BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

IMPACT OF TECHNOLOGICAL CRIMES IN MICRO-FINANCIAL INSTITUTIONS

(A CASE OF GETBUCKS HARARE)

BY

MUNESUISHE MASHINYA

B201174B

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

JUNE 2024

APPROVAL FORM

Title: Impact Of Technological Crimes in Micro-Financial Institutions. A Case of Getbucks Harare

To be completed by the student

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

.... 07/06/2024

(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.

....01/10/2024

(Signature) Date

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.

.... 24/09/2024

(Signature of Chairperson) Date

RELEASE FORM

NAME OF STUDENT: MUNEUISHE MASHINYA

DISSERTATION TITLE: Impact Of Technological Crimes in Micro-Financial Institutions. A Case of Getbucks Harare

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

YEAR GRANTED: 2024

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

SIGNED …………..

PERMANENT ADDRESS: 2725 Lenana Park Tynwald East
Harare

TELEPHONE: +263786105937/+263716062095

EMAIL: munesumashie@gmail.com

DATE: ..../…………../............................

DEDICATION FORM

I want to dedicate this dissertation to my devoted parents, whose unwavering support, encouragement, and hard work have enabled me to complete this work and inspired me to follow my passion for learning and study. I have been privileged to have Miss Chitiyo as my supervisor and my peers Chipo and Frank for their support and assistance during my academic path. I am grateful for our fascinating discussions and the sleepless hours we spent working together before deadlines. My deepest gratitude is also extended to my cousin Takunda and other family members. I could not have completed this assignment without the priceless knowledge and abilities I gained during my undergraduate education. The research project's direction and results have been greatly influenced by the critical thinking, analytical reasoning, and research techniques I have acquired. I appreciate the chances and resources that came with my undergraduate degree, and I'm determined to keep pursuing my academic goals with the same zeal and commitment that have helped me get this far. In addition to adding to the body of knowledge in my subject, my research project should demonstrate the value of a solid academic foundation. To sum up, I dedicate this research project to my undergraduate studies because they have formed the foundation of my academic career and have helped me to be ready for the opportunities and challenges that lie ahead. I am grateful to everyone who has helped and encouraged me along the journey. Above all, I am grateful to God Almighty for his unwavering protection, love, and direction during my academic career.

ABSTRACT

Technological crimes have an impact on the lives of individuals and can have a variety of consequences, including financial loss and reputational damage. Numerous technological crimes have emerged because of the internet's explosive expansion, e-commerce, and the numerous other transactions that take place online. The research aimed to examine the causes and impacts of Technological crimes in the financial industry, with a particular emphasis on Getbucks Microfinance. The following objectives served as the study's guidelines: To demonstrate the nature of technological crimes in micro-financial institutions, to discuss the causes of technological crimes in micro-financial institutions, to determine the extent to which technological crimes affect micro-financial institutions' performance, and to highlight and recommend best practices to address technological crimes in micro-financial institutions. The researcher used a descriptive case study research design on a sample size of 65 participants with the questionnaire and interviews as the main data collection instruments. The study employed stratified random sampling and purposive sampling methods to choose participants. Data was analyzed using Microsoft Excel 2016 and the Statistical Package for Social Sciences (SPSS) version 20, after which it was displayed using tables and bar graphs. The results showed that DOS, malware, phishing, hacking, identity theft, and card fraud are the most popular ways used by fraudsters to carry out these cybercrimes in financial services. Significant impacts have resulted from cybercrime, such as financial losses, reputational damage, business trading disruption, and loss of sensitive data. Economic factors, weak security systems, lack of cybersecurity awareness, and poor recruitment practices are all associated with the causes of cybercrime. The researcher strongly recommended stiff penalties, stringent laws and regulations, and training facilities as effective measures against technological crime in micro-financial institutions.

ACKNOWLEDGEMENTS

Without the numerous and varied contributions from various stakeholders, the research project would not have succeeded. First, I would like to express my gratitude to my advisor, Miss Chitiyo, for her understanding, persistence, and extensive knowledge. I found her guidance to be quite helpful when conducting research and writing this project.

Additionally, I would like to thank my placement supervisors at Old Mutual Zimbabwe, Tichaona Bgwoni, and David Muzori, for their advice and assistance during my attachment. I also want to thank Getbucks Harare for their help and commitment and the advice, critiques, and recommendations throughout the data collection process.

I want to sincerely thank my wonderful parents and sibling (Goodmore, Esther, Russell) for their unwavering support for the last four years while I've been a student. Your unwavering love and concern for me have inspired me to achieve success. Thank you so much for that, you were there for me when I needed you most.

TABLE of Contents

LIST OF TABLES

List of Figures

ABBREVIATIONS

MFIs - Micro-financial institutions

ICT- Information communication technology

ICSPA- International Cyber Security Protection Alliance

CHAPTER I

INTRODUCTION

1.1 Background to the study

The emergence of Information communication technology (ICT) has made it easier for businesses to transact internationally, regionally and locally. According to Howe and Pelser (2022), advancement in ICT has resulted in the proliferation of electronic payment systems such as credit and debit cards, mobile payments, and electronic banking. The evolution of ICTs and the introduction of telecommunications services such as social media platforms, with no exception to emailing through the use of cell phones, computers, and the internet, has brought both positive and negative impacts to the world at large and commerce in particular (Gupta, 2017).

Customers now generally prefer online services because they are considered practical, economical, and simple to operate. The threat of cybercrime in financial institutions has grown due to the widespread usage of non-cash-based payment mechanisms. According to (Mugari, Gona, Maunga, and Chiyambiro, 2016), electronic payment methods have caused financial institutions to be more vulnerable to technological crime dangers, including fraudulent RTGS transfers and electronic card fraud. Cybercriminals utilise electronic banking and transfer systems to launder money, so using them puts users at risk of losing their wealth (Mugari et al., 2016). Some of the major negative impacts of electronic payment systems and information communication technology advancement include insolvency, reputational damage, financial crisis, and others due to rampant cybercrime.

Globally, it is reported that cybercrime is prevalent and skyrocketing rapidly. According to Lewis (2018), internet service providers record about 80 billion automated scams daily by cybercriminals to identify cybercrime targets. According to the US National

Crime Agency (2020), 1 million computer misuse fraud cases were reportedly perpetrated by households in Wales and England alone.

Regionally, South Africa recorded card data breaches amounting to R739.9 million in 2017 and R873.3 million in 2018, representing an 18% rise. (SABRIC 2018). Siddique and Rerman (2011) recognized the following technological crime types: credit card fraud, phishing, and identity theft. Technological crimes cybercrime cost the world 114 billion dollars, while the expense of combating cybercrime is twice that much (Symantec Cyber Crime Report, 2012)

Technological crimes, a global concern, have not spared Zimbabwe's financial sector. Despite minimal empirical study on the problem in Zimbabwe's financial sector, an examination of reports by Mugari et al., (2016)'s submissions indicate that technological crimes are a growing threat in Zimbabwe's financial sector and must be addressed. Considering this, the researcher became interested in investigating the repercussions of cybercrime further.

1.2 Problem statement

The rapid growth of technological crimes in the virtual world has become one of the biggest threats to the financial services sector since individuals and organisations relying on the Internet are also increasing at an alarming rate (Raghavani & Parthiban, 2014). Due to internet use, the risk of cyber-attacks has increased, thus this has increased hacking, phishing, viruses, identity theft and card fraud; hence, the researcher needs to explore the impact of technological crimes in micro-financial institutions. Munyoro (2021) finds it especially alarming that TM Pick n Pay lost $22 million to email hackers who were allegedly targeting the country's largest companies. According to Munyoro (2021), following instructions in a bogus email sent in the name of TM Pick n Pay's financial manager to transfer money from an account at the Avondale branch of Steward Bank, four business accounts were completely emptied. An analysis of reports by Sibanda (2020), submissions confirms that technological crimes are a growing threat in Zimbabwe. The National University of Science and Technology and the Harare Institute of Technology were also attacked, with hackers demanding more than $6 billion to restore material to their websites, the cyber attackers got into the institutions' websites and temporarily gained control of the servers that hosted websites and emails. According to Matambura (2017), OK Zimbabwe's Money Wave System was breached in 2017 and a cyber-fraudster stole $70,000 by transferring the funds to his Money Wave card. The scammer allegedly utilised the card to make fraudulent purchases of merchandise from numerous businesses (Matambura, 2017).

The problem of security breaches in electronic commerce has resulted in the loss of confidence in emerging technologies, loss of clients by companies and general scepticism among economic stakeholders. Therefore, cybercrime has become a concern in the virtual world; hence the study aimed at assessing the impact of cybercrime in micro-financial institutions in Zimbabwe and offer viable and practical solutions.

1.3 Objectives of the research

1. To demonstrate the nature of technological crimes in micro-financial institutions.
2. To discuss the causes of technological crimes in micro-financial institutions.
3. To determine the extent to which technological crimes affect micro financial institutions’ performance.
4. To highlight and recommend best practices to address technological crimes in micro-financial institutions.

1.4 Research questions

1. Which forms of technological crimes are prevalent in micro financial institutions?
2. What are the causes of technological crime in micro financial institutions?
3. What are the effects of technological crimes in financial institutions?
4. Which recommendations are proffered to combat technological crimes and protect micro financial institutions?

1.5 Significance of the research

The core of this research is to assess the impact of technological crimes in micro-financial institutions in Zimbabwe. The research shall be essential to different stakeholders with no exception to the following.

1.5.1 The Government

The study shall assist the government in identifying intervention areas to scourge technological crimes in micro-financial institutions. The study is envisaged to assist the government in policy formulation geared at combating the scourge of cybercrime in e-commerce in general and the financial services sector in particular.

1.5.2 Financial Institution

The study will give an insight into micro-financial institutions in Zimbabwe to be aware of cyber-crime-related threats to their business. The study will also unveil opportunities for micro-financial institutions to secure their businesses against the identified threats. Since micro-financial institutions frequently use ICT to run their businesses daily, it is therefore crucial for them to know the risks and threats to their business.

1.5.3 Researchers

This study shall assist other students in understanding the risk of committing technological crimes such as cybercrimes since they have access to all the tools perpetrators use to defraud micro-financial institutions and the world at large.

1.5.4 General public

The study seeks to inform the general public about the prevalence and impacts of technological crimes on micro-financial institutions and the economy. It is therefore envisaged to broaden cyber-crime awareness among economic stakeholders to improve alertness and prevention.

1.6 Assumptions of the research

The assumptions of the research are-

1. Technological crimes are rampant in micro-financial institutions.
2. Current measures against technological crimes are inadequate.
3. Data gathered will be accurate.
4. Stakeholders in the study will cooperate with the researcher to the best of their abilities.

1.7 Delimitations of the study

The study focuses on micro-financial institutions geographically located in Zimbabwe. The study focuses on the impact of technological crimes in micro-financial institutions. The respondents of the study involve customers and employees in MIFs

1.8 Limitations of the study

Some of the major limitations of the study involve:

1.8.1 Confidentiality

Due to the confidentiality of some company information, some of the respondents do not disclose all the information about the company affairs. Since respondents do not disclose sensitive information about company secrets, some important information might be omitted in this research. To overcome this challenge, the researcher had to explain the purpose of the study to the respondents so that they would appreciate and give accurate information.

1.8.2 Scarcity of resources

The researcher might be faced with resource limitation challenges to gather both primary and secondary data. The researcher might need the resources to fund such processes as printing and transportation which may be beyond the researcher's disposal income. The researcher would get assistance from family, friends, and personal savings to finance the project.

1.9 Summary

The above chapter presented the background of the study illustrating the roots of the problem statement, research objectives, and the research questions accompanying the study. The researcher also looked at the underlying assumptions, the significance of the study, its delimitations, and limitations. Chapter II covers the empirical data on technological crimes as well as the conceptual and theoretical framework that guided the research.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

This section of the research explores the works of other scholars on the impacts, causes, measures, and challenges of cybercrimes in micro financial institutions. Through a thorough examination of cybercrime data from many publications, including books, articles, newspapers, and journals, a literature review can offer a thorough grasp of the goals of the study. This chapter shows the conceptual framework, theoretical framework, and empirical evidence review while showing the knowledge gap.

2.1.1 Purpose of Literature Review and Conceptual Framework

A literature review consists of conceptual and theoretical frameworks. As a result, the literature study contributed to a full grasp of previous studies and new cybercrime tendencies (Snyder, 2019). According to Shikalepo (2020), a conceptual framework is defined as specific ideas used by the researcher in the research study.

2.1.2 The concept of technological crimes

Technological crimes are crimes committed using electronic and digital technology to assault computers or computer networks (Payne, 2020). RBZ (2015), went on to state that it is illegal access to a computer system to delete, modify, or damage computer data. According to Mugari (2017), existing definitions of technological crimes emerged experimentally and tended to differ depending on the insight of protectors and victims. All definitions agree that technological crimes involve the misuse of a computer network system. Technological crimes are various, and the study shall review different forms of technological crimes about how they abuse internet technology.

2.1.3 Forms of Technological Crimes.

Cybercrime occurs in different ways, and Aggarwal et al., (2015), mentioned different forms of cybercrime, although the research is revealing few of them. Consequently, it's critical to understand the many forms and modus operandi of technological crimes.

2.1.3.1 Phishing

According to Rastenis, Ramanauskaitė, Janulevičius, Čenys, Slotkienė, & Pakrijauskas, (2020), phishing is defined as sending false emails to gain confidential information against the victim. (Boateng & Amanor 2014) referred to phishing as an attack on individuals and organisations to obtain private information that will be used for fraudulent activities. For example, someone may receive a fake message alerting them to the possibility that malware has compromised their account and requesting personal information to correct their account. This information is subsequently utilised for the phisher's purposes (Boateng & Amanor 2014). Diaz, Sherman, & Joshi (2020) defined phishing as fraud against businesses and financial institutions through stealing the identity of customers. Despite businesses' willingness to accept the risk of fraud, evidence suggests that an increasing number of customers are shunning e-commerce because of the possibility of phishing.

2.1.3.2 Hacking

According to Oliver and Randolph (2022), hacking means accessing a person’s computer without his or her knowledge to gain personal and confidential information. Hacking is unlawful access to the internal systems or databases of an individual or organisation’s confidential information (Gupta & Anad, 2017). Magutu et al., (2011) observe that online access to personal information has made it easier for thieves to defraud organizations and individuals. As a result, unauthorised access can harm a company's internal operations by exposing critical information about its customers (Banal and Zahedi, 2015). As banks shift to online platforms, they are more exposed to hacking, potentially leading to huge losses. Banal and Zahedi (2015) found that a lack of trust from customers can harm a company, leading to lower revenue and an increased chance of failure.

2.1.3.3 Card Fraud

According to Australian Payment Network (2019), card fraud is a form of crime involving the illegal use of unauthorised personal information or accounts to misrepresent the victim’s information. Bank credit and debit cards are stolen or copied by fraudsters, who then use them to access bank clients' bank accounts or make online purchases. Shukur and Kurnaz (2019) identified two forms of card fraud: online and offline. They went on to define online card fraud as fraud committed through the abuse of the internet, and gadgets while offline card fraud means theft or stealing of a physical card for illegal intention. Due to the increasing adoption of online banking, clients are especially susceptible to card theft (Mugari, 2016).

2.1.3.4 Malware

According to Mugari (2016), malware refers to attacks when the fraudster installs malicious software to scam the hard drive to collect information, usually credit card numbers and social security numbers. According to Aggarwal., (2020), malicious software means using software to gain access to a system and steal confidential information or damage the hardware of the system to disrupt its normal operation. Uppal et al., (2014) went on to identify two main types of malware attacks: contagious, for instance, worms and viruses. Uppal et al., (2014) and Mugari (2016) agreed that when an unauthorised program or virus is installed into the computer software, it replicates itself in the process to infect the whole system hence the denial-of-service system. Unlike viruses, worms infect through storage devices for example universal serial bus -USB and emails to limit the storage of the device while a Trojan is a form of malware that conceals itself as a legitimate program that victims download from the internet and is used by perpetrators for stealing personal information of the victims (Uppal et al., 2014 & Mugari 2016).

2.1.3.5 Identity theft

Identity theft is defined as the unauthorised use of sensitive information for criminal purposes (Zweighaft, 2017). As a result, identity theft happens when fraudsters gain enough information about a person's identity, such as their name and address, to defraud a victim. Victims, whether alive or deceased, lose money because of identity theft when criminals use their names to get mortgages, credit cards, and bank loans. Thus, using stolen identity information, fraudsters can obtain credit cards, acquire loans, open bank accounts, and take over existing accounts (Zweighaft, 2017).

2.1.3.6 Denial of service (DoS) attacks

According to Belous & Saladukha (2020), a denial-of-service (DoS) assault happens when a malicious cyber threat actor prevents legitimate users from accessing network resources, including information systems and devices. Cyber attackers can then target an e-mail address, a website, online activity, or any other action that is dependent on the compromised machine. DoS attacks impair system performance by inhibiting the flow of information from sender to recipient (Maahs, 2018). This would prevent clients' demands from being met, and clients would be unable to access the website. A DoS assault, for example, could be part of a simple blackmail attempt performed by hackers for financial benefit, toward the MFI, these attacks may affect emails and online accounts. DoS assaults can also be employed by firms to disrupt their competitors' Internet business activities (Mansfield-Devine, 2016).

2.1.4 Causes of Technological Crimes in micro-financial institutions

2.1.4.1 Economic Factors

According to Wall (2024), financial incentives might also contribute to cybercrime. This is because many cyber-attacks are carried out for financial benefit. Cybercriminals go so far as to steal personal information, breach bank accounts, and spread ransomware. Additionally, the lack of well-paying job opportunities in the formal sector has pushed some individuals to explore alternative means of generating revenue, which may include targeting MFIs through various cyber-attacks (Chikoto & Mapira, 2020). These cybercriminals are unconcerned about the losses suffered by their victims as long as they make financial profits. This is why cybercrime can cause considerable losses for victims.

2.1.4.2 Weak Security Systems

Cybercrimes are frequently the result of security system weaknesses or flaws and not everyone values security, some even fail to update security systems regularly (Pasculli, 2020). According to Pillay, Ntuli, and Ehiane (2023), if software or operating systems are not updated regularly, fraudsters can exploit certain security flaws. As a result, it is increasingly harder to avoid cybercrime. As technology develops, cybercriminals and how they obtain confidential information also become more advanced. More than any other sector, the financial services industry is frequently the target of cybercriminals (Mugari & Olotula, 2021). Over the past few years, the banking industry has seen a rise in cyberattacks and data breaches as cybercriminals have successfully penetrated the system by employing a variety of techniques, including hacking, phishing emails, and malware (Mugari, 2016). Financial services companies have a lot of valuable information, which makes them a prime target for cybercriminals. According to Pasculli (2020), as attacks increase in frequency and regulators become more vigilant, financial institutions are under increasing pressure to act.

2.1.4.3 Lack of Cyber-Security Awareness

Many people are still uninformed of and unprepared for the risks of the digital world, individuals or organizations who do not understand and are aware of digital security standards may neglect simple security issues such as password updates (Alzubaidi, 2021). Individuals or organizations unintentionally click on questionable links without realizing the security implications. Individuals like these are frequently more exposed to cybercrimes since they unintentionally aid the actions of cybercriminals. Cybercriminals, according to Picciano (2021), take advantage of the fact that not all users of digital banking are computer literate. As a result, banking clients are typically compromised through phishing, vishing, or the installation of malware via a link that gives the cybercriminal access to the victim's online banking profile.

2.1.4.4 Poor recruitment practices

One of the key causes of technological crimes in banks is a lack of thorough background checks and screening processes during the recruitment stage (Shumba et al., 2013). Inadequate candidate vetting can result in the hiring of personnel with a history of cybercrime or a history of unethical activity, endangering the bank's systems and customer data (Greenfield, 2016). The use of inadequate or outmoded recruitment technologies, such as automated screening methods, can potentially raise the likelihood of technological crimes. These technologies may fail to recognize advanced cybercrime strategies, allowing malicious candidates to pass through the employment process (Greenfield, 2016).

2.1.5 Impacts of Technological crimes in Microfinancial institutions.

2.1.5.1 Financial loss

According to (Siahaan & Budi, 2018; Al-Alawi et al., 2020), cybercrimes cause financial losses to businesses and individuals. Although information communication technology has made it easier for communities to benefit from it, cybercrime has found an opportunity to engage in both ordinary and professional crime, resulting in severe financial losses. Financial institutions play a central role in the economic-financial performance hence they are prone to attack by cybercriminals. According to Al-Alawi (2020), companies rely on financial institutions for banking purposes to transact online. However, online transactions cause colossal losses to artificial persons and individuals.

In addition, to control viruses and malware, institutions purchase security software to limit the likelihood of assaults, thus computer criminality raises overhead costs and lowers corporate profits (Ibrahim, 2019). Since banks run their banking transactions using the internet, that exposes them to the risk of cyber-attacks. According to Ziding, (2016), customers use ATM networks that cybercriminals can also access, once cybercriminals get access to the ATM network, customers' funds can be lost, and their important information can be misused resulting in rigorous financial losses. Institutions risk paying compensation and legal fees to recoup their losses, which hurts the profitability of the company (Ibrahim, 2019).

2.1.5.2 Reputational damage

According to Ghann and Owiredu (2022), banks with an enormous number of clients are the main targets for cybercriminals. This exposes the financial institutions to the risk of reputational damage. Once an attack has been made on any of the clients, it will damage the business's reputation, resulting in other clients losing confidence in the victimised financial institution. Cybercriminals usually transfer funds from victims' accounts to their mule accounts, and they rely on hacking, illegal use of passwords, personal identification numbers (PINs), and clients' credit card numbers. Once an attack has been made, the client victims will shift the blame to the bank accusing them of negligence with their customer accounts. A bank may lose the trust and confidence of its clients because of a data breach or successful cyberattack. Clients may decide to do business with another MFI if they no longer trust the institution to preserve their private information, which would reduce the bank's market share and profitability (Onchomba, 2018). In the end, the bank will lose both its funds and clients leading to insolvency.

2.1.5.3 Disruption of business trading

According to (Al-Alawi et al., 2020)'s study, cybercrimes may disrupt the trading of businesses especially those in online business due to the risk of theft of the organisation's information, resulting in heavy financial losses. They also added that the business may need to cater for paying costs of data breaches and the victimised institution may also need to clean its name, by doing so it may end up paying for the damages and fines to companies affected. Cybercrime also decreases an institution's productivity, as MFIs take steps to prevent it by securing their networks. This is time-consuming and reduces productivity. An increase in business expenditure towards fines will negatively affect its cash flow resulting in failure to meet its day-to-day running cost leading to insolvency.

2.1.5.4 Loss of Sensitive Data

Cheema et al., (2022) define sensitive information as data that provides an organization with a competitive advantage in commercial negotiations or when creating a business plan. Lewis (2018), states that cybercriminals can obtain private customer data, such as bank or financial records, from an organisation and resell it to other criminal organisations or utilize it as a means of extortion. The sensitive data can then be used for business espionage. Suits against businesses would arise from certain sensitive business information. People who believe that the company has violated their privacy may file a lawsuit, which could incur expensive legal fees for the company (Lewis, 2018). It is challenging to measure this type of loss because the victim would not be able to determine why a contract was lost, a negotiation went sour, or an underbid occurred (McAfee, 2014). The recovery costs from these attacks could end up costing MFIs a lot of money. Similarly, the MFIs lose their competitive advantage if they misplace sensitive information.

2.1.6 Recommend best practices to address technological crimes in micro-financial institutions.

2.1.6.1 Education and Training

According to Rao & Saini (2012), education and training facilities should be conducted through workshops and seminars. Education and training of the public about the impact of cybercrimes act as an awareness of the dangers of committing technological crimes to individuals and businesses, nationally, regionally, and the world at large. Workers should receive frequent training on how to identify suspected intrusions and be updated on new viruses and potential hacker attack strategies. According to (Hawkins, 2018), businesses ought to implement a cyberattack mitigation plan. Security threats include opening dangerous emails, going to hacked websites, downloading infected files, and utilizing the Internet for banking (Williams et al., 2018). Programs for employee security training can aid in reducing the likelihood of network viruses and breaches.

2.1.6.2 Constantly update antivirus and anti-spyware software

According to Mawunge (2017), a security tool called antivirus software (or antivirus program) is made to guard against, find, and eliminate viruses and other kinds of malware from computers, networks, and other devices. Mugari (2017), stated that there is a need to install and constantly update security features for example firewalls data recovery sites, antispyware, and antiviruses to minimise the threat of cyber-attack by cybercriminals. Mugari (2017), went on to say that the use of antivirus was a proactive measure that could be used by financial institutions to protect their sensitive data from intrusion.

2.1.6.3 Cyber Security Audits and Compliance Checks

According to Slapnicar et al., (2022), cyber security audits and compliance checks are extensive evaluations of the banks’ networks, information systems, and procedures that find flaws and vulnerabilities that hackers might use. By carrying out a cybersecurity audit, a microfinance can find and fix problems that might lead to an expensive compliance infringement, a data breach, or another significant cybersecurity incident. To add on, MFIs will be able to maintain business continuity, gain customer confidence, and improve security posture.

2.1.6.4 Use of Secret Socket Layer- (SSL)

According to Kertysova et al., (2018), as a way to prevent technological crimes in the banking sector, some organisations have adopted the use of a secret socket layer protocol. The secret socket layer fetches the SSL certificate and verifies if it has expired, checks whether it is issued by an authorised browser, confirms if the same browser that issued the certificate is still the same as the one using it, and only allows the original browser to access the data requested (Laudon & Traver, 2012).

2.1.6.5 Strong passwords and data encryption

According to Njeru and Ngaitho (2019), when passwords are inefficiently managed, it makes it easier for cybercriminals to access the network and its server layer hence passwords must be kept strong, managed, and supported with encryption locks and must be changed on regular intervals while avoiding writing them down in any diaries or piece of paper as well as removing automated connection to the network server. The use of password encryption and reduction to secure code-related threats must be put in to protect codes. Encryption also protects files and data for audit purposes as well as avoiding unauthorised access to data (Laudon & Trevor, 2012).

2.2 Theoretical Framework

Reimann and Jain (2021), state that the theoretical framework is the research guide or blueprint, it acts as the groundwork upon which research is constructed. Based on the definition, it can be revealed that the theoretical framework constitutes the amalgamation of ideas of giants in the field of technological crimes. These theories are going to be used to reveal the causes, impacts, measures, and challenges of technological crimes in MIFs. Routine activities theory, Rational Choice theory, and space transition theory are to be explored.

2.2.1 Routine Activity Theory

The routine activity theory was developed by Cohen & Felson (1979) and it holds special significance for examining crime data. Mugari (2017) stated that crime is normal and can be committed when there is an opportunity. Cohen and Felson (1979 stated three elements that should be present for a crime to occur namely a motivated offender with both criminal intentions and the ability to act on their desires, a suitable targeted victim, as well as the absence of a capable guardian against crime that is motivation, incentive, and opportunity respectively. (Mugari 2016, Kodellas, Fisher & Wilcox 2015), agreed that both time and space should converge with the three elements of the routine activity theory for a crime to occur. The three elements of the routine activity theory are given below.

According to (Cohen & Felson, 1979), a suitable target is an individual's availability as a victim such as one's attractiveness to the offender. According to (Leukfeldt & Yar, 2016) capable guardians are end users or technical administrators and automated protection for example virtual private networks, anti-viruses, ID identification, firewalls, and ant-intrusion software that prevent cyber-attacks, their absence raises the likelihood of cyber-attacks. (Trong, 2020) defined the likely offender as a person willing to commit a crime where an opportunity arises in the absence or presence of a capable guardian. The presence of the elements of the routine activity theory must converge for crime to occur.

Hutching and Hayes (2009) used routine activity theory to address phishing, a common sort of cybercrime in banks. Hutching and Hayes (2009) linked the availability of a suitable offender to increased internet usage. This implies an increase in the number of people with the technological know-how to perform phishing. The presence of a suitable target is detected when there is a rise in the number of persons engaging in prospective victim behaviours, such as more people utilizing the Internet and Internet banking.

Cohen and Felson (1979) argue that opportunity should be eliminated to prevent crime. As the criminal environment is complicated by the fact that the criminal is no longer bound by a physical place, it provides an excellent chance for motivated cybercriminals in the absence of regulatory mechanisms. As a result, MFIs should use antivirus, firewalls, and encryption keys to prevent computer fraud (Mugari 2016). Regardless of the type of crime, the Routine Activity Theory was well suited to describing the reasons behind technical crimes. In Zimbabwe, MFIs lack the essential security infrastructure to tackle cybercrime, allowing fraudsters to take advantage. Thus, the results of this study will demonstrate how the three criminogenic components of the Routine Activity

Theory converge in the business environment of the MFI industry.

2.2.2 Rational Choice Theory

The theory was constructed by Cornish & Clarke (1986). Cornish and Clarke (1986) state that fraudsters are rational and make a choice to commit a crime based on the cost that is the punishment and benefit of offending. Therefore, it is expected that cybercrime will happen anytime a decision is made to conduct a crime since the benefits of doing so exceed the risks (Cornish & Clarke, 1986). However, McQuade (2006), implied that offenders are rational people who compare or weigh the benefits against the risks likely to be faced when one pursues a certain criminal behaviour. Thus, if the benefits of cloning a card outweigh the expenses, a person may choose to commit card fraud. In support of the rational choice theory, Mugari (2017) stated that there is a need to impose strict punishment as a measure to control cybercrimes. (Wada & Odulaja, 2012), also added that financial institutions must put electronic mechanisms such as data encryption, surveillance cameras, automated system control, and user IDs to deter cybercrime risks although it is not easy to detect. Difficulties in the detection of cybercrimes give opportunity for cyber criminals to pursue their agenda since the benefits are more than the costs. This theory was very crucial for this study since it informed how to model cybercrime prevention strategies in MIFs like Getbucks.

2.2.3 Space Transition Theory

The Space Transition Theory was constructed by Jaishankar (2007) to explain the nature of the behaviour of criminals or persons who bring their conforming and non-conforming behaviour in the physical space. The theory relates crime to the movement of criminals from one space to another. According to Mugari et al., (2017), people who commit crimes in the physical space have the potential to commit crimes in cyberspace due to their status and position. They attributed the increase in cybercrimes to a lack of deterrent factors in cyberspace, dissociative anonymity, and identity flexibility gave perpetrators a chance to commit technological crimes. High social standing by criminals gives rise to cybercrimes in financial institutions (Mugari et al., 2017). The theory also emphasizes that individuals with repressed criminal behavior in the physical environment are more likely to commit a crime in cyberspace than they would in the real area due to their status and position (Jaishankar, 2008; Wada, Longe & Danquah, 2012). According to Jaishankar (2008), the dynamic structure of online allows offenders to escape through intermittent undertakings. In this study, the theory therefore explains the increase in cybercrime in MFFs, particularly among culprits with high social standing.

2.3 Empirical evidence

This section reveals secondary information from other scholars on the causes, impacts, measures, and challenges of cybercrimes.

Mugari, Gona, Maunga, and Chiyambiro (2016) described the prevalent types of cybercrime in Zimbabwe's banking industry in their study, **“Cybercrime-The emerging threat to the financial services sector in Zimbabwe.”** They used descriptive and explanatory approaches to elaborate on different forms of cybercrimes, threats, and preventive strategies. The study looked at four Harare-based financial institutions to determine the prevalence of cybercrime. A total of 48 participants from four commercial banks were recruited using stratified random sampling and purposive sampling techniques. The primary research instruments were a questionnaire and in-depth interviews. According to the research findings, cybercrime in banks consists of hacking, phishing, identity theft, and malware. They highlighted that financial institutions are building cybersecurity measures to combat cybercrime, but their efforts are lagging behind technological innovation. Moving on to the main findings, the study indicated that hacking was the most common type of cybercrime widespread in financial institutions, followed by phishing and card fraud with low prevalent rates.

In the study titled **"Study of the Impact of Cybercrime on Business in Canada."** The International Cyber Security Protection Alliance (2013), researched cybercrime's prevalence and impact on Canadian corporate operations. A quantitative analysis was conducted with Canadian businesses. The study found that cybercrime was very widespread among Canadian organizations, with 69 percent reporting some type of attack in the previous year. The types and severity of attacks varied according to the nature and size of the firm. Malicious code attacks were identified as the most common, followed by phishing and social engineering. Denial of service attacks were also stated to be slowly emerging in the sector. The retail sector saw the fewest denial of service attacks.

Atul et al., (2013) conducted a study "**Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector**." The data was gathered through a survey methodology. The original data was collected by questionnaires delivered to diverse respondents in the state of Uttarakhand. Customers who had been victims of cybercrime, as well as technical personnel from the bank, were chosen as survey participants. Secondary data was gathered from several published studies, both nationally and globally. The researchers discovered that cyber criminals employed a number of cyber-attack strategies to target specific banks in India, including identity theft, hacking, phishing, and card fraud. Furthermore, information security rules encourage the protection and well-being of information resources.

Another empirical research was done by Uppal et al., (2014) titled "**Basic survey on Malware Analysis, Tools and Techniques, India"** which gave an overview of the nature of malware, detection techniques, and its impacts in business organisations. Secondary data was used in the study namely online articles, journals, and books. The research findings stated that there are two types of malware: contagious and masked. They categorized viruses and worms as infectious and concealed. According to their findings, a virus enters a computer without permission, replicates itself, and infects the entire system, causing denial of access to services. These are gathered by downloading information from the internet. The research found various techniques to detect malware namely the signature-based detection technique, heuristic detection technique, and hybrid analysis.

Mugari, Kunambura, Obioha and Gopo (2023) conducted study on the "**Trends, impacts, and responses to cybercrime in Zimbabwe's retail sector,"** they presented a detailed explanation of the effects of cybercrime on the retail sector. This study used a mixed research approach and comprised 38 retail players from Bindura chosen through stratified random and purposive sampling. Data was acquired utilizing a closed-ended questionnaire and an in-depth interview guide. SPSS was used to examine quantitative data, while summative content analysis was used for qualitative data. Their main findings stated that the retail industry's cybercrime mostly consists of virus propagation, hacking, and card fraud. The study discovered that cybercrime has serious consequences for the retail sector, including increased security costs, theft of sensitive data, and direct financial losses. Furthermore, it was established that the existing internal procedures and policing efforts to prevent cybercrime in the retail industry could be more effective.

Acharya and Joshi (2020) published a study named **"Impact of Cyber-attacks on Banking Institutions in India"** The study relied on secondary data from official publications, research papers, and analyses of cyber dangers and crimes that have resulted in massive financial losses in prior years. The research detailed the effects of cybercrime on financial institutions, cyber security measures implemented to mitigate the effects of cybercrime, and the establishment of effective cybersecurity processes. The major findings were that banks have been the primary victims of cybercrime in India, with enormous malware assaults stealing valuable and sensitive information and creating reputational damage. The research provides ideas for cybercrime knowledge that will benefit banks, society, and other financial organizations.

The International Cyber Security Protection Alliance (ICSPA) (2022) conducted research titled **"Study of the Impact of Cybercrime on Business in Canada"** which focused on the prevalence of cybercrime and its impact on corporate operations in Canada. A quantitative survey was conducted among Canadian businesses. The target population comprised businesses having Canadian operations and 10 or more employees from most economic sectors, except public administration. The overall cybercrime was rather widespread among Canadian organizations, with 69 percent reporting some type of attack in the preceding year. Malicious code attacks were discovered to be the most common, followed by phishing. The major effects of cyber-attacks were described as disruption of business trading and reputational loss.

Boateng, Budu, Isabalija, and Olumide (2011) investigated the prevalence of cybercrime in Ghana, as well as its forms and effects, in their paper **"Cybercrime and Criminality in Ghana: Its Forms and Ramifications"**. The study used an exploratory research technique. The data was collected using an interview guide. According to the study's findings, unemployment, a lack of solid legislation, and a lack of dedication on the part of bank employees and money transfer operators all contribute to cybercrime. The recommended solutions included the necessity for strong legislation and supporting the Police's cybercrime unit to execute harsh sanctions. The researchers discovered that the attackers were mostly young and had some technical knowledge of how to commit cybercrime.

Obeng-Adjei (2017) conducted a study titled **"Analysis of Cybercrime Activity: Perceptions from a South African Financial Bank."** The primary goal of the study was to investigate the origins, consequences, and major forms of cybercrime that occur in banking institutions. To accomplish this, an interpretive research approach was used with a case study in one of South Africa's largest banks, where cybercrime is currently a hot topic and is garnering attention from senior management. The major interviewees were Cybercrime division specialists as well as other bank stakeholders with a vested interest in the bank's efforts to reduce cybercrime vulnerability. Primary data was collected through semi-structured interviews. Secondary data was also collected, allowing for data triangulation. The study showed that weak security and access restrictions, low awareness and user education, low conviction rates, and perceived material benefit are the most important reasons driving cybercrime. Additionally, the study recommended that to combat the ever-increasing rate of cybercrime, banks should consider implementing stronger security and access controls to protect customer information, raising user awareness and education, implementing effective systems and processes, and actively participating in industry-wide focus groups.

Hasan (2022) **conducted a study entitled "Cybercrime Techniques in Online Banking".** The results were gathered using a five-point Likert scale questionnaire. The survey's target audience was confined to IT professionals working in small and medium-sized enterprises (SMEs). This study's statistical analysis was carried out using SPSS v26.0 on Windows. This was performed using descriptive statistics. The study was done using a quantitative survey, which revealed that cybercrime has a detrimental impact on the financial services sector. The study found that 24.9% of financial institutions were exposed to cybercrime and 8.5% to electronic commerce. The study's primary findings stated that the impact of cybercrime was created by security weaknesses in cyber techniques, which resulted in the theft of some consumer information. The study found that cybercrime is a danger that encompasses a wide range of online criminal actions in a variety of contexts. The research also stated that companies must be aware of the impact of cybercrime to make appropriate measurements. The study recommended that financial institutions perform extensive internal and cyber security analyses, as well as defense training, which prompted prior research on the impact of cybercrime on online banking use and the potential for big data.

Another research by Siahaan (2018), **Impact of cybercrime on technological and financial developments,** revealed that the more complicated the technology, the higher the level of criminal activity. The study argued that before the digital world, there were physical threats only and cybercrime only emerged since the beginning of the use of internet networks by organisations for instance in the past, transacting with a credit card needed a manual swapping machine but the use of the internet enabled transactions to be made online. The study revealed that anyone can be a victim of cybercrime given the increase in several organisations connected to the internet which hackers can easily abuse. The study also revealed that more developing markets are prone to the risk of cybercrime since they have a higher role in the global supply chain so competitors would want to gain competitive advantage through accessing business plans of the victims, making them attractive to cybercriminals. Cybercriminals take advantage of weak security systems management since several technology users are failing to take basic protection measures. The study articulated that many companies tend to focus more on their economic value circulation and neglect the basic protection of their products while cyber perpetrators use simple technology to identify their targets and automate the creation and delivery of software and easy monetisation of their proceeds of crime. The study recommended that cybercrimes affect technology, individuals, and companies' finances through severe losses and cyber-enabled financial crises. To curb cybercrimes, the study suggested that there should be adequate security in corporate networks when communicating with the external world.

Balan, Otto, Minasian, and Aryal (2017) published a study titled **"Data Analysis of Cybercrimes in Business"** that outlined cyber security risks and their impact on US-based firms. The search was carried out utilizing a survey and big data methods. The study discovered that one of the key causes of the growth in cyberattacks was people's lack of awareness of the crime, making many people and organizations vulnerable to cyber-attacks. The survey also discovered that organisations in the United States had incurred significant financial losses because of cyberattacks. The report recommended that enterprises put in place cyber security measures such as data encryption and password authentication to limit the number of cyber breaches and to lessen the likelihood of cybercrime.

Al-Alawi and Al Basaam (2020) conducted a study named “**Study of the Cybercrime Cost and the Risk of Criminal Threats to the Banking Sector”,** which focused on cybercrime costs, losses, and the risk of criminal threats to the banking industry, as well as suggestions for reducing the risk of criminal threats to enterprises. The study employed a quantitative research method, with 168 self-administered questionnaires distributed to 119 IT personnel, just 10 of which were not returned. According to the study's findings, 46% of respondents were unsure about their knowledge of security issues. The study concluded that proper execution of security risks necessitated awareness and training. The survey also found that there are no specialised professional IT security certificates, indicating a lack of interest in training courses that raise awareness and advancement in the sector of rapid technological revolution. The major findings concluded that staff education and awareness of technological crimes can prepare them to function as a human firewall to fight against any cyberattack.

Mugari and Olutola (2021) did a study titled **"Electronic Card Payment Risks: Combating Card Fraud in Zimbabwe during the Liquidity Crisis."** which examined the nature of fraudulent activities involving card payment systems and made recommendations to combat electronic card fraud. A questionnaire and interviews were used to collect data for the study, which was conducted in Harare's primary business center with 136 respondents. In addition, the poll discovered that card cloning appears to be on the rise in Zimbabwe's retail business. The report recommended the use of two-factor authentication when using digital banking platforms to counter card fraud. The major findings also highlighted that organizations must conduct thorough pre-employment checks and lifestyle assessments. To add on, the paper reviewed that penetration testing and cyber security audits were among the most crucial measures to detect and counter cybercrimes in organizations. The study also recommended internal control strategies such as job rotation, stringent supervision, and regular cybersecurity compliance checks as potential ways to decrease cybercrime.

Frank and Odunayo (2013) conducted a study **entitled "Approach to Cyber Security Issues in Nigeria: Challenges and Solutions."** The research's goal was to help firms lessen their vulnerability to cybercrime. The study's data was collected through interviews, online questionnaires, and surveys. The survey discovered that cybercriminals were often between the ages of 18 and 25 and that they primarily lived in cities. The report also revealed that cybercrime in Nigeria ranged from fraudulent lotteries to the most sophisticated digital fraud. The study proposed several measures to prevent cybercrime, including the promotion of cyber ethics and rules, education, and the formation of programs and IT forums. The study recommended the government of Nigeria to develop work opportunities for youths and establish IT labs/forums. This can contribute to the development of IT in Nigeria while also rewarding individuals for their innovative efforts. To add to the recommendations, Frank and Odunayo (2013), argued the importance of educational campaigns, the use of address Verification Systems (AVS), the use of Interactive Voice Response (IVR), IP Address tracking, use of Video Surveillance Systems, use of antivirus and anti-spyware Software and firewalls to detect and protect a computer network from unauthorized access.

2.4 Gap Analysis

Numerous scholars have been attracted to the subject of cybercrime in financial institutions, and numerous investigations have been carried out throughout multiple nations, emphasizing diverse facets such as safeguarding clients from this peril, among other things. Although Mugari (2016)'s groundbreaking research found that computer virus infection was widespread in Zimbabwe's financial institutions, technological dynamism may have changed the nature of cybercrime. With the advent of digitalization, virus distribution may no longer be the primary driver of the major categories of technological crimes.

According to an ICSPA survey, the most common types of cybercrime in businesses were malicious software and virus attacks. Similarly, a study by Boateng et al. (2011) that investigated the prevalence, types, and effects of technological crimes revealed that it was increasing in Ghana. The agencies lacked the technical know-how to deal with the problem. These studies offer a thorough grasp of technological crimes, although their conclusions might not line up with those of the financial institutions in Zimbabwe. Furthermore, this study attempted to close a research gap left by Boateng et al.'s study, which did not particularly examine the effects of cybercrime in the finance industry.

While Achrya and Joshi (2020) investigated cybercrime effects on financial institutions, the study's conclusions might not apply to cybercrimes committed in Zimbabwe. This is because Zimbabwe and India have different technology systems. This study attempted to fill a research gap caused by the contextual variations between institutions in Zimbabwe and India.

Mugari et al., (2016) discovered in another study that the most recurrent threat facing financial institutions was hacking. Mugari et al., (2016) suggested control strategies such software upgrades, firewalls, and training as practical ways to fight cybercrime. Nevertheless, the study ignored the root causes of cybercrime in favor of concentrating only on the effectiveness of countermeasures. Understanding the driving forces behind a particular type of cybercrime is necessary before developing effective countermeasures. The methods found to combat cybercrime may no longer be effective due to their adaptable nature.

According to an ICSPA survey, the most common types of cybercrime in enterprises were malicious software and virus attacks. Similarly, a study by Boateng et al. (2010) that looked into the prevalence, types, and effects of cybercrime revealed that it was increasing in Ghana. The agencies did not have the necessary technical know-how to deal with the problem. These studies offer a thorough grasp of cybercrime, although their conclusions might not line up with those of the retail industry in Zimbabwe. Furthermore, this study attempted to close a research gap left by Boateng et al.'s study, which did not particularly examine the effects of cybercrime in the retail industry.

There is still a significant study deficit on technological crimes, despite the empirical studies mentioned above providing a solid foundation. State security issues have been the subject of numerous studies on cybercrime, mainly in the US, Asia, Europe, and West Africa. Moreover, a large number of the few previous researches on technological crimes concentrated on the hazards posed by technological crimes in banks and state-run institutions. Different nations and environments can see different manifestations of this crime. The study concluded that there is still much to learn about cybercrime, especially in the retail sector where technology is always changing. Because of this, the current study aimed to supplement earlier studies by presenting fresh information and research topics regarding the characteristics of cybercrime as well as

2.5 Chapter Summary

This chapter focused on the conceptual and theoretical framework about the study. It revealed previous studies on the nature of technological crimes, causes, impact and measures put in place by individuals and institutions against technological crimes in financial institutions.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

This chapter shall look at the methodology of the research and to study the responses to the research questions mentioned in the first chapter. It describes various terms as they were used in the study. The research design, data collection strategies, sampling plans, and data analysis methodology used in the study were also explained in detail in this chapter.

3.1.1 Research Design

According to Siedlecki (2020), research design means a plan for the study that shows the framework for data collection. It therefore defines how the research is going to be carried out. Its primary goal is to enable the researcher to tackle the research problem as clearly and successfully as feasible. For this study, the researcher combined the beneficial features of qualitative and quantitative research designs. The researchers employed a descriptive case study research design as a result.

(Ridder, 2017) defines descriptive case study research design as a method of analysis that combines precise research on a particular contemporary marvel in its natural environment, drawing on a variety of data sources. A case study research design aids in gathering sufficient data about the firm's primary operations in microfinance institutions. The researcher was able to thoroughly comprehend the behavioral pattern of the unit in question thanks to the case study research design. The case study design produced a useful hypothesis and data that helped test it, which allowed the body of generalized knowledge to grow richer. Additionally, the descriptive case study research design was suited for this study since it allowed the researcher to investigate issues including where, when, and how technological crimes were occurring. This made it easier to get a solid understanding of technological crimes and how they affect microfinance institutions. Furthermore, the fact that this design used a variety of methods and sources for data collection made it the preferred option above others. Questionnaires and interviews were some of the methods used to gather data. Furthermore, the descriptive case study research approach included visual aids like charts to help the reader grasp the incidence of cybercrime in MIFs. As noted earlier this chapter focuses on problem finding and problem solving.

3.1.2 Population study

A collection of the total elements for interface is defined as the population study (Cooper 2003). Data was collected from Getbucks employees and clients. Personnel of the mentioned Microfinance also served as trustworthy sources of information for the study because they are regularly exposed to the risks associated with technological crimes at work, providing accurate and trustworthy information about the risks of technological crimes in Microfinance institutions. Information was gathered from Getbucks Microfinance staff members and customers. Additionally, because they deal with the risks posed by electronic payment systems daily at work, employees of the aforementioned MIF served as trustworthy sources of information for the study, providing accurate and authentic information about the risks of cybercrime in MIFs. Stated differently, Getbucks served as a one-stop shop for gathering data. One of the company's operating segments is Consumer Lending, which offers personal loans to members of the public sector. For corporate clients, the Small and Medium Enterprise (SME) Lending segment offers loans and other credit facilities. School Fee Loans, Savings Accounts, Consumer Loans, Money Markets, SME Bank Products, Home Plan Loans, and other services are among the products offered by the company.

3.2 Population sample

N sample means a subset of the selected population size to participate in the study (Stratton, 2021). To keep project costs to a minimum, the researcher selected a sample size that was neither too large nor too small. The respondents of the study were Getbucks employees and clients. As a result of limited time and funding, the study used a population sample of 65 respondents to represent the whole population at Getbucks micro financial institution. This ensured that sufficient information was not limited and that the respondents did not feel intimidated. Researchers now have a better knowledge of the nature of technological crimes in microfinances according to the study's findings.

3.2.1 Sampling procedure

According to Stratton (2021), the sampling procedure is the process of selecting a segment of the population to represent the total population. In this study, stratified random sampling and purposive sampling techniques were used. Zimbabwe's major cities are home to many MIFs; a thorough examination of each one would yield a more complete picture of the results. Unfortunately, only a case study of Getbucks Microfinance was selected for this study due to time and budget constraints. Researchers were able to better understand cybercrime in microfinances thanks to the study's findings, which were also applied to other microfinance institutions in Zimbabwe. In table 3.1, the population constituency is compiled.

Table: 3.1 Sample size

N=65

Department	Scheduled Interviews	Conducted Interviews	Response Rate
IT	2	2	100%
Human Capital	1	1	100%
Credit Control	2	2	100%
Finance	5	5	100%
Total	10	10	100%

(Source: Primary data, 2024)

For this study, representatives from the IT, HR, credit control, and finance departments were chosen, along with accounts administrators, ICT specialists, clients, and general managers. There were 65 participants in total: nine from the IT department, five from the human capital department, twenty-two from the credit control department, and twenty-nine from the finance department.

Participants were chosen using a combination of non-probability and probability sampling techniques. Using methods of selective sampling and systematic random selection, the participants were selected from Getbucks Microfinance. The sections that follow covered the two sampling methods.

3.2.2 Stratified Random Sampling

Stratified random sampling is a sampling technique where a population is divided into different divisions or strata (Sharma, 2017). The ultimate subjects were randomly chosen from different subgroups. This method selects participants from several departments to guarantee that the sample accurately reflects the divisions. Targeting employees and individual account holders, the researcher stratified the responses from the interviewees. Using stratified random sampling reduced the bias in sample selection and made sure that certain microfinance departments weren't over or underrepresented. The sample size was chosen considering the experience level of each employee and dividing the workforce and clients into several departments. The departments selected 65 respondents in total to complete questionnaires, guaranteeing that every subject in the population had an equal chance of being selected for the sample.

3.2.3 Purposive Sampling

The researcher went on to use purposive sampling which was defined by (Bornstein, Jager & Putnick, 2017) as a non-probability sampling technique where the researcher chooses only study participants who, in their opinion, meet the study's objectives. Using this sampling strategy involved selecting study participants at random from the study population. Participants were selected based on pre-established traits or skills, such as those of clients and staff. Less rigorous, practical, and doable under time and resource restrictions were the benefits of using purposeful sampling. Because the expert informants were all Getbucks employees who were relevant, competent and perceptive, the study was more efficient. Purposive sampling aided in the researcher’s ability to weed out irrelevant responses that did not make sense for the study. Responses yielded comprehensive information because the primary informants were employed by the organization. Finding pertinent, trustworthy, and credible informants was made easier by using purposeful sampling to meet the study's objectives.

3.3 Research instruments

Pandey and Pandey (2021) defined an instrument in research as a device or tool used to collect data through surveys, interviews, or observation. Interviews and questionnaires were the research instruments used to gather data on the impact of technological crimes on micro financial institutions, from employees and clients. To facilitate participants’ responses, the questionnaire was split into two subsections. The respondents' age, gender, degree of education, and place of residence were the main topics of discussion in the first section. The second portion aimed to gather data regarding the types of technological crimes, their causes, and their effects on MIFs. A pilot study was carried out to confirm the questionnaires' reliability. Dissertations and journal articles were used to collect secondary data.

3.3.1 Questionnaires

A questionnaire is defined as the inclusive use of every technique of data collection, each individual is asked to respond to the same set of questions in the predetermined order as the researcher's design (Saunders et al., 2009). The researcher used questionnaires to gather qualitative data from the respondents. The questionnaires were made up of both closed and open-ended questions. Open-ended questions allowed respondents to think broadly before expressing their emotions and opinions while closed-ended questions are confined to specific categories of views to determine if the respondents agree or do not agree with the researcher's assumptions.

The study used questionnaires because they ensured confidentiality and created an environment of secrecy thus making participants cooperate willingly without any fears. In turn, Getbucks employees were able to answer comfortably. In addition, the researcher's absence lessened bias. The questionnaire was more effective than interviews because respondents had more time to fill in the questionnaire, resulting in accurate information and proper communication. Additionally, the responders had ample time to search for necessary records. Respondents to questionnaires could remain anonymous, which was advantageous if the questions posed were sensitive for respondents to answer.

On the other hand, questionnaires were costly because of the need to pay for printing services, typing, distribution, and collection time. It was difficult to know if the respondents willingly participated since questionnaires were distributed randomly. Some respondents did not disclose ideal facts on contentious issues in writing, but the same ideals could be well said in interviews.

A lack of communication between the researcher and the respondent caused issues with the questionnaire to go unaddressed, which led to some skewed responses. Furthermore, the questionnaires were personally distributed and collected by the researcher.

3.3.2 Interviews

According to Monday (2020), an interview is defined as an objective conversation between two or more people intending to provide feedback on a particular subject. One technique for collecting data is through semi-structured interviews, which create a conversation that allows the intended respondents the opportunity to share their opinions on a certain subject. Among the chosen sample size consisting of clients and employees, ten respondents were interviewed in semi-structured interviews.

Interviews enabled respondents to express their feelings accurately since they had a platform to ask for clarification of questions unlike in questionnaires. To reduce the possibility of being a victim, the interviews were conducted in private, and all interview materials were handled with secrecy. The primary advantage of interviewing participants for the study was that it enabled the investigator to get detailed information and explanations that could not be obtained via the questionnaire. The use of visual ads made it flexible for the respondents. In addition, it made it possible for the researcher to respond to the interviewees' comments, allowing them to discuss themes and subjects as they emerged.

Even though in-person interactions have numerous advantages, conducting interviews took a lot of time because the researcher had to get to know the participants before starting the interviews. Additionally, a few participants were unable to freely express themselves because of privacy and confidentiality issues, which restricted the scope of the interviews. To get past these barriers, the researcher needed to build trusting relationships with the interview subjects and reassure them that the information they provided would be kept private and used only for the study.

3.4 Data collection procedures

According to Couper (2017), data collection means any information obtained during a research study. The researcher asked for written permission from the University to carry out the study. At Getbucks, the researcher physically distributed questionnaires. After agreeing to take part, those who were interested were asked to sign a consent form attesting to their free will and knowledge of the study's goals. Using a questionnaire, the researcher used a variety of questions designed to provide data essential for meeting the study objectives. The questionnaires were delivered to the employees and clients in a total of 65 copies. The questionnaires were given to the respondents a week to be completed, after which the researcher collected each one separately. Ten respondents were purposefully chosen for the interviews. To complete the interview within the allocated time, the researcher set up a time with the respondents and used an interview guide. Each respondent had a different time limit, ranging from eight minutes. Semi-structured in-person interviews with individuals were carried out.

3.4.1 Validity and Reliability

Validity is defined as the extent to which a test measures what it is supposed to measure and the appropriateness with which inferences can be made depending on the test observations (Kothari, 2004). Reliability was defined by Robinson (2019) as the degree to which an evaluation can measure with measuring techniques or instruments to come up with consistent results. The questionnaires and interview guide were thoroughly examined to incorporate validity. To come up with the validity and reliability of data, a pilot test was conducted, and the research questions were designed carefully. In addition, to estimate the amount of time and resources needed to complete the examination and identify any sample issues, the interview guide and the questionnaires were pre-tested beforehand. To ensure coordinated responses, straightforward questions were asked to come up with direct responses.

3.5 Ethical considerations

According to Resnik (2015), ethics means norms that distinguish or define behavior that is acceptable and unacceptable. In this research, participants were given the right to withdraw from the research whenever they needed. In compliance with Resnik (2015), the research was carried out under participants’ consent clarifying that only voluntary participants were needed, and they were free to withdraw from the research of their choice. All the information given in the research was kept confidential. Also, the research sample terms were to improve understanding by the respondents, no jargon was used in the research questions. The research questionnaires and interview guide had no option for jotting the names of the respondents. This assured them that the information was going to be confidential. More significantly, every research volunteer received fairness, respect, and decency.

3.5.1 Pre-testing the instruments of the research

The research instruments were pretested before administering them to the respondents to ensure accuracy. The purpose of pre-testing the questionnaires and interview guide were to reveal ambiguous meanings, make short and precise questions, remove poor wording of the research questions, and ensure that the research instruments were clear to the researcher. However, pre-testing the research questions was time-consuming to the researcher due to the need to redo the same task twice. Previous researchers also made recommendations and the feedback from the pre-test was used in constructing the research questions.

3.5.2 Data processing, analysis and feedback

According to (Haberman & Miles 2004), data processing, analysis, and feedback means data reduction, display, conclusion, and verification. (Haberman & Miles 2004), went on to cite three core elements of qualitative data analysis as simple as data reduction. They defined data reduction as selecting, focusing, simplifying, and transforming data observed in written field notes. The research considered a variety of data to ensure proper management and evaluation to be made successfully. Data visualisation involves putting qualitative statistics into an examination for assessment to suit a meticulous objective. Usually, data is displayed using descriptive statistics in the form of figures, text, charts, tables, graphs, percentages, and frequency to form systematic trends and patterns that show interrelationships between variables. Both quantitative and qualitative analysis was performed on the survey data that was collected. Data collected via questionnaires was analyzed using SPSS software, and tabular and graphical displays were added using Microsoft Excel software. The researcher collected the responses, looked over them for insights and meaning, contrasted and compared the different answers from the respondents, and finally deciphered the meaning to generate useful data. Data presentation, analysis, and conclusions are properly defined in chapter four.

3.6 Chapter summary

This chapter focused on research methodology which is made up of the research design or plan, population size, targeted population, sampling techniques for instance stratified sampling and purposive sampling techniques, data validity, and reliability testing. The next chapter focuses on data presentation, analysis, and conclusion.

CHAPTER IV

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 Introduction

This chapter focuses on data presentation, analysis, and discussion of instruments that the researcher utilised. Data analysis was done to show the impact of technological crimes in micro-financial institutions, nature, causes, and measures to address technological crimes at Getbucks (Pvt) Ltd. The results of the study are presented in the form of visual graphs, charts, tables, and percentages.

Table 4.1: Questionnaire response rate

Department	Questionnaires issued	Questionnaires returned	Response rate
IT	7	6	86%
Human Capital	4	3	75%
Credit Control	20	18	90%
Finance	24	23	96%
Total	55	50	91%

[Source: raw data 2024]

Table 4.1 reveals that 55 questionnaires were distributed across several departments. Of the 55 distributed, 50 were responded to, resulting in a 91% response rate. This means that most questions were completed. However, just 8% of the questionnaires distributed were unanswered, since respondents stated that they were busy. Creswell (2014) says that a response rate of more than 50% is necessary for the researcher to acquire impartial results; however, the response rate for this study was significantly higher than 50%, fully supporting the research aims.

4.1.1 Interview Response Rate

Table 4.2 Interview Response Rate

Department	Scheduled Interviews	Conducted Interviews	Response Rate
IT	2	2	100%
Human Capital	1	1	100%
Credit Control	2	2	100%
Finance	5	5	100%
Total	10	10	100%

[Source: Primary Source, 2024]

The researcher planned to conduct ten interviews, selecting two respondents from each department and Human Capital. The observations from the interviews imply that 100% of the participants who were invited to the interviews attended and were effectively interviewed. This shows that interviews helped conduct research queries due to the high response rate. Another expert indicated that a response rate of more than 50% is sufficient for the researcher to produce impartial results; hence, for this study, the response rate was larger than 50%, fully supporting the research objectives (Creswell 2014).

4.2 Demographic information of respondents

Demographic information was acquired, including age, gender, education level, place of residence, and period of residence. The variables were depicted as they appear in the table below.

Table 4.3: Demographic distribution of questionnaire respondents

Demographic category	Demographic variable	Frequency	Percentage %
Gender	Female	33	60
	Male	22	40
	Total	55	100
Age Distribution	Between 18-24 Years	10	18.18
	25-34	14	25.45
	35-44	20	36.36
	45 years and above	11	20
	Total	55	100
Level of Education	O and A level	5	9.09
	Diploma Level	13	23.64
	Undergraduate Degree	23	41.82
	Postgraduates	12	21.82
	Total	55	100
Area of Residence	High Density	12	21.82
	Low Density	21	38.18
	Medium Density	15	27.27
	CBD	7	12.73
	Total	55	100
Period of Residence	Below 2 years	12	21.82
	2-5 years	21	38.18
	6-10 years	15	27.27
	Above 10 years	7	12.73
	Total	55	100

[Source - raw data, 2024]

Gender of Respondents

Table 4.2 shows that 60% of the respondents were female, while 40% were male, indicating that females predominated in the surveys. Gender sensitivity guided the dissemination of the questionnaire, and no evidence of bias of any kind was identified.

Age of Respondents

The age of the respondents varied from 18 to above 45 years of age. The age of respondents is presented in table 4.3, which shows both the frequency and percentage of the number of respondents that fall in the age classes or categories as shown above.

The age range of each respondent who took part in the research study is also shown in the table. The age range of 25-34 years included 25.45% of the respondents, while the interval of 35-44 years had the largest frequency in the age distribution, indicated by 36.36%. Of the entire research population, respondents over the age of 45 made up 20%, while respondents of 18-24 years made up just 18.18%. This age distribution reveals that many survey respondents were middle-aged individuals who might have had more work experience in the industry.

Qualifications of Respondents

The table also indicates the distribution of respondents based on their qualifications. Their qualifications were categorized as O' & A' level certificates, national certificates & diplomas, undergraduate degrees, and other levels. The respondents with undergraduate degrees were ranked the highest with 41.82% of the total respondents. This was followed by diplomas with 23.64%, which ranked the second highest and 21.82% of the respondents were post-graduates. Respondents with ordinary and advanced level certificates were ranked fourth with the least number of participants. Most respondents who participated in the research were well-educated with tertiary-level qualifications. They promoted authentic and reliable data to be extracted from the research since most respondents were knowledgeable about technological crimes in MIFs.

Residential area

The low-density residential region had the highest reply rate (38.18%) because that is where the majority of the population resides. The respondents' demographics were as follows: 21.82% lived in high density, 12.73% in the CBD, and 27.27% in medium density.

4.3 Research Findings

4.3.1 Nature of technological crimes in micro-financial institutions

The forms of cybercrime that were common in the respondents' organizations were asked to be indicated, and the results are summarized in the table below.

Table 4.3: Prevalence of technological crimes N=50

TECHNOLOGICAL CRIMES	1		2		3		4		STATISTICS	
	FREQ	%	FREQ	%	FREQ	%	FREQ	%	MEAN	S.D
Phishing	1	2	4	8	19	38	26	52	3.4	0.728
Malware	2	4	5	10	20	40	23	46	3.28	0.809
Card Fraud	3	6	5	10	18	36	24	48	3.26	0.876
Hacking	6	12	5	10	14	28	25	50	3.16	1.037
DoS	7	14	8	16	13	26	22	44	3	1.088
Identity Theft	5	10	20	40	15	30	10	20	2.6	0.926

[Source – Raw data, 2024]

Key: *Freq- Frequency; %- Percentage, SD- Standard Deviation, 1- Doesn't occur, 2- Less than prevalent, 3-Prevalent, 4- Very prevalent*

4.3.1.1 Phishing

As shown in Table 4.3, 93% of respondents believed that phishing was the most prevalent technological crime in MFIs, whereas 10% denied that corruption was prevalent in MFIs. The mean statistic of 3.4 and an SD of 0.728 indicate that phishing has emerged as a source of financial fraud in Zimbabwe. Since the research made decisions based on majority rule, the inquiry revealed that phishing is rampant in the financial sector.

According to the interview responses, customers revealed that cybercriminals usually send false emails asking victims to resend their banking passwords or account numbers to fix a supposed account glitch. The perpetrators claim to be legitimate bank employees with the hidden intention to conceal funds. Although (Mugari's, 2016; and ICSPA, 2013) findings revealed that phishing was less prevalent in the financial sector, it is worrying to note that the harmful threat was found to be the most prevalent technological crime in MFIs.

4.3.1.2 Malware

A significant majority of 86% of respondents agreed that malware was one of the most common types of technological crime in MFIs, whereas just 14% believed that malware was widespread in MFIs. The respondents revealed that malware attacks occur when perpetrators send a corrupt link to the victim resulting in them taking over the operating system of the victim. With a statistic mean of 3.28 and a standard deviation of 0.809, these findings demonstrate that despite the passage of time, the introduction of new technologies has resulted in new methods of propagating malware through worms and viruses in the banking industry. Malware is common in MFIs because it is hidden when it enters the computer without authorization. This research supports the findings of Uppal et al., (2014), who identified Malware as a widespread cybercrime in banks.

In an interview, a computer expert stated, "One major difficulty we are experiencing is the infiltration of computers by malware such as viruses, botnets, and worms. These malware have cost us a lot of money because they destroy a large amount of corporate data if not backed up." This is caused by the use of unsafe gadgets to access personal information.

4.3.1.3 Card Fraud

Table 4.3 demonstrates that 84% of respondents agreed that card fraud is prevalent in MFIs, whereas 16%, or a smaller fraction, objected. The mean value of 3.26 with a standard deviation of 0.876 indicates that card fraud is becoming a more prevalent occurrence in the financial industry. Because MFIs use money transfers from one person to another in transactions, victims disclose their credit card and identity details, which if obtained by cybercriminals can be used to conduct fraud. This is mostly due to the growing acceptance of card payment systems, fueled by liquidity constraints, as cited in Bamrara et al., (2013).

During an interview, one of the interviewees stated that the cashless environment increases the vulnerability to card fraud due to the use of swiping equipment. These findings suggest that the increase in card usage is exposing MFIs and consumers to card fraud. Despite its limited existence, as observed by Mugari (2016), the current study discovered that card fraud is currently a source of worry in the banking industry. The increase in card fraud is due to the country's cash crisis, which has driven practically everyone to acquire a debit card. As a result, fraudsters have used this to their advantage, preying on unwary client cards. These findings indicate that credit card use has led to an increase in card fraud.

4.3.1.4 Hacking

Hacking was regarded as common among MFIs, with 78% of respondents agreeing and 12% disagreeing. Hacking had an average of 3.16 and a standard deviation of 1.037. Given that banks execute a large portion of their operations through internet platforms, hackers have discovered new routes for criminal activity. As a result, respondents expressed concern that fully adopting online transactions would be costly if they were hacked. After analysing the study's findings and those of previous studies, it is clear that hacking is a persistent crime, as identified by Mugari (2016). Fighting cybercrime in banks is challenging, as it remains one of the most common types.

During the interviews, two Accounts administrators mentioned that cyber fraudsters are increasingly targeting the financial sector because most of commerce is being done online for a variety of reasons, including growing use of new business practices. Financial institutions have been a prime target for hackers seeking to steal information for fraudulent purposes. The findings of this study also reveal that it is rapidly gaining traction in the financial sector.

4.3.1.5 Identity theft and DOS

Identity theft was regarded as less common in the banking industry, with 40% responding that it does not occur and 20% indicating that it is very common. Of the ten interviewees, only one agreed that identity theft occurs in MFIs at Getbucks. According to Bamrara et al., identity theft is less prevalent in MFIs. DoS is also deemed less widespread in Zimbabwe's retail sector, as seen in table 4.3, with 14% of respondents responding that it is less than prevalent and 16% indicating that it does not occur. To add on, this is supported by research conducted by (ICSPA) who stated that DOS was less prevalent.

4.4 Causes of technological crimes in micro-financial institutions

Table 4.4: Major causes of technological crimes

Causes of technological crimes	SD		D		A		SA		STATISTICS	
	Freq	%	Freq	%	Freq	%	Freq	%	Mean	S.D
Economic Factors	2	4	3	6	30	60	15	30	3.16	0.71
Weak Security Systems	3	6	4	8	25	50	18	36	3.16	0.817
Lack of Cybersecurity awareness	12	24	5	10	18	36	15	30	2.72	1.144
Poor recruitment practices	11	22	18	36	12	24	9	18	2.38	1.028

[Source – raw data 2024]

Key: *Freq- Frequency; %- Percentage, S.D- Standard Deviation, SD-Strongly Disagree, D-Disagree, A-Agree, SA- Strongly Agree.*

4.4.1 Economic Factors

As depicted in table 4.4, 90% of the respondents agreed that economic factors were the highest causation of technological crimes in MFIs, whereas 10% disagreed with the majority's assessment that cybercriminals are driven by economic factors to commit crimes. Since money is typically the driving force behind cybercrimes, perpetrators frequently hide behind internet networks in the knowledge that it will be difficult to catch them. Cybercriminals are drawn to the money held by MFIs, and the lack of employment opportunities increases the vulnerability of MFIs to cyberattacks. According to the respondents, cybercriminals typically use identity theft, phony emails, and other tactics to extract money in exchange for rewards from their victims (Viraja, 2021). This finding resonates with Boateng et al., averment that economic factors push cybercriminals to commit cyberattacks in financial institutions due to their services such as loans, and online banking.

In an interview, one customer had this to say, "I once lost some money after I got scammed by a cyber-criminal". These findings reveal that idleness causes criminals to go to extreme measures to gain finance. Thus, the government should increase employment opportunities to reduce cyber-attacks.

4.4.2 Weak Security Systems

Out of the 50 responded questionnaires, 86% confirmed that weak security systems were a cause of technological crimes in MFIs, despite 14% of the respondents who indicated that it was not a common cause of technological crimes. With a statistical mean of 3.16 and a standard deviation of 0.817, weak security systems seem to be the second major cause of technological crimes in banks. More than half of the respondents agreed that opportunity provides a possibility for cybercriminals to commit crime, implying that the information was accurate. Cybercriminals use system vulnerabilities to get access to a bank's network or data.

Ineffective security measures may include obsolete software, poor passwords, and insufficient encryption standards providing a chance for cybercriminals in the absence of a capable guardian such as updated antiviruses, firewalls, and other sufficient security measures. guardian. Any flaws in these areas can allow motivated offenders to penetrate bank systems and carry out illegal actions. Similar findings were discovered by Siahaan (2018), in which it was discovered that weak security systems contributed to banks being attacked by cybercriminals. In an interview, one accounts administrator said, “The tactics and methods used by cybercriminals are evolving, and banks lack efficient systems.”

4.4.3 Lack of Cybersecurity awareness

Out of the 50 Questionnaires responded, 66% confirmed that Lack of Cybersecurity awareness was one of the causes of technological crimes, whereas 24% disputed that it was a common causation in MFIs. With a statistic mean of 2.72 and a standard deviation of 1.144, respondents stated that cybercriminals plan to target financial institutions because they know that some customers and employees lack adequate knowledge of technological crimes. Al-Alawi and Al Basaam (2020) found that a lack of cybersecurity awareness is a contributing factor to technological crimes in financial institutions.

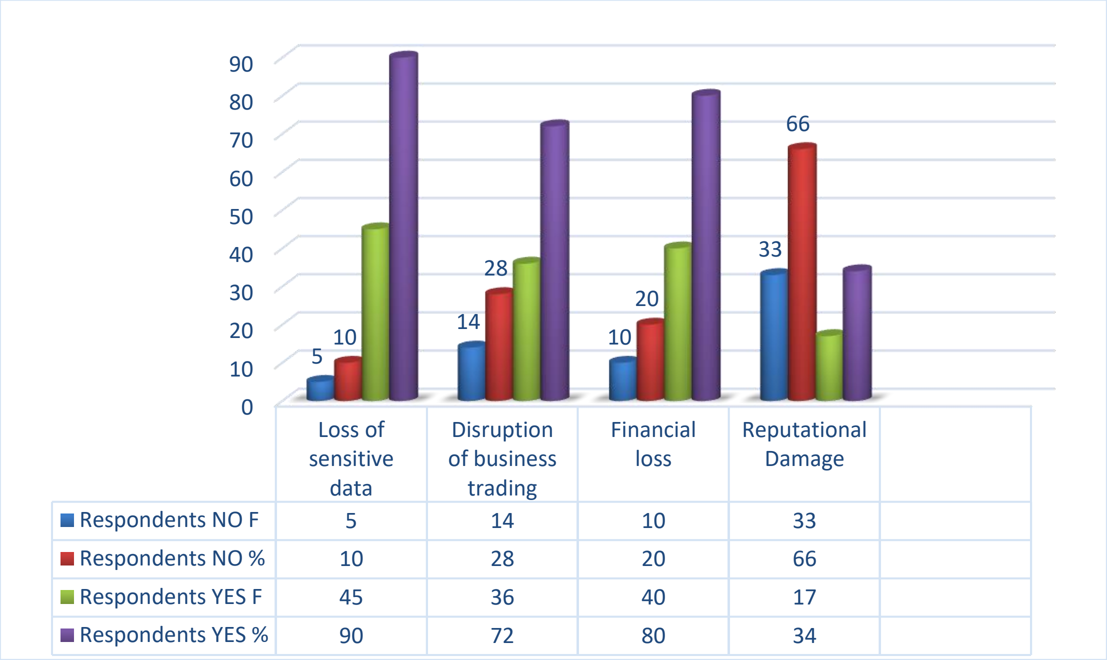
In an interview, one of the interviewees stated that “although not everyone experiences cybercrime, those who do will often be soft targets who readily provide answers to the criminals' inquiries about their bank account information and ID numbers.” These findings showed that employees and customers lack knowledge of cybercrime and cybersecurity, thus they are prone to be targeted by criminals as criminals would take advantage of this vulnerability. MFIs should therefore hold awareness campaigns, education seminars and regular examinations to employees in order to protect employees and clients.

4.4.4 Poor recruitment practices

The table reveals that, according to 58% of respondents disagreed that poor recruitment practices contributed to cyber-attacks, whereas 42 % inclined that poor recruitment practices were a causation of cyber-attacks at Getbucks. The statistical mean was 2.38 with a standard deviation of 1.028 shows that cybercriminals typically have moral or ethical motivations for their actions, such as a desire to exact revenge on their victims by causing harm to computer networks, due to the hiring of individuals who later become insider threats, who may have malicious intentions from the start, or they may become dissatisfied owing to poor treatment, a lack of advancement possibilities, or other causes, causing them to engage in cybercrime. These findings are supported by Viraja (2021), who stated that poor background checks before hiring employees may lead to organisations hiring cyber criminals, which may lead serious threats to the institution.

Therefore, banks should enforce strict recruitment policies to ensure that workers have the required skills, expertise, and ethical standards to protect banking systems and data. This may also be ensured through thorough background checks before hiring employees to work for the institution.

4.5 Impact of Technological Crimes in micro-financial institutions



	Loss of sensitive data	Disruption of business trading	Financial loss	Reputational Damage	
🟦 Respondents NO F	5	14	10	33	
🟥 Respondents NO %	10	28	20	66	
🟩 Respondents YES F	45	36	40	17	
🟪 Respondents YES %	90	72	80	34	

[Source – raw data 2024]

Fig 4.1: Major impacts of technological crimes in micro-financial institutions

4.5.1 Financial loss

Figure 3 illustrates that financial loss was ranked as the most significant impact of technology crimes, specifically cybercrime in all its manifestations. Out of the 50 questionnaires returned, 80% acknowledged that cybercrime causes significant financial loss to victims, whereas 20% declined that financial loss was an impact of technological crimes. The results from those who declined were because the respondents had never experienced loss of money from cyber-criminals. Electronic theft of the victim's finances causes a financial crisis and disrupts the victim's cash flow, ultimately leading to insolvency. This was also corroborated by Mugari et al., (2023). They demonstrated that cybercrime causes significant financial damage for individuals and corporations. Financial institutions employ automated teller machines (ATM) networks, which hackers can also access, leading to the theft of funds to the offenders' mule accounts.

These findings were also supported by (Cohen & Felson 1979) who mentioned that the attractiveness of the targeted victim causes crimes. To put it in the context of cybercrime in micro-financial institutions, cybercriminals are motivated by the circulation of money in financial institutions.

Two interviewees experienced direct financial losses, with one stating, "I lost a lot of money after a cybercriminal penetrated my accounting system and transferred money to his account." It took a long time to realize I had been robbed by a cybercriminal. Financial institutions employ automated teller machines (ATM) networks, which hackers can also access, leading to the theft of funds to the offenders' mule accounts.

4.5.2 Reputational damage

Figure 4.1 demonstrates that 34% of the participants indicated that their organisation had never suffered from reputational damage. Thes results show that some organisations may be quick to react to cyber-attacks before the general public discovers the major impact. However, if the news of an organisation being cyber attacked gets out to the public, clients may lose faith and confidence in the affected financial institution, resulting in loss of revenue for the victim. However, despite the findings by (Acharya and Joshi, 2020; ICSPA 2022) which stated that reputational damage is a cause of concern after a cyber-attack, it is worrying to note that in some countries reputational damage has occurred in the financial sector.

Similar conclusions emerged from the interviews, with only one interviewee stating that the MFI had never suffered from reputational damage due to technological crimes. The interviewee revealed that cybercrimes are usually complex, and multi-transactions make it difficult for law enforcement to trace the transactions. The interviewee also revealed that most of the cyber-attacks on individuals go unreported since cybercrime is still a modern form of crime hence some people do not know where exactly to go and report.

4.5.3 Disruption of business trading

Fig 4.1 above demonstrates that disruption of commercial trading was the third most significant impact of cybercriminals in microfinancial institutions. A group of 72% of respondents claimed that cybercrime disrupts commercial transactions, whereas 28%, declined that disruption of business trading was an impact in MFIs. Loss of client information to cybercriminals may disrupt the firm's day-to-day operations. This was also reinforced by (ICSPA 2022), who stated that the victimized company would be required to pay fines for criminal breaches, increasing the victim's expenditure operations and disrupting business operations.

This type of impact causes institutions to take time in setting up measures that will mitigate the attack after it would have occurred, as well as time consumption in restoring systems and networks.

4.5.4 Loss of sensitive Data

Of all the participants, 90% conceded that cyber-attacks led to loss in sensitive data, through malware and hacking. The respondents confirmed that organisations may lose sensitive data which may compromise their operations. Only 10% of the respondents indicated that loss of sensitive data does not occur in MFIs. Most respondents stated that cybercrime will push the victim to update their company methods in order to keep their information secure. This was also endorsed by Acharya and Joshi, (2020), who stated that institutions would need to adapt their past operational processes to protect their information from cybercriminals. These results showed that there are now greater opportunities for illicit activity on the internet.

In an interview, one IT expert had this to say, "With the rise of online transactions, businesses are more vulnerable to malware attacks and run a very high risk of losing important business data."

4.6 Recommendations proffered to combat technological crimes and protect micro-financial institutions.

Table 4.5: Recommendations to combat technological crimes

Measures against technological crimes	Respondents			
	NO		YES	
	F	%	F	%
Education and Training	12	24	38	76
Constantly update antivirus and anti-spyware software	7	14	45	90
Cyber security Audits and Compliance Checks	0	0	50	100
Strong Passwords and data encryption	7	14	43	86

[Source; raw data 2024]

Key- F- Frequency, %-Percentage

4.6.1 Cyber Security audits and compliance checks

As shown in Table 4.5, all respondents (100%) acknowledged that cyber security audits are useful for reducing the risks associated with cybercrime. Furthermore, every respondent acknowledged that using cyber audits would be a good method to reduce the possibility of cyberattacks at Getbucks. These results were in line with those of a study conducted in 2021 by Mugari and Olotula (2021), which found that one of the most popular methods for shielding a company from cyberattacks was to do compliance inspections and cyber security audits.

Similarly, every interviewee stated that they would like to see compliance inspections and cyber security assessments put into place. MFIs must implement cyber security audits and compliance checks to reduce cyber-attacks. This measure is for the long run as it is a precautionary measure.

4.6.2 Constantly update antivirus and anti-spyware software

The observations from the research show that 25% of the respondents mentioned that downloading of anti-spyware software is one of the measures to curb technological crimes. Although research done by Frank and Odunayo (2013), who stated that, antiviruses and anti-spyware softwares were not effective measures to protect large institutions, this research found out that several of the respondents preferred the use of these tools and found them as effective measures. Spyware is capable of stealing login passwords and monitoring a user's browsing activities, so anti-spyware programs detect and remove spyware and are used to safeguard user privacy and stop identity theft. Similarly, one may also prevent oneself from an attack by downloading anti-virus software that detects and quarantines infected files. By doing so, an individual can successfully prevent malware such as worms, viruses, and spyware and protect themselves from identity theft and ransomware attacks

Similarly, five interviewees stated that their primary line of defense against malware and spyware attacks is the usage of antivirus and anti-spyware software. One of the five interviewees acknowledges the fact that using antivirus software was their first line of defense against fraud.

4.6.3 Strong passwords and data encryption

A substantial 86% of respondents confirmed they encrypted their data and used strong passwords for their devices and systems, compared to 14% who either used weak passwords or didn't know what data encryption was. As a result, a portion of the participants lacked knowledge regarding data encryption as a safeguard against cybercrime for their organizations. These findings were consistent with the findings of research by Bala et al., (2017) who stated that strong passwords and data encryption was an effective countermeasure against technological crimes.

Six interviewees also attested to the MFI's use of data encryptions as a safeguard against cybercrime on their computers. Two of the clients who were interviewed revealed that they were ignorant of data encryption. To secure themselves, users must create strong passwords that include capital letters, numbers, and characters. However, some users use their date of birth as passwords which is unsafe, thus computer users must refrain from using such passwords.

4.6.4 Education and training

Table 4.5 shows that 76% of the respondents revealed that education and training of employees and clients about technological crimes helps to prevent the crime’s increase, whereas 24% declined the necessity of education and training. Micro-financial institutions should prioritize training staff members on data protection regulations, empowering them with knowledge of cyber security to ensure they are constantly vigilant against external intrusions, and educating them through self-awareness initiatives Research done by Al-Alawi et al., (2020) indicated that financial institutions and organizations must train their clients and employees respectively about recent happenings in the domain of technological crimes as well as highlighting measures that should be put in place against technological crimes.

4.7 Other measures to curb Technological Crimes.

4.7.1 Use of Secret Socket Layer-SSL

Of all the questionnaire respondents, 56% suggested that using the secret socket layer (SSL) protocol is required to stop cyberattacks against bank backend web services. When a browser requests access to a website's data, it first retrieves the SSL certificate and verifies that it is valid, issued by a recognised authority, and being used by the website for which it is intended. If all these criteria are met, the browser is then granted access to the website's data.

4.7.1 Awareness campaigns

About 70% of the respondents implied that awareness campaigns should be conducted to the general public on the threat of technological crimes. Awareness campaigns were ranked the fourth highest measure against technological crimes. This was also supported by (Viraja, 2021) who mentioned that organizations, media, and educational institutions should make enough efforts to spread awareness to help individuals and businesses on cybercrimes worldwide. They were of the idea that in this technological era, everybody uses smartphones while unaware that they're vulnerable to cyber-attacks. They suggested that media should assist in advertising measures and informing the public on the impact of cybercrimes on the government, individuals, and organisations.

Several interviewees stated that educating the public and providing media attention may significantly increase knowledge of cybercrime in Zimbabwe's financial industry. This was corroborated by an ISCPA poll that found the best methods for increasing public awareness of cybercrime were events, media coverage, and education.

4.8 Chapter Summary

In this chapter, the researcher analysed the data, and the research observations were presented in the form of tables, pie charts, and bar graphs. Based on the research findings, technological crimes are prevalent in MIFs. Cybercrime has devastating impacts on micro-financial institutions, they result in severe financial losses, reputational damage and disturb business operations. Various measures were proposed to curb cybercrimes in micro-financial institutions, including the need to train staff, clients, and skilled law enforcement agencies, the use of SSL, downloading of anti-virus software and providing awareness campaigns to the public. However, the increase in technology has remained the major challenge in curbing cybercrime hence criminals find new ways of attacking.

CHAPTER V

SUMMARY, CONCLUSION & RECOMMENDATIONS

5.0 Introduction

This chapter provided a summary of the research observations along with study recommendations and conclusions derived from the findings.

5.1 Research summary

The study focused on the impact of technological crimes in micro-financial institutions, the study of Getbucks Harare, Zimbabwe. In chapter one, the research was concerned with rampant technological crimes in micro-financial institutions including the backing sector at large due to the emergence of electronic banking and the Internet. Increase in technology has given a chance for cybercriminals to steal money electronically. The chapter detailed the background of the study, statement of the problem, research objectives and research questions, assumptions of the research, limitations and delimitations, significance of the study to different stakeholders and a summary of the chapter at its bottom. To conduct the research, the research was guided by four objectives and questions of the research with the third being the main objectives of the research as listed below.

1. To demonstrate the nature of technological crimes in micro-financial institutions
2. To discuss the causes of technological crimes in micro-financial institutions
3. To determine the extent to which technological crimes affect micro financial institutions' performance.
4. To highlight and recommend best practices to address technological crimes in micro financial institutions and research questions were as follows.

5.2 Research questions

1. Which forms of technological crimes are prevalent in micro financial institutions?

2. What are the causes of technological crime in micro financial institutions?

3. What are the effects of technological crimes in financial institutions?

4. Which recommendations are proffered to combat technological crimes and protect micro financial institutions?

In chapter two, the research considered previous literature from relevant studies about the nature, causes, impacts, and recommendations about technological crimes in micro-financial institutions in the financial sector. A variety of secondary information was looked up on such as textbooks, journals, online publications, and articles. The theoretical literature, empirical evidence, and conceptual framework were all presented and critically assessed in this chapter as well.

The third chapter of the research looked at the methodology or research plan. The research design, targeted population, population sample size, data collection procedures, sampling techniques, data presentation and analysis, interviews, and questionnaire respondents were highlighted in this chapter.

Chapter four of the research analysed and evaluated the observations of the research. It aimed at answering the research questions as well as discussing the results of the study. The results of the study were presented in the form of tables and bar graphs. The frequency of the respondents and percentages were used to classify the number of respondents per outcome.

5.3 Summary of research findings

Pertaining to the nature of technological crimes, phishing, hacking, identity theft, card fraud, malware, and DOS were found as the most prevailing forms of technological or in micro-financial institutions, respectively. The researcher discovered that the two most common forms of technological crimes in micro-financial institutions were phishing and hacking. DOS was found to be less common in the financial sector, although the data indicated that it was slowly making its way there.According to the observations of the research, the main causes of technological crimes were attributed to economic factors, weak security systems, lack of cybersecurity awareness, and poor recruitment practices. personal respectively.

Although electronic banking has easy business in micro-financial institutions, it has also resulted in the loss of sensitive data, disruption of business trading, financial loss, and reputational damage to the business, respectively. The question of the impact of cybercrime in micro-financial institutions was the major objective of the research. Technological crimes have a huge effect on the future of the organisation as it may take time for institutions to get back to normal business trading in the event of an attack.

Despite the impacts of technological crimes in micro-financial institutions, individuals, organizations, and governments have put some measures in place to curb micro-financial institutions. These included education and training, constantly updating antivirus and anti-spyware software, cyber security audits and compliance checks, strong passwords and data encryption, awareness campaigns, and use of secret socket layer (SSL) respectively. It was suggested in the research that MFIs regularly update their security software and carry out penetration tests to reduce the likelihood of cyber-attacks.

5.4 Conclusions of the research

Based on the study, one can deduce that different scholars contributed to the subject of cybercrime in a way to come up with the best practices, but technological advancement has remained the main threat to the financial services sector. The use of mobile payment systems, electronic banking, internet, and computers has sustained cybercrime worldwide and technological crimes have become a threat to the financial services sector. From the research, it was brought to the conclusion that technological advancement has become the major threat to the financial services sector in Zimbabwe and the world at large. Worldwide use of electronic banking systems has attracted cybercriminals to invade the banking sector which has resulted in heavy financial losses. Due to the use of mobile banking, ATMs, and RTGS, criminals have found a new way of invading the financial sector hence there is a need for individuals, organizations, governments, nations, and global collaboration of all stockholders to find new ways of addressing cybercrime. There is a need for individuals, organizations, nations, and the world at large to unite efforts to implement and mitigate cybercrime at each level. Additionally, strict punishment of offenders, maintaining KYC policies and global cooperation are the major recommendations for curbing technological crimes.

5.5 Recommendations by the researcher to mitigate cybercrime

The increase in cybercrimes in micro-financial institutions and the banking sector at large has caused negative effects to the sector and the economy at large. Due to the heavy effects of cybercrime, it is significant to recommend or put measures in place to fight the enemy that has brought devastating effects such as financial loss, reputational damage and other several impacts. From the research findings, it was recommended that;

5.5.1 Stiff penalty must be imposed on cybercriminals.

As a deterrent factor, punishment of offenders has been found the best way to mitigate cybercrimes in the financial services sector. Since criminals are rational, there is a need for regulators in conjunction with law enforcement agencies such as the investigations such as the Central Intelligence Department (CID), Criminal Investigations Department (CIO), Police, and the Prisons and Correctional services to exercise the law against offenders. Criminals are rational individuals who outweigh the benefits and costs of offending before committing a crime. Once criminals realize that the benefits of committing a crime are more than the cost (penalty), they may decide to breach the law hence there is a need for the judicial to impose severe penalties to offenders.

5.5.2 Specify stringent laws and regulations

The study recommended that there must be specific laws and regulations that sue or prosecute those convicted or breach of the law. These laws include the Australian, Canadian, and the United States of America anti-spam laws for example The Spam Act (2003), CASL, and CAN-SPAM Act (2003).

5.6 Recommendations by the study

Based on the findings of the study, the following recommendations were made:

5.6.1 Strong passwords and data encryption

Clients and employees must utilise distinct user IDs and passwords for various accounts and refrain from writing them down. By adding more characters, digits, and special characters to the passwords and changing them frequently, you can make them more difficult. This may be used in addition to encrypting sensitive information.

Since cybercrimes impact of micro-financial institutions which the economy depend on, there is a need for individuals, educational institutions, organizations, and nations to collaborate in providing awareness campaigns, and educational facilities to the public on specific laws that prosecute cybercriminals, providing knowledge to the victims to about where they should report any cases of cybercrimes such as the Cybercrime Act.

5.6.2 Training facilities

Financial institutions are the target of cybercriminals hence there is need for organizations to train their employees and clients about precautionary measures that must be practiced to deter and minimize cybercrimes in micro-financial institutions. Micro-financial institutions must work together with the Financial Intelligence Unit of the Reserve Bank of Zimbabwe in complying with the cybercrime laws to train their employees and other stockholders. Many cases of cybercrime go unreported due to a lack of knowledge by the public, so educational facilities to the public on specific laws that prosecute cybercriminals, and providing knowledge to the victims about where they should report any cases of cybercrimes such as the Cybercrime Act is of importance Suspicious attempts to illegally access one's account must be taken as a potential suspect and strictly monitored through strong passwords and personal identification numbers.

5.7 Recommendations of the study

Technological crimes are increasing rapidly in micro-financial institutions and have become the biggest threat to the global economy at large hence there is a need for individuals, organizations, nations, and the world to unite and find new ways to prevent cybercrimes in financial institutions. Cybercrime has become the emerging threat to the financial services sector in Zimbabwe hence there is a need for all stakeholders to put together new strategies to mitigate cybercrime. Governments must impose strict laws against cybercriminals.

Other recommendations were also listed below-

- Use of VPN-Virtual Private Network for remote work rather than exposing RDP-Remote Desktop

- Use of artificial intelligence to enhance the protection of digital systems and data from cyber threats.
- Monitoring RDP access as well as disabling it when it is not in use.
- Working folders must not include shared exe form and must only be downloaded from a safe repository or storage only when needed and has been approved by the recommended IT security.
- Reporting suspicious requests and emails to the IT security department in time.
- Restriction of sharing personal details to unknown websites
- Strengthening email security to identify corrupt attachments.
- Use of multifactor authentication for legitimate access
- Backing up data in a safe location regularly

LIST OF REFERENCES

Acharya, S., & Joshi, S. (2020). Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures. PalArch's Journal of Archaeology of Egypt/Egyptology, 17(6), 4656-4670.

Aggarwal, P., Gautam, A., Agarwal, V., Gonzalez, C., & Dutt, V. (2020). Hackit: a human-in-the-loop simulation tool for realistic cyber deception experiments. In Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, July 24-28, 2019, Washington DC, USA 10 (pp. 109-121).

Adel, I., Al-Alawi, A., Sara, M., & Al-Bassam, S. (2020). Study of the Cybercrime Cost and the Risk of Criminal Threats to the Banking Sector. Xi'an Jianzhu Keji Daxue Xuebao/Journal of Xi'an University of Architecture & Technology, XII, 252–270. https://doi.org/10.37896/JXAT12.04/770

Al-Alawi, A. I., Al-Bassam, S. A., & Mehrotra, A. A. (2020). Assessing The Factors of Cybersecurity Awareness in the Banking Sector. Arab Gulf Journal of Scientific Research. 37(4):17-32

Atul, P., Bamrara, Singh, G., & Bhatt, M. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. International Journal of Cyber Criminology, 7, 49–61. https://doi.org/10.2139/ssrn.2488413

Gupta, A., & Anand, A. (2017). Ethical hacking and hacking attacks. Int. J. Eng. Comput. Sci, 6(6), 2319-7242.

Balan, S, Otto J, Minasian E, Aryal, A. 2017._Data Analysis of Cybercrimes in Businesses. Journal of Information Technology and Management Science, Vol. 20, pp. 64–68, doi: 10.1515/itms-2017-0011

Bamrara, Dr. A., Singh, G., & Bhatt, M. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2488413

Belous, A., Saladukha, V. (2020). Computer Viruses, Malicious Logic, and Spyware. In: Viruses, Hardware and Software Trojans. Springer, Cham. https://doi.org/10.1007/978-3-030-47218-4_2.

Boateng, R., Budu, J., Isabalija, R., & Olumide, L. 2011. ‘Sakawa- Cybercrime and Criminality in Ghana’: Journal of Information Technology Impact, Volume (11): 85-100.

Bornstein, M. H.; Jager, J.; Putnick, D. L. (2017). Sampling in Developmental Science: Situations, Shortcomings, Solutions, and Standards. Developmental Review, 33(4), 357–370. doi:10.1016/j.dr.2013.08.003. ISSN 0273- 2297. PMC 4286359. PMID 25580049).

Cheema, A., Tariq, M., Hafiz, A., Khan, M. M., Ahmad, F., & Anwar, M. (2022). [Retracted] Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review. Security and Communication Networks, 2022(1), 8379532.

Cohen, E and Felson, M., 1979. ‘Social Change and Crime Rate Trends: A Routine Activity Approach’, Volume 44(2): 588-605.

Couper, M. P. (2017). New developments in survey data collection. Annual review of sociology.

Cyber Crime: Rise, E. a. (2020, July 1).Retrieved July 1, 2020, from https://www.researchgate.net/publication/344349620

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. Cryptologia, 44(1)

Ghann, P., & Owiredu, J. (2022). The Effect of Cybercrime on Financial Institutions: A Case Study of Mumuadu Rural Bank, Osino in the Fanteakwa District-Eastern Region, Ghana.

Goel, S. (2016). Cyber-Crime: A growing threat to Indian banking sector. Paper presented at the 3rd Int. Conf. Recent Innov. Sci. Technol. Manag. Environ.

Ibrahim, U. M. A. R. U. (2019). The Impact of Cybercrime on the Nigerian Economy and banking system. NDIC Quarterly, 34(12), 1-20.

Gupta, C. M., & Kumar, D. (2020). Identity theft: a small step towards big financial crimes. Journal of Financial Crime, 27(3), 897-910.

Hasan, R. (2022). Cybercrime Techniques in Online Banking. 13, 524.

Hedayati, A. (2012). An analysis of identity theft: Motives, related frauds, techniques and prevention. Journal of Law and Conflict Resolution, 4(1), 1-12.

Howe, E. L., & Pelser, A.-M. (2022). Cybercrimes in the Eswatini banking sector Implementing Routine Activity Theory analysis. Ensorvoot, 43, 1-16

https://www.herald.co.zw/hackers-fleece-supermarket-of-22m/

ICSPA. 2013. Study of the Impact of Cybercrime on Business in Canada retrieved from www.icspa.org on 28/06/15.

Kamal, M. M., Chowdhury, I. A., Haque, N., Chowdhury, M. I., & Islam, M. N. (2012). Nature of cyber crime and its impacts on young people: A case from Bangladesh. Asian Social Science, 8(15), 171.

Lewis, J. (2018). Economic impact of cybercrime, no slowing down. McAfee.

Mawunge, T. 2017. An analysis on the impacts of cybercrime on retail sector. A survey of Harare CBD.

Mansfield-Devine, S. (2016). Open banking: opportunity and danger. Computer Fraud & Security, 2016(10), 8-13.

Monday, T. U. (2020). Impacts of interview as research instrument of data collection in social sciences. Journal of Digital Art & Humanities, 1(1), 15-24.

Matambura, T. (2017). “Man hacks into OK ZIM system, steals $70k”, The Herald [Online], available at: www.herald.co.zw/man-hacks-intook-zim-system-steals-70k/.

Mugari, I. (2017). “Cyberspace enhanced payment systems in the Zimbabwean retail sector: opportunities and threats”, International Journal of Economics and Financial Issues, Vol. 7 No. 3, pp. 760-767.

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), 135-143.

Mugari, I., & Olutola, A. A. (2021). Electronic Card Payment Risks: Combating Card Fraud amidst Liquidity Crisis in Zimbabwe. African Journal of Business & Economic Research, 16(3).

Mugari, I., Kunambura, M., Obioha, E. E., & Gopo, N. R. (2023). Trends, impacts and responses to cybercrime in the Zimbabwean retail sector. Safer Communities, 22(4), 254-265.

Newman, M., & Gough, D. (2020). Systematic reviews in educational research: Methodology, perspectives and application. Systematic reviews in educational research: Methodology, perspectives and application

Oliver, D., & Randolph, A. B. (2022). Hacker definitions in information systems research. Journal of Computer Information Systems, 62(2), 397-409.

Obeng-Adjei, A. (2017). Analysis of cybercrime activity: Perceptions from a South African financial bank (Doctoral dissertation, University of the Witwatersrand, Faculty of Commerce, Law and Management, School of Economic and Business Sciences).

Pandey, P., & Pandey, M. M. (2021). Research methodology tools and techniques. Bridge Center.

Pasculli, L. (2020). The Global Causes of Cybercrime and State Responsibilities: Towards an Integrated Interdisciplinary Theory. Journal of Ethics and Legal Technologies (JELT), 2(1), 48-74.

Payne, B. K. (2020). Defining cybercrime. The Palgrave handbook of international cybercrime and cyberdeviance, 3-25.

Picciano, A. G. (2023). Future technological trends and research. In Data Analytics and Adaptive Learning (pp. 303-322). Routledge.

Pillay, P., Ntuli, P. N., & Ehiane, S. O. (2023). Exploring the prevalence of cybercrime in the banking industry in KwaZulu-Natal, South Africa. International Journal of Membrane Science and Technology, 10(1), 1763-1775.

Raghavan, A. & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. International Journal of Current Research and Academic Review, 2, pp. 173-178.

Rastenis, J., Ramanauskaitė, S., Janulevičius, J., Čenys, A., Slotkienė, A., & Pakrijauskas, K. (2020). E-mail-based phishing attack taxonomy. Applied Sciences, 10(7), 2363

Reimann, M., & Jain, S. P. (2021). Maladaptive consumption: Definition, theoretical framework, and research propositions. Journal of the Association for Consumer Research, 6(3), 307-314

Reserve Bank of Zimbabwe. 2015. Annual report. Harare [Online] www.rbz.co.zw/assets/nps-first--quarter-activity-report-march-2016.pdf [Accessed: 02/03/2022].

Saini, H., Rao, Y. S., Panda, T. C. J. I. J. o. E. R., & Applications. (2012). Cyber-crimes and their impacts: A review.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students doi: https://doi.org/

Sharma, G. (2017). Pros and cons of different sampling techniques. International journal of applied research, 3(7), 749-752.

Shikalepo, E. E. (2020). Defining a conceptual framework in educational research. Namibia University of Science and Technology 7p.

Shukur, H. A., & Kurnaz, S. (2019). Credit card fraud detection using machine learning methodology. International Journal of Computer Science and Mobile Computing , 8(3), 257-260.

Siahaan, A. P. U. (2018). Impact of Cybercrime on Technological and Financial Developments.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, 333-339.

South African Banking Risk Intelligence Centre (SABRIC) (2018), “Annual crime states”, South Africa, SABRIC.

Stratton, S. J. (2021). Population research: convenience sampling strategies. Prehospital and disaster Medicine, 36(4), 373-374.

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297-307. Article 6. http://www.cisjournal.org/journalofcomputing/archive/vol5no4/vol5no4_6.pdf

Uppal, D., Sinha, R., Mehra, V., & Jain, V. (2014, September). Malware detection and classification based on extraction of API sequences. In 2014 International conference on advances in computing, communications and informatics (ICACCI) (pp. 2337-2342). IEEE.

Wall, D. S. (2024). Cybercrime: The transformation of crime in the information age. John Wiley & Sons.

APPENDICES

APPENDIX 1: CONSENT LETTER

Bindura University Of Science Education

P. Bag 1020
Bindura
Zimbabwe

To whom it may concern

REF: Request for completion of a Questionnaire

I am a senior student at the mentioned university pursuing a Bachelor of Commerce (Honours) Degree in Financial Intelligence. As a partial fulfilment of my program, the University mandates me to conduct research on a relevant topic of study. My area of study focuses on **The Impact of Technological Crimes in Micro-Financial Institutions in Zimbabwe;** hence I have chosen your organization as the best.

Attached herewith is a questionnaire that I will utilize for data collection. I would greatly appreciate receiving honest responses that are not influenced in any way but instead accurately reflect your experiences within the banking institution. Please peruse the questions carefully and answer them to the best of your ability. Rest assured that the information obtained will be kept confidential and used solely for academic purposes.

What is the purpose of the research study?

The study seeks to find out the impacts of technological crimes in micro-financial institutions in Zimbawe.

What can you withdraw from this study having agreed to participate?

Taking part in this research study is voluntary. Instead of being in this research study, you have the following option.

-decide not to participate in this research study.

Your assistance would be greatly appreciated.

Yours faithfully

Mashinya Munesuishe

APPENDIX II: QUESTIONNAIRE FOR RESPONDENTS

INSTRUCTIONS TO RESPONDENTS

1. Please do not write your name on the questionnaire.

2. Indicate the appropriate answers by ticking the spaces provided in this section.

SECTION A: DEMOGRAPHIC DATA

1. Indicate your gender

a) Male [ ] b) Female

2. Indicate your age range.

a) Between 18-24 years [ ] b) 25 – 34 years [ ]
c) 35 – 44 years [ ]

d) 45 years and above [ ]

3. What is your highest level of education?

a) Ordinary level [ ] b) Advanced level [ ] c) Diploma level [ ] d) Undergraduate Degree level [ ] e) Other specify ---.

4. Area of residence?

a) high density [ ] b) Low density [ ] c) Medium density [ ] d) CBD[ ]

5. Period of residence

Below 2 years [ ] 2-5 years [ ] 6-10 years [ ] Above 10 years [ ]

Section B: Nature of Technological crimes.

6. The following are some of the common forms of Technological crimes in microfinance institutions. Could you please provide the prevalence rates of these in your organization?

Type of technological crime	Less than Prevalent	Doesn't Occur	Prevalent	Very Prevalent
Phishing				
Hacking				
Card Fraud				
Malware				
DOS				
Identity Theft				

7. What additional forms of technological crimes are common at your company? Please let us know if there are any below.

……………………………………………………………………………………………

…………...

Section C: Causes of technological crimes.

8. The factors listed below are seen to be potential causes of technological crimes in microfinance institutions. Do you think any of the following have happened at your company as a result of technological crimes?

Causes of technological crimes	Strongly Disagree	Disagree	Agree	Strongly Agree
Economic Factors				
Weak Security Systems				
Lack of Cybersecurity awareness				
Poor recruitment practices				

Section D: Impact of technological crimes.

8. Has your organization suffered any of the below due to technological crimes?

Impact	NO	YES
Financial loss		
Reputational damage		
Disruption of business trading		
Loss of sensitive data		

Section E: Recommendations to combat cybercrime.

10. Below are some of the strategies that companies adopt to combat cybercrime. In your opinion, what measures can be put in place to curb technological crimes (Tick only 3).

Measure	NO	YES
Education and training		
Constantly Update antivirus and anti-spyware software		
Cyber security Audits and Compliance Checks		
Strong Passwords and data encryption		

11. In addition to the measures above, what other measures has your organization put in place to fight cybercrime? Please indicate below:

....

....

....

Appendix III: Interview guide.

1. What is your gender ?
2. What causes cybercrimes in most cases?
3. What are the most common forms of cybercrime in micro-financial institutions?
4. What are the major impacts of technological crimes in micro-financial institutions?
5. Which measures were put in place against cybercrimes in micro-financial institutions?
6. What challenges are faced in curbing cybercrimes in micro-financial institutions?
7. How effective are the foresaid strategies in preventing technological crimes?

(THANK YOU FOR YOUR TIME AND YOUR PARTICIPATION IS GREATLY APPRECIATED)