BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

THE IMPACT OF CYBERCRIME ON THE PERFOMANCE OF FINANCIAL INSTITUTIONS IN ZIMBABWE. A SURVEY OF BANKS IN HARARE CENTRAL BUSINESS DISTRICT

BY

VANESSA R NGWENYA

(B201604)

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE BACHELOR OF COMMERCE HONORS DEGREE IN FINANCIAL INTELLIGENCE OF BINDURA UNIVERSITY OF SCIENCE EDUCATION FACULTY OF COMMERCE.

JUNE 2024

RELEASE FORM

Student Number: B201604B

Dissertation Title: The impact of cybercrime on the performance of financial Institutions in Zimbabwe.

Degree Title: Bachelor of Commerce Honours Degree in Financial Intelligence.

Date 2024

Permission is granted to Bindura University of Science Education Library to produce copies of this research and lend or sell those copies for private, scholarly or scientific purposes only. The author will always reserve publication rights of neither the project nor extensive extract, from it may be printed or otherwise reproduced without the author‟s written permission.

Signed ----------

APPROVAL FORM

TITLE: AN ANALYSIS ON THE IMPACT OF CYBERCRIME ON THE PERFOMANCE OF FINANCIAL INSTITUTIONS DOMICILED IN HARARE.

TO BE COMPLETED BY THE STUDENT:

I CERTIFY THAT THIS DISSERTATION MEETS THE PREPARATION GUIDELINES AS PRESENTED IN THE FACULTY GUIDE AND INSTRUCTIONS FOR TRYPING DISSERTATION

---------- ----------

(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 SUPERVISOR) (DATE)

TO BE COMPLETED BY THE CHAIR OF THE DEPATMENT:

I CERTIFY TO THE BEST OF MY KNOWLEDGE, THE REQUIRED PROCEDUREDS HAVE BEEN FOOLLOWED AND THE PREPARATION CRITERIA HAVE BEEN MET FOR THIS DISSERTATION.

---------- ----------

(SIGNATURE OF THE CHAIR PERSON) (DATE)

DECLARATION FORM

I, B201604B, DECLARE THAT THIS RESEARCH STUDY HAS NOT BEEN SUBMITTED FOR ANY DEGREE AND THAT ACKNOLODGEMENTS HAVE BEEN MADE TO THE CONTRIBUTIONS OF OTHERS WHERE APPROPRIATE.

NAME OF THE STUDENT: VANESSA REBECCA NGWENYA

SIGNATURE.....

DATE.....…

ABSTRACT

Despite efforts over the years to fortify internal bank controls as a defense against cybercrime, financial institutions continue to suffer financial losses as a result of cybercrime, which also negatively impacts their operations. According to (Kabanda, 2012), cybercrime is becoming more common in Zimbabwe. The estimate that the number of cybercrimes rose by 21.8% between 2010 and 2019 (ZRP 2020) provided evidence for this. In contrast to the 9% of incidents that were documented between 2002 and 2009.The main aim of the study was to analysis on the impacts of cybercrime on the performance of financial institutions in Zimbabwe, is a survey of banks located in Harare Central Business District. The study was guided by the following objectives, to determine the impacts of cybercrime on the performance of financial institutions, to analyse the advancement of technology in the banking sector , to identify types of cybercrime prevalent in financial institutions and to recommend policies that can be put in place to reduce impacts of cybercrime in Zimbabwe. A descriptive survey research design was employed in this study with the goal of painting an accurate and clear image on the impact of cybercrime on the performance of financial institutions. The sample size of 42 respondents was derived using stratified random sampling and convenience sampling techniques. Data was gathered using questionnaires and interview guides. From the study it was found out that technological advancement necessitates cybercrime. Phishing and electronic card fraud, were considered to be more prevalent in financial institutions, hacking being the least. From the research findings, it was deduced that Cybercrime have a negative impact on the performance of financial institutions in Zimbabwe as it causes financial and non- financial impacts. The negative impacts includes reputational loss, direct financial loss and productivity loss. Basing on the conclusion of the study, it can be recommended that, constant educational programs, upgrading system on regular basis, implementation of shielded authentication and use of multi-layer security can help financial institutions to safeguard against cybercrime.

ACKNOWLEDGEMENTS

First and foremost, praises and thanks to the Lord, the Almighty, for His showers of blessings throughout my research work to complete the research successfully
I would like to express my deep and sincere gratitude to my research supervisor for providing invaluable guidance throughout this research. It was a great privilege and honour to work and study under her guidance. I am extremely grateful to my dad for his love, prayers, caring and sacrifices for educating and preparing me for my future. I am very much thankful to my sister for her prayers and valuable support to complete this research work. I am overwhelmed and grateful to those who helped me to complete this research.

DEDICATION

I would like to dedicate this dissertation to my dad, who always strengthen me during hardships, and always stand by my side. Your love keeps me going, thank you for being there and supporting me during my research, not forgetting the chief of all things our Lord Jesus Christ.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.0 Introduction

The purpose of the research study was to assess the impact of cybercrime on the performance of financial institutions in Zimbabwe. This chapter covered the following topics: the study's background, the problem description, its objectives, research questions, significance, assumptions, delimitations, limitations, definition of important words, and a summary of the findings

1.1 Background of the study

The word ‘cyber’ is synonymous with computer, computer system and computer network, so it can be said that cybercrime occurs when any illegal activity is committed using a computer network. According to (B.D, 2000), defined cybercrime as a computer mediated activity which is conducted through global electronic networks that are either considered illicit by certain parties. Cybercrimes have been classified into four categories (Wall, 2001). These four categories includes cyber-deceptions, cyber-violence, cyber-pornography and cyber-trespass. The frauds in e-banking sector are called cyber-deception and it is defined as an immoral activity which includes theft, credit card fraud and intellectual violations. Mostly frauds are committed because of two goals that is to gain access to the user’s account and steal personal information and transfer funds from one account to another and also to undermine the image of the bank and block the banks server so that the customer is unable to access personal account.

In terms of number of cybercrime incident ransom ware, identity theft and phishing attacks India has been ranked among the top five countries. According to Global Economic Crime Survey 2014 conducted by PwC, cybercrime was one of the top economic crimes which was reported by various organizations across the world including India. According to (National Crime Records Bereau, 2015), reported that a total of 5752 people were arrested in 2013 registering 74.3% increase over the previous year.

In China the most famous case of cybercrime occurred in 2006 when Li Jun the author of Panda worm met online with Wang Lei a Web master and Zhang Sun an envelope

stealer. Li June and Wang Lei set up several websites which infected visitors with the Panda virus. They sold traffic to Zhang Sun by allowing him to link this Web-based Trojan to the websites. The visitors of the websites were infected by several Trojans and virtual goods mainly online game and QQ logins were stolen. Millions of machines were believed to have been infected across China and the losses due to this incident were estimated to be up to 100 million RMB (US $14 million). Li June made estimated profit of around 150000 RMB (US $22156) (Zhuge 2008). In 2007 Li June and his accomplices were caught by uncover police pretending to be a potential buyer of his malware.

Kenya suffered the most losses in East Africa, losing $171 million to cybercriminals. Tanzania lost $85 million, while Ugandan businesses lost $35 million, according to (A, 2017). According to the Cisco Annual Cyber Security Report (2017), more than one-third of the firms who suffered a breach in 2016 reported significant customer, opportunity, and revenue loss of more than 20 percent. Africa lost a record $2 billion to cybercriminals in 2016 alone, according to (E.F.G, 2016).

According to the Zimbabwe National Risk Assessment Report (2015), cybercrime resulted in the theft of nearly $26,000 from a CABS client. The Zimbabwe Republic police (ZRP) released statistics showing that over $40 million was lost to cybercrime in the first quarter of 2019. In the same time frame, the ZRP Cybercrime Unit's officials were only able to recover $1.468 million. This figure is especially concerning because it indicates that fewer than 4% of the money that was lost was found. In 2018, Reserve Bank of Zimbabwe released a report detailing 13 instances of credit card fraud, 24 instances of unapproved bank account access, 10 instances of identity theft, and 20 instances of phishing.

1.2 Problem statement

In Zimbabwe, practically all financial institutions are enhancing their operations by obtaining cutting-edge technologies, and this has shown to be effective. Nonetheless, this has made it necessary for more people to have access to banking services. In Zimbabwe, nearly every adult who is older than 18 has a bank account. However, as a result of these new technology adoptions, cybercrimes have increased from negligible to very high levels in the twenty-first century.

According to (Kabanda, 2012), cybercrime is becoming more common in Zimbabwe. The estimate that the number of cybercrimes rose by 21.8% between 2010 and 2019 (ZRP 2020) provided evidence for this. In contrast to the 9% of incidents that were documented between 2002 and 2009. On the other hand, as new technologies are developed, ICT is growing daily. This demonstrates that as financial technology advances, so do the number of cybercrimes committed.

Despite efforts over the years to fortify internal bank controls as a defense against cybercrime, financial institutions continue to suffer financial losses as a result of cybercrime, which also negatively impacts their operations. The study's focal point is this.

1.3 Research Objectives

The main goal of the study is to determine the impact of cybercrime on the performance of financial institutions in Zimbabwe. The study's other goals are to:

1. To identify the types of technological advancement in financial institutions in Zimbabwe
2. To identify the different kinds of cybercrimes that are common in Zimbabwe
3. To recommend policies that would lessen the impact of cybercrimes in Zimbabwe.

1.4 Research Questions

The study set out to address the following:

- What are the technological advancement that are being adopted by financial institutions in Zimbabwe?
- What are the types of cybercrime prevalent in financial institutions in Zimbabwe?
- What are the impacts of cybercrime on performance of financial institutions in Zimbabwe?
- What methods can be employed to decrease the effects of cybercrime on financial institutions in Zimbabwe?

1.5 Significance of the study

- To banks in Zimbabwe

The banking industry in Zimbabwe can modify its processes in order to eradicate cybercrime by using the knowledge gained from this study.

- To policy makers

Finally, the study is anticipated to be significant because bank regulators and policy makers can use the data acquired.

- Importance to the researcher

The research will serve as a training ground for conducting research and give the researcher research abilities, so the student will have a thorough grasp.

- To Bindura University

Students at Bindura University of Science Education who could conduct a related study in the future can utilize the research as a source for subsequent efforts. The investigation may also offer some insight on cybercrime and how it affects Zimbabwe's financial institutions in Zimbabwe.

1.6 Assumptions

The research was guided by the following assumptions:

- The researcher assumed that the information is readily available and with little or no restrictions.
- The researcher assumed that there is a relationship between cybercrime and technological advancement.
- The researcher assumed that the respondents will deliver information that is free from bias and also return all distributed questionnaires in time.

1.7 Delimitation of the study

The study focused on financial institutions with their headquarters located in Harare since a wealth of information regarding these organizations can be accessed there. Determining the impact;p. of cybercrime on financial institutions' performance was the primary goal of the research project. 2018–2021 was the time frame covered. During

the study, the Zimbabwe Republic Police (ZRP) cybercrime department, bank clients, risk management staff, IT department, e-banking staff, and compliance staff were all considered respondents.

1.8 Limitation of the study

When conducting the survey, the researcher encountered the following difficulties:

Confidentiality

Certain banks held information that they deemed confidential, and as a result, they were reluctant to divulge information that was necessary for the advancement of this study. Certain respondents felt unsafe and uneasy sharing information because they believed it would damage their reputation. The survey's completion was hampered by this obstacle. The researcher did not, however, ask for the names of the respondents or the banks, and they were informed that their identities would not be disclosed. Therefore, in order to safeguard both the Respondent and the Bank, such information was documented in a confidential way.

Financial limitations

Another constraining aspect was a lack of funds for transportation, internet material access, and printing-related expenses. However, the researcher was able to raise some money from friends and family members as well as pay for the research project out of own pocket to make sure it was a success.

Large population and sample size

The population size allowed the researcher to collect sufficient data regarding the many types of cybercrime and how they affect the operations of financial institutions. To address this challenge, the study represented the relative variance of cybercrime in the banking system using a database of well-known banks.

Bureaucracy challenge

Due to the numerous control mechanisms used by financial organizations, information retrieval takes longer than expected. The researcher overcame this by writing bank managers a letter that made it simple and timely to gather information.

1.9 Chapter summary

This chapter primarily focused on providing the study's background, problem statement, research aims, research questions, importance, delimitations, and limits. The following chapter, which reviews the literature, discusses the theoretical underpinnings, conceptual framework, and empirical data about the effect of cybercrime on financial institutions' performance.

CHAPTER 2
LITERATURE REVIEW

2.0 Introduction

This chapter focuses on research on how cybercrime affects the effectiveness of governmental institutions. It consists of a number of studies on cybercrime conducted by various scholars. The theoretical underpinning for the research and empirical review is thoroughly covered in this chapter.

2.1 CONCEPTUAL FRAMEWORK

2.1.1 Definition of terms

Cybercrime

Roderic Broadhurst (2019), defined cybercrime as "offenses committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, directly or indirectly, using modern telecommunication networks such as the internet (including websites and email) and mobile phones (including SMS and MMS)." According to David S. Wall (2015),"Cybercrime refers to criminal acts that are committed through the use of information and communication technologies." Jonathan Clough (2012), "Cybercrime involves the use of digital technologies to commit or enable criminal offenses." According to David Wall (2011),"Cybercrime comprises those criminal acts that are committed by individuals or groups of individuals using modern information technology as the primary means of criminal activity."

1.1 Concept of banking technology

According to Chang (2003), the continued uptake of services like smart card banking, mobile banking, telebanking, and internet banking, among others, has fuelled the development of banking technology.(Tina, 2003). According to Aysan (2014), due to advances in banking technology, customers must conduct financial transactions online through secure websites.(M.A.M, 2014)

1.2 Cyberspace

Gibson (1984) described cyberspace as the networked collections of computers used for communication, information storage, and other purposes.(Gibson, 1984). According to David Clark (2010), it is necessary to define cyberspace's aim, which has been described as the processing, manipulation, and exploitation of information through the facilitation and progress of human to human contact, in order to fully comprehend its nature.(Clark, 2010)

2.1.2 Types of technological advancement.

Internet (online) banking

Internet banking, according to Yibin (2003), is the provision of low-cost and retail banking services and products via the internet. According to Chang and Hamid (2010), internet banking is the practice of allowing clients to make financial transactions online or electronically without physically visiting a bank. The internet has becoming more widely used, with data from Zimbabwe's Postal and Telecommunications Regulatory Authority (2015) indicating a 50% penetration rate in 2015. Internet banking has grown more rapidly in Zimbabwe since Powertel, Africom, and Econet introduced broadband service.

Mobile banking

According to Arcand, Promiene, Brun, and Rajaobelina (2017), mobile banking is a service that banks provide to their clients so they can use their mobile devices to complete financial transactions without physically visiting the banks. Similarly, Okiro (2013) described mobile banking as the provision of banking and financial services through a device such a mobile phone. Usually, SMS or the internet are used for it. Haris (2010) conjectured that clients can obtain financial services using mobile banking from the comfort of their own homes. According to MPS (2012), mobile phone adoption has increased sharply throughout Africa, with Zimbabwe leading the way. In Zimbabwe, mobile money offers faster and more convenient banking services and payment options. In Zimbabwe, practically all banks have embraced mobile banking services.

Biometric Authentication

According to McKinsey & Company (2018), to strengthen security and streamline customer authentication procedures, financial institutions are introducing biometric authentication techniques like voice, facial, and fingerprint recognition.

2.1.3 The types of cybercrimes

Electric card fraud

According to RBZ (2015), a significant cybercrime that many nations suffer is electronic card fraud. Banks now have ATMs where consumers can withdraw cash using their own cards thanks to technological advancements.(RBZ, 2015).Metcalf and

Kirst as point out in Mugari (2016), however, point-of-sale assaults may lead to the theft of data or bank cards. According to Burns and Stanley (2002) the money is then taken from ATMs using the stolen cards. Application fraud, lost and stolen cards, mail intercept fraud, and counterfeit fraud are some examples of card fraud types.(A, 2002) A study from the Zimbabwe Republic Police in 2019 revealed that in the first quarter of 2018, at least $200,000 was lost due to electronic card fraud.(Zimbabwe Republic Police, 2019)

Phishing

According to Nieles et al. (2017), phishing is a method for gathering potentially sensitive information that could be exploited for criminal purposes. Phishing has been classified as a type of identity theft by Baegh (2012). Phishing attacks utilize counterfeit emails purporting to be from a bank or financial institution, a government agency, or another person (US-CERT, 2006). The email contains links to a fake website and asks the victim for private information. Intruders can access the victim's personal account information and finances if they click the link and give them the needed information. Phishing is a prevalent form of cybercrime in Zimbabwe, according to the Reserve Bank of Zimbabwe, and occurrences are progressively increasing.

Vishing

Vishing, according to TTC (2008), is a strategy in which businesses or individuals are conned into giving financial or other information to hackers over the phone. Vishing is persuading a victim to provide personal information via IP-based voice messaging tools. According to Boateng and Amanor (2014), vishing is a crime that is carried out using a short message. For instance, a victim may receive a message informing them that their account has been infected with a virus and that they must send their own information for correction in order to fix the problem. According to Ollman (2007), the words "voiceshing" and "phishing" are combined to form the phrase "vishing”.(G, 2007)

Malware attacks

According to KMPG (2011), malware assaults are characterized as software injections into information systems that cause system degradation.KPMG (2012).The majority of mobile banking services evaluate financial statements, money transfers, alerts for

credits and debits, and bill payments. Gaikwad, cited in Mugari (2017), asserts that malware infiltrates a computer system via data transfers over the internet. Examples of malicious software include worms, Trojan horses, back doors, keystroke loggers, root kits, and spyware. This aligns with the way malware functions and acts. Roughly 46% of businesses receive infected emails (Verizon, 2020).

Hacking

According to Mugari et al. (2016), hacking is a type of computer crime that has been around for millennia and involves gaining illegal access to databases and systems in order to obtain personal or corporate information. Hacking, as defined by Cyber Laws (2015), is the act of a cybercriminal altering a computer's hardware, software, or settings in order to accomplish an objective not intended by the device's original creator. Online thieves increasingly find it easier to steal from both individuals and organizations since it is so easy to access personal information. Hackers aim to gain a great deal of personal information by targeting a computer host with a large database. OK Zimbabwe, for instance, recently experienced a financial setback of $70,000 as a result of a hack into their Money Wave system. ZRP recorded 72 reported occurrences between the years 2011 and 2015, with 39 of those cases being banks. 2015's Sibanda 2.3 Facts and figures. The research that were conducted and published by some authors are listed under the empirical evidence. Case studies and surveys are generally included in these. Technology Revolution Gives Cybercrime a Boost: Cyber-attacks and Cyber security, A Singh and S Singh (2019). A research study on the technological revolution and rise in cybercrime was done by Singh et al. in 2019. The report referred to the current period as the "digital era," during which time technology is advancing more quickly than ever before each day. These technical advancements also foster crime, and with the aid of computers, criminality becomes cybercrime. This study's conclusion was that enterprises should take every precaution against cybercrime, including using firewalls, biometrics, updated software and hardware, anti-virus software, and firewalls, as well as more sophisticated tactics and technologies. One of the goals of the study was to highlight the problem of developing technology and how it relates to cybercrime.

2.1.4 The impacts of cybercrime

Financial Losses

According to Accenture (2019), financial institutions can sustain significant financial losses as a result of cybercrime. In 2019, financial services organizations incurred an average cost of $18.5 million due to cybercrime, up 11% from the previous year.

Reputational Damage

According to International Mo netary Fund (2018), financial organizations' reputations can be severely damaged by cybercrime. An IMF working paper from 2018 titled "The Impact of Cyber Attacks on Financial Markets" emphasizes how reputational harm from hacks can result in a decrease in client acquisition and retention.

Productivity loss

According to McAfee (2014), productivity loss is the loss of potential revenue that an organization experiences as a result of operational inefficiencies. Cybercrime can impact an organization's productivity, for instance, if a large amount of data is taken from the organization or if sensitive customer information is compromised. While they work to recover from the loss, an organization might have delays or snags in other productive areas.

IT Costs and Cost of Security

Information and technology are the extra expenses associated with protecting the business's operational environment and recouping from cyberattacks, according to McAfee (2014). The expenses of shielding the operational environment include purchasing updated systems and recognizing and controlling threats. Additionally, employing a cyber-security expert may incur expenses for the company.

2.1.5 The methods that can be employed to reduce effects of cybercrimes

Robust Cybersecurity Frameworks

According to Financial Stability Board (2018), to defend against cyber risks, financial institutions should set up and maintain strong cybersecurity frameworks with extensive rules, procedures, and controls. Access restrictions, network security, data encryption, incident response, and employee awareness training are a few topics that these frameworks ought to address.

Multi-factor Authentication (MFA

According to National Institute of Standards and Technology (NIST) (2017), using multi-factor authentication, which asks users to confirm their identity with numerous pieces of evidence, can greatly improve security. One-time passcodes, security tokens, biometrics, and passwords are a few examples of the various components that may be involved.

Continuous Threat Monitoring and Detection

According to Deloitte (2019), Advanced threat monitoring and detection systems that constantly scan networks, systems, and apps for any suspicious activity or signs of compromise should be implemented by financial institutions. This makes it possible to identify cyberthreats early on and to respond and mitigate them quickly.

2.2 Theoretical Literature

Cohen and Felson's routine activity theory had a major influence on this investigation. Other pertinent theories were taken into consideration, nevertheless.

2.2.1 Routine activity theory

Part of the classical school paradigm, the notion presupposes a rational offender. Lawrence Cohen and Felson created the theory of routine activity. The idea identified the elements of criminal activity. Felson (1998) delineated the elements of crime that necessitate combination, namely the motivated criminal, suitable targets, and absence of supervision.

This theoryt is based on the idea that a lot of crimes are done by persons who see opportunities to commit crimes whenever they go about their regular lives. The regular use of mobile and internet banking systems opens the door for criminal activity. The idea can be used to this research study since the banking industry's technical advancements have led to an increase in motivated offenders and an increase in cybercrime risk.

2.2.2 Fraud theory

The fraud hypothesis was put forth by Donald Cressey in 1953. He attempted to illustrate the theory with a triangle diagram that highlighted three requirements that had to be met in order for someone to conduct fraud. The components consist of

opportunity, pressure, and rationalization.According to Wells (2011), a person's viewpoint can drive them to commit fraud. Perceived pressure is represented by the element at the top of the triangle, while perceived opportunity and rationalization are represented by the two elements at the bottom (wells 20011 in Rasha and Andrew, 2012).

Perceived Pressure

This is the main factor that motivates people to commit crimes. According to Cressey, cited in Lilly (2015), fraud is seen to be committed by someone who has an unmet financial need that they are unable to satisfy through legal methods, leading them to participate in unlawful activity. According to Albrecht et al. (2006), a person's motivation is greatly influenced by how they perceive things. For example, if someone is having financial difficulties that they cannot resolve by legal means, they may contemplate turning to criminal means, like document forgery or theft, in order to get over their situation. Cybercriminals may act illegally because they are under pressure of some kind.

Perceived Opportunity

The methods used to commit crimes are described by perceived opportunity. According to Lilly (2015), opportunities are what allow someone to engage in fraudulent activity. Cybercrime is more likely to occur when there is less chance of being caught.

Perceived Rationalisation

This is the final component of the triangle, and it happens when the great majority of people commit a crime for the first time. According to Gwanyanya (2017), rationalization is a mentality that permits someone to consciously engage in criminal

behavior and justify their illegal conduct. For this reason, some cybercriminals conduct crimes while offering every excuse under the sun to justify their behavior.

2.3 Empirical evidence

Under the empirical evidence are the studies that were made by some authors and were published. These include mainly case studies and surveys.

2.3.1 Articles on the impacts of cybercrime on the performance of financial institutions

International Cyber Security Protection Alliance (ICSPA) (2014): Study of the Impact of Cybercrime on Business in Canada

The purpose of the study was to evaluate the incidence of cybercrime and its impact on Canadian corporate operations. The target group for the survey was the banking industry, aviation and shipping, telecommunications, and aerospace industries. Information was gathered through interviews and questionnaires. According to the study's findings, 69% of Canadian organizations reported having experienced cyberattacks. The most common types of attacks were discovered to be malware, phishing, and social engineering. These attacks have a significant effect that could result in reputational harm and financial loss. With the exception of the location and period of the investigation, this study's emphasis on the effects of cybercrime on Canadian firms is consistent with existing studies, and the researcher plans to focus on financial institutions in Harare.

Akinbowale et al, (2020). – Analysis of cybercrime effects on the banking sector

The purpose of the study was to investigate how cybercrime affects the banking industry. The balance score card was employed in the study. The results demonstrated that cybercrime is on the rise and that it is detrimental to banks and overall economic growth. In order to prevent cybercrime, the researcher suggested the following strategies: banks should create an alert system that can increase client awareness; they should also install and integrate big data technologies into their system.

Njeru and Gaitho (2019) - Investigating the extent to which cybercrime influences performance of commercial banks in Kenya.

The study's goal was to determine how much cybercrime affects Kenya's commercial banks' performance. The tier one bank in Kenya was the focus of the study because it has the greatest number of customers served. According to the study's findings, the majority of respondents believed that the cost of cybercrime insurance is having an impact on banks' performance, which in turn has an impact on how innovative they are. Banks reimburse victims whose information has been compromised with at least 2% of their earnings, and the reputational damage is severe. Numerous respondents said that frequent cyberattacks tended to harm the bank's reputation, which in turn had an impact on business operations. The study's findings prompted the researcher to investigate whether the banking industry in Zimbabwe experienced a similar situation.

Boating et al (2011) – Cybercrime and criminality in Ghana: its forms and Implications.

The study's main goals were to determine how common cybercrime is in Ghana and to look at its types and effects. The research employed a qualitative interviewing methodology to collect data, and 40 participants were chosen from the legal, financial, and IT sectors. The results of the investigation demonstrated that cybercrime is suddenly on the rise in Ghana and that the law enforcement does not have the necessary technical expertise to handle the issue. Furthermore, the cybercriminals possess the expertise and youth necessary to perpetrate cybercrime. According to study findings, a lot of cases remain unreported because people are afraid of looking foolish and don't trust the system.

2.3.2 Articles on the types of technological advancement in financial institutions

Jain N and Shrivastava V-International Journal of Computer application Issue 4, Volume 1 (2014) –Cybercrime changing everything; an empirical study.

This study looked at a broad overview of cybercrime, the motivations of those who commit it, and a detailed examination of different types of cybercrimes and uncommon situations that may come up throughout the prevention, detection, and investigation stages. The development of internet technology has increased the chances for cybercrime. The scope of computer crimes has expanded to include, among other things, software piracy, cyber extortion, and cyber laundering. Law enforcement officials are dissatisfied with lawmakers' inability to maintain cybercrime legislation

current with the rapidly evolving technology landscape. Legislators must simultaneously strike a balance between conflicting interests. This study has a connection to the one currently underway since it took into account the problem of the expansion of internet technology, which was the root of cybercrime.

Mugari et al. (2016) claim that cybercrime is becoming a bigger danger to Zimbabwe's financial services sector. With the speed at which technology is developing, the researchers looked into cybercrime in Zimbabwe's financial services sector. The poll was launched at four financial institutions in Harare to find out how often cybercrime is in these establishments. Purposive sampling and stratified random sample were both used in the research project. As the main study tools, questionnaires and interviews were used to collect data from a sample of respondents. The most frequent forms of cybercrime in banks, according to the report, are hacking, phishing, malware, and identity theft. The study's findings indicate that cybercrime is necessary as a result of technological improvement in financial institutions. The research also showed that cybercrime is common in underdeveloped nations, with Zimbabwe being one of them. The study recommended putting control mechanisms in place to combat cybercrime, including firewall installation, antivirus software updates, and training. The study's findings indicate that cybercrime poses a serious threat to the financial industry, and the problems will only become worse given how quickly technology is developing. This study is successful in identifying the prevalent cybercrimes in financial institutions. One of the researcher's goals is to achieve this.

Boating et al (2011) – Cybercrime and criminality in Ghana: its forms and implications.

The study's main goal was to investigate the incidence of cybercrime in Ghana and to look into its nature and effects. In order to collect data for the study, 40 respondents were chosen from the banking, IT, and law enforcement sectors. The results of the investigation demonstrated that cybercrime is suddenly on the rise in Ghana and that the law enforcement does not have the necessary technical expertise to address the issue. More so, the cybercriminals are youthful and proficient in their use of technology. According to the research findings, many cases are not reported because people don't trust the system or are afraid of looking foolish.(R Boateng, n.d.).

2.3.3 Articles on the types of cybercrime

The study conducted by Mugari, Gona, Maunga, and Chiyambiro (2016) aimed to determine the forms of cybercrime that are common in financial institutions and the efficacy of the present measures in place to combat cybercrime in these organizations. Respondents were chosen from four Harare-based commercial banks. According to their research, hacking was an issue in these banks, with 75% of respondents on average admitting that it happened where they worked. They also mentioned that some of the measures that had been implemented to reduce cybercrime included education and training through seminars and workshops, strict security, ongoing updates to technology, communication, and information, and the installation and upkeep of security measures like firewalls, anti-virus software, and firewall data recovery sites. According to Mugari (2016), who studied the efficacy of anti-fraud measures in the retail sector, hacking, identity theft, and dangerous software are the three main cybercrimes that affect the financial industry. On the list of tactics to reduce crime, control measures like firewalls, software updates, and training came in first.

According to Mugari et al. (2016), cybercrime is a growing threat to Zimbabwe's financial services industry. As technology advances rapidly, the researchers conducted a study on cybercrime in Zimbabwe's financial services industry. To investigate the prevalence of cybercrime in these institutions, the survey was piloted at 4 financial institutions in Harare. Purposive sampling and stratified random sample were both used in the research project. As the main study tools, questionnaires and interviews were used to collect data from a sample of respondents. The most frequent forms of cybercrime in banks, according to the report, are hacking, phishing, malware, and identity theft. The study's findings indicate that cybercrime is necessary as a result of technological improvement in financial institutions. The research also showed that cybercrime is common in underdeveloped nations, with Zimbabwe being one of them. The study recommended putting control mechanisms in place to combat cybercrime, including firewall installation, antivirus software updates, and training. The study's findings indicate that cybercrime poses a serious threat to the financial industry, and the problems will only become worse given how quickly technology is developing. This

study is successful in identifying the prevalent cybercrimes in financial institutions. One of the researcher's goals is to achieve this.

Chen E (2022), the evolving landscape of cybercrime: emerging threats and countermeasures. The study findings revealed that phishing, credit card skimming, malware and ransomware attacks are the frequent types of cybercrimes in financial institutions.

2.3.4 Articles on the policies that would lessen the impact of cybercrime

According to Mugari (2016) on the study of the effectiveness of anti-fraud measures in the retail sector he concluded that the types of cybercrimes that are prevalent in the financial sector are hacking, identity theft and malicious software. Control measures such as training, updating software's and firewalls topped up the list of strategies to curb crimes.

Pascal Pouani Tientcheu (2021), his study focused on security awareness strategies used in the prevention of cybercrimes. The participants included seven information security officers listed on social media who manage information security within organizations located in the northeast geographic region of the United States. The data were collected using semistructured interviews, The National Institute of Standards and Technology documentations and analyzed using thematic analysis. The study findings revealed that developing a cybersecurity culture within the organization and frequently training employees or end-users on how to prevent against cybercrimes are the types of policies that can be used to prevent cybercrimes.

Holt and Bossler (2014) , on the study of understanding cybercrime in real world policing and law enforcement. The study findings revealed that training to increase knowledge and provide standardised responses to reports of cybercrimes, as well as increased public engagement and signposting may help improve reporting rates and experiences. Increased knowledge about cybercrimes and those involved may also improve investigative preparedness and increased ability to empathize with victims and suspects to obtain better results at interview, generate more accurate and identy appropriate evidence.

2.4 Gap analysis

Empirical research on the impact of cybercrime on financial institutions' performance can be found in the literature. These research concentrated on cybercrimes that rise from local to international levels and are fueled by technology innovation. A study on the relationship between the rise in cybercrime and the technological development was carried out by Singh (2019). They found that as technology advances and becomes more sophisticated, the potential consequences of cybercrime are terrifying. For this reason, businesses need to employ every security measure at their disposal to thwart cybercriminals, such as firewalls, antivirus software, biometrics, and updated software versions. This study disregarded the issue of technology evolution and cybercrime in financial institutions, which becomes the researcher's area of focus and leaves a void for future research.

The study by Njeru and Gaitho (2019) looked at how much cybercrime affects commercial banks of Kenya. The results demonstrated that the majority of respondents believed that the cost of insurance against cybercrime affects banks overall profitability. There may be a research gap due to time and geographical factors.

The prevalence of cybercrime and its impact on businesses' operations were investigated in a study carried out by ICSPA Canada. According to this report, phishing was the most frequent attack, followed by malware and virus attacks. Because this study only examined the incidence of cybercrime in a broad business setting, it left a research gap; consequently, the researcher will focus exclusively on financial institutions in Harare.

2.5 Chapter summary

The chapter highlighted the literature review upon which the study was based. The scholar managed to point out some associated studies which were found to bear significance to the research in this chapter. The next chapter focuses on the research methodology used in the study.

CHAPTER 3
RESEARCH METHODOLOGY

3.0 INTRODUCTION

The chapter aims to describe the survey's methodology. The choice of Zimbabwe as the study's midpoint is justified by the researcher. This chapter discusses the population being studied, the sample population, sampling methods, research instruments used for data gathering, data display, and data collection protocols. The data will be collected by primary and secondary data using a hybrid methodology that combines qualitative and quantitative methods.

3.1 RESEARCH DESIGN AND JUSTIFICATION

The design offers a framework for the action plan and a road map for addressing the goals of the study. A research design, according to Mounton (2001), is a plan for conducting research. In order to provide a precise and understandable picture of how cybercrime affects financial institutions' performance, a descriptive survey research design was used in this investigation.J (2001)

William et al. (2013) define a descriptive research design as one that, in addition to documenting events, tabulates, exhibits, and describes data. The researcher was able to collect data by means of analysis, comparison, and measurement. The designs were advantageous to the researcher since they made use of both primary and secondary data. It was made possible by the idea to translate qualitative input into numerical instructions.

3.2 TARGET POPULATION

A target population, as defined by Wgener (2003), is a collection of people and things of interest from which a sample is drawn for study. In order to lay the groundwork for determining sample units and sample size, it was imperative to clarify the target population.Wegner (2003). The intended audience in Zimbabwe was the country's commercial banks. Three savings banks, twelve commercial banks, three building societies, and the Zimbabwe Republic Police made up the target population, totaling eighteen banks registered with RBZ bank clients. The target demographic was selected based on the complexity, high level of professionalism among the workforce, and usage of ICT systems; these establishments are also prime targets for cybercrime operations.

3.3 SAMPLING TECHNIQUES

According to Remenyi (1995), sampling is the process of choosing a small group of individuals to provide information from which generalizations about a broader group of people can be made. Sampling techniques are ways to choose parts of a particular group to represent the whole group. As a result, the researcher collected data using convenience and stratified sampling strategies.

STRATIFIED RANDOM SAMPLE

According to Kothari (2004), a population is separated into sub-populations, and a sample of objects is taken from each group. The sample is represented by stratified

random sampling in a population where the population is not homogeneous. As a result, it is possible to weight and connect the sampling results to provide accurate population estimates. This method was used by the researcher to acquire information from various departments inside the financial institutions in Zimbabwe, which served as a proxy for the strata. The stratified random technique enabled the use of additional research methods and processes to be applied in various subsets and offered appropriate data for studying a range of subgroups.(C.R, 2004)

CONVINIENCE SAMPLING

The goal of convenience sampling is to gather data from a population that is easily accessible to the researcher. The researcher chose people who are simple to get in touch with, including bank customers and police officers. The newly developed method, nonetheless, had a fairness flaw because some demographic segments will be over or underrepresented.

SAMPLE SIZE

The researcher collected a sample of 12 risk management personnel, 13 e-banking personnel, 12 from compliance department, 3 bank customers and 2 from cybercrime unit in the ZRP. The sample constituted 42 respondents.

3.4 RESEARCH INSTRUMENTS

Instruments, as defined by Leedy and Ormrod (2005), are appropriate means for acquiring data required to address research challenges. In order to thoroughly comprehend his study problem, the researcher will employ questionnaires and interviews as research instruments. These will enable him to obtain first-hand knowledge while also asking secondary data.(J.E, 2005)

QUESTIONNAIRES

In a questionnaire, each respondent was asked to provide an answer to the same set of questions, according to Sanders, Wright, and Horn (1997; 106) who characterize this method of data collection. The chosen participants received questions from the researcher in order to perform the study. Open ended and closed ended questions were used to categorize the surveys. Closed-ended questions contain options for responses

and topics that responders can select.(S.P Wright, 1997). According to Scandura and Williams (2000), the selected respondents were instructed to choose from a range of responses to the closed-ended questions. The range of replies gathered were wider because respondents were not restricted to providing their own words in response to open-ended inquiries.(Williams, 2000)

A standard questionnaire was created in order to provide answers to the questions that the study's objectives posed and to allow for comparable outcomes. Aside from being important for the analysis of the information obtained from the respondents, the questionnaire also included questions about educational attainment, gender, experience in the finance industry, the connection between ICT and cybercrime, and the various kinds of cybercrimes and how common they are in financial institutions.

ADVANTAGES

The survey helped to shape the information that was needed from responders.

The privacy of respondents, which encouraged honest responses, was guaranteed via questionnaires.

DISADVANTAGES

The researcher saw that questionnaires were costly as a result of transportation costs and other associated costs.

To overcome the above challenge, researcher focused heavily on data privacy in order to avoid being victimized by superiors. The researcher used online platforms in place of in-person interviews.

INTERVIEWS

According to Kotler (1999), an interaction between a researcher and respondents is referred to as an interview. To ensure fairness in the research, the information received from questionnaires and interviews was combined.(Phillip Kotler, n.d.)

ADVANTAGES

The researcher learnt that doing interviews was less expensive than using questionnaires.

The interviews provided the study with the option to request clarification when necessary.

Interviews archived a high response rate.

DISADVANTAGES

Some respondents were biased against cybercrime, thereby making comparative analysis difficult.

Some information that respondents considered confidential appeared to be difficult to collect owing to fear of being victimized by supervisors.

To overcome the above challenge, researcher focused heavily on data privacy in order to avoid being victimized by superiors. The researcher used online platforms in place of in-person interviews.

3.5 DATA COLLECTION PROCEDURES

They describe the steps the researcher took to control the study instruments and collect information from respondents. To make sure that all questions were completed, the researcher would regularly check in with the chosen respondents. This was accomplished through phone calls. Before conducting interviews, a comprehensive set of study questions was compiled into an interview guide. The researcher also made phone appointments with management for a few weeks before to the interview date. Copies of the interview guidelines were also supplied to the compliance department, IT and risk manager. In order to make sure the guidelines reached the intended recipients, a phone call was made in addition to the email correspondence.

Demographics was used to analyse that was gathered in chapter IV. To respond and assess each goal graphs, tables, pie charts and statement based on percentages were used.

3.6 DATA ANALYSIS AND PRESENTATION

Large volumes of data was made intelligible after the data collection procedure. The gathered data was analyzed using both qualitative and quantitative methods.

QUANTITATIVE DATA

To illustrate quantitative data, a combination of tables and graphs was employed. The researcher was able to combine obtained data into tables through presentations. To further facilitate comparison and comprehension, some of the data was quantified in percentages to represent the proportion of respondents.

QUALITATIVE DATA

The researcher used summative content analysis to infer qualitative data such that it has meaning. The information gathered was utilized to formulate verbal conclusions. The employment of a qualitative technique supplemented the use of quantitative data.

3.7 DATA VALIDITY AND RELIABILITY

The precision of the interpretation's value is referred to as validity. According to Campbell (1979), validity is the degree to which a data gathering process accurately measures the target outcome. The stability of measure, or the degree of consistency of a measuring tool that produces consistent results for the same person every time it is used, is referred to as reliability. Internal consistency was utilized to assess the instruments' dependability in order to guarantee their reliability. When multiple questions in a questionnaire require the same response, this is referred to as internal consistency, and it is used to verify that respondents are providing accurate information. The respondents were asked the same questions in several wordings in order to verify reliability.

By using a pilot test, the researcher aimed to improve validity and reliability. Pilot testing is essentially the process of testing a key informant interview guide, observation form, or survey on a small sample of people to see if it will function as intended in the real world. To ensure that all members of the sample comprehended the questions and interpreted them in the same way, pilot testing was helpful. It was inevitable that as the pilot questionnaires were completed and reviewed, a few unexpected issues would come to light. These issues could range from small ones like question number duplication to more serious ones like misinterpreted question wording that called for new questions, response options, or wording changes.

3.8 ETHICAL CONSIDERATIONS

The researcher additionally considered ethical considerations when performing the study to guarantee the efficacy of the research methodology and the privacy of the data gathered. Furthermore, the names of the respondents did not need to be known at any stage of the study.

SUMMARY

The study instrument, data collection methods, and research design were all described in this chapter. The analysis and display of data is the subject of the following chapter.

CHAPTER 4
DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 INTRODUCTION

This chapter focuses on presenting the data that has been acquired, analyzing it, and then having a debate. Tables are used to present the data. The data presentation was predicated on how cybercrime affected the operations of financial firms with headquarters in Harare.

4.1 RESPONSE RATE

Jack and Fincham (2019) define response rate as the quantity of questionnaires obtained from respondents from total questionnaires that were administered. The

response rate should be around 60% of the questionnaires administered (Jack and Fincham, 2019).

4.2 Response rate for questionnaire

Table 1

Respondents	Questionnaires issued	Questionnaire returned	Responde rate
Commercial banks	15	14	93%
Building society	13	13	100%
Savings Banks	11	10	91%
ZRP	3	3	100%
Bank customers	2	2	100%
Totals	44	42	95%

Source: Primary Data

Table 1 displays the 44-question administered questionnaire response rate, with 2 of the questions being non-response. This was due to the fact that 42 people responded to the questionnaires because they were spoiled. Consequently, this indicates that 95% of respondents responded. The researcher who collected the data with diligence was recognized with a 95% response rate. After effective follow-ups, the intended respondents completed the questionnaires before they were collected. A 95% response rate indicates the validity of the data.

4.3 Response rate for interviews

Table 2

Interviews	Issued	Success	Failure
Respondents	11	9	2
Percentage	100%	82%	18%

Source: Primary data

From table 2 above, the aim was to interview 11 respondents, unfortunately, only 9 respondents were interviewed. This then meant that 82% was success rate for

conducted interviews while, a failure of 18% was recorded. 2 respondents failed to show up for interview due to that, one of them attended emergence, meeting on the day of interviews, the other one did not provide a reason for failing to attend the interview. The data that was gathered through interviews was used to complement the data that was gathered from questionnaires.

4.1.2 Demographic information of respondents

Table 3

Variable	Description	Frequency	Response rate
Gender	Male	25	60%
	Female	17	40%
	Total	42	100%
Age range	21-30years	10	24%
	31-40years	16	38%
	41-50 years	10	24%
	Above 51 years	6	14%
	Total	42	100%

Educational level	Professional course	9	21%
	First degree	16	38%
	Post graduate degree	11	27%
	Other qualification	6	14%
	Total	42	100%
Employment position	Senior management	10	24%
	Middle management	24	57%
	Other positions	8	19%
	Total	42	100%

Gender

The gender distribution of study participants is shown in Figure 2. With participation rates of 60% and 40%, respectively, the data indicates that men engaged at a higher rate than women. According to data, men predominate in the banking sector. This observation aided the researcher in identifying trends that might be related to the rise in cybercrimes.

Age range

Source: Primary

Table 3 shows that 24% of respondents were between the ages of 21 and 30; 24% were between the ages of 41 and 50; and 14% were over the age of 51. With a response rate of 38%, the data shows that the bulk of respondents were between the ages of 31 and 40, with a smaller age group being between the ages of 51 and above. According to this review, people in a sufficiently mature age range should be knowledgeable about the topic being studied because they are involved in all facts of it.

Educational Level

Table 3 shows that (21%) of employees have completed a professional course, (38%) have completed a first degree, (27%) have completed a postgraduate degree, and (14%) have completed additional qualifications. This indicates that a substantial percentage of the chosen respondents were literate, which makes their answers to the questions trustworthy and relevant.

Employment position

Source primary data

Table 3 lists the employment positions of the selected study participants. Three other kinds of respondents were identified: senior management, middle management, and other roles. According to the table, middle management accounted for 57% of the respondents, senior management for 24%, and other roles for 19% of the respondents. The bulk of responders were middle management since they possessed the information that the researcher needed to know, according to the findings.

4.4 Types of technological advancements in financial institutions

Table 4

statements	SD	D	A	SA	TOTAL
Automated Teller Machine	0	8%	25%	67%	100%
Electronic Banking	0	12%	22%	66%	100%
Biometric authentication	0	52%	26%	22%	100%

Key

SD	D	A	SA
Strongly disagree	disagree	agree	Strongly agree

Source: Primary

From table 4 above, the researcher found out that the most prevalent type of technological advancement in financial institutions was Automated Teller Machine with a response rate of 67% , followed by Electronic Banking with 66% response rate. Biometric Authentification was considered to be low with a response rate of 22%.

Automated Teller Machine

According to the information collected by the researcher regarding the types of technological advancement in the financial sector , a total of 92% of the respondants agreed that automated teller machine is the type of technological advancement that is most prevalent in financial institutions. From the interviw responses it clearly shows that automated teller machine is the type of technological advancement that most banks in Zimbabwe have adopted to because it has the highest response rate of 92%. The responders who were interviewed went on to detail the advancements in technology from 2015 onward. In 2015, the nation's automated teller machines (ATMs) saw very little use, and banking was limited to banking halls. The results of a study conducted by Singh et al. (2019) were related to the findings, which showed that technology in the banking industry is still changing and will continue to evolve.

Electronic Banking

From table 4 above, majority of respondents (88%) in total considered electronic banking to be among the type of technological advancement that many banks have adopted . From the interview responses, it clearly shows that electronic banking is among the types of technological advancement that are being used by the banks because it has a high response rate of 88%. The findings were similar with the research conducted by Haider Basil Ali (2023), It was discovered that there is a high degree of adoption of electronic management in the banking industry in a case study that was conducted on Babel Bank in Iraq, where the mean value was 4.163 also the standard deviation was 0.735.

Biometric authentication

From table 4 above, majority of respondents (52%) disagreed that biometric authentication is among the type of technological advancement that banks have adopted

. According to the interview responses, it clearly shows that biometric authentication is not among the types of technological advancement that are being adopted by banks because it has response rate of 52%. The findings were different from the research conducted by Stuart Dobbie (2020), It was discovered that biometric authentication has become widely used for payment authorisation and verification across a range of banking activities, in a case study that was conducted on Barclays, HSBC and Santander banks.

4.5 Types of cybercrimes in financial institutions and their prevelance

Table 5

statements	SD	D	A	SA	TOTAL
Hacking	0	16%	24%	60%	100%
Identity theft	0	12%	38%	50%	100%
Electronic card fraud	0	9%	24%	67%	100%
phishing	0	5%	43%	52%	100%
Malware	0				

attacks		12%	48%	40%	100%

Source: Primary

The survey results shown in Table 5 seem to support the notion that financial institutions in Zimbabwe are concerned about cybercrime. The highest percentage of respondents (67%), who thought that electronic card fraud was common in financial institutions, followed by hacking (65%), identity theft (50%) and phishing (52%). Malware attacks were deemed to be the least common, with 40% of respondents believing that they were not common in the financial sector.

Hacking

84% (in total) of respondents, or the majority, classified hacking as a cybercrime with a high occurrence rate. According to the interviewees' answers, hacking is the most prevalent kind of cybercrime in Zimbabwe's financial institutions. The results aligned with a 2016 study by Mugari et al. that noted hacking as a significant issue for financial institutions. Additionally, research conducted in 2010 and 2014 by Siddique and Rehman and Raghavan and Parthiban recognized hacking as the most prevalent cybercrime in financial institutions. Because of their nature and the services they offer, financial institutions have a wealth of client data at their disposal. Because hackers desire to obtain client information, this has made financial institutions targets for their attacks.

Identity theft

The findings showed that identity theft is one of the concerning forms of cybercrime in institutions, with 88% of respondents citing its rather high incidence. Identity theft is one of the most common types of cybercrimes at financial institutions, as seen from the interviewees' answers. The results are consistent with the study carried out by Mugari et al. (2016), who found that identity theft had an average occurrence rate and came in second place. Akinbowale et al.'s 2020 study also shown identity theft to be a growing issue in financial institutions. It is important to remember that identity theft has been shown to be the primary cybercrime in financial institutions. This is because the primary goal of the criminal is to obtain specific customer information that they can use to commit additional crimes.

Electronic Card Fraud

According to table 5 above, 91% of respondents in total thought that electronic card fraud was a possibility. is the most prevalent; nevertheless, 9% of the respondents felt that it is not. It is evident from the interview responses that there is a serious risk of electronic card fraud in addition to other concerns. Some respondents countered that as more people are using plastic money, card fraud is still on the rise and is predicted to do so in the future. According to a 2019 study by Njeru and Gaitho, identity theft is the primary cause of card fraud, a prevalent cybercrime in organizations.

Phishing

Table 5 above demonstrates that 95% (in total) of respondents thought that phishing had a high frequency of occurrence. Because phishing has the highest response rate of 95%, it is evident from the interview results that it is the most common form of cybercrime. The results aligned with the research conducted by Mugari et al. (2016), which similarly revealed that phishing was common in Zimbabwe's financial institutions. The study's findings concurred with one by Wada & Odulaja (2012), who listed phishing as one of the primary threats to organizations.

Malware attacks

The majority of respondents of 88% (in total)thought that the prevalence rate of malware assaults was high. It is also reasonable to conclude from the interviewees' comments that malware assaults frequently occur in Zimbabwean financial institutions. The study's findings are consistent with those of a 2014 study conducted by Europol, which identified malware assaults as one of the primary risks to private information held by individuals and organizations in the financial sector.

4.6 Impacts of cybercrime on financial institution

Table 6

statements	SD	D	A	SA	TOTAL
Reputational loss	0 -	17%	33%	50%	100%
Other losses	0 -	57%	31%	12%	100%
Direct financial loss	0 -	19%	29%	52%	100%

Productivity loss	0 -	24%	36%	40%	100%

Source: Primary Data

According to table 6, 81% of respondents indicated they had directly lost money as a result of insurance costs and electronic fraud incidents, 76% of respondents said they had lost productivity, and 12% said they had suffered other minor losses like regulatory or compliance issues. Additionally, 83% of respondents said that cybercrime had negatively impacted their reputation. Phishing, malware, and virus attacks were shown to be responsible for both financial loss and damage to one's reputation, according to an ICSPA (2014) study.

Reputational loss

Table 6 shows that a total of 83% of respondents stated that cybercrime damages financial institutions' reputations in Zimbabwe. Wall (2007) believed that a corporation may experience harm to its reputation as a result of hacking. Clients may come to distrust these financial institutions, particularly when transacting online. Similar research findings were found by Njeru and Gaitho (2019), who found that persistent cyberattacks on an organization have a tendency to negatively impact customers' perceptions of the organization, which in turn disrupts overall business performance.

Direct financial loss

According to the results, 81% (in total) of the respondents agreed that financial loss has the most influence on financial institutions. It is evident from the interview responses that nearly all of the respondents from the chosen institutions mentioned that they had once suffered financial loss as a result of cybercrime. Similar findings were reported in a 2011 study by the Global Economic Crime Survey, which demonstrated the disastrous effects of cash loss on an organization's performance. According to some of the respondents surveyed, financial loss has an impact on financial institutions' ability to be innovative, which can directly damage the institutions' overall performance. Some respondents expressed regret over the fact that cybercrime incidents are concealed from the public to prevent consumers and investors from becoming worried by the insecurity or to preserve their brand.

Productivity loss

Additionally, 76% (in total) of respondents said that one of the main effects of cybercrime is a loss of productivity. Similar findings were found in a research study

conducted by Dzomira (2014), where the majority of respondents focused on the influence that cybercrime in financial institutions has on productivity loss.

Interview Responses

The researcher interviewed respondents concerning the impacts of cybercrimes. According to the respondents reputational loss is one of the impacts of cybercrime because cybercrime such as hacking can result in a decrease in acquisitin and retention.

Respondents also mentioned that direct financial loss as another impact of cybercrimes on financial institutions because cybercrimes such as electronic card fraud results of financial losses.

According to the respondents productivity loss is another impact of cybercrimes. This is because if sensitive information about customers is taken from the organization and they work on recovering the loss an organization might have delays in other productive areas resulting in productivity loss.

4.7 Policies to lessen cybercrime in financial institutions

Table 7

Statements	SD	D	A	SA	TOTAL
Invest in new technology	0 -	19%	29%	52%	100%
Awareness improvement	0 -	12%	40%	48%	100%
Cybercriminal law	0 -	17%	29%	55%	100%
Cybersecurity department	0 -	14%	29%	57%	100%

Table 7 shows that, in order to combat cybercrime, financial institutions must invest in new technology, according to a total of 81% of respondents. Financial institutions can now, however, replicate with the rapidly advancing technology. The answers from the interviews make it quite evident that purchasing new technology is a successful strategy for thwarting cybercrime. This approach aligned with a study by Singh and Singh (2019), which suggested that in order to protect themselves from cybercrime, organizations should work to obtain new technologies such as updated antivirus software, biometrics, and software updates, among others.

Figure 8 shows that a total of 88% of respondents felt that awareness needs to be raised. However, several respondents countered that awareness efforts help people understand cybercrime, particularly for consumers who may fall victim to such schemes. Additionally, several respondents believed that since ignorance has been linked to some cybercrime instances, financial institution staff members had to regularly obtain cybersecurity training. The interviewees' comments unequivocally demonstrate that raising awareness is a useful strategy for lowering the incidence of cybercrime. According to Frank et al. (2013), one of the drawbacks of combating cybercrime is that there is a dearth of awareness and training regarding how to handle the increasing demands and incidents related to cyber security.

Based on the data presented in Table 7, a total of 84% of the participants expressed the opinion that effective legislation addressing cybercrime is necessary. Effective cybercrime regulations are necessary, according to other respondents, because Zimbabwe's current laws are insufficient and ineffective in preventing cybercrime. The belief held by 50% of the interviewees that the current laws are insufficient provided support for this. According to Susan W. Brenner (2012), coordinated legislative frameworks across countries are necessary to combat cybercrime and emphasize the importance of international cooperation.

4.8 Chapter Summary

The chapter looked on the presentation and analysis of data that was gathered from primary sources. The data was presented using tables. Relevant discussions were made. Chapter 5 will focus on the summary, conclusion and recommendations.

CHAPTER 5
CONCLUSIONS AND RECOMMENTATIONS

5.0 Introduction

The findings, recommendations, and conclusions are the main topics of this chapter. The purpose of the study was to examine how cybercrime affects financial organizations' performance. The forms of technological advancement in financial institutions, the types of cybercrimes, regulations that would minimize the impact of cybercrime, and the effects of cybercrime on the performance of financial institutions served as the research objectives that drove the study's conclusions.

5.1 Summary of major research findings

- To identify the types of technological advancement in financial institutions in Zimbabwe
- To identify the different kinds of cybercrimes that are common in Zimbabwe
- To determine the impacts of cybercrime on the performance of financial institutions in Zimbabwe
- To recommend policies that would lessen the impact of cybercrimes in Zimbabwe.

Types of echnological advancement

From the information collected by the researcher it clearly shows that the types of technological advancement that are prevalent in the banking sector includes automated teller machine, electronic banking and biometric auntentication. Automated teller machine and electronic banking were considered to be the most prevalent types of technological advancement that are being used by banks and biometric authentication was considered not commonly used.

Types of cybercrime

According to research findings, identity theft, phishing, malware attacks, hacking, and electronic card fraud are only a few of the cybercrimes that are common in financial institutions. Malware attacks were thought to be the least common, while hacking and identity theft were among the most common cybercrimes. Electronic card fraud and phishing were thought to be rather common.

Impacts of cybercrime

Research findings revealed that, the impacts of cybercrimes includes reputational loss, direct financial loss, productivity loss and other losses. The majority agreed that reputational loss is the major impact of cybercrime in financial institutions with a response rate of 81% in total , followed by direct financial loss and productivity loss.

Strategies to reduce cybercrime

From the research survey, respondents recommended the following strategies so as to reduce the impacts of cybercrime in financial institutions; Financial institutions should invest in new technology in fight against cybercrime. There is need to improve

awareness campaigns and education to both customers and employees Financial institutions should have fully functional cyber security department and reduce budget constraints. There is need for an effective cybercriminal law to be in place.

Conclusion

Based on the findings, the advancemennt of technology in the banking sector brought about improvements in banking services, but it was coupled with its own dark side. As technological advancement was progressing in the banking sector, cybercrime was also following behind. Technological advancement plays a pivotal role in fuelling cybercrimes, the advancement of computer and internet technology is the commonly used modus operandi by cyber criminals to swindle money from victims. Cybercrime being prevalent, with hacking, identity theft, electronic card fraud and phishing as the common prevalent cyber threats. From the research findings, it can be deduced that Cybercrime have a negative impact on the performance of financial institutions in Zimbabwe as it cause financial and non- financial impacts. Control measures such as investing in new technology, awareness campaigns, having a cyber-security department which covers updating of anti-viruses and security measures, were the considered strategies to curb cybercrime. In spite of the existence of these measures to protect financial institutions from being victims, keeping their security systems up to date is challenging, as it is being outperformed by the fast variations in technology.

Recommendations

Below are the recommendations made by the researcher;

- Financial service providers should ought to use protected verification that is not vulnerable to web spoofing
- Bank and law enforcers should be development of laws that regulates the usage of and electronic banking system in Zimbabwe.
- Constant educational programs to be steered to aware the handlers and bank employees on how to always ensure secure online transactions.
- Financial institutions should renovation and conserve all decamped technologies in time to prevent systemic error and malfunctioning of systems
- Financial institutions should always upgrade their system on regular basis to catch up with technological advancement.

If the mentioned recommendations are implemented, the preventive approaches

implementation may advance from effective to a much more effective.

REFERENCES

Ajani, E. F. G. (2016). The impact of cybercrimes on global trade and commerce. International Journal of Information Security and Cybercrime (IJISC), 5(2), 31-50.

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020), "Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature", Journal of Financial Crime, Vol. 27 No. 3, pp. 945-958.

Amedu. (2005). Domestic electronic payment in Nigeria: The challenges.

Arcand, M., PromTep, S., Brun, I., & Rajaobelina, L. (2017). Mobile banking service quality and customer relationships. International Journal of Bank Marketing.

Association of Certified Fraud Examiners, (2009). Report to the Nation on Occupational Fraud and Abuse Study.

Arcand, M., PromTep, S., Brun, I., & Rajaobelina, L. (2017). Mobile banking service

quality and customer relationships. International Journal of Bank Marketing.
Aysan, M. A. M. (2014). Implementation of electronic fund transfer using new symmetric key algorithm based on simple logarithm. International Journal of Advanced Research in IT and Engineering, 3(4), 10-16.Central bank of Nigeria. Banking Act Chapter 24:24
Baxter, L. A., & Babbie, E. R. (2003). The basics of communication research. Cengage Learning.
Binuyo, A. O., & Aregbeshola, R. A. (2014). The impact of information and communication technology (ICT) on commercial bank performance: evidence from South Africa. Problems and perspectives in management, (12, Iss. 3), 59-68.
Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management.
Burns, P., & Stanley, A. (2002). Fraud management in the credit card industry. Federal Reserve Bank of Philla Payment Cards Center Discussion Paper, (02-05).
Ciciretti, R., Hasan, I. & Zazzara, C. (2008). Do internet Activities Add Value? Evidence from the Traditional Banks. Journal of Financial Services Research, 22, 95118.
Cisco, (2017). Annual Cybercrime Report.
Cooper .R .D and Schindler .P.S., (2003). Business Research Methods, 8th Edition, McGraw-Hill, New York.
Chang, J.S. (2008), An analysis of advance fee fraud on the internet. Journal of Financial Crime, Vol.15 No. 1. pp. 71-81.
Chang, H., & Abdul Hamid, M. (2010). An empirical investigation of internet banking in Taiwan. Global Journal of Business Research, 4(2), 39–47.
Cloward, R. A. (1959). Illegitimate means, anomie, and deviant behavior. American sociological review, 164-176.
Cyber warfare report of 2019.
Daniel, E. (1999). Provision of E-Bankink in the UK and Ireland. International Journal of Bank Marketing. UBS London.
Deitel,H, Deitel, P. Steinbuhler , K. (2001). Wireless internet and mobile business. Nova Southeastern University. Boston College.
Dew, K. (2012). Innovation Segregation by Two Australian Merchant Banks: A Private Alternative to the Financial Patent for Protecting Financial Innovations and

Informing Investors. Working Paper, available at http://ssrn.com/abstract=995960, accessed on 22 September 2021

Dube, T., Chitura, T. and Runyowa, L. (2009). Adoption and use of Internet Banking in Zimbabwe: An Exploratory Study, Journal of Internet Banking and Commerce, Vol. 14 No.1, pp. 1-13

Essinger, J. (1999). The virtual banking revolution: the customer, the bank and the future. International Thomson Business Press.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. Police research series, paper, 98(1-36), 10.

Frank, I., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. International Journal of Cognitive Research in science, engineering and education, 1(1), 100-110.

Gono, G. (2012), Monetary Policy Statement issued in terms of the Reserve Bank of Zimbbawe Act Chapter 22:15, Section 46

Goodman, M. (2011). International dimensions of cybercrime. In Cybercrimes: A multidisciplinary analysis (pp. 311-339). Springer, Berlin, Heidelberg.

Hancock, D. R., Algozzine, B., & Lim, J. H. (2021). Doing case study research: A practical guide for beginning researchers.

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. Computer Law & Security Review, 25(6), 528-535.

Hutcchings. A. & Hayes, H. (2009) Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the „Net"? Current Issues in Criminal Justice Volume 20 Number 3.

Jayawardhena, C. & Foley, P. (2000). Changes in the banking sector-the case of internet banking in the UK. Internet Research: Electronic Networking Applications and Policy, 10(1), 19-30.

Kabanda, (2012). The Essence of Cyber Security. http://www.theindependent.co.zw. Assessed on 21.11.21.

Kadleck C. (2005), Banks battle against growth of electronic payment fraud. Crain"s Cleveland Business 26. No.3, http://www.craincleveland.com.

Jaishankar, K. (2008). Space Transition Theory of cybercrimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet. (pp.283301) Upper Saddle River, NJ: Prentice Hall.

Karjaluoto, H., Mattila, M. & Pento, T. (2012). Factors underlying attitude formation

towards online banking in Finland. The International Journal of Bank Marketing, 20, 261-273.
Keys, W. (2008). Submission To The Department Of Broadband, Communications And The Digital Economy. In Respect Of The Abc And Sbs: Towards A Digital Future.
Kotler, P. (1999). Marketing in the network economy. Journal of marketing, 63(4_suppl1), 146-163.
Kothari, C. R. (2004). Research methodology: Methods and techniques. New Age International.
Koong, Liu and Wei. (2006). An Examination of Internet Fraud Occurrences. Research Gate.
Koops, B. J., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime. Datenschutz und Datensicherheit-DuD, 30(9), 553-556.
KPMG (2011). Cyber Crime – A Growing Challenge for Governments July 2011, Volume.
Leedy, P. D., & Ormrod, J. E. (2005). Practical research (Vol. 108). Saddle River, NJ, USA: Pearson Custom.
KLevin, A., & Ilkina, D. (2013). International comparison of cybercrime. Privacy and Cyber Crime Institute, Ted Rogers School of Management, Ryerson University
Krone, T. (2005). Hacking Motives: High Tech Crime Brief.
Moyo, M., & Christoph Stork, D. (2012). Understanding what is happening in ICT in South Africa: A supply-and demand-side analysis of the ICT sector.
Mounton, J. (2001). How to succeed in your masters and doctoral studies. Van Schaik, 166.
Mugari, I. (2017). Cyberspace enhanced payment systems in the Zimbabwean retail sector: opportunities and threats. International Journal of Economics and Financial Issues, 7(3), 760-767.
Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime-the emerging threat to the financial services sector in Zimbabwe. Mediterranean Journal of Social Sciences, 7(3 S1), 135.
McAfee, (2017). Report on the Global Cost of cybercrime.
McQuade, Samuel.(2008) “Cybercrime.” In The Oxford Handbook of Crime and Public Policy, by Michael Tonry. Oxford: Oxford University Press, 2011.
National Payment System Act Chapter 24:23

Nwaolisa, E. F., & Kasie, E. G. (2012). Electronic retail payment systems: User acceptability and payment problems in Nigeria. Arabian Journal of Business and Management Review (OMAN Chapter) Vol, 1(9).
Panel, F. A. (2009). Cyber crime: social networking and virtual worlds.
Piquero, A. R., & Tibbets, S. G. (2001). Rational choice and criminal behavior: Recent research and future challenges. Routledge.
Postal and Telecommunication Regulatory Authority of Zimbabwe. (2020).
PMG (2012), Cybercrimes: A financial sector overview, www.kpmg.com/in. accessed on 29/03/24
RBZ (2017). Quarterly Annual Report 31 December 2017.
Reserve Bank of Zimbabwe Banking Regulation Policy No.1-2017/BDS on Corporate Governance. RBZ Publications, Harare.
Rust, R. and Lemon, K. (2001). E- Service and the Consumer. International; Journal of Electronic Commerce.
Sandywell, B. (2010). On the globalisation of crime: the Internet and new criminality (pp. 38-66).
Sanders, W. L., Wright, S. P., & Horn, S. P. (1997). Teacher and classroom context effects on student achievement: Implications for teacher evaluation. Journal of personnel evaluation in education, 11(1), 57-67.
Saunders, M., 2005.Research Methods for Business Studies, 3rd Edition, Pearson Education, New Delhi.
Saunders, M. and Lewis, P. and Thornhill, A. (2007) Research Methods for Business Students. 4th Edition. Essex, England : Prentice Hall.
Scandura, T. A., & Williams, E. A. (2000). Research methodology in management: Current practices, trends, and implications for future research. Academy of Management journal, 43(6), 1248-1264.
Sherman, L. W., & Eck, J. E. (2003). Policing for crime prevention. In Evidence-based crime prevention (pp. 309-343). Routledge.
Shiels, H., McIvor, R., & O'Reilly, D. (2013). Understanding the implications of ICT adoption: insights from SMEs. Logistics Information Management, 16(5), 312-326
Shinder, D.L. (2002), Scene of the Cybercrime. Computer Forensics Handbook, Syngress Publishing.
Shuabi A. (2010). Role of Electronic Banking in Indian Economy. UP Technical University.

Tahiru, A. (2017). Cyber Security in Africa: The Threats and Challenges!. Cyberpolitik Journal, 3(5), 91-104.

The Zimbabwe National Risk Assessment Report of 2015.

Ollmann, G. (2007). The vishing guide. IBM Global Technology Services.

Okiro, K. (2013). The Impact of Mobile and Internet Banking On Financial Performance Of Financial Intitutions in Kenya. European Scientific Journal.

Usman, A.K. and Shah M.H. (2013), Critical Success Factors for Preventing e-Banking Fraud. Journal of Internet Banking and Commerce, Vol. 18 No. 2.

US-CERT, A. (2006). Government Organization,". Using Wireless Technology Securely, 1-9.

Wall, D. (2007). Cybercrimes and the Internet. Crime and the Internet.

Wada, F., & Odulaja, G. O. (2012). Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories. African Journal of Computing & ICT, 5, 69-82.

Wegner (2003). Applied Business Statistics, (4th Edition), University Cape Town Press.

Yar M, (2005). „The novelty of "cybercrime": An assessment in light of routine activity theory". European Journal of Criminology, Vol 2 (4) pp 407-427.

Verizon North, L. C. (2020). Federal Communications Commission. Proceeding Number, 19, 354.

Yibin, M. (2003). E- Banking, Trends, Challenges and Policy Implications. Research Journal Vol 5- issue 6.

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2013). Business research methods. Cengage learning.

Zimbabwe Republic Police, Cybercrime Unit 2019

Zimbabwe Republic Police Cybercrime Unit, 2020.

APPENDIX

My name is Vanessa R. Ngwenya a fourth year student at Bindura University of Science Education pursuing a Bachelor"s of commerce honours Degree in Financial intelligence. I have created this questionnaire to obtain information for a research study in partial fulfillment for the BCOMF.I degree.

I kindly request for your participation in this research study on the topic entitled "**THE IMPACT OF CYBERCRIME ON THE PERFOMANCE OF FINANCIAL INSTITUTIONS IN ZIMBABWE. A SURVEY OF BANKS IN HARARE CENTRAL BUSINESS DISTRICT**" The main objective of this research study is to analyse the impact of cybercrime on the performance of financial institutions. The study also attempts to identify types of cybercrime prevalent in Zimbabwe. The researcher assures you that all the information provided will only be used for scholary research purpose only and will be treated with confidentiality therefore, please feel free to express your true and honest opinions on the issue raised. Your assistance will be greatly appreciated

SECTION A

QUESTIONNAIRE GUIDE

Read each question carefully and tick or fill in your response in the space provided to each question below,

1. Gender

   Male ( )

   Female ( )

2. Indicate your age gap?

20-30 years ( )

30-40 years ( )

40-50 years ( )

Above 50 years ( )

3. How long have you been working at that institution?

Less than 5years ( )

6-10years ( )

11-15years ( )

16-20years ( )

4. Which department do you specialize in?

Human Resource ( )

Internal Audit ( )

Risk Management ( )

Security and Fraud ( )

Finance ( )

5. Has there been any advances in technology at the institution?

Yes ( )

Not sure ( )

No ( )

If yes what are the improvements?

.....……

6. What are the technological advancement used in your organization.

Automated Teller Machine ( )

Electronic Banking ( )

Biometric Authentication ( )

7. Have there been any instances of cybercrimes at your organization?

Yes ( )

No ( )

8. If yes what was the type of cybercrime from the following?

Hacking ( )

Electronic fraud ( )

Identity theft ( )

Malware attacks ( )

Phishing ( )

9. What are the impacts of cybercrime on the performance of banks?

……

……

……

……

10. What strategies can be put in place to combat cybercrime?

……

……

……

……

……

……

SECTION B

INTERVIEW GUIDE

1. What are the technological advancement that are used in your organization?
2. What do you think are the causes of cybercrimes at your organization?
3. What are the types of cybercrimes that the organization suffered before?
4. What are the impacts of cybercrime on the perfomance of the organization?
5. What strategies/policies can be put in place in order to combat cybercrime?