BINDURA UNIVERSITY OF SCIENCE EDUCATION FACULTY OF COMMERCE

DEPARTMENT OF BANKING AND FINANCE

An Analysis Of Cybercrime Effects On Banks Financial Performance Case Study Of Zb Bank (2018-2022).

SUBMITTED BY

B1850914

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE BACHELOR OF COMMERCE HONOURS

DEGREE IN BANKING AND FINANCE OF BINDURA UNIVERSITY OF SCIENCE EDUCATION.

JUNE 2023

APPROVAL FORM

The undersigned certify that they have supervised the student B1850914 dissertation entitled ‘An analysis of cybercrime effects on banks financial performance case study of ZB bank submitted in partial fulfillment of the Bachelor of Business Studies (Honours) Degree in Banking and Finance.

To be completed by the student

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

……. ……../……./……..

Signature of the student Date

To be completed by the supervisor

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

……. ……../……./……..

Signature of the student Date

To be completed by the Chairman of the Department

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

……. ……../……./……..

Signature Date

RELEASE FORM

NAME OF AUTHOR:	**B1850914**
DISSERTATION TITLE:	An analysis of cybercrime effects on banks financial performance in a case study of ZB bank (2018 to 2022)
DEDREE TITLE:	Bachelor of commerce honours Degree in Banking and Finance
YEAR DEGREE TO BE GRANTED:	**2023**

Permission hereby granted to the Bindura University of Science Education library to produce single copies of the dissertation to lend such copies for, scholarly scientific research purpose only. The Author reserves other publications rights extensive extracts. I further agree that permission for multiple copying of this work for scholarly purposes may be granted by me and the Dean of commerce. It is understood that copying or publication of this work for financial gain shall not be allowed without my written permission.

Signed ……

Date …….

Permanent address and contacts: 3306 Retreat Park Waterfalls Harare

DEDICATION

This research project is dedicated to my family members, my supervisor and all other people that were supporting me in the doing this project. Thank you all and God bless you.

ACKNOWLEDGMENTS

First and foremost, l would like to honor the One who has taken me this far, my Lord and Savior, Jesus Christ. I would also like to acknowledge and thank my academic supervisor for his patience, firm guidance and support as well as the staff at ZB bank that were sampled for their assistance in providing factual data for this research study to be valid. I also feel indebted to my parents for their profound support and generous help throughout the dissertation work. My appreciation goes to my family who have been there to hold me down financially and being supportive since day one. I also would like to appreciate my friends for their motivation and assistance whenever school pressure got hold of me.

ABSTRACT

Over the past two decades, banks have made extensive use of information and communication technology (ICT), which has led to an increase in cybercrimes like phishing, card fraud, and virus distribution in Zimbabwe's banking sector. The primary focus of this study was an analysis of cybercrime effects on banks financial performance case study of ZB bank (2018 – 2022) the objectives were, to find out the types of cybercrimes and their effects, either direct or indirect on banks performance, and to determine the relationship between cybercrime effects and the financial performance. A total of 39 participants were selected by the researcher for a descriptive research design together with a questionnaire, and a documentary assessment as the main data collection tools. Data analysis was conducted using both the statistical package for social science (SPSS)version 20 and Mircosoft excel 2013, with the results presented through graphical representation and tables. The three most frequent forms of cybercrime in the banking sector are card fraud, hacking, and virus distribution. Direct financial losses, higher security costs, and reputational damage were found to be the main effects of cybercrime on the banking industry. The study also showed that some current countermeasures against cybercrime in the banking industry are effective and others are not, depending on a number of factors. Relationship between ZB Bank's performance and cybercrimes, with 39 respondents as the sample size, 39 respondents overall, and a significance level of 0.05. The findings indicate that independent variables and the dependent variable have a -.621** negative correlation, and the p-value is.05, which is higher than 0.001. Researchers concluded that the variables are not correlated when the p-value exceeds the level of significance. ZB Bank has discovered that cybercrime has a detrimental effect on banks' financial performance. This suggests a strong negative correlation between cybercrime and ZB Bank performance. The study recommended that in order to curb off the high rate of cybercrime in the banking industry it should ensure that its employees also changes their passwords after every three months on their accounts and the bank should always be up to date with the changing technology so as to have an insight on how to handle cybercrimes. There is need for more research on the impact of cybercrimes on financial statements of various organisation.

Contents

CHAPTER ONE

INTRODUTION

1.1 Introduction

The research problem is primarily introduced in this chapter. It devotes its attention to understanding the origins of the issue. Assumptions that will be used in conducting the research were also examined, along with the problem statement, primary objectives, and importance of the study.

1.2 Background of study

Financial and banking industry is a sizable industry, institutions have a large global customer base. Over time, more vulnerable groups and weaker sections of society have access to banking services. According to the 2017 Global Findex database, since 2011, nearly 1.2 billion adults have had bank accounts. As per research, most Zimbabwean are adopting digital technology with more than half of them that is 51% opting for online banking mediums. Additionally, 26% of them utilize mobile banking facilities to access services offered on their bank' websites. Cyber risks have grown to be a significant area of concern as a result of the exceptional growth of digitization in banks. Over the past ten years, there has been an increase in cyber intrusions and attacks. In addition to seriously harming the crucial banking processes, this unprecedented rise in crime has cost the system a tremendous amount of money. The world has lost USD 114 billion each year due to cases cybercrimes, and USD 274 billion is spent fighting the crimes.

There are numerous internet entry points, outdated defence technologies, and system and software flaws in banks' use, making them extremely vulnerable to sophisticated attack methods used by hackers. The primary objective of banking institutions is to be required to have a cyber security plan in place. As threats to the cyber infrastructure in its regulated entities have increased over time, numerous regulatory measures and cybersecurity tools have been developed in response to increasing complexity and frequency cybersecurity incidents. Given the need to continuously evaluate the state of cybersecurity and new threats, it is crucial to monitor the progress made by banks in enhancing their cybersecurity preparedness and response.

Along with the rate at which new technological advancements are made, cybercrime has been rising. According to Bell (2002), as a result of the risks present in the information and communication sector, users of the internet and other technologies have recently had to deal with numerous criminal activities coming from cyberspace. It is time to address this criminal activity because its costs have reached a critical level. As cybercrime becomes a bigger problem, many organizations try to safeguard themselves by educating staff members about the very real risks associated with using the internet. This research aims to discuss how cybercrime affects banks' financial performance.

1.3 Problem statement.

Due to the increasing reliance of people and businesses on the internet, cybercrime is becoming a greater threat in the virtual world. The likelihood of being attacked by cybercriminals worldwide has increased as a result of the use of the internet and other technologies. It is necessary to investigate cybercrime because there are more instances of theft, phishing, computer viruses, and hacking. The banking industry has been able to reach more customers thanks to the development of technology, but Consumers who frequently feel hesitant and uneasy about selecting such services now face an increased risk.

The banks must evaluate their present business practices. In this essay, the research is primarily concerned with analysing how cybercrime affects banks' financial performance. Analyse the connection between cybercrime and bank financial performance as well. In Zimbabwe, where little is done to understand the effects of these internet crimes on bank performance, the goal of these studies is to analyse the main effects of cybercrime.

1.4 Objectives of study

Hence the objective of this study is to review the threats inherent in the existing and emerging technologies, and their effects on banks financial performance of ZB Banks.

- To determine the effects of cybercrimes on banks financial performance in case of ZB bank.
- To find out the types of cybercrimes and their effects, either direct or indirect on banks performance.
- To determine the relationship between cybercrime effects and the financial performance.

1.5 Research questions

The main questions are that how does the cybercrime imposes effects on banking financial performance. In order to satisfy the said objectives, the researcher will make use of the following research question:

- What effects does cybercrime have on the financial performance of bank?
- What are the types of cybercrimes that affects banks?
- What are challenges faced by banks in trying to deal with cybercrimes?

1.6 Hypothesis

- H1: Does cybercrime has an impact on the banking financial performance
- H2: Does cybercrime has no impact on banking financial performance

1.7 Assumptions

- The following premise served as the study's foundation:
- Cybercrimes effect on performance assumed to be applicable to most banks Zimbabwe.
- They are numerous factors that affect bank financial performance but, in the research, only types of cybercrimes will be considered
- It is assumed cybercrime is the only factor that affects financial performance of ZB Bank
- the primary topics under investigation and those that will remain constant throughout the research are cybercrime and financial performance.

1.8 Significance

1.8.1 To all the banks in Zimbabwe

The findings will be relevant to all the bank managers and the investors of ZB bank to take into consideration how cybercrimes have impact on in the banking financial performance. This study will be a guideline on how the ZB bank should be aware of cybercrimes in their banking financial performance and should be able to have a mutual understanding of the effects of cybercrime in banking financial performance

1.8.2 To the university

The discoveries will surface a way to give new knowledge to other students for future research purposes1. Due to this research the university will always be able to achieve its objective of informing research skills to the students.

1.8.3 To the researcher

The student will learn and increase the knowledge of the effects of cybercrime on banking financial performance and finding ways on how to the banking financial performance can be improved despite the effects of the cybercrimes. The study will also be done in halfway gratification of the fundamentals of Bachelor of Commerce Honours degree in Banking and Finance by the Bindura University of Science Education

1.9 Limitations of the Study

Although the research was conducted in Harare, the researcher examined the ZB bank's major reports, and not all information was disclosed in those reports. So, a way to have access information from inside I had to request for a visit to the banks department specifically IT and internal audit as way to overcome the summarised information in the reports and get first-hand information form the executive personal form those important departments of the bank. This helped to have a more detailed information about cybercrimes in banks specifically ZB bank.

Not all respondents understood the demands of the questions, so the researcher had to clarify them in order to preserve the validity of the research findings. It was really difficult for the participants to understand the requirements of the question and the demands of the research. As a way to overcome this problem I had to set up a meeting with agreed participants. We read the questions and try to explain want was need for us to get clear and unambiguous information. We read questions and ask if they were any problem and we move forward. This help a lot because it reduces the discontent of information since they now have understood the question and also saves time in trying to filter out information.

Due to respondents' desire for privacy and confidentiality, gathering information from them was challenging. The researcher promised complete confidentiality in order to obtain access to this information. As a researcher we had to insure confidentiality of all the information gathered and participants confidential so that they won’t be repercussions for them to give out sensitive information. This one was a major condition since more of this information is highly classified and cannot be accessed by everyone. I had to insure its privacy and only for education use. At one point the give a copy to sign as a declaration to ensure that information will be confidential and cannot be shared of any member unless for educational purposes only.

1.10 Delimitations of the study

The research was conducted in Zimbabwe mainly Harare. Data used was collected from the executive reports, audited financial reports, reports from accounting firm in Zimbabwe and investors reports of ZB bank. Only customers and members of executive management were taken into consideration as respondents to this study, along with middle managers, lower level managers, accountants, senior accounts clerks, and accountants. Between January 2018 and December 2022, the study's scope was covered.

In order to get access to the information required to ensure that they will be privacy and confidentiality of the availed information and only used for academic purposes.

In order to ensure consistency and uniformity of the required data l had to explain some of the important demands so as not to ruin the research findings

1.11 Ethical considerations

These are of principles that will guide my research design and practices. Throughout this research these practices will be adhered. These ethics will help to improve credibility of this research. As a researcher I have considered the following to help the integrity of my study.

1.11.1 Informed consent

in data gathering and research it involves different people from different jurisdiction, age, gender and etc. It was of utmost importance for all stakeholders and individuals requires adequate information on the benefits, risks and research findings to make informed decisions on their participation and approval of the study. This helped because participants were sharing information without discrete.

1.11.2 Confidentiality

was as an important issue to consider since some the information is not for public consumption. As a researcher we had to insure confidentiality of all the information gathered and participants confidential so that they won’t be repercussions for them to give out sensitive information. This one was a major condition since more of this information is highly classified and cannot be accessed by everyone. I had to insure its privacy and only for education use.

1.11.3 Potential for harm

for every information shared outside the organisation has a potential harm to the organisation. A number of participants was reluctant to share information with the fear of and law suits of unknown harm that may be caused by the data shared. It was import to assure the stakeholders

that it was for educational purpose and fulfilment of a degree program as a requirement and produce student ID and some will give you a form of declaration so that if anything come up in the future.

1.12 Definition of key terms

Financial performance – The firm's financial performance measures how sound its finances are, or the outcome of management decisions and how they are carried out to enhance overall performance (Greenwood & Jovanovic, 1990). The extent to which an organization increases sales, profits, and return on equity is postulated as financial performance an integrated tool consisting of four variables, internal business processes, customers, learning and growth has been suggested by various authors to promote the use of both financial and non-financial performance measures. Solvency, profitability, liquidity, and efficiency make up the first four categories of the commonly used financial performance measures (Crane, 2010).

Cyber Crime – is an illicit act that involves a computer, a network or a linked device. Although most cybercrimes are committed to generate profits for the culprits, some are carried out to damage or incapacitate particular computers or devices. These cybercrimes include phishing attempts, which are designed to steal user data like login credentials, credit card numbers, and PINs to access the victim's bank account or take over social network data. Cybercriminals who commit identity theft attempt to obtain sensitive personal information, including social security numbers, Aadhar information, credit card numbers, and other related information, in order to pose as someone else and profit from using their name. Trojans and viruses Viruses are purely commercial. of malicious codes that reproduce themselves without the assistance of humans, much like human viruses. A destructive program known as a Trojan virus spreads quickly but, unlike viruses, does not replicate itself. These are triggered when spam email attachments are opened. Phishing It is the use of social engineering over the phone to obtain access to public users' private personal information in order to demand ransom.

1.13 Summary

The research problem, the study's goals, context, research questions, justifications, study limitations, and research scope were all presented in this chapter. The literature reviews of various authors are examined in the next chapter, along with what other authors have to say about the problems that have been raised and additional empirical studies that have been conducted in the problem's area of research by other authors

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

This chapter examines the review of pertinent literature. It includes theoretical, conceptual, and empirical research on the costs associated with cybercrime and their financial impact on banks. An analysis of a ZB Bank case study

2.1 Theoretical review

This theoretical review, which will be based on a number of earlier banking theories, will help explain how the ZB bank operates. This group includes the technology theory, the opportunity cost theory, and the space transition theory.

2.1.1 Space Transition Theory

In his book on Internet crimes from 2007, Jaishankar developed and published this theory (Jaishankar 2007). Theoretical justifications for the sharp rise in cyber-related crimes have been insufficient. Cybercrimes are a concept that this space transition theory seeks to explain. According to this theory, people who typically feel as though their criminal nature is suppressed by physical space are more likely to commit crimes online than they would in a physical setting because of their status and role. This type of crime is linked to traits like dissociative obscurity and identity flexibility, which make it simple for people to commit crimes. New criminal activities in the economic and social spheres have been spawned by the development of information and communication technologies. The financial performance of financial institutions, specifically banks, has been greatly impacted by all of these activities. According to this theory, those involved in cybercrimes are not hardcore criminals but rather members of the white-collar class who work in closed environments like banks. Detection becomes challenging, and costs rise over time until it is evident how the intrusions' financial impact is affected. Thus, it is theorized that one of the key elements significantly influencing the rising costs that banks are experiencing in relation to cyberspace loopholes is the complex nature, traits, and behaviour of the offenders within the information and communication environment. The theory's tenets state that people with repressed criminal behaviour have a propensity to commit crimes online that they otherwise wouldn't because of their status and position. In

cyberspace, criminals are provided with the opportunity to engage in cybercrime due to identity flexibility dissociative anonymity, and the absence of deterrents. It is probable that criminal behaviour that originates in cyberspace will eventually transition to physical space and may even be transferred back to cyberspace. Offenders occasionally venture into cyberspace, and the dynamic spatiotemporal nature of cyberspace gives them a chance to get away. In order to commit crimes in real life, strangers are likely to band together online. Cyberspace crime is likely to be committed by physical space associates working together. Cybercrime is more likely to be committed in closed societies than in open societies by people. Cybercrimes could result from a clash between the physical world's norms and values and the virtual world's norms and values. The history demonstrates that there has always been a connection between crime and technology. Although the equipment has changed over time, the fundamental concepts of crime have not.

2.1.2 Technology Theory

Johnson (1985) philosophy of computing argues that the solution to cybercrime lies in developing and designing technology solutions that provides validation, authentication, non – repudiation and verification using computer security theories. These theories and models, according to Johnson (1985) The suggests that computer security theories should be utilized in designing and developing solutions to cybercrimes. This is achieved through the use of software engineering models, network protocols, cryptography, stenography, and other techniques that provides a degree of security for both users and the information infrastructure. Johnson (1985), the reason why cybercrime is so prevalent today on the internet is because a mechanism allowing a host to selectively reject messages was not incorporated from the start into the internet's protocols. The development in this area only gave thought to what the technology could do for them and what profit margins it would produce; they didn't give careful thought to what harm the technology could do to them in terms of losses and costs. Technology theory examines the systemic flaws that each piece of technology currently being used in financial institutions did not have in mind when it was first developed. Due to technological shortcomings in the systems used in their daily operations, banks are currently spending a lot of money on things like reputational damage costs, opportunity costs, security costs, and other expensive factors. Technology is undergoing a revolution in today's society with the development of computers and telecommunications, the majority of businesses and a large number of people have come to rely heavily on computers and networks to perform daily tasks (Howard, 1997; Sterling, 1992). According to Howard (1997), 13 million host systems were

able to access the internet in 1996. According to estimates, the population will have increased and will reach just over 200 million by the year 2003. The haste to adopt new technology has also given rise to a new type of criminal behaviour and activity known as hacking. According to Hutchison (1997) and Stoll (1985), hacking is a criminal activity that depends on computer networks, including the internet Hackers are people who engage in illegal activities such as hacking computers. Over the years, the term "hacker" has come to mean a variety of things, from experiences with highly imaginative desires. All of these characteristics of the digital context reflect modern society.

2.3.1 The Routine Activities theory.

The Routine Activity Theory, which Cohen and Felson (1979) introduced, is crucial for the analysis of crime statistics. Suitable targets, an unguarded population, and a motivated criminal are essential ingredients in crime science, according to Felson (2013). Opportunity is the key factor in determining crime, according to Felson (1980), many crimes are committed in people's everyday routines because they offer them enticing circumstances to do so. According to Tibbets (2012), opportunity is a necessary condition for any given crime to be committed.

According to Cohen and Felson (1979), opportunity should be eliminated in order to prevent crime. Because there are few controls in place and the criminal is no longer constrained by a physical location, this presents a good opportunity for motivated cybercriminals. Banks should use antivirus software, firewalls, and encryption keys to lessen the likelihood of computer fraud (Mugari, 2016). The Routine Activity Theory was a good fit to explain the motivations behind cybercrime regardless of the type of crime. Because Zimbabwean banks lack the security knowledge needed to fight cybercrime, and this gives fraudsters more space to maneuverer. Therefore, the Routine Activity Theory was pertinent to this exploration because it summarized the underlying philosophies of the research.

2.2 Conceptual framework.

The subsection focuses on representation of the relationship between variables, or the characteristics or properties.

2.2.1 Types of cybercrimes.

2.2.2 Hacking

The act of gaining unauthorized access to digital systems and networks to interfere with them is called hacking. Hacking is illegal because it involves breaking into systems without authorization or trying to get around security measures, such as by breaking into customer banking websites or online accounts. Unauthorized users have the ability to access systems and use them for extended periods of time without being detected. There could be significant losses in money, data, and reputation as a result of this. Banks are significantly impacted by hacking, and this impact is primarily negative and will eventually have an effect on performance.

2.2.3 ATM/Debit/Credit card frauds

The perpetrator of these frauds typically attaches a skimming device to an ATM or POS keypad so that it is undetectable. Customers' card information and PIN are sent to the installed skimmer, which can be used to steal money, whenever they enter their information. The Zimbabwean police published a report in March 2018 stating that at least $200 000 had been lost due to bank card cloning had been lost to bank card cloning. This will result in large customers lose large amount of funds and in the long run will put a dent on banks reputation and customer will lose faith about safety of their funds and also rise in legal fee if customers sue the bank. Most online credit card frauds occur when a customer uses their direct or credit card to make online payments, this giving fraudster an advantage to hack the details and passwords of the costumer’s cards and misuse them, hence the banks need to secure all the online transaction to avoid hacking of credit card numbers by hackers

2.2.4 Email Fraud

Email and websites have evolved into quick, simple, and preferred forms of communication in the modern world. Occasionally, email fraud is committed by hackers or mischievous organizations who send emails to bank customers saying things like, "Congratulations you have won such a huge amount to enchase it please share your bank details, because the amount mentions the customer will put their credit numbers into the page of the hacker thus giving the hacker an advantage to misuse the costumers card since the credit numbers is been provided. The hacker makes a crime which is also known as cybercrime according to law.

2.2.5 Phishing

Phishing is one of the online type of frauds whereby its aim is to trick people to give away their money by sending them unsolicited messages stating that they should put their login in details such as usernames and passwords in order to access their accounts

2.2.6 Virus and Trojans

A backdoor is a malicious type of a computer program which is used to gain access to confidential information managed by online banking systems. Malicious codes that replicate themselves like human viruses without human assistance are all that viruses are. A destructive program known as a Trojan virus spreads quickly but, unlike viruses, does not replicate itself. These are triggered when spam email attachments are opened. They pose a high risk, and potential outcomes could include a lack of accessibility to crucial services, data, or funding; a decline in confidence that could lead to asset fire sales, runs on banks, or disruptions in payment or price discovery. By interacting with and amplifying other financial security flaws like leverage and run risk, less serious cyber incidents may also have an impact on the stability of the economy. Due to the potential intentionality of cyber events, this possibility is more likely.

2.2.8 Ransom ware

One of the most significant online threats is it. Until a certain amount of money is paid, this type of malicious software is designed to prevent access to a computer or group of computers. Until an amount of money is paid to the attackers, they threaten to release sensitive data. One popular ransomware attack is called Maze. Important data in the banking industry is encrypted until a certain amount of money is paid so as to decrypt it and this has a negative effect on banks as 90% of them have encountered ransomware in the past years.

2.3 Actors of cybercrime

The perpetrators of banking fraud can be divided into four groups: nefarious exploiters, money mule operators, victims, and security personnel. The characteristics of each of these actors are described below individually.

2.3.1 Cyber Criminals

These malicious exploiters can be divided into five sub categories, according to the OECD report from 2007. Innovators (who look for security flaws in the system to get around the banks' protective measures). Amateur (who are novices in this field and have only basic computer knowledge, which a cybercriminal can take advantage of). Insiders (who work within the bank to leak critical information in an effort to exact some sort of retribution). Copies (they like to replicate straightforward tasks). Criminals (who are highly organized and knowledgeable and may take advantage of all the aforementioned parties in order to their own financial gain)

2.3.2 Victims,

The banking industry can be divided into two groups, according to OECD (2007): banks and customers of these banks. entities, SMEs, or sizable multinational companies can all be users or clients. Individual users and SMEs make the greatest number of dangerous externalities when they involve in risky online behaviour or ignores the precautions made when making a transaction (Asghari, (2010); Mannan & van Oorschot, (2008).

2.3.2 Security Guardians

Because they improve the current banking system, aid in removing flaws, and create systems to lessen banking frauds, they are the most important actors in this system. In the issue of the banking sector it can employ third party who will be able to provide protection from such threats

2.4.1 Determinants of financial performance of commercial banks.

Quach's (2005) proposed a hypothesis which categorizes performance factors into two major groups internal and external factors. Internal factors affecting performance are those that are within the control of the organization and can be broadly classified into two categories financial and non-financial variables.

2.4.1.1 Financial Variables

The decisions affecting the firm's goals are primarily centred on financial factors in the balance sheet and income statement. Creation of innovation, new product development, environment scanning unmet marketing needs and opportunities and identification are some of the main management’s responsibilities. Quach (2005). Asset quality, capital sufficiency, liquidity, and solvency make up the internal manageable factors. In 2002, Richardson.

2.4.1.2 Liquidity

The capacity of the organization to meet short-term financial requirements as they mature without impairing the smooth operation of the organization's operations is measured by liquidity. According to Zenios et al. (1999), liquidity measures provide a clear indication of a company's ability to pay off all of its debts even if all of its assets are liquidated. The working capital and current ratio are the advised measures and mostly employed measures of liquidity. The current ratio is a metric for comparing current assets to current liabilities. The firm is said to be more liquid if the ratio is high Working capital is a measurement of the amount of money

that is available to finance daily operations, such as buying inputs and stocking up on inventory. Quach (2005).

2.4.1.3 Solvency

Solvency is a metric used to compare the amount of borrowed money a company uses as capital to the amount of owners' equity that owners have invested in the business. Measures of solvency give a clear indication of an organization's capacity to meet all of its obligations in the event that the firm's assets had to be sold. While liquidity is short term, it involves both short- and long-term assets Quach (2005). The debt to asset ratio and the equity to debt ratio are two commonly used financial ratios to assess solvency, according to Quach (2005). These two solvency ratios all offer comparable data

2.4.1.4 Profitability

The level of a company's ability to turn a profit from the labor, capital, and management that it employs is known as profitability. Is there a specific parameter that describes how well a company can use its resources from its main source of revenue? The relationship between a business's revenue and outlays, as well as its income level in relation to the nature of its investments, is what determines its profitability. Quach (2005). The following four crucial profitability ratios: ROA, ROE, operating profit, and net income

One of the main factors that has adversely affected the profitability of commercial banks in Zimbabwe, specifically ZB bank, is cybercrime. The rise in cybercrime has caused banks' overhead costs, such as skilled labour, security investments, and other costs, to rise. The use of technology has had a positive ripple effect, but the bank needs to increase its investments in safe systems, skilled labour, and ongoing system maintenance. Long-term profitability will suffer as a result of the ongoing expenditures required to combat cybercrime.

2.4.4 Financial Performance

Financial performance measures how well and efficiently an organization uses its capital, whether it be in the form of physical assets or cash, to generate wealth and increase shareholder value. Wall (2001) proposed the integration of four variables including financial, business process, customers and growth, to measure both financial and non-financial performance in businesses. These measures of financial soundness include indicators such as insolvency, equity, profitability, return on assets and liquidity

2.4.5 Non-Financial Factor

All the elements that have no direct bearing on the firm's performance are referred to as non-financial variables. Zenios et al. (1999) assert that a company's ownership structure, whether private or public, has an impact on its performance.

The economy's level of technological development is crucial for the efficient operation of banks. Because technology is advancing, the business environment is changing. Commercial banks in Zimbabwe have suffered a number of negative effects as a result of cybercrime. It has caused commercial banks in Zimbabwe to incur additional costs. The banking industry is compelled to assess its current procedures in order to analyse and manage its risks effectively in order to combat all forms of electronic fraud Risk management now uses methods that are based on technology. Almost everyone accesses to financial services as a result of the advancement of IT and the extensive use of mobile networks in daily life. Technology has enabled the easy use of banking services due to its availability and low cost.

Consequently, the probability of becoming a victim of cyber-attacks has risen significantly. Cyber criminals have devised advanced techniques to not only pilfer money and financial information but also to monitor businesses and obtain confidential data that indirectly impacts the financial stability of banks. USD 114 billion has been lost each year as due to cybercrimes, and nearly twice that amount is spent fighting them.

2.5 Challenges faced by banks in dealing with cybercrimes

Cybersecurity in banking has been significantly hampered by a few contributing factors. Some of these are as follows:

2.5.1 Lack of Knowledge

Over the years the knowledge of cyber security has been scarce only a few companies made ill investment to upgrade it. hence, the rapidly changing nature of technology makes it challenging to invest in knowledge.

2.5.2 Budgets that are Too Small and Poor Management

Cybersecurity receives little budgetary attention because it is regarded as low priority. Programs that deals with cyber security are given less significance by top management, who continue to pay it little mind. They could have done so because they didn't fully appreciate the gravity of the risks.

2.5.4 Identities and Access are Poorly Managed

Cyber security has always emphasized on identity and access management, especially in the current scenario where cybercriminals can gain access to network by compromising a single login. Although some progress has been made, there is still much work to be done in this are

2.5.4 Increase in Ransom ware

Ransom ware is becoming a bigger threat, as evidenced by recent computer attacks. In order for the cybercriminals not to be detected by the protection codes they have introduced the use of new techniques of cybercrimes

2.5.6 Smartphones and Apps

Most banking institutions now primarily use mobile devices for business transactions. The fact that the base is expanding daily makes it the best choice for exploiters. Mobile phones have expanded their use, making them a more appealing target for hackers.

2.5.7 Social Media

The widespread use of social media has increased hacker exploitation. Less knowledgeable customers reveal their data to the public, which the attackers use to their advantage.

2.6 Empirical review

A study on the effects of online crime in the Indian banking industry was conducted by Siddique & Rehman in 2011. Their study's objective was to determine the impact of online criminal activity on India's banking and financial sector as well as to develop a conceptual framework for that impact. Their research indicates that the major objective of the Indian financial sector is to completely eradicate any possibility of online crimes. In this procedure, the costs that must be incurred to guarantee safeguard transactions are identified. Siddique & Rehman found that a number of cyber activities, including ATM fraud, money laundering, and credit card fraud, take place over network connections. This study found that one of the costs and concerns that the banks anticipate is that these activities may result in customer trust being lost, which could result in business being lost as some customers may choose to do business with other banks.

Hannan & Blundell (2004) conducted yet another study on the topic of electronic crime and how it's not the only concept to be concerned about. Their research primarily focused on two case studies, with one of the studies analysing the significant and critical factors influencing

the distribution of electronic criminal activities in Australia. The study's second section attempted to address the expenses associated with the banks' legal framework. According to the study, failing to implement legal requirements and security measures has a number of negative effects and costs for banks. The study offered a variety of alternatives and fixes needed to address policy strategies for future growth. The impact of cybercrime on bank finances was the main topic of Raghavan & Parthiban's (2014) study. Their study's main aim was to issue out the criminal activities been done in the banking sector In-depth analyses of criminal activities and scenarios within the networks were conducted, and each scenario's actors were identified. The study also identified and outlined the various criminal behaviours focuses on banking industry, as well as the motivations of those responsible This study found that one of the costs resulting from such vice is the financial loss, which is a direct cost and a major global problem impeding the development of systems.

Moore, Clayton, and Anderson (2009) claim to have written a paper on the economics of online criminal activity. Their research indicates that a number of unproductive nuisance hackers are the cause of online criminal activity. The paper notes that banking institutions encounter numerous challenges when attempting to limit their experience to operational risks brought on by network connections. Their research revealed that there are important methods and advancements that can effectively combat online fraud. For this to be fully effective, the institutions must be willing to pay for security costs. Secondly, the study suggested that before Banks can fight online crime, but first they must comprehend it from an economic perspective.

According to Douglas and Loader (2000), cybercrime is the term used to describe computer-mediated activities carried out through vast electronic networks that are either illegal or regarded as unlawful by some parties. Banking frauds are defined as cybercrimes that involve the illegal removal or transfer of money from one account to another using online technologies (Wall, 2001).

According to Wall (2001), there are four main types of cybercrimes: cyber addictions, cyber pornography, cyber violence, and cybertrespass. Cyber-deception, refers to unethical activities that involves stealing, credit card fraud, and infringement of intellectual property is a subcategory of banking frauds (Anderson et al., 2012).

The banking industry has been the victim of numerous frauds and cybercrimes, including credit card fraud, cyber money laundering, and ATM fraud. In general, these frauds are done with the intentions of escorting money from bank accounts and transferring them to another bank

account in some cases, cybercriminals access accounts and steal a small amount of money using their banking credentials, such as their PIN, passwords, certificates, etc. In other cases, they may want to steal all the money and transfer it to mule accounts Cybercriminals occasionally just want to ruin the reputation of the bank, so they shut down the servers (Claessens et al., 2002; Hutchinson & Warren, 2003) and prevent customers from accessing their accounts.

It is necessary to look into methods to raise awareness of the steps that can be taken to combat cybercrimes in the banking sector because the defence system of the industry has many threats. However, there haven't been many studies done in the past that could offer suggestions for how to reduce the risks and stop such crimes Florêncio & Herley(, 2011); McCullagh & Caelli, (2005). We must comprehend and describe the attackers and defenders in this environment in order to comprehend the fraud system in the banking sector. The various actors involved in cybercrimes are thus described in the following section.

Globally, the banking industry is facing challenging and challenging problems as a result of geopolitical and macroeconomic factors. The banking sector must access its current protocols to efficiently analyse and handle risks. A technology-driven approach to risk management has been adopted. More people have access to financial services as a result of the advancement of IT and the widespread use of mobile networks in modern life. Technology has made sure that banking services are available to everyone due to its affordability and accessibility (KPMG, 2011).

The chance of being the target of a cyberattack has grown as a result, though. Cybercriminals have created sophisticated methods for not only stealing money and financial data, but also for snooping on companies and accessing vital business data that indirectly affects financial performance. According to the Symantec Cyber Crime Report (2012), nearly USD 114 billion is lost globally due to cybercrimes each year, and USD 274 billion is spent to combat them.

The average time it takes for banking facilities to fully recover from a cyberattack is 10 days, which intensifies production costs. When compared to global losses, the Indian banking sector's financial losses make up nearly 3.5% of the cash loss. The cost of recovering from the crime is USD 4 billion, and USD 3.6 billion is spent to thwart similar crimes from occurring in the future. According to Muthukumaran B. (2008), the average amount of time needed to resolve a crime in the Indian banking sector is 15 days, which is longer than the average worldwide. To develop a model that can help in managing and responding to such threats, the

banking sector must cooperate with international law enforcement agencies and watchdog groups to fight these cybercrimes. Banking industry needs to review its existing processes to effectively assess and manage risks. the main concern is the lack of reliable data collection services that can detect patterns in cybercrime and create a model to address them. However, banks on the global have ranked cybercrime as their top five risks (Stafford, 2013).

To sum up, because most systems lag behind the tools used by cybercriminals, it is necessary to develop flexible systems that can withstand and defeat incoming attacks. The hour before, during, and after the attack calls for a strong defence system to stop it.

2.7 Extent of cybercrimes in developing and developed countries

In accordance with the study's problem and its stated goal, a summary of recent and related literature is provided in this subsection. To demonstrate why a review of earlier studies is necessary, an evaluation of those studies is made. When researching how customers viewed banking services, Rao and Suvarchala (2018) concentrated on the time after demonetization. Customers find using banking services to be very daunting, and devaluation has significantly changed how they feel about banking and financial services, according to research. They disclosed that No –Performing Asset problem is one of the major difficulties faced in Indian banking sector

A study by Alwan and Al-Zubi (2016) the high incidence of cyber insecurity in Jordan's commercial banks raises the importance of prioritizing privacy and security concerns. To safeguard customers' sensitive information, the banking industry must implement security measures that address the risk of authorised intrusion and hacking, given the internet's universal accessibility. In order to successfully compete with other banks, banking services are being revised, according to Alagarsamy and Wilson (2013), both as a defence against cybercrime and to accommodate customers' dynamically changing needs and preferences. Tasking is something that customers expect from banks, especially in terms of speed, accuracy, and security. Despite the challenges, banks are continuously adopting new technologies and innovative solutions to meet customer needs and stay ahead of competition. This is done by expanding their client base, attracting new clients, and retaining existing ones

According to Tariq (2018), the effect of cyberattacks on financial institutions was investigated by comparing the instances of cyberattacks reported across five different continents. The conclusion showed that direct and indirect losses can be used to categorize losses brought on by cyberattacks. Theft of money and data breaches make up the direct loss. Customer

annoyance and reputational damage make up the indirect loss. This study recommended various preventive measures for financial institutions to decrease cyber-attacks, such as implementing strict internal security measures, conducting regular cyber security assessment, providing cyber security training and performing cyber security audits.

The impact of cybercrime, data breaches, and security lapses on corporate stock returns was examined by Arcuri et al. in 2017. The research found that news of cyberattacks caused significant market declines, with financial institutions suffering more frequently than other institutions. Additionally, the study found that open, non-confidential cyberattacks are the most dangerous, particularly for the financial industry. Internal control is viewed through the lens of Balan et al. (2017Furthermore, it was stressed that strengthening internal control is essential to prevent inadequate security because it has made some organizations immune to fraud. As a result, organizations will be able to fight cyber fraud more effectively and pro-actively with the consolidation or reinforcement of internal control measures.

The growth of cybercrime and the difficulty of its investigation process necessitate the adoption of the proper mitigating measures, according to Kumudha and Rajan's (2018) critical analysis of cyber phishing and its effects on the banking sector. However, many nations are vulnerable to cybercrimes due to the slow pace at which such measures are implemented (Ivezic, 2017). According to Malik et al. (2018), cybercrime effects on the banking sector have a negative impact on Pakistani banks' efficiency, with the severity ranging from 60% to 80%.

2.9 Research gap

It is clear from the empirical review of Raghavan & Parthiban's studies from 2014 that they focus on how cybercrime affects banks generally. The studies don't break down the costs that banks must consider and pay for both before and after cyberattacks, or whether these costs have gotten to the point where banks must think twice and conduct a thorough analysis of the effects of cybercrime on financial performance. By attempting to analyse the effects of internet crimes on banks' financial performance, the study fills in the research gap.

2.9 Summary

Cybercrime is a serious issue that is both real and urgent. It is frequently impossible to identify crimes based on newly available information because it is not always reliable. The impact of cybercrimes and other serious crimes on the banking industry's financial performance is a topic of research. Information technology is the driving force behind the banking industry's

continued progress and expansion in the current, globalized environment. Besides the elements considered, they should be inclusion of direct and indirect costs of cybercrime, as well as their place in the constantly changing and developing field of information technology.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter will focus on and outline the study's methodology while considering all of the assumed procedures and activities. This chapter discusses the techniques, styles, methods used to gather, prepare, and analyse data. The following sections make up this chapter: research design; target audience; sample design; tools; and data collection methods.

3.1 Research design

A descriptive research design is a strategy for gathering data and information from interview or questionnaires given to a sample or target population. A descriptive research design, according to Berry (2004), is used to understand a sensation and the relationships between the variables in a particular position. Because it gathers first-hand information through the use of questionnaires and interviews, the researcher chose this descriptive research design. The research methodology used to establish a connection between cybercrimes and ZB Bank's financial performance was sound. Descriptive research enabled the gathering of both quantitative and qualitative data, and some statistical methods were employed to compile the data.

3.2 Target Population

According to Mugenda & Mugenda (2003) target population is the population that will be used to generalize and extract the research findings, a target population consists of all the respondents in the study. The population target in this study is one a commercial bank in Zimbabwe using ZB Bank as the case study and the intended number of participants is forty-one (41)

3.3.0 Sample size

Sample size represents the number of units selected from a population for research study. In this study it used the Slovins 2009 sample size formula to calculate the required sample size.

n = the size of the sample

N = the population size

e= the marginal error and is 5%

the sample size for employees is calculated as

$$41/1 + 41(0.05\text{^}2) \ = \ 39$$

Hence the sample size for the employees is 39

Saunders et al (2007) shows contents that for a sample to be representative, it should be about 39 respondents.

3.3. 1 Sampling techniques

Sampling is the process of choosing a group of people to serve as a representative sample of the larger population from which they were drawn. "Coolican" (1990). The study employed the probability-based sampling which is stratified and random sampling

According to Cooper and Schindler (2001), probability sampling refers to the selection of a sample from a population, random sampling. Random sampling is when the researcher selects a subset of participants in a random manner

The stratified sampling technique helps create a sample by first dividing the people into strata of small groups with comparable features, according to Remanyi (2002). The researcher first divides the population into strata based on some shared characteristics in the population data, and then randomly chooses samples from each stratum. This sampling technique was justified as a way to boost productivity and make sure that a specific departmental group was properly represented in the sample.

3.4 Data collection

This is a crucial component of the study because it provides accurate information from which the researcher can draw conclusions. Schindler, 2006. The study was based on both primary and secondary information that was taken from the ZB Bank website, ZB Bank's financial statements, publications, market and trend analysis, and industry analysis. The study looked at the five-year period from 2018 to 2022.

3.4.1 Primary data

These facts were gathered from the original sources. According to Anderson et al. (2013), the best way to learn about the population's feelings, memories, experiences, motivations, emotions, and reasons for acting in particular ways is to ask them. The data gathered for this

study consists of questionnaire responses and findings from primary sources. The main information was gathered through questionnaires distributed to the accounting department, the research department, the e-banking department, and the audit department. Primary data collection has a very strong and consistent justification because it is crucial to providing current and accurate information. However, gathering this information is expensive because it requires more communication and interpersonal skills to approach the right people and gain access to the information because it is confidential.

3.4.2 Secondary Data

According to Collins (2000), secondary data is information that has already been filtered and gathered for another purpose but is still pertinent to the subject of the study. secondary information taken from publications, audited financial statements, the ZB Bank website, trends analysis, and industry analysis. The information was assembled from textbooks, academic articles, management journals, financial gazette, the internet, and other Reserve Bank of Zimbabwe documents. Since they have been checked for veracity, window dressing, misrepresentation, and bias and are ready for publication, secondary sources of higher quality. It takes less time and money to gather this data.

3.5 Research instruments

3.5.1 Questionnaire

Gupta (2019) is a research tool that consists of a number of questions created with the intention of gathering data. Is a method of gathering data in which respondents must respond to questions in a specific way? It represents information in writing and calls for a written response in accordance with the question. Self-administered questionnaires were used by the researcher in this study to access and collect the necessary data from ZB bank managers and employees. Middle managers, lower level managers, senior managers, managers, accountants, and bankers all received questionnaires. After two weeks, the questionnaires were collected once more.

Due to its many benefits, the researcher chose to use questionnaires as one of the main techniques. A questionnaire is much more cost-effective than an interview because it can produce a lot of data for a lot less money. Since respondents are not required to provide their names on questionnaires, confidentiality and privacy of the information provided are guaranteed. This aids in the efficient collection of information from respondents. The main flaw with questionnaires is that they are optional, meaning that respondents can choose whether

or not to respond. When using language, spelling, and jargon to accurately capture information, the researcher must take great care. The makeup of the target population must be carefully considered. For a favourable response rate, the researcher needed to make a lot of phone calls. The survey's limitations included the fact that some respondents took their time, which delayed the data analysis.

3.5.2 Documentary review

Literature from the organization under consideration for this study has been gathered. Annual reports, financial statements, and other pertinent bank reports make up the literature. Before primary data was collected, this method of documentary review was used to give the background and knowledge of the study Wide-ranging data had been gathered prior to the collection of field data, and this was used to verify the primary data that the field would later collect and to provide statistical support.

3.6.0 Reliability and Validity

3.6.1 Validity

The survey's validity is determined by how well it captures the necessary metrics. It measures what it is intended to measure when a measurement is said to reproduce an underlying study to a certain extent. According to Leady (2001), an attempt was made to enable if a particular type of measure actually measures what it's expected to measure. People who knew how to use and were familiar with cybercrimes received the questionnaires. The respondents were experts, so they offered reliable data that they were confident would be useful for the study. By ensuring that the ZB bank is been represented by the sample, the sampling procedure ensured the validity of the data collected.

3.6.2 Reliability

According to Mugenda (2003), the extent to which research methods produce the same result is referred to as reliability. A specific method used repeatedly on the same aspect would yield consistent outcomes. It has to do with how consistently and accurately an instrument measures the quality that it is designed to measure. When a study is reliable, it means that if it were conducted by another researcher using the same methodology, they would come to the same conclusions. To determine whether the reasons given have any bearing on other studies, the results will also be compared to those of earlier studies.

3.7 Data Analysis and Processing

According to Lancaster (2005), data analysis is the process of breaking down large amounts of data into manageable portions, spotting patterns, creating summaries, and using statistical methods. The analysis of both quantitative and qualitative data collected from the banks' annual reports and questionnaires was aided by descriptive and inferential statistics as well as statistical software such as SPSS V.21.0 and Ms Excel. Figures, charts, percentages, tabulations

3.8 Summary

Background information on conducting research was provided in the chapter. The tools used in the study were examined. It mainly concentrated on the research design, research tool, data collection, data analysis, and process. A sample of respondents, which included stakeholders and employees of ZB Bank, was the focus of the data collection. Questionnaires and secondary data from bank reports and records are a few of the data collection techniques that was used. The presentation and analysis of the chapter's findings will be in the one after this one.

CHARPTER IV

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 Introduction

The presentation, discussion, and interpretation of the research findings are this chapter's primary objectives. Data analysis and research results discovered during the research procedure are included in this chapter. Tables, bar graphs, and pie charts are all used in the presenting of data. To strengthen the validity and dependability of the research findings, primary and secondary data were utilised

4.1 Questionnaire response rate

The response rate displays the proportion of real completed questionnaires in comparison to the total number of questionnaires distributed by Gupta (2019). Below is a breakdown of the survey response rate:

Table 4.1 Questionnaire response rate

Sample	Targeted sample	Achieved sample	Response rate %
Service Centres	6	5	83
Bank Executives	10	9	90
E-banking department	5	5	100
Computer Security	5	5	100
Others	10	10	100
Audit	5	5	100
Total	41	39	94%

Source: Researcher 2023

The table 4.1 The target sample of the surveys sent to bank executives, service centres, computer security, e-banking, and others is clearly displayed. The E-banking division, computer security, and other audit departments had the highest response rate of 100. Nine of the ten executive-targeted questionnaires were completed and returned, yielding a response rate

of 90%, which is considered to be successful. The response rate for service centres was 83%. 94% of respondents overall and 100% of respondents to the audit. According to Bryman and Bell (2013), the response rate of 94% is suitable to reduce findings to be valid and reliable.

4.2 Respondents Profile

4.2.1 The education level of respondents

Table 4.2 Educational level of respondents

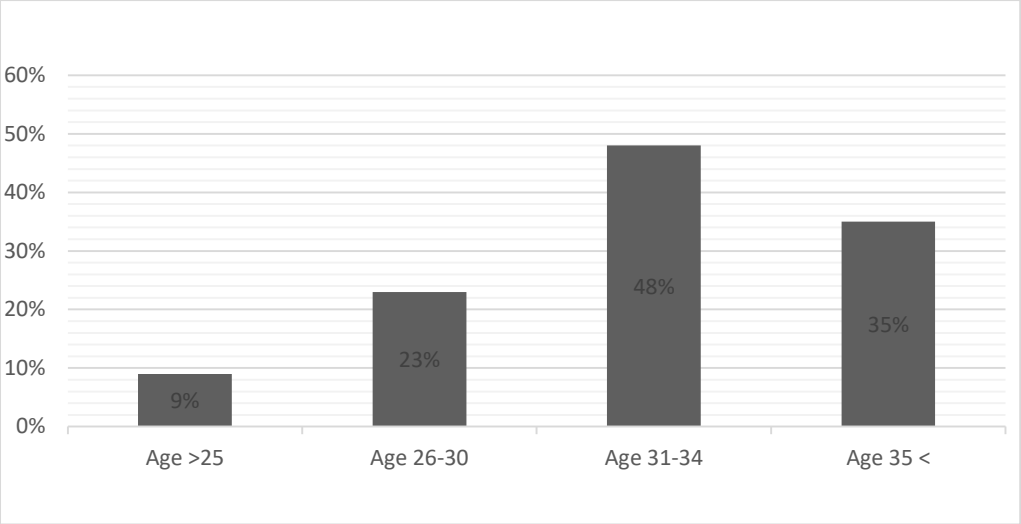
Level of Education	Frequency	Percentage %
PhDs	7	17
Masters	14	37
Degree	18	46
Total	39	100%

Source: researcher 2023

According to Table 4.2, 46% of the respondents had a degree, 37% had a master's degree, and 17% had a PhD. As a result, the respondents can accurately supply information, evaluate the information provided by the questionnaire, and understand it because they can read and write. The information gathered was thought to be reliable, present findings, and be consistent. Bell (2015) posited that the respondents should be capable of reading, comprehending, and interpreting questionnaires in order for the results to be reliable.

4.3 The Age structure of respondents

Figure 4.3 Age Structure



Source: researcher 2023

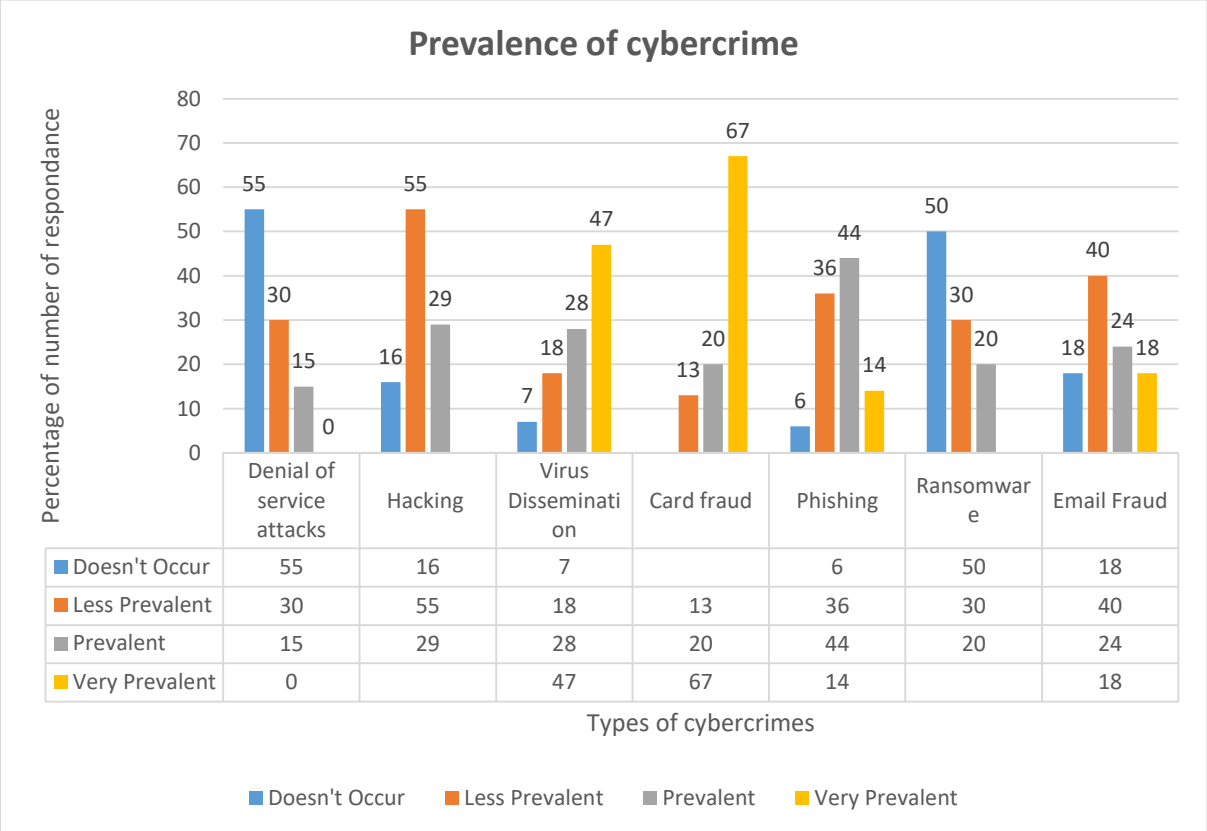
Figure 4.3 makes it clear that the majority of banking sector employees are between the ages of 31 and 34, where they account for 48% of the workforce. Ages 35 and older are next with 35% of the workforce, followed by those between the ages of 26 and 30 with 23%, and youth between the ages of 25 and under with 9% of the workforce. Due to their expertise, which the banking industry needs to continue operating, and the fact that they are mature enough, older people continue to dominate the business, despite expectations that younger people's data would be more reliable.

4.4 Research Findings.

4.4.1 Types of Cybercrime.

The types of cybercrime that were widespread in ZB Bank were requested from the respondents, and the results are summarized in the figure below.

Figure 4.4: Major types of cybercrimes prevent in ZB Bank.



[Source: Researcher 2023]

4.4.2 ATM/Debit/Credit card frauds

According to 67% of the respondents, Card Fraud is the most common form of cybercrime in the banking industry, as seen in figure 4.31. The other 20% of respondents affirmed that ZB bank in particular has a high level of card fraud. These results demonstrate that, despite the passage of time, the development of new technologies has brought with its new means of virus transmission in the retail industry. Additionally, the results demonstrate that high ATM/Debit/Credit card frauds are encouraged by unrestricted computer access, reluctance by customers, a lack of customer knowledge, and an increase in informal trading in the economy where there are numerous POS machines in society and on the streets where customers congregate will swipe their card at any accessible machine to make purchases of items or to buy US dollars on the street, which leads to a significant number of card fraud instances.

In a similar vein, the majority of respondents noted that card fraud was widespread and that it was encouraged by unlawful change money. A computer expert from the bank verified that many of these situations are connected to unlawful foreign currency deals, where the majority of the customers are duped. As the bank works to secure stronger card technology, these card scams have lost them money. The report conducted by Mugari (2016), which highlighted card frauds as one of the most prevalent cybercrimes in the Targets in Zimbabwe's retail sector are primarily banks.

4.4.3 Virus dissemination.

Virus spread, which is shown in Figure 4.3.1, is the second most common kind of cybercrime in banks, according to 47% of the respondents. These results demonstrate that, despite technological advancements, cybercriminals have developed new vectors for virus dissemination that work against all the firmware and controls in place to safeguard banks against such incidents. Additionally, the results indicate that internal workers' unauthorized access to computers and the internet contributes to high rates of virus infection.

In a similar vein, the vast majority of interview participants noted that virus spread was a common occurrence in their field of work. Numerous respondents agreed that computer infection by viruses like Trojan horses, worms, and botnets is their worst problem. These infections have cost the bank a lot because they impede the operations of some service centres and destroy a lot of crucial business data if they are not backed up. The investigation of Mugari (2016), which identified virus infection as one of the most common cybercrimes in the Zimbabwean retail sector, validated these conclusions.

4.4.4 Hacking.

With more than 55% of the respondents inclined to agree that it was prevalent and 27% affirming that it was a very common sort of cybercrime, hacking was also highlighted as another frequent type of cybercrime the bank has been suffering in recent years. Because the ZB bank and its customers now conduct their business through online platforms like internet banking, mobile banking, and WhatsApp banking, hackers have discovered a variety of ways to manipulate customers and use this system to access victims' finances, causing loss for both the bank and the customers. The respondents bemoaned their increased anxiety over the full use of digital channels, which could increase costs for both the bank and the clients. If criminals gained access to the system from the bank's side or from consumers, it might cost them money and harm their reputation over time. It is extremely disheartening to observe that hacking seems

to be gaining ground in the banking sectors around the world, notwithstanding Mugari's (2016) findings that virus spread was more common in the retail banking industry than hacking.

As a result of the proliferation of currencies, the de-dollarization of the economy, and hyperinflation, some respondents implied that cybercriminals are now targeting the banking industry, since the majority of transactions are conducted online. Since more transactions are being conducted online and the cashless economy is being promoted, there is a surge in cyberattacks because some people are less aware of them. There is also a greater adoption of contemporary corporate practices. Only 16% of respondents said that hacking doesn't happen. Hacking was reported to be the most prevalent kind of cybercrime in financial institutions, per Mugari's analysis from 2017. Findings from this study also demonstrate that is quickly entering the other retail sector.

Along with DoS, the majority of respondents (55%) said that BEC is an uncommon event in Zimbabwe's banking industry, while 30% said it is less common. These results imply that BEC is a type of cybercrime that has not yet spread to Zimbabwe.

Less respondents supported ransom, with 50% of them believing it doesn't happen. Others have emphasized that BEC and ransom are widespread in industrialized nations with better developed technologies. Banks and other industries in Zimbabwe have not fully embraced new technologies to rely entirely on e-commerce. Although banks have implemented the technology, they are still not fully exposed, making these types of attacks extremely unheard of. The Internet Crime Report (2020), which found that ransomware and BEC were more prevalent in industrialized nations like the UK and the USA, backed these conclusions.

4.5 Effects of Cybercrime on ZB bank Financial performance

Table 4.5: Major effects of cybercrime.

Impact	YES		NO	
	Frequency	**Percentage %**	**Frequency**	**Percentage %**
Direct financial loss	27	69.23	12	30.76
Additional network security costs	34	87.17	5	12.82
Loss of sensitive data	30	76.92	9	23.07
Reputational damage	8	20.51	31	79.48
Loss of intellectual property	13	25.64	87	48.71

[Source: Researcher 2023] N=39

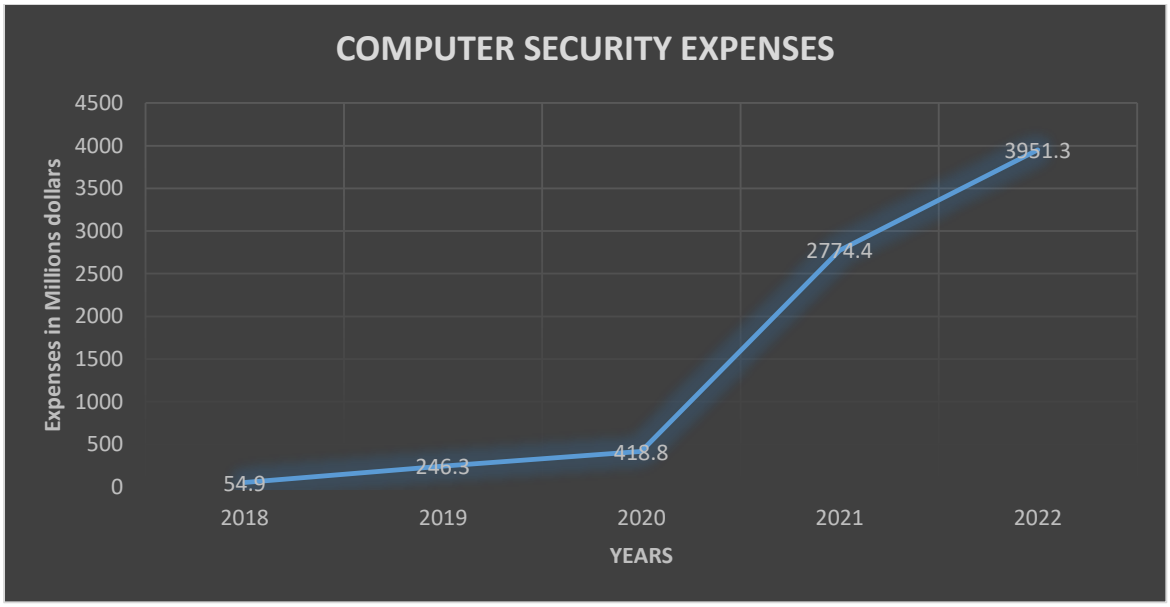
4.5.1 Additional Cost of Securing Networks.

With confidence, 87.17% of the respondents, as indicated in table 4.5, acknowledged that the bank had incurred additional costs to secure their systems and offer secure service to customers. Only 12.82% of respondents from the bank stated the doubt, but as demonstrated by audited financial accounts over a five-year period, they had incurred any additional expenditures. This is due to significant expenditures on new technology, licensing of the best system for cyberattack security, and employee and customer education, all of which have a significant negative impact on the banks' financial performance, particularly their profitability. When the bank updates its software to safeguard customers' safety and prevent computer viruses, it incurs additional expenditures each month, expenditures of employing IT specialists and insurance premiums in an effort to guarantee system security. This will be supported below with analysis of ZB bank financial statements from 2018 to 2022

4.5.2 Effects of Additional Cost of Securing Networks on Bank performance.

The graph below shows how ZB Bank's computer-related expenses increased between 2018 and 2022 to show how the bank has been spending in computer security in previous years. This

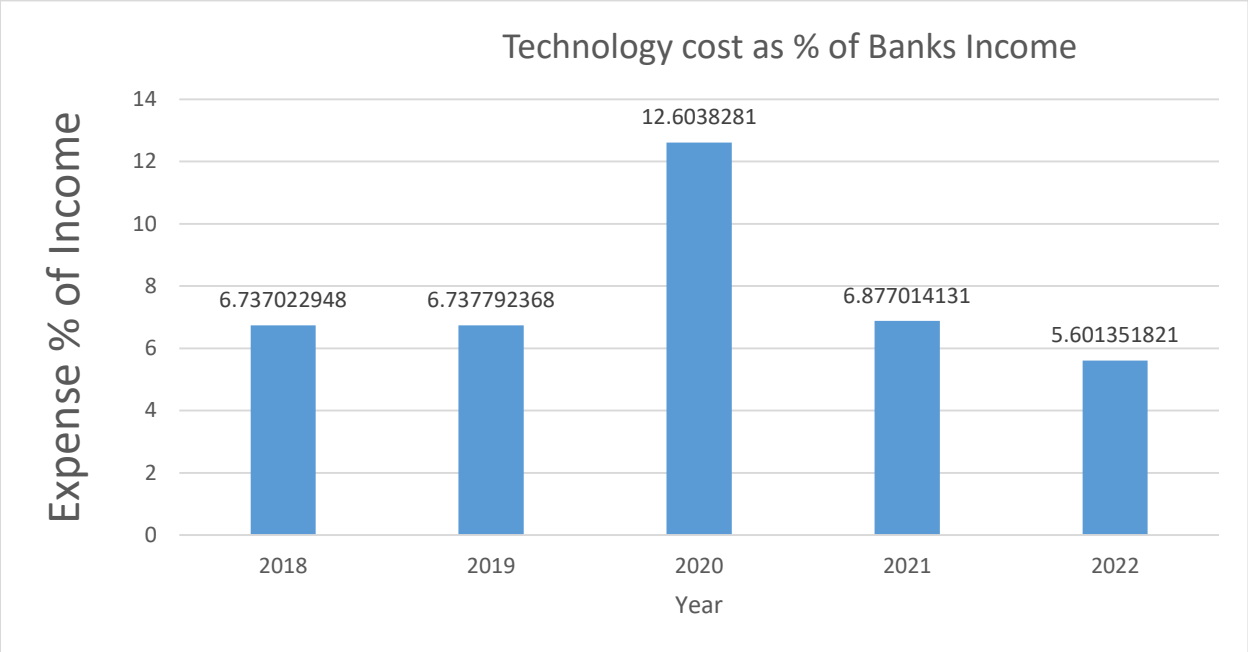
demonstrates the amount of costs the bank incurs annually to combat financial sector cybercrimes. This cost includes purchases of systems, hardware, security, and computer systems.



Source: Researcher 2023

The graphic above shows how the bank is dealing with steadily rising computer-related expenses. From 2018 to 2020, as shown in the accompanying graph, the cost was rising steadily yet alarmingly quickly. It increased exponentially from 418.8 million to 3.951 billion in just two years, from 2020 to 2022. This was taken from financial statements for banks that had been audited. The cause for this rise is the rising volume of electronic transactions along with the discovery of COVID 19 in 2020, which made people and consumers stay inside during lockdowns. Due to this, more people are using electronic channels, and banks are investing in technology and security mechanisms.

4.5.3 Effects of computer information technology cost on ZB Banks total Income.



Source: Researcher 2023

The data was taken from the bank's financial statements from 2018 to 2022, as shown in the image above. It demonstrates that the bank kept its technical costs below 7% of revenue in 2018 and 2019. Banks are able to maintain those costs at 7% of their overall revenue during those two years. The breakout of the contagious disease COVID-19, which changed the entire way of doing business to more online transactions, caused the prices to climb rapidly to 12.6% in 2020, nearly double from the previous years. Lockdowns and travel restrictions forced businesses to use more online methods of conducting business.

In 2020, the bank began allowing its employees to work from home and encouraged customers to use digital channels. As a result, the cost of technology at ZB Bank nearly doubled. The cost recovery rate fell back to less than 7% in 2021 compared to earlier years. As can be seen from the examination of ZB Bank's financial records from 2018 to 2022, a sizable portion of the bank's revenue is consumed by technology costs. Since cybercrime entails and needs to be combated in order for the bank to remain in operation, the consequences of these costs are quite recognizable and have an impact on ZB Bank's financial performance over time.

4.5.4 Direct financial loss.

Out of the 39 questionnaires that were returned, 69.25% of the respondents said that the bank and its customers had both suffered sizable financial losses as a result of cybercrime, with consumers bearing the majority of the costs. However, 30.72 percent of the respondents said that the bank had not suffered any sizable financial losses as a result of cybercrime. Among those who said they had no financial losses, it is noted that most losses are borne by the client. Bank clients in Zimbabwe who have their cards copied or skimmed are the main victims of these situations because they reluctantly provide their personal identification number (PIN) to strangers in exchange for money or other illegal transactions.

They proposed that this loss would primarily be borne by customers and that it would have long-term effects, such as victims suing the bank or spreading false information about it, which would harm the bank's reputation and cause customers to avoid it, lose significant clients, and compromise secure systems. These conclusions were backed by study by Mugari (2017), which found that most respondents admitted to have lost money to cybercrime at some point. Given that it involves both the bank and the customer closing huge sums of money, this has a significant impact on ZB Bank's financial performance. Customers are the primary victims of cyberattacks in Zimbabwe due to patterns and attacks, not the clients cover the majority of the losses, but in the long run the bank's reputation will be damaged as wary clients migrate elsewhere to avoid cybercrime. Over time, direct financial loss has a ripple impact on a bank's financial performance.

4.5.5 Reputational Damage.

Table 4.4 shows that 21.5% of respondents indicated that their bank has experienced reputational harm as a result of cybercrime losses and the impact of cyberattacks related to the bank's digital platforms. They disclosed that the bank had lost quite a few significant clients, and as a result, they had lost their market share and competitive advantage in the financial services sector to other banks including CBZ and NMB Bank. They needed to develop and draw in more business since as a result, their revenues were being weakened and declining. However, 79.5% of respondents claimed that the bank has not experienced reputational harm as a result of cybercrime because, in most cases, customers' negligence results in them disclosing their security to fraudsters, for instance.

These results show that the bank is making every effort to secure its systems so that they won't encounter any problems. They then leave it up to the customers to fulfil their responsibility of

keeping their information and ATM cards private and secure in order to reduce cybercrimes. They hypothesized that the bank is working extremely hard to provide customers with an efficient system that will inform them on every transaction on their phones and allow them to alter their PIN and block an account whenever they feel it is unsafe in order to prevent unauthorized access to their accounts.

One of the responses brought up how the cloning of the card of a well-known customer damaged the bank's reputation. Numerous clients lost faith in the bank, but an examination revealed that it was the clients' fault. This data revealed that because it undermines customer loyalty and confidence, cybercrime hurts businesses. Overall, the results revealed that ZB Bank did not care about reputational harm because they maintain that the system is secure and that customers are typically to fault when something goes wrong. Although it is impossible to precisely quantify how reputation damage affects a bank's financial performance, institutions who are the targets of more serious hacks may notice that their brand image has been severely damaged.

Customers and other significant stakeholders could feel less confident entrusting a bank with their private data if the bank's IT system has been compromised at least once in the past, according to (Investopedia.com). Target experienced a negative impact on its reputation following a data breach in 2013 which compromised credit card information of over 40 million consumers. The company incurred of $18.5 million to fix the security issue. If this occurs to ZB Bank, it will have a significant negative impact on its stocks, clientele, and profitability, which will hurt the bank's financial performance.

4.5.6Loss of business data

From the survey, 77% of those polled admitted that the bank has lost important business data as a result of malware infestation and user lockout on computers. They acknowledged that their bank had at some point misplaced private information, endangering both their operations and very life. Only 23% of respondents said their bank has never lost client information as a result of cyberattacks. Banks are now extremely vulnerable to malware assaults due to the proliferation of online transactions, which puts them at danger of losing important corporate data. These results showed that the internet has improved corporate practices, expanded consumer bases, and increased revenue while also opening up new opportunities for illegal activity.

The association between the disclosure of a security breach and adverse consequences on Banks or any company supports the findings. When breaches involve unlawful access to sensitive data, Mugari (2016) examines public companies and discovers a significantly substantial unfavourable market response. Stafford (2013) discovered that within two days of the notification, breached organizations experience an average 2.1% market value loss. According to Balan et al. (2017), data breaches have a negative and statistically significant impact on a company's market value on the day of the announcement. They also find statistically significant reactions 10 days after the news reports, and they note that the Japanese stock market reacts to news reports of cyberattacks more slowly than the US market.

Gupta (2019) conducted the analysis across two different subperiods and discovered a strong negative impact of information security breaches on firm stock market results. Attacks related to availability breaches are believed to have the biggest detrimental impact on stock market returns and, consequently, the financial performance of banks, especially those that are listed on public exchanges like ZB bank.

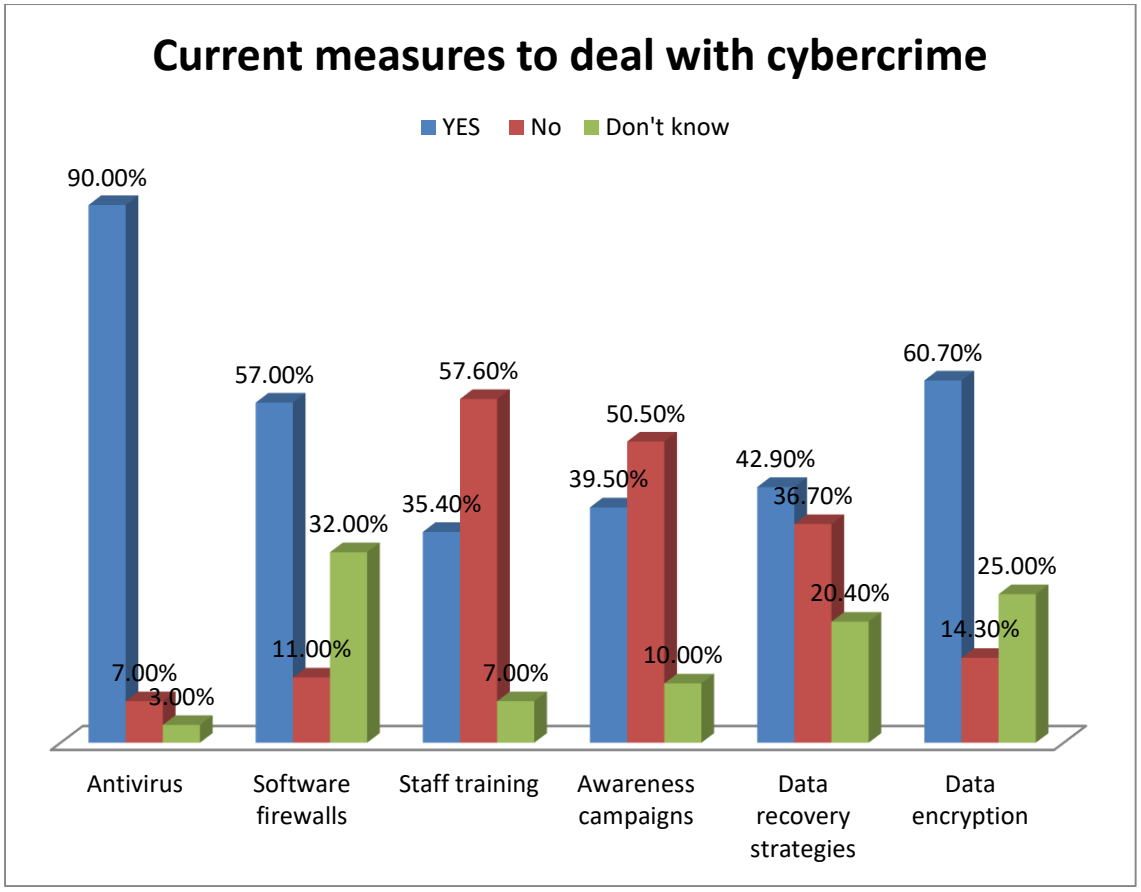
4.5.7 Loss of intellectual property.

Only 13% of participants, as shown in Table 4.4, reported that the bank had lost intellectual property, whereas 87% of respondents said they had never lost any intellectual property. These findings demonstrated that intellectual property theft is not a frequent occurrence in Zimbabwe. This is due to the fact that the majority of cybercriminals have financial motivations, making it very unprofitable to steal and sell intellectual property. These findings concurred with those of Kreshetri (2005), where the majority of respondents stated that they had never experienced the loss of intellectual property due to cybercrime

4.6 Current measures to deal with cybercrime

To reduce the organization's loss from cyber-related crimes, prevention and detection costs are incurred. The introduction of reactive techniques to address the recognized cybercrime situations, such as disaster recovery response costs, results in reaction costs. Online transfers of stolen money or full account takeovers have an impact on bank finances. This can also entail sowing doubts about the financial institution's dependability and safety. According to Lewis and Baker (2013), opportunity costs associated with cybercrime might be viewed as indirect costs or image-related costs. These measures have an impact on technology expenses, as was previously discussed, and because they raise costs, they have a significant impact on ZB Bank's financial performance. Below, these metrics will be examined

Figure 4.6 Measures to minimize cybercrime and also have effect on Bank financials



[Source: Primary data, 2022] N=39

Figure 4.6: Current Preventive measures against cybercrime in the Banking industry.

4.6.1 Antivirus

90% of the respondents, as shown in figure 4.1, agreed that their organizations used antivirus software to reduce the risks posed by cybercrime. This shown that in the retail banking sector, using antivirus software is a typical technique to combat cybercrime. Additionally, every single one of the 90% of respondents agreed that using antivirus was a good method to reduce the risk of cyberattacks. These results were in line with those of Mawunge's (2017) study, which showed that antivirus software was the most often used defence against cyberattacks in the banking industry.

However, using antivirus software has a cost because owners must pay to use the full functionality of the software while being protected by an efficient antivirus. Since it can limit

the privileges one has on a computer system, the confirmed is the first line of defence on all bank computers and systems.

4.6.2 Software firewalls.

Although 11% of the respondents had minimal awareness about firewalls, 57% of the respondents said that software firewalls were employed to protect computer systems. Only 27% of the respondents said they did not know about or utilize software firewalls as a precaution to secure their computers since the information and technology department should handle such matters; most of these respondents were from service centres and claimed to only be knowledgeable about how branches operate.

Many of the people who claimed that the bank wasn't utilizing firewalls weren't computer experts, therefore their knowledge of firewalls was limited. Computer experts for banks' IT departments indicated that the best way to combat cybercrime is to combine software firewalls with other preventive measures like antiviruses and passwords. The majority of banks had implemented firewalls on their computers and systems. Balan et al (2017) supported this finding by recommending the use of strong passwords and firewalls as practical measures to combat cybercrime in workplace.

4.6.3 Data encryption.

A whopping 60.7% of respondents from the bank said they encrypt their data, compared to a total of 14% who don't and 25% who are unaware of the practice. As a result, several of the respondents were illiterate and unaware of data encryption as a defence for their companies against cybercrime. However, the majority of service centre respondents demonstrated that they were unaware of data encryption because it is only relevant to the IT department and all they are familiar with is how to use internal systems.

4.6.4 Data recovery strategies.

Additionally, as shown in figure 4.1, 42.9% of respondents verified that banks had data recovery methods in place, while 20.40% of respondents said they were unaware of such plans. Only 36.7% of respondents stated that they had no data recovery plans, and the 36% who acknowledged that they were unaware of recovery facilities worked in areas unrelated to IT? Every year in October, the IT department confirms that it has a highly successful recovery process that is carried out centrally. According to research by Balan et al, businesses were

shown to be very susceptible to cybercrime losses since they were ignorant of the crime and had no plans for data recovery.

4.6.5 Staff training.

Users of computers and networks are educated about cybercrime awareness in ZB Bank, but the research found that the majority of respondents said that staff members are not trained in this area, which increases the likelihood of cyberattacks. According to about 57.6% of respondents, the bank does not provide staff training. 7% of respondents claimed they were unaware of staff training, while 35.4% acknowledged that they were offered staff training awareness. During the data collection, one of the executives mentioned that employees were reluctant to attend the training. He gave the example of a bank-funded program that was intended to train employees but had no upkeep, which led the bank to revoke the trading that it had advertised via internal email. Training is essential in the battle against cybercrime since, according to research by Boateng et al. (2011), authorities in Ghana lacked the investigative, controlling, and technological competence to tackle cybercrime.

4.6.7 Awareness Campaigns.

Since the general people will be using these products, the majority of respondents agreed that awareness programs on the advantages and risks of embracing ICT in the banking industry should be made available to them. The majority of respondents, as seen in figure 1, were likely to confirm that the bank did not run any awareness initiatives on cybercrime. The research by Mugari (2016) revealed that more than half of respondents were unaware of the laws controlling cybercrime in Zimbabwe, which corroborated these findings. In order for the general public to know where to report cybercrime incidents, the state should commission a cyberlaws awareness campaign. Mugari (2016), who argued for the organization of workshops and seminars for players in the retail sector to be informed on risks posed by adopting ICT, supported these findings.

4.7 The connection between performance and alternative banking channels

Table 4.7: The correlation between performance and Cybercrimes

		Cybercrimes	Financial Performance
Cybercrimes	Pearson Correlation	-1	-.621
	Sig. (2-tailed)		.005
	N	39	39
Financial Performance	Pearson Correlation	-.621	-1
	Sig. (2-tailed)	.005	
	N	39	39

Correlation is significant at the 0.05 level (2-tailed)

The relationship between ZB Bank's performance and cybercrimes is shown in table 4.9.1, where N is the number of respondents 39, and 0.05 is the level of significance. The results show that independent variables have a negative correlation to the dependent variable of -.621**, and the p-value is .05, which is greater than 0.001. When the p-value is greater the level of significance, researchers draw the conclusion that the variables are not corelated. In conclusion, ZB Bank has found that cybercrime have a negative impact on banks' financial performance. This suggests that cybercrime and ZB Bank performance have a significant negative correlation. As evidenced by ZB Bank, cybercrime have a negative effect on the bank's business.

4.8 Chapter summary

This chapter's primary objective was to present and analyse the data that had been collected for the study using surveys and secondary data sources from the ZB website. A sizable portion of the information presented in this chapter was derived from questionnaire responses, financial

statements from the previous five years, and reports. The majority of findings agree with both theoretical and empirical literature. The summary, conclusion, and recommendations based on the study's findings will all be included in the next chapter.

CHAPTER V

SUMMARY, CONCLUSION AND RECOMMENDATION

5.0 Introduction.

The objective of this section is to provide a brief overview of the study's discoveries while concentrating on the conclusions and recommendations.

5.1 Summary of research findings.

According to the researcher's findings about the types of cybercrime that are most common in the banking sector, card fraud, virus spread, and hacking are the main ones. Additionally, it was discovered that phishing was rapidly entering the banking industry. On the other hand, the study found that ransomware and BEC scams were uncommon occurrences in the banking industry. Identity theft and Denial of Service attacks were also noted as being less frequent in banks, despite the fact that statistics indicated they are gradually making their way into the retail industry. Despite the advantages of adopting technology in the banking industry, it was found through research that the majority of customers and banks were vulnerable to the expensive consequences of cybercrime. The majority of respondents who used online platforms like ATM cards to respond confirmed that the bank had experienced direct or indirect financial losses due to cybercrime. Additionally, it was found that cybercrime costs ZB Bank a lot, including reputational damage, which reduces competitive advantage and has a negative impact on the bank's financial performance. The study also revealed that banks incur incremental additional costs, such as insurance premiums, IT consulting fees, and software update costs, to secure their systems

The financial implications of cybercrimes on bank performance, particularly in developing economies like Zimbabwe, represent a highly sensitive issue. A very vulnerable target are nations like Zimbabwe due to structural and institutional imbalances. Because of the growing use of information technology, it is now even more likely that someone will benefit fraudulently from a cybercrime. Cybercrimes has caused a severe loss of hundreds of millions annually, and it has incurred a negative impact on the bank's performance at the same time increasing the financial losses. According to reports, the cumulative impact of cybercrimes creates a worrisome framework about how sensitive economies are to any kind of cyberattacks, like market manipulation and fraudulently obtaining access codes to customers' bank accounts.

The negative publicity image scandals, reputational damage, loss of customer confidence, loss of company data decreased efficiency, interruptions in business operations, exposure of private customer data or authorized entry to exclusive product advancements and loss of proprietary information, and other extremely significant issues are just a few of the non-financial effects of cybercrimes on banks. Given certain non-financial ramifications, it can be very challenging to estimate the cost of cybercrime attacks with any degree of accuracy. Additionally, the non-financial effects of cybercrime are rather challenging to quantify, but they unquestionably have a very high impact with extremely dramatic effects on banks' financial performance

The relationship between ZB Bank's performance and cybercrimes is shown in table 4.9.1, where N is the number of respondents 39, and 0.05 is the level of significance. The results show that independent variables have a negative correlation to the dependent variable of -.621**, and the p-value is .05, which is greater than 0.001. When the p-value is greater the level of significance, researchers draw the conclusion that the variables are not corelated. In conclusion, ZB Bank has found that cybercrime have a negative impact on banks' financial performance. This suggests that cybercrime and ZB Bank performance have a significant negative correlation. As evidenced by ZB Bank, cybercrime have a negative effect on the bank's business.

5.2 Conclusion.

Cybercrime in Zimbabwe's retail banking sector is primarily characterized by the spread of viruses, hacking, and card fraud. According to the study, the growth in card fraud in the banking industry has been facilitated by the increased use of cards for payments. There is a high likelihood that cybercrime will increase in the banking sector of Zimbabwe given the ongoing growth of online payment systems following innovation in ICT infrastructure. The primary goal of this study was to examine the financial and non-financial repercussions of cybercrimes that will affect ZB Bank's financial performance.

Due to recent developments in information technology, cybercrime has become an inevitable part of modern life. The actual, extremely unsettling insight, however, points to a developing industry for cybercrime. In developing nations like Zimbabwe, where Internet traffic is currently growing significantly, attacks from cybercrime are becoming more commonplace. As a precaution, security and prevention strategies need to advance in terms of technology and available funding.

In order to achieve effective results and protect banks and all involved customers from losing funds, trust, operations, and also from negatively affecting the financial performance of involved companies like ZB bank, the strict measures anti-cybercrime threat should involve businesses, forensic departments, government agencies, public institutions, and even regular people as Internet users.

5.3 Recommendations.

Each employee should have their own user account, and a rule requiring password changes every three months should be in place. Unauthorized software downloads and installations by employees must be strictly prohibited. All staff members must be made aware of the risks associated with downloading or opening email attachments from unknown senders. Inform staff members of the value of maintaining the confidentiality of any sensitive information pertaining to the institute. Because firewalls obstruct all communication from unauthorized sources, the IT department of a bank must make sure that they are activated on each workstation and Internet-connected device in the company.

Banks must enable two-factor authentication (2FA) on all online accounts, whenever possible, using 2FA apps or physical security keys. All PC operating systems would receive routine security updates thanks to the Department. Anti-spyware and anti-virus software must be installed on all PCs in order to check for the presence of ransomware or other harmful software on the network. Wireless networks and all passwords need to be kept secure and protected. As more customers use mobile devices, banks must use verification techniques like dynamic device authentication and web-based transaction verification.

Banks must notify customers and send them automated messages confirming the accuracy of their transactions. Customers must be provided with information on how to confirm the reliability of any sources requesting personal account information. Additionally, customers must receive guidance on how to use the bank's websites safely. Use a secure network when using a banking application or online banking.

5.4 Recommendations for further study.

Cybercrime is a rapidly spreading global threat that has negative effects on all industries, with the banking sector being the most severely affected. These effects include financial loss and

much more. Therefore, more study needs to be done on the impact of cybercrimes on the financial statements of various organizations.

References.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M. & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer Berlin Heidelberg

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

Bell, R. E. (1995). The prosecution of computer crime. Journal of financial crime, 9(4), 308-325

Bryman, A. & Bell, E. 2015. Business research methods. 4th Edition. UK: Oxford University Press.

Claessens, J., Dem, V., De Cock, D., Preneel, B., &Vandewalle, J. 2002. On the security of today's online electronic banking systems. Computers &Security, 213: 253-265

Douglas, T., & Loader, B. D. 2000. Cybercrime: Security and surveillance in the information age: Routledge

Das, S. & Nayak, T. 2013. 'Impact of Cyber Crime: Issues and Challenges': International Journal of Engineering Sciences & Emerging Technologies, Volume 6 (2): 142-153.

Florêncio, D., & Herley, C. 2011. Where Do All The Attacks Go? Economics of Information Security and Privacy III pp. 13-33. Springer New York

Hannan, M., & Blundell, B. (2004). Electronic Crime-it's not only the big end of town that should be worried. In Australian Computer, Network & Information Forensics Conference (pp. 94-102)

Hutchinson, D., & Warren, M. 2003. Security for internet banking: a framework. Logistics Information Management, 161: 64-73

Jaishankar, K. (2007). Establishing a theory of cybercrimes. International Journal of Cyber Criminology, 1(2), 7-9.

Ghazi-Tehrani, A.K & N. Pontell, H.N. 2021. Phishing Evolves: Analyzing the Enduring Cybercrime, Victims & Offenders, 16:3, 316-342, DOI:10.1080/15564886.2020.1829224

Gupta, S. 2019. Ethical hacking terminologies. Ethical Hacking – Learning the Basics. https://doi.org/10.1007/978-1-4842-4348-0_1

Kothari, C. (2004). Research Methodology, Methods and Techniques. New Delphi: International P Limited.

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 11(4), 541-562.

Leedy, P.D. & Ormrod, J.E. 2001. Practical research: planning and design. 7th edition

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. The Journal of Economic Perspectives, 23(3), 3-20.

Mugenda, O.M., &Mugenda, A.G. (2003).Research methods qualitative & quantitative approaches. Nairobi: African Centre for Technology Studies

Mugari, I., Gona, S., Maunga, M and Chiyambiro, R. 2016. 'Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe': Mediterranean Journal of Social Sciences, Volume 7 (3): 135

Mugari, I. 2017. Perspectives on Cyber- Threats to the Retail Sector. A Case Study of ZB bank international Journal of Innovative Research and Development Vol 5 (3)

Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances.

Siddique, I., & Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector-An Overview. International Journal of Business & Information Technology, 1(2).

Stafford P. (2013) [Online] Cybercrime threatens global financial system. Available at: http://www.ft.com/cms/s/0/9804988c-3722-11e3-9603-00144feab7de.html#axzz2tMwSTsmF

Slovin's 2009. Research Methods of Business: A Skill-Building Approach 2nd Edition, John Wiley and Sons, Inc, New York, USA, pp 253 ff.

Schindler (2001). Impact of Electronic Crime in Indian Banking Sector-An Overview. International Journal of Business & Information Technology, 1(2).

Wall, D. 2001. 1 Cybercrimes and the Internet. Crime and the Internet: 1.

APPENDICES

APPENDIX 1: RESEARCH ASSISTANCE LETTER

BinduraUniversityofScienceEducation
P.Bag1020
Bindura
Zimbabwe

To whom it may concern.

RE: REQUEST FOR RESEARCH ASSISTANCE.

My name is Chirimuta Doreen P an undergraduate student at the Bindura University of Science Education, studying for a Bachelor of Commerce (Honours) Degree in Banking and Finance. As a requirement of my studies, I'm carrying out a research "**ANALYSIS OF CYBERCRIME EFFECTS ON BANKS FINANCIAL PERFORMANCE. (A CASE STUDY OF ZB BANK).**"

I would be much thankful if you could participate in this process by sharing your experiences pertaining to cybercrime. May you kindly assist me by completing the attached questionnaire?

Your participation in this study is voluntary and should you at any moment decide to withdraw your participation, you are free to do so without any prejudice. You are also advised that no financial or any other benefit will accrue to you for your participation the study.

I provide assurance that the data gathered will be only used for the purpose of this research and will be treated with utmost confidentiality.

Yours Faithfully

Chirimuta Doreen P

APPENDIX 2: QUESTIONNAIRE

Section A: Demographic Data

Please indicate by putting a tick below

1. Gender male [ ] female [ ]

2. Age below 25 [ ] 25-29 [ ] 30-34 [ ] over 35 [ ]

3. How much time have you spent working in your organisation?

Less than 1 year	1-3 years	4-6 years	Above 6 years

4. Stationed department or Cluster.

Please indicate below

Service centres [ ]

E Banking [ ]

Audit [ ]

Bank Executives [ ]

Computer Security [ ]

5. Please indicate your position below

Managers [ ] Supervisor [ ] Middle Level [ ] Entry level [ ]

Other [ ] Specify:……..

Section B: Types of cybercrime.

6. Below are some of the common forms of cybercrime in business. Please indicate their prevalence rates in your organisation:

Type of cybercrime	Doesn't occur	Less than prevalent	Prevalent	Very prevalent
Denial of service attacks				
Hacking				
Virus Dissemination				
Card fraud				
Phishing				
Ransomware				
Email Fraud				

7. What other cybercrime are prevalent in your organization. Please indicate below if there are any.

……
…….....
.....

Section C: Impact of cybercrime.

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

Impact	Yes	No
Direct financial loss		
Additional network security costs		
Loss of sensitive data		
Reputational damage		
Loss of intellectual property		

9. What other effects has your organisation suffered due to cybercrime?

……
……
……
……

Section D: Measures to minimise cybercrime.

10. Below are some of the strategies that companies adopt to curb cybercrime. Please indicate whether the measures are available in your organisation.

Measure	Yes	No	Don't know
Antivirus			
Software firewalls			
Data encryption			
Data recovery strategies			
Staff training			
Awareness campaigns			

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

.....
.....
.....

12. What is your overall comment on the cyber security system in your organization?

Very ineffective		Not effective		effective		Very effective	

Section E: Measures that can be taken to minimise cybercrime

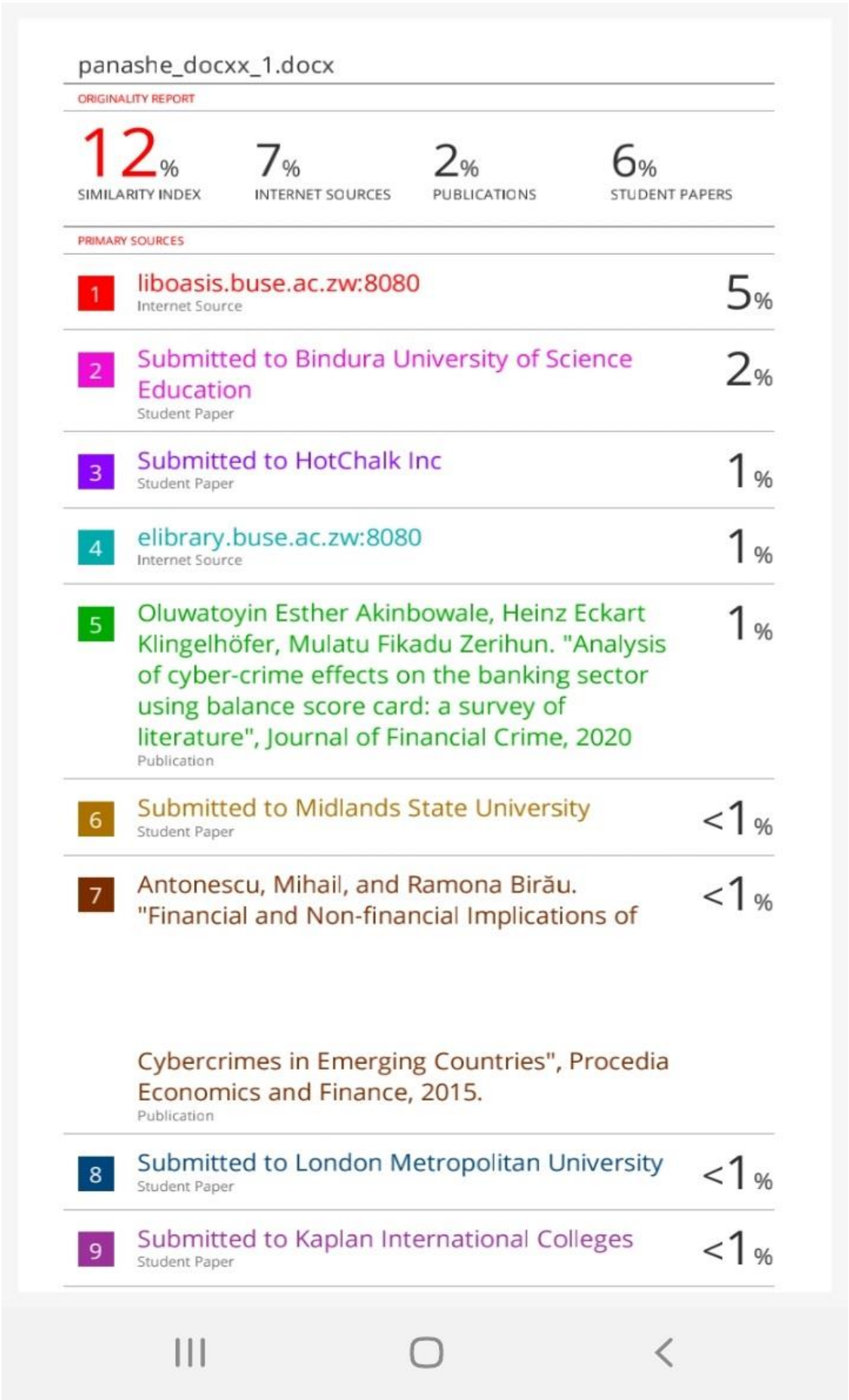
13. What measures can be taken to minimise cybercrime in the retail banking sector.....
.....
.....
.....

14. In your own opinion, how can the government assist in the fight against cybercrime?

……
……
……
…….

End of Questionnaire

Thank you for your cooperation.



panashe_docxx_1.docx

ORIGINALITY REPORT

12%	7%	2%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	liboasis.buse.ac.zw:8080 Internet Source	5%
2	Submitted to Bindura University of Science Education Student Paper	2%
3	Submitted to HotChalk Inc Student Paper	1%
4	elibrary.buse.ac.zw:8080 Internet Source	1%
5	Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer, Mulatu Fikadu Zerihun. "Analysis of cyber-crime effects on the banking sector using balance score card: a survey of literature", Journal of Financial Crime, 2020 Publication	1%
6	Submitted to Midlands State University Student Paper	<1%
7	Antonescu, Mihail, and Ramona Birău. "Financial and Non-financial Implications of Cybercrimes in Emerging Countries", Procedia Economics and Finance, 2015. Publication	<1%
8	Submitted to London Metropolitan University Student Paper	<1%
9	Submitted to Kaplan International Colleges Student Paper	<1%