Edgar Minasian and Arun Aryal (2017) and Letizia Paoli, Jonas Visschers, Cedric Verstraete and Elke Van Hellemont (2017) dissent to the problems mentioned by previous studies and this is due to economic and structural differences.

The modus operandi of cybercrimes in developed countries are not necessarily the same that in developing countries, and the main contributors may be technological differences, knowledge concerning the crime and security measures, hence may not address those challenges pointed out in this study. The ease with which cybercrime crosses national borders, irreconcilable differences between national legal frameworks, and deceptions employed by cyber criminals obstruct categorization and prevents crime fighters from interrogating suspects and collaring offenders (Brown, 2015). This means how one country manages cybercrime may differ in what others also do, mostly in terms of lenience and strictness and how the economic structure operate and are being managed. Availability of resources is also a contributor. Therefore, the researchers' opinion will be on studies, mainly those from within Zimbabwe to minimize irrelevance and maximize applicability.

2.9 Chapter summary

In a nutshell chapter 2 was centered on reviewing other literature in relation to the researcher's research. It also took note of conceptual framework, previous studies with correlation to this one. The researcher also made use of theories to give sense of direction and a brief summary of the previous studies. The next chapter focuses on research methodology.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter centers on examining the methodologies and strategies employed to investigate the effects of cybercrime on the retail sector. It outlines the research design and methods, data collection tools, sampling strategies and techniques used for gathering information.

3.1 Research design

Kirshenblatt and Barbara (2006) describe research design as the comprehensive plan that connects all components of a study in a logical and consistent way to ensure the research problem is effectively addressed. It serves as a blueprint for data collection, measurement, and analysis. It may take various forms, such as scientific, historical, descriptive, or case study approaches. For this particular research, the case study method was employed.

3.1.1 Justification of the research design

To gain a deeper understanding of the research problem, the study adopted a case study methodology, concentrating specifically on retail stores in Bindura. Robson (2002) defines a case study as a research strategy involving a detailed empirical examination of a particular phenomenon within its real-life context, utilizing multiple data sources. The study incorporated both primary and secondary data to gather, analyze, and evaluate information thoroughly.

The researcher chose the case study method due to its cost-effectiveness and its ability to facilitate a comprehensive analysis of documents and allow for prolonged observation of events. This approach provided valuable insights into the causes, processes, and context of the issue under investigation, while also laying the groundwork for potential future research on a larger scale. Moreover, the case study design allowed the integration of diverse data collection methods, which

supported the verification and validation of findings. As it reflects real-world situations, the case study offered an authentic representation of the research outcomes.

3.2 Target population

Christiane (2005) describes a population as the complete group of elements from which samples are selected. Collis and Hussey (1993) further explain that it encompasses all individuals, objects, or events the researcher aims to examine. In essence, a population refers to a specific group made up of distinct units relevant to the study. This research focuses on the town of Bindura, located in the Mazowe Valley within Zimbabwe's Mashonaland Central province, approximately 88 kilometers northeast of Harare. The town's central business district (CBD) hosts various retail outlets, including those selling household items, groceries, clothing, electronics, motor vehicle accessories, farming tools, and food products.

3.3 Sample population

Sample size which was chosen added up to 60. The researcher chose a minimum number of 60 respondents to represent the whole population for an ideal sample which will provide more realist, measurable and accurate information. This is associated with no or less biased results during the research. The researcher gave out 50 questionnaires to till operators and other workers(employees) from different retail shops, she also interviewed 5 IT engineers and the remaining 5 to the branch managers making the 60 in total. The selection aimed to include diverse roles within the supermarkets to gain comprehensive understanding of cyber security practices and challenges.

3.4 Sampling techniques

Trachoma (2006) defined sampling as the process of selecting specific unitsuch as individuals or organizations—from a larger population of interest, with the goal of studying the selected sample to draw conclusions that can be generalized to the entire population. Given the impracticality of studying an entire large population, Welman and Kruger (2001) emphasized the importance of using a sample to represent the broader group. In this research, both stratified and purposive sampling techniques were employed.

3.4.1Stratified Random Sampling

According to Showkat and Parveen (2017), stratified random sampling involves dividing the population into distinct subgroups or strata based on specific characteristics, and then randomly selecting a set number of units from each group. In this study, retail employees were grouped by department such as till operators, procurement, sales, and accounting based on the differing nature of their roles and perspectives. Participants were then randomly selected from these groups to ensure the sample reflected the population's diversity.

3.4.2Purposive Sampling

Purposive sampling involves the deliberate selection of participants based on the researcher's judgment and the specific requirements of the study. The researcher applied expert sampling a type of purposive sampling to select individuals with knowledge of cybersecurity in the retail sector. The aim is to gather detailed and relevant data from knowledgeable individuals. For this research, the sample included five branch managers and two Information Technology (IT) professionals, all chosen for their ability to provide valuable insights into the topic through the interview.

3.5 Research instruments

The researcher only used two data collection methods as her main research instruments during the study. These instruments are, questionnaires and interviews.

3.5.1 Questionnaires

Best and Khan (2003) describe questionnaires as written tools consisting of structured questions designed to gather data for analysis. Aakker (1995) similarly defines them as a collection of questions aimed at capturing participants' opinions on a specific topic. In this study, questionnaires served as the primary data collection method and were distributed to all selected participants. The questionnaire begins with an introduction or cover letter that explains the purpose of the survey, assures confidentiality and provide instructions on how to complete it. There are also demographic questions which help to categorize respondents. This is followed by main questions which is the core of the questionnaire. This section consists of open and closed questions as well as scale questions. The questions are organized into sections to make the questionnaire logical and easy to follow. Then lastly there is the closing section, this includes thanking the respondents for their time.

Advantages of Using Questionnaires

The use of questionnaires in this study presented several advantages that enhanced the data collection process. They were easy to distribute and generally yielded quick responses, making them efficient for reaching a broad range of participants. Some respondents also reported gaining new insights into cybercrime while completing the forms, suggesting that the questionnaires served both research and educational purposes. Anonymity and confidentiality were preserved, which encouraged open and honest responses, especially when dealing with sensitive topics. Additionally, questionnaires were cost-effective, requiring minimal resources beyond the printed forms. They allowed participants to complete them privately and at their own pace, which reduced bias and external pressure.

Disadvantages of Using Questionnaires

One major limitation was the researcher's inability to probe deeper into responses, which sometimes led to incomplete or superficial answers. The questions had to be straightforward, as not all participants fully understood the content without further explanation. Some questionnaires that were distributed for completion at the participants' convenience were never returned, negatively affecting the response rate. There was also noticeable resistance from high-ranking individuals, particularly those with tight schedules, who were less willing to participate. To address these challenges and improve the reliability of the data, the researcher prioritized distributing questionnaires to interested participants and conducted follow-ups to ensure timely and relevant feedback.

3.5.2 Interviews

Collins and Hussey (2000) define interviews as a method of data collection involving direct questioning of selected individuals to explore their views, opinions, and motivations. Interviews were used in this research to supplement the limitations of written questionnaires, with a focus on gathering insights from randomly selected management staff.

Advantages of Interviews

Interviews offered several advantages that greatly enriched the data collection process in this study. One of the key strengths was the flexibility they provided, as questions could be rephrased or

clarified during the conversation to match the respondent's level of understanding. This adaptability ensured that participants were fully engaged and that their responses were as accurate and comprehensive as possible. Additionally, interviews allowed the researcher to observe non-verbal cues such as facial expressions, tone, and body language, which provided valuable insights into the participants' true feelings and attitudes insights that would not have been captured through written responses alone. The interactive nature of interviews also enabled the researcher to ensure that all key questions were addressed, while immediate feedback and follow-up questions helped to probe deeper into certain issues. This dynamic exchange fostered richer, more detailed responses, making interviews an effective tool for gathering in-depth information.

Disadvantages of Interviews

The interview process also presented some challenges. It was time-consuming, as building rapport and trust with participants required careful and often lengthy preparation before any data could be collected. Furthermore, concerns about confidentiality and privacy occasionally limited how much participants were willing to disclose, especially when discussing sensitive topics related to cybersecurity. To address these issues, the researcher made a deliberate effort to create a safe and respectful environment by clearly explaining the purpose of the study and assuring participants of the confidentiality of their responses. This approach helped to build trust and encouraged honest, meaningful dialogue throughout the interview process.

3.6 Data Collection Procedure

The researcher personally administered the questionnaires to participants involved in the retail sector. These included management, employers, and company employees. Questionnaires were collected once the respondents had completed them. Additionally, interviews were conducted with company directors, managers and ICT professionals. During the interviews, the researcher recorded the participants' responses and perspectives.

3.7 Validity and Reliability

Validity and reliability are crucial parts of a strong research design. Validity means how well a research tool measures what it is supposed to measure (Weiner, 2007). In this study, the researchers made sure the questionnaires and interview guides matched the research goals and the existing literature on cybersecurity in retail. To improve content validity, they asked for advice from

academic supervisors and industry experts while creating these tools. Additionally, they only gave questionnaires to people working in relevant fields, such as operators, IT staff and branch managers, whose jobs are closely related to cybersecurity issues. This approach helped ensure that the data gathered accurately represented the experiences and views of those directly impacted by cybersecurity concerns in supermarkets located in Bindura CBD.

Reliability, according to Weiner (2007), refers to how consistently a measurement tool produces stable results when used under similar conditions. To make sure their study was reliable, the researchers followed standard procedures for distributing questionnaires and conducting interviews. Every participant received the same questions, and interviews were done following a consistent method to reduce bias from the interviewer. They also ran a pilot test with a small group to check how clear and consistent the questionnaire items were. Based on feedback, they made necessary changes before using the final version of the tools. These steps helped ensure that the tools would provide consistent results, thus improving the overall reliability of the study.

3.8Data Presentation and Analysis

Qualitative data were analyzed using both deductive and inductive methods (Spencer, Ritchie, & O'Connor, 2004; Lathlean, 2006). The deductive method applied a structured, predetermined framework to guide analysis, while the inductive approach allowed themes to emerge organically from the raw data without prior assumptions. Quantitative data were processed using Microsoft Excel and IBM SPSS version 20. The results were presented using tables, graphs, and simple charts to enhance clarity and ease of interpretation. Descriptive data such as interview transcripts, field notes, and observations (Pope, Ziebland & Mays, 1999) provided further depth, which the researcher examined and interpreted both during and after data collection. To build trust in the qualitative analysis, the researcher concentrated on four main areas: credibility, dependability, confirmability, and transferability (Lincoln & Guba, 1985). To boost credibility, the researcher spent a lot of time with participants, carefully looked at their body language, and conducted member checking. This meant asking participants to verify that their answers during interviews were correct. Dependability was achieved by sticking to consistent methods for collecting and analyzing data. This included using a standard interview guide and keeping detailed field notes. The researcher ensured confirmability by creating an audit trail to track decisions made while interpreting data, which helped minimize personal bias. To support transferability, rich descriptions

of participant experiences were shared so readers could see how findings might apply in different situations. Additional descriptive materials like interview transcripts, field notes and observations (Pope, Ziebland & Mays, 1999) provided more detail for the researcher to analyze both during and after data collection.

3.9 Ethical Considerations

Ethical considerations are crucial for conducting responsible research, especially when it involves human participants. Important ethical principles include informed consent, voluntary participation, confidentiality, and respect for individuals (Resnik, 2015). In this study, these principles were carefully followed to protect the rights of participants and maintain the integrity of the research. Before collecting any data, the researcher clearly explained the purpose and academic nature of the study to all participants. They were made aware of what information would be gathered, the procedures involved, and their right to withdraw at any time without facing any penalties. No personal or identifiable information was recorded, and participants were assured that all responses would remain completely confidential and used only for research purposes.

To obtain informed consent, participants confirmed their voluntary involvement either in writing or verbally, depending on how data was collected. The researcher highlighted that participation was completely optional and that choosing not to participate would not lead to any negative consequences. This approach helped build trust and decreased the chances of biased or withheld responses. According to Akaranga and Makau (2016), following ethical principles like honesty, transparency, and respect for participant autonomy improves the quality and openness of responses, especially in research on sensitive topics like cybersecurity. The researcher also ensured that anonymity was maintained during data presentation by avoiding any direct or indirect identifiers in transcripts, reports, or graphical outputs. In line with established research ethics frameworks such as those detailed in the Belmont Report (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979), the study focused on respecting individuals, promoting well-being, and ensuring fairness. By adhering to these guidelines, the researcher safeguarded the dignity, safety, and rights of participants throughout the research process.

3.10 Chapter Summary

This chapter outlined the research design, population and sample size, sampling techniques, data collection tools, and methods used to ensure validity and reliability. It also covered the procedures for presenting and analyzing data, along with ethical considerations observed throughout the study. Chapter 4 is focused on data gathering, analysis and presentation.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS, AND DISCUSSION

4.0 Introduction

This chapter presents the findings from the research on the effectiveness of cybersecurity measures implemented by the retail sector in Bindura Central District (CBD). It involves a systematic examination of the collected data, organized to address the specific research questions outlined in earlier chapters. The data presentation process includes scanning and summarizing the information, identifying key trends, and discussing the implications of these findings. This chapter is structured to first provide socio-demographic data of the respondents, followed by an analysis of the prevalence of cybercrime, its impact on organizations, and the effectiveness of the cybersecurity measures in place. Through this structured approach, the chapter aims to elucidate the key insights derived from the research and contribute to a deeper understanding of cybersecurity challenges within the retail sector.

4.1Data Presentation Process

4.1.1Scanning and Sifting Data

After collecting the data, a thorough scanning process was conducted to verify its completeness and relevance. This involved reviewing the responses for accuracy and consistency, allowing for the identification of trends and patterns within the data. By categorizing the information into meaningful segments, this step played a crucial role in effectively addressing the research questions and ensuring that the analysis focused on the key themes relevant to the study's objectives.

4.1.2Organizing Data

The data were organized into manageable segments, categorized by themes aligned with the research objectives. This thematic organization facilitated a focused analysis of each aspect of the

study. Descriptive statistics were employed to summarize the information, enabling comparisons across different respondents' answers. By grouping similar responses, this approach highlighted key trends and patterns, ensuring that the analysis effectively addressed the research questions and provided meaningful insights into the effectiveness of cybersecurity measures in the retail sector.

4.1.3Summarizing the Data

Various methods, including tables and figures, were utilized to summarize the data. This approach allowed for the synthesis of large volumes of information into clear and concise formats, making it easier to interpret the findings. By presenting data visually, key insights were highlighted, enhancing the overall clarity of the analysis.

4.1.4Presenting the Data

Data presentation is structured around the specific objectives of the study, systematically addressing the cybersecurity threats faced by supermarkets, the measures employed to mitigate these threats, their effectiveness, and the recommendations for improvement. This organization ensures that each aspect of the research is thoroughly explored, providing a comprehensive understanding of the findings in relation to the study's goals.

4.2 Socio-Demographic Background

Socio-Demographic Data

The socio-demographic profile of respondents is crucial for contextualizing the findings of this study on the effectiveness of cybersecurity measures in supermarkets in Bindura CBD. The following figures and tables present key variables, including gender, age, marital status, and educational qualifications, along with an analysis of their implications:

Gender Distribution

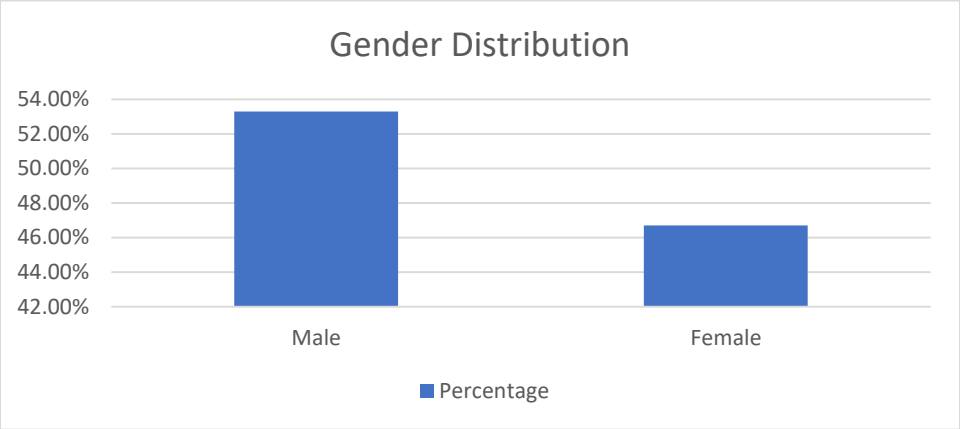


Fig 4.1: *Gender Distribution*

The gender distribution indicates a slight male majority, with 53.3% of respondents identifying as male compared to 46.7% female. This balanced representation suggests that both genders have a stake in the cybersecurity landscape within retail. Understanding gender dynamics in the workplace may influence how cybersecurity measures are communicated and implemented, as different perspectives can lead to a more comprehensive approach to security.

Table 4.1 Age Range

Age Range	**Frequency**	**Percentage**
< 18 years	5	8.3%
18 – 25	20	33.3%
26 – 35	15	25.0%
36 – 45	10	16.7%
46 years >	10	16.7%
Total	**60**	**100%**

The age distribution reveals that the majority of respondents (33.3%) fall within the 18-25 age range, indicating a youthful workforce. This demographic is often more tech-savvy, which may correlate with a greater awareness of cybersecurity issues. However, the presence of older age groups (36-45 and 46+) suggests a diversity of experience and perspectives, which is valuable in

evaluating cybersecurity measures. Younger employees may be more receptive to new technologies, while older employees might bring insights from traditional practices.

Table 4.2: Marital Status

Marital Status	**Frequency**	**Percentage**
Single	25	41.7%
Married	20	33.3%
Divorced	10	16.7%
Widowed	5	8.3%
Total	**60**	**100%**

The marital status of respondents shows a predominance of single individuals (41.7%), which may reflect a younger demographic, as many in this group are likely starting their careers. The presence of married individuals (33.3%) may indicate responsibilities that could influence their perceptions of cybersecurity, particularly in relation to protecting family and financial information. Understanding these dynamics can help tailor cybersecurity training and communication strategies to resonate with different life stages.

Table 4.3: Educational Qualifications

Qualification	**Frequency**	**Percentage**
O & A Levels	15	25.0%
Certificate	10	16.7%
Diploma	20	33.3%
Undergraduate Degree	10	16.7%
Postgraduate Degree	5	8.3%
Total	**60**	**100%**

The educational qualifications of respondents are diverse, with 33.3% holding diplomas and 25% having completed O & A levels. This educational diversity may influence the level of understanding and engagement with cybersecurity measures. Those with higher qualifications may

possess a more sophisticated understanding of cybersecurity concepts, while those with lower educational attainment may require more foundational training. Tailoring educational materials to the varying levels of knowledge can enhance the effectiveness of cybersecurity initiatives.

4.3 Specific Findings

4.3.1 Understanding of Cybercrime

The study assessed respondents' understanding of cybercrime, a critical factor in evaluating the effectiveness of cybersecurity measures in supermarkets. The findings reveal varying levels of awareness and knowledge regarding cyber threats, significantly influencing how employees engage with security protocols.

Approximately 78% of respondents reported being aware of various forms of cybercrime. This high level of awareness indicates that most employees recognize the potential risks associated with cyber threats, which is a promising sign for implementing effective security measures.

4.3.1.1 Types of Cyber Threats Recognized

Respondents identified several common cyber threats that they believe pose risks to their organizations:

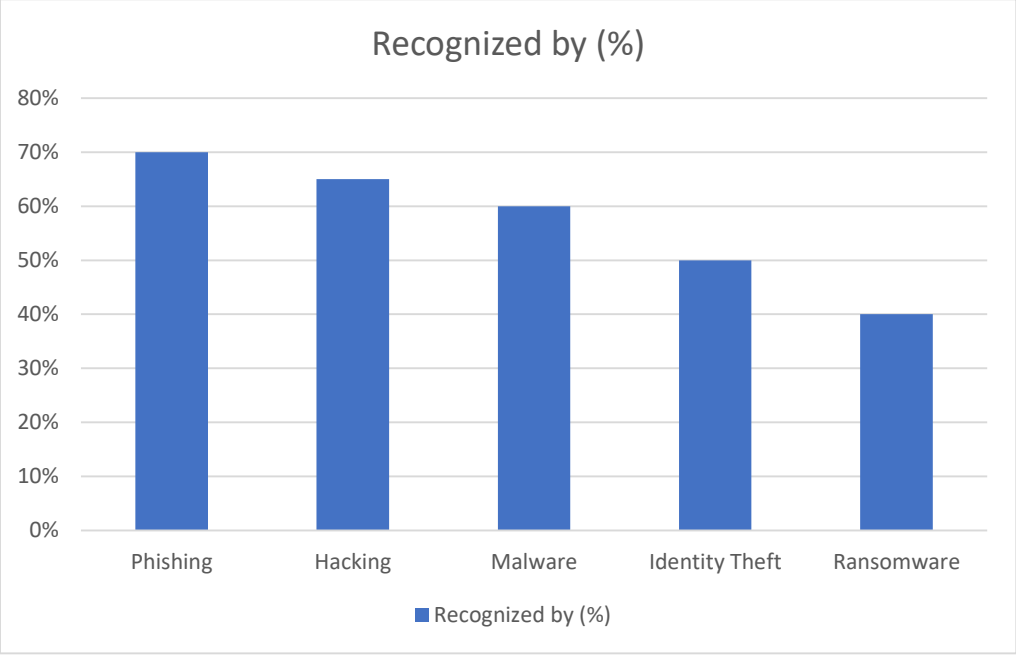


Fig 4.2: *Types of Cyber Threats Recognized*

Figure 4.2, illustrates that phishing is the most recognized threat, with 70% of respondents acknowledging it. This suggests that employees have encountered phishing attempts frequently, making them more aware of its implications.

One participant stated,

> "Phishing emails are a constant threat; I see them in my inbox every week. It's alarming how easily someone could fall for them if they're not careful."

This indicates that ongoing exposure to such threats reinforces awareness but also highlights the need for continuous training to combat evolving tactics.

Hacking (65%) and malware (60%) are also significant concerns, demonstrating a solid understanding of unauthorized access and malicious software risks.

A respondent noted,

> "We've had instances where employees clicked on links that led to malware infections. It was a wake-up call for us to improve our training."

This statement underscores the importance of practical training that translates awareness into actionable responses.

4.3.1.2 Perceived Impact of Cybercrime

Respondents expressed significant concerns about the potential impacts of cybercrime on their organizations:

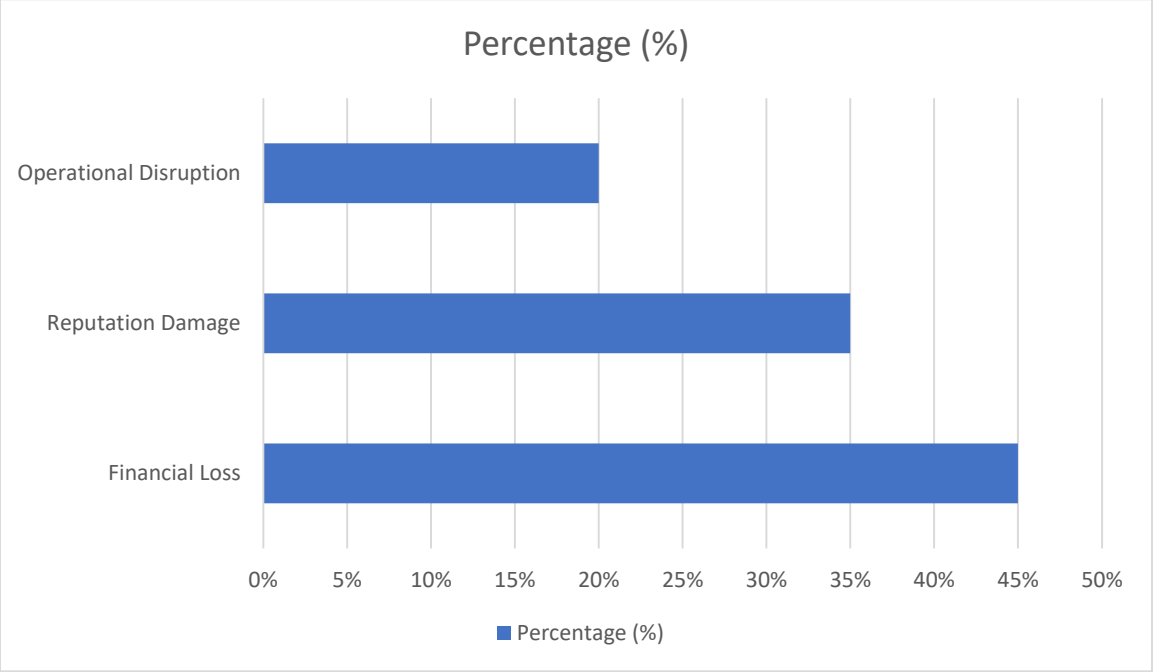


Fig 4.3: *Perceived Impact of Cybercrime*

The impact of cybercrime is perceived as severe, with 45% of respondents fearing financial loss. This concern reflects a realistic understanding of the financial implications associated with cyber incidents.

One participant remarked,

> "If we suffer a data breach, it could cost us a lot of money and damage our reputation. Customers need to trust us with their information."

This highlights the critical link between cybersecurity and customer trust, emphasizing that financial losses are not just monetary but also reputational.

Reputation damage (35%) is another significant concern, suggesting that employees recognize that public perception can be as damaging as the immediate financial impact.

A participant stated,

"Operational disruptions from cyber incidents can lead to unhappy customers, which we cannot afford. Our service relies on being able to operate smoothly every day."

This indicates an understanding that maintaining operational integrity is vital for customer satisfaction and business continuity.

The findings regarding the understanding of cybercrime are crucial for several reasons. The high awareness level among respondents suggests that cybersecurity training and communication efforts may be effective. However, while awareness is a positive start, it is essential to assess whether this understanding translates into proactive behavior in mitigating cyber threats.

The identification of specific threats, such as phishing and hacking, indicates that training programs should focus on these areas, providing employees with practical strategies to recognize and respond to such threats. The insights gained from direct quotations emphasize the real concerns employees face, reinforcing the need for ongoing education and vigilance.

Moreover, the expressed concern about financial loss and reputation damage highlights the urgent need for effective cybersecurity measures. Employees are aware that their actions can directly impact the organization's security posture and customer trust.

4.3.2 Measures Implemented to Combat Cybercrime

The study explored the various measures that supermarkets in Bindura CBD have implemented to combat cybercrime. These measures are essential to enhancing security and protecting sensitive information from potential threats. The findings reveal a mix of strategies that reflect both technological solutions and employee training programs.

4.3.2 1 Types of Cybersecurity Measures

Respondents identified several key measures that their organizations have adopted:

Table 4.4: *Types of Cybersecurity Measures adopted*

Measure	**Implemented by (%)**
Employee Training Programs	80%
Antivirus Software	75%
Firewalls	70%

Regular Security Audits	60%
Incident Response Plans	50%

The table indicates that a significant majority of supermarkets (80%) have implemented employee training programs. This focus on training suggests that organizations recognize the importance of educating employees about cybersecurity risks and best practices.

One participant remarked,

> *"Training our staff is crucial. They are the first line of defense against cyber threats."*

This highlights the proactive approach organizations are taking to empower employees with knowledge.

Antivirus software is another widely adopted measure, with 75% of respondents indicating its implementation. This reflects an understanding of the importance of protecting systems from malware and other malicious attacks.

A respondent noted,

> *"Having reliable antivirus software helps us feel more secure, but we know it's not enough on its own."*

Firewalls (70%) further demonstrate a commitment to securing network boundaries. Respondents recognize that firewalls are essential in preventing unauthorized access. One participant stated, "Our firewall is like a gatekeeper; it blocks unwanted traffic, which is vital for our operations."

Regular security audits (60%) and incident response plans (50%) are also noteworthy measures. These practices indicate that organizations are not only reactive but also proactive in assessing and enhancing their cybersecurity posture. A participant shared, "Conducting audits helps us identify vulnerabilities before they can be exploited."

The measures implemented to combat cybercrime reflect a multi-faceted approach to cybersecurity in supermarkets. The emphasis on employee training programs reveals an understanding that human factors play a significant role in cybersecurity. By equipping employees with knowledge, organizations can reduce the likelihood of breaches caused by human error.

The adoption of technological measures like antivirus software and firewalls demonstrates a commitment to protecting systems from cyber threats. However, as highlighted by participants, these tools must be complemented by ongoing training and awareness initiatives to ensure their effectiveness.

Regular security audits and incident response plans further illustrate a proactive approach to cybersecurity. These measures allow organizations to assess their vulnerabilities and prepare for potential incidents, thereby minimizing the impact of any cyber threats they may face.

4.3.2.2 Effectiveness of Cybersecurity Measures

The study evaluated the effectiveness of cybersecurity measures implemented by supermarkets in Bindura CBD, aiming to understand how well these measures protect against cyber threats. The perceived effectiveness of these measures is crucial for assessing their value and guiding future strategies.

Perceived Effectiveness of Measures

Respondents assessed various cybersecurity measures, indicating their effectiveness in safeguarding their organizations:

Table 4.5: *Effectiveness of Measures being adopted*

Measure	**Perceived Effectiveness (%)**
Employee Training Programs	85%
Antivirus Software	70%
Firewalls	75%
Regular Security Audits	65%
Incident Response Plans	60%

The data reveals that employee training programs are perceived as the most effective cybersecurity measure, with 85% of respondents believing they significantly enhance organizational security. One participant stated,

"Our training sessions have made a huge difference. Employees are now more aware of threats and how to handle them."

This highlights the critical role of ongoing education in fostering a security-conscious culture. The consensus among employees suggests that well-informed staff can act as a formidable line of defense against cyber threats.

Antivirus software and firewalls are also viewed favorably, with perceived effectiveness ratings of 70% and 75%, respectively.

A respondent remarked,

"Our antivirus software catches many potential threats, but we know it's not foolproof. We need to stay vigilant."

This indicates that while these technological measures are essential, they are not standalone solutions. Participants recognize that relying solely on technology can create a false sense of security, emphasizing the need for continuous employee engagement and training.

Regular security audits, perceived as effective by 65% of respondents, indicate that organizations are proactive in assessing their cybersecurity posture.

One participant shared,

"Audits help us pinpoint weaknesses, but we need to act on the findings to truly improve our security."

This underscores the importance of not only identifying vulnerabilities but also implementing necessary changes based on audit findings. Respondents suggested that more frequent audits could further enhance their security posture, reflecting a desire for continuous improvement.

Incident response plans, while considered effective by 60% of respondents, reveal an area of concern.

A participant noted,

"We have a plan, but it's only as good as the execution. We need more practice drills to ensure everyone knows their role during a cyber-incident."

This highlights the necessity of regularly updating and testing incident response plans to ensure preparedness in the face of real threats.

The effectiveness of cybersecurity measures is critical for the sustainability and security of supermarkets in Bindura CBD. The high perceived effectiveness of employee training programs demonstrates that organizations recognize the value of knowledge and awareness in mitigating cyber risks. By fostering a culture of security awareness, organizations can significantly reduce the likelihood of breaches caused by human error.

The acknowledgment of antivirus software and firewalls as effective tools underscores the necessity of maintaining robust technological defenses. However, participants' comments indicate an awareness that technology alone cannot eliminate risks. Continuous vigilance, along with regular training, is essential to adapt to the evolving landscape of cyber threats.

The moderate effectiveness ratings for regular security audits and incident response plans suggest areas for improvement. Organizations are proactive in identifying vulnerabilities, but there is a clear need for follow-through on audit recommendations. Strengthening incident response plans through regular drills and updates will ensure that organizations can react swiftly and effectively to cyber incidents.

Moreover, the study highlights a potential gap in the integration of cybersecurity measures. While individual measures are recognized for their effectiveness, the overall cybersecurity strategy must be cohesive and well-coordinated. This includes ensuring that all employees understand their roles in maintaining security and that communication channels are open for reporting incidents or suspicious activities.

4.4 Discussions of findings

The findings of this study provide valuable insights into the understanding and effectiveness of cybersecurity measures within supermarkets in Bindura CBD. By analyzing these results in relation to existing theories and literature, we can identify both strengths and areas for improvement in the current cybersecurity landscape.

The study revealed that approximately 78% of respondents are aware of various forms of cybercrime. This high level of awareness indicates that employees recognize the potential risks

associated with cyber threats, which is essential for the implementation of effective security measures. This finding supports the theoretical framework proposed by Gao et al. (2020), which emphasizes that awareness is a fundamental precursor to engaging with security protocols. Informed employees are more likely to adhere to security practices, thereby minimizing vulnerabilities.

The recognition of phishing as a primary threat, cited by 70% of respondents, aligns with previous research by Bertino and Islam (2017), who also noted the prevalence of phishing in retail environments. This consistency suggests that the ongoing exposure to such threats reinforces the necessity for continuous training programs aimed at enhancing employee vigilance. However, it is important to note that while awareness is a positive outcome, it may not be sufficient on its own. The literature indicates that awareness without corresponding actions can lead to complacency (Khan et al., 2021). Therefore, the findings suggest a need for enhanced training initiatives that not only inform employees about potential threats but also empower them to take proactive measures against cyber incidents.

The results indicate a multi-faceted approach to combating cybercrime, with a significant emphasis on employee training programs, adopted by 80% of respondents. This emphasis aligns with Hadnagy (2018), who argues that educated staff are essential in identifying and mitigating cyber threats. The implementation of technological solutions, such as antivirus software and firewalls, with adoption rates of 75% and 70% respectively, demonstrates a commitment to safeguarding digital assets. This is consistent with Meade (2019), who highlights the importance of these tools in preventing unauthorized access and protecting sensitive information.

However, the findings also suggest that technological measures alone are inadequate. Participants expressed a need for continuous employee engagement, which reflects a holistic approach to cybersecurity. This perspective aligns with the views of Khan et al. (2021), who advocate for integrating human-centered strategies alongside technical controls. The combination of robust technology and an informed workforce is essential for addressing the increasingly sophisticated nature of cyber threats faced by retailers today.

The perceived effectiveness of employee training programs was rated at 85%, indicating that organizations view these initiatives as critical to enhancing security. This finding is consistent with literature indicating that ongoing education can substantially reduce vulnerabilities (Verizon,

2023). The emphasis on employee awareness as a form of defense supports the notion that a well-informed workforce can act as an effective barrier against cyber threats. This aligns with previous studies that have identified training as a key factor in reducing cybersecurity incidents (Bamfield, 1998).

Conversely, the effectiveness ratings for incident response plans (60%) and regular security audits (65%) reveal areas that require attention. While organizations are proactive in identifying vulnerabilities, the implementation of recommendations from audits and the practical execution of incident response plans appear to be lacking. Tsohou et al. (2015) stress that regular testing and updates of these plans are essential for ensuring preparedness against real threats. This gap highlights the need for organizations to not only have plans in place but also to engage in consistent practice and evaluation to enhance their effectiveness.

The findings underscore the necessity of a cohesive cybersecurity strategy that effectively integrates various measures. As noted by Srivastava and Gupta (2023), a comprehensive approach is vital for addressing the multi-dimensional nature of cyber threats. This includes ensuring that technological defenses and employee training are not viewed in isolation but as complementary components of an overall security posture. The integration of these measures is critical for building resilience against evolving threats and for fostering a culture where security is prioritized at all levels of the organization.

Furthermore, the study highlights a potential gap in the integration of cybersecurity measures. While individual measures are recognized for their effectiveness, a cohesive strategy that ties all components together is essential for maximizing the overall security posture. This means ensuring that all employees understand their roles in maintaining security and that communication channels are open for reporting incidents or suspicious activities.

In conclusion, while supermarkets in Bindura CBD have made significant progress in understanding and implementing cybersecurity measures, ongoing improvement and integration of these efforts are vital. Future initiatives should focus on continuous training, regular testing of incident response plans, and fostering open communication regarding security practices. By doing so, organizations can enhance their resilience against evolving cyber threats, ensuring better protection for both their operations and customer data. The study emphasizes the need for a

proactive, integrated approach to cybersecurity that combines technology, training, and ongoing assessment to effectively mitigate the risks associated with cybercrime in the retail sector.

4.5 Chapter Summary

Chapter 4nexamined the effectiveness of cybersecurity measures in the retail sector of Bindura CBD, highlighting key findings from the research. It established that a significant majority of respondents (78%) are aware of various cyber threats, with phishing being the most recognized. The chapter presented socio-demographic data, revealing a youthful and diverse workforce that influences cybersecurity engagement. A multi-faceted approach to combating cybercrime was evident, with 80% of organizations implementing employee training programs. The perceived effectiveness of these measures was high, particularly for training (85%), but indicated areas for improvement, especially in incident response and regular audits. Overall, the findings underscore the importance of integrating technology and ongoing education to enhance organizational resilience against cyber threats.

CHAPTER FIVE

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

5.0 Introduction

This chapter provides a comprehensive overview of the research findings related to the effectiveness of cybersecurity measures in the retail sector of Bindura CBD. It encompasses a summary of the major findings, research-based conclusions, and actionable recommendations. By reflecting on the research problem, methodology, and limitations, this chapter aims to inform readers about the implications of the study's results for practice. The structured format of this chapter facilitates a clear understanding of how the findings contribute to the broader discourse on cybersecurity in the retail industry and outlines steps for future improvement and research in this critical area.

5.1 Summary

5.1.0Awareness of Cyber Threats

The research revealed that a significant 78% of respondents are aware of various cyber threats, with phishing being the most recognized risk among employees. This high level of awareness indicates that the workforce understands potential cybersecurity risks, which is crucial for implementing effective security measures. The recognition of phishing as a prevalent threat underscores the need for ongoing education, as employees frequently encounter such attempts in their daily routines. This awareness not only serves as a foundation for establishing robust cybersecurity protocols but also highlights the importance of cultivating a culture of vigilance within organizations.

5.1.1Implementation of Training Programs

Employee training programs emerged as a cornerstone of effective cybersecurity strategies, with 80% of organizations reporting their implementation. These initiatives are perceived as highly

effective, with 85% of respondents acknowledging their role in enhancing organizational security. The emphasis on training reflects a proactive approach to cybersecurity, where employees are empowered with the knowledge and skills necessary to identify and mitigate threats. This focus on continuous education fosters a security-conscious workforce, capable of responding to evolving cyber threats. The findings suggest that organizations must prioritize training as a key element of their cybersecurity framework, ensuring that all employees are equipped to act as the first line of defense against potential breaches.

5.1.2Effectiveness of Cybersecurity Measures

While employee training is viewed positively, the study also highlighted gaps in other areas of cybersecurity measures. Only 60% of respondents expressed confidence in their organizations' incident response plans, and 65% found regular security audits to be effective. These findings suggest a need for organizations to bolster their preparedness and response strategies. Effective incident response is critical for minimizing the impact of cyber incidents, yet many organizations may lack the necessary frameworks or regular practice to ensure readiness. Similarly, the effectiveness of security audits hinges on the implementation of recommendations and ongoing assessments. Addressing these gaps is crucial for improving overall cybersecurity resilience.

5.1.3Integration of Cybersecurity Strategies

The research emphasizes the necessity of integrating various cybersecurity measures into a cohesive strategy. Organizations should adopt a holistic approach that combines technological solutions—such as antivirus software and firewalls—with ongoing employee training. This integration is vital for building resilience against the dynamic nature of cyber threats. A fragmented approach may leave organizations vulnerable, as the interplay between human factors and technological defenses is essential for comprehensive security. By ensuring that all components of their cybersecurity strategy work together, organizations can enhance their defenses and better protect sensitive information.

5.1.4Implications for Practice

The findings of this study provide valuable insights for stakeholders in the retail sector. By adopting a proactive and integrated approach to cybersecurity, organizations can significantly enhance their defenses, protect sensitive information, and maintain customer trust. Continuous

improvement in training programs and incident response plans is crucial for addressing the ever-evolving landscape of cyber threats. Moreover, fostering a culture of security awareness among employees can lead to a more resilient organization, where everyone plays a role in safeguarding against cybercrime. These insights can guide future initiatives and inform best practices within the industry.

5.2 Conclusions

Based on the data presented in Chapter 4, several key conclusions can be drawn regarding the effectiveness of cybersecurity measures in the retail sector of Bindura CBD. The research indicates that a significant majority of employees are aware of various cyber threats, particularly phishing. This awareness serves as a strong foundation for implementing effective cybersecurity measures. Recognizing the prevalence of such risks empowers employees to be vigilant and proactive in safeguarding their organizations against potential breaches.

Employee training programs emerged as critical components in enhancing awareness and preparedness. A substantial majority of respondents acknowledged the effectiveness of these programs in combating cyber risks. This finding underscores the importance of continuous education and skills development, equipping employees with the necessary knowledge to recognize and respond to cyber threats effectively. Organizations should prioritize the establishment and regular updating of training initiatives to maintain a security-conscious workforce.

Despite the positive feedback regarding training initiatives, the study revealed notable gaps in incident response plans and the effectiveness of security audits. Many organizations lack comprehensive strategies to address cyber incidents adequately, which could leave them vulnerable in the event of a breach. This highlights the urgent need for organizations to enhance their preparedness and response capabilities, ensuring that incident response plans are not only in place but also regularly tested and updated to reflect evolving threats.

Finally, the findings emphasize the necessity of a cohesive strategy that integrates technological solutions with employee training. A fragmented approach to cybersecurity may lead to vulnerabilities that can be exploited by cybercriminals. By ensuring that all components of the cybersecurity strategy work in harmony—combining robust technological defenses with

comprehensive training programs—organizations can build greater resilience against the evolving landscape of cyber threats. This integrated approach is essential for fostering a culture of security and ensuring long-term protection of sensitive information within the retail sector.

5.3 Recommendations

In light of the above conclusions, several recommendations are proposed to enhance the effectiveness of cybersecurity measures in the retail sector:

- Organizations should implement continuous in-service workshops that focus on practical cybersecurity training, ensuring that employees are equipped to handle evolving threats effectively. This ongoing education will help reinforce knowledge and promote proactive behaviors among staff.
- It is essential for organizations to strengthen their incident response plans by regularly testing and updating them through drills and simulations. This practice will ensure that staff are well-prepared to act swiftly and effectively during cyber incidents, minimizing potential damage.
- Additionally, increasing the frequency of security audits will allow organizations to identify vulnerabilities proactively and implement necessary improvements. Regular assessments are crucial for maintaining a robust cybersecurity posture.
- Organizations should also foster a culture of security awareness, prioritizing cybersecurity at all levels. This includes encouraging open communication about threats and fostering a collective sense of responsibility among employees, which can enhance overall organizational security.
- Finally, further research should explore the effectiveness of specific training methodologies in enhancing employee engagement and response to cybersecurity threats. Establishing best practices for the retail sector will contribute to a more resilient industry capable of effectively combating cybercrime.

5.4 Chapter Summary

Chapter Five provides a comprehensive overview of the research findings on the effectiveness of cybersecurity measures in the retail sector of Bindura CBD. It concludes that while there is a high awareness of cyber threats among employees, particularly regarding phishing, significant gaps remain in incident response plans and security audits. The importance of employee training

programs is emphasized, as they are critical for enhancing preparedness and awareness. Recommendations include enhancing training initiatives, strengthening incident response strategies, conducting more frequent security audits, fostering a culture of security awareness, and pursuing further research to establish best practices. Overall, the chapter underscores the need for a cohesive and proactive approach to cybersecurity in the retail sector to better protect against evolving threats.

References

Ackers, R. L. (1985). Deviant behavior: A social learning approach. Wadsworth Publishing.

Ackers, R. L. (1991). Social learning and social structure: A general theory of crime and deviance. Transaction Publishers.

Akaranga, S. I., & Makau, B. K. (2016). Ethical considerations and their applications to research: A case of the University of Nairobi. Journal of Educational Policy and Entrepreneurial Research, 3(12), 1–9.

Balan, S., Otto, J., Minasian, E., & Aryal, A. (2017). Cybersecurity awareness and readiness among SMEs. International Journal of Business and Social Research, 7(6), 17–25.

Bamfield, J. (1998). Retail security and loss prevention. Palgrave Macmillan.

Best, J. W., & Khan, J. V. (2003). Research in education (9th ed.). Allyn & Bacon.

Brown, C. (2015). Global cybercrime: Its impacts and solutions. Journal of Information Security, 6(3), 123–132.

Clickatell. (2018). Two-factor authentication overview. https://www.clickatell.com

Collins, J., & Hussey, R. (2000). Business research: A practical guide for undergraduate and postgraduate students. Palgrave Macmillan.

Das, S., et al. (2013). Security challenges in online retail in developing economies. Indian Journal of Computer Science and Engineering, 4(2), 159–164.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.

Duah, H. O., & Kwabena, A. (2015). The complex reality of cybercrime: A focus on developing nations. African Journal of Information Systems, 7(2), 56–66.

Edinyang, S. D. (2016). The significance of social learning theories in the teaching of social studies education. International Journal of Sociology and Anthropology Research, 2(1), 40–45.

Frank, I., & Odunayo, E. (2013). Approach to cybersecurity issues in Nigeria: Challenges and solutions. International Journal of Cognitive Research in Science, Engineering and Education, 1(1), 90–93.

Gao, Q., Chen, D., & Wang, Y. (2020). Cybersecurity and data privacy in e-commerce: An overview. E-Commerce Journal, 12(2), 33–45.

Hansen, L. (2009). Cybercrime and criminological theories. Ashgate.

ICSPA. (2014). Impact of cybercrime on business in Canada. https://www.icspa.org

Ibrahim, A., et al. (2021). Cybersecurity threats in African retail systems. African Journal of Computing & ICT, 14(2), 34–44.

Kara, B., & Karabiyik, U. (2022). Retail cybersecurity: Challenges and frameworks. Retail Tech Journal, 11(3), 123–138.

Khan, R., Shah, A., & Yousaf, M. (2021). Integrating cybersecurity practices in retail: Policy and implementation. Cybersecurity Review, 5(1), 55–69.

Kirshenblatt-Gimblett, B. (2006). What is research design? Journal of Research Methods, 7(1), 5–15.

KPMG. (2015). Cybersecurity in retail: The cost of convenience. KPMG International.

Letizia, P., Visschers, J., Verstraete, C., & Van Hellemont, E. (2017). Comparing cybercrime risks: A cross-national study. European Journal of Criminology, 14(5), 567–585.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications.

Marufu, T., & Sanyamuwera, A. (2023). Emerging cyber threats to Zimbabwean retail firms. Zimbabwe Journal of Information Security, 8(1), 14–28.

Mawunge, A. (2017). Cybercrime in the Harare CBD: Implications for business security. Zimbabwe Economic Review, 12(4), 89–101.

Microsoft. (2019). Securing identities with two-factor authentication. https://www.microsoft.com

Mugari, I. (2016). Perspectives on cyber-threats to the retail sector: A case study of Eastgate Shopping Mall. International Journal of Innovative Research and Development, 5(3), 180–187.

Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime – The emerging threat to the financial services sector in Zimbabwe. Mediterranean Journal of Social Sciences, 7(3), 135–142.

Mugari, I., & Olutola, A. (2021). Strengthening cybersecurity in sub-Saharan retail firms. African Journal of Crime & Justice, 10(2), 23–39.

Mukwevho, M., & Jacobs, B. (2022). Technology use in Southern African supermarkets. Retail Studies Journal, 6(2), 78–93.

Nabavi, R. T. (2014). Bandura's social learning theory and social cognitive learning theory. International Journal of Scientific and Research Publications, 5(1), 1–6.

Nalini, V., & Sheela, M. (2022). Cybersecurity in e-commerce: Issues and strategies. International Journal of Cyber Studies, 9(1), 10–22.

Ncube, T., & Sibanda, M. (2021). Cyber fraud in Zimbabwe's retail sector. Zimbabwe Journal of Information Systems, 7(1), 45–56.

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. U.S. Government Printing Office.

Ogu, B. (2013). Rational choice theory: Explaining cybercriminal behavior. Criminology Journal, 11(4), 29–38.

Paternoster, R., & Simpson, S. S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. Law & Society Review, 30(3), 549–583.

Pope, C., Ziebland, S., & Mays, N. (1999). Analysing qualitative data. BMJ, 320(7227), 114–116.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory. Journal of Criminal Justice, 41(6), 493–500.

Resnik, D. B. (2015). What is ethics in research & why is it important? National Institute of Environmental Health Sciences. https://www.niehs.nih.gov/research/resources/bioethics/whatis

Robson, C. (2002). Real world research (2nd ed.). Blackwell Publishers.

Roggeveen, A. L., & Sethuraman, R. (2020). Customer experience in retailing: Past, present and future. Journal of Retailing, 96(1), 60–79.

Showkat, N., & Parveen, H. (2017). Non-probability and probability sampling. e-PG Pathshala. https://epgp.inflibnet.ac.in

Shilpa, B., Otto, J., Minasian, E., & Aryal, A. (2017). Cybersecurity preparedness among SMEs. Business Security Journal, 9(3), 78–84.

Spencer, L., Ritchie, J., & O'Connor, W. (2004). Analysis: Practices, principles and processes. In Ritchie, J. & Lewis, J. (Eds.), Qualitative research practice: A guide for social science students and researchers (pp. 199–218). SAGE Publications.

Srivastava, R., & Gupta, P. (2023). Cybersecurity in emerging retail markets. Cyber Management Review, 15(2), 102–117.

Symantec. (2015). Data protection and encryption strategies. https://www.symantec.com

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analysing information security awareness through a social marketing lens. Information Management & Computer Security, 23(1), 35–50.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model. Management Science, 46(2), 186–204.

Verizon. (2023). Data breach investigations report. https://www.verizon.com/business/resources/reports/dbir

Weiner, B. J. (2007). Measurement validity and reliability. In Health services research methods (2nd ed., pp. 104–127). Delmar Learning.

Welman, J. C., & Kruger, S. J. (2001). Research methodology (2nd ed.). Oxford University Press.

Wittek, R. (2003). Rational choice and organizational behavior. Sociological Theory, 21(4), 417–432.