BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

CHALLENGES OF CYBERCRIME IN THE FINANCIAL SECTOR. A CASE STUDY OF STEWARD BANK LIMITED FROM 2020-2021.

BY

CHELSEA NOLLIET CHIMBWANDA

B192321B

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

JUNE 2023

APPROVAL FORM

Title of Dissertation: Challenges of cybercrime in the financial sector. A Case study of Steward Bank Limited from 2020 - 2021.

To be completed by student

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

Signature of student …..……. Date …..…….

To be completed by supervisor

This dissertation is suitable for submission to faculty.

Signature of supervisor …….. Date ……..

To be completed by the chair of the department

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

Signature of chairperson……. Date…….

RELEASE FORM

Name of author: Chelsea Nolliet Chimbwanda

Dissertation title: Challenges of Cybercrime in the financial sector. A case study of Steward Bank Limited from 2020- 2021.

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

Year granted: 2023

Bindura University is thereby granted permission to produce single copies of this dissertation and to lend or sell such copies for private, scholarly or scientific purposes only.

The author reserves publication rights and neither the dissertation nor extensive extracts from it may be printed or otherwise reproduced without the author's written permission.

Signed……

Address: 4 Fambayi Crescent

Chitungwiza, Zengeza 3

Harare, Zimbabwe

DEDICATION

I dedicate this research project to God Almighty, the source of all wisdom and knowledge. As I embarked on this journey, I was reminded of the words in Philippians 1:6 which say, "And I am sure of this, that he who began a good work in you will bring it to completion at the day of Jesus Christ." I acknowledge that it is only through God's guidance and grace that I have been able to complete this project. I am grateful for His unwavering love, faithfulness, and provision throughout the entire process. God's hand has been evident in every stage of this research project, and my heart is filled with gratitude for His divine intervention.

ABSTRACT

The increased use of technology in the financial sector has led to an increase in cybercrime, which has become a significant threat to financial institutions and their customers. The cost of cybercrime to the global economy has been estimated to be in the trillions of dollars. Therefore, this study was conducted to assess the challenges of cybercrime in the financial sector and a case study of Steward Bank Limited was chosen. The purpose of the study was to identify the cause of cybercrimes in the financial sector, assess the impact of cybercrime on Steward Bank, evaluate the current strategies utilised by Steward Bank to deal with cybercrime and recommend on the best strategies that can be implemented so as to curb cybercrimes in the financial sector. The study was conducted using a case study approach since it was deemed to be the most appropriate for the research. Stratified random sample and purposive sampling procedures were used to select the sample size of 97 participants with 81 responding from four departments in Steward Bank, with the questionnaires and in-depth interviews serving as the primary research tools. Data was analysed using SPSS and represented in graphical and tabular forms. The research found out that poor cybersecurity measures was the major cause of cybercrime in the financial sector. Significant impact of cybercrime on Steward Bank which the research findings revealed was data loss. The current measures to deal with cybercrime that were evaluated showed that they are generally considered to be effective, with employee training and security policies and procedures, being most effective measures. The researcher recommended that developing a comprehensive cybersecurity strategy, use of multi-factor authentication, regularly updating software and systems, conducting regular vulnerability assessments, penetration testing, partnering with cybersecurity experts and also to stay informed about emerging cyber threats and trends, can be more effective measures to curb cybercrime in the financial sector. Future research should concentrate on evaluating the effectiveness of cybersecurity measures implemented by financial institutions and identifying areas for enhancement.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my family Mr. Tafadzwa and Mrs. Caroline Chimbwanda, my brothers Sean, Seth and my sister Whitney for their unwavering support and encouragement throughout my academic journey. Their love and belief in me have been a constant source of motivation and inspiration. Also, l extend my appreciation to my supervisor Mrs. Chitiyo for providing invaluable guidance and feedback throughout the research process. Her expertise and dedication have been instrumental in shaping the direction of this study. Additionally, I want to thank Bindura University for providing the necessary resources and facilities to conduct this research. The institution has played a crucial role in my academic growth and development. Finally, I would like to express my appreciation to all those who participated in the study and contributed to its success. Their willingness to share their insights and experiences has been instrumental in advancing our understanding of the challenges of cybercrime in the financial sector.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.0 Introduction

The chapter covers several important aspects of the study, including the background knowledge, the problem statement, the study's purpose, the research questions, and the study's significance. It also discusses the study's key assumptions, limitations, and delimitations, as well as provides definitions and summaries.

1.1 Background of the study

The widespread utilisation of the internet and other technologies has intensified the risk of cyber-criminal attacks all over the world. With the frequency of incidents of theft, phishing, computer viruses, and hacking on the upsurge. According to The Fintech Times (2021) cybercrime, often known as computer-related crime, is a growing worldwide problem that threatens all sectors of the economy. Hackers can use the internet's anonymity to their benefit in order to take advantage of businesses and people thanks to the development of technology, which is now used continuously and everywhere. Cybercrime is more prevalent in the financial services sector than in almost any other industry (The Fintech Times, 2021).

According to BlackFog (2019), cybercrime is a lucrative business and criminals are increasingly targeting the financial sector in their pursuit of quick monetary gain. As the frequency and complexity of cyberattacks increase across all sectors, the financial sector in particular is under relentless attack from hackers, falling prey to cyber security incidents around 300 times more than other industries. This industry has the highest cost for cybercrime at $18.3 million for the average business. While cyber threats vary in their approach and impact, data exfiltration, malware, phishing, and Distributed Denial of Service (DDoS) are the most prevalent among attackers who

are focused on gaining access to confidential transactional data, user account information, and control over transactional systems with the intent to steal funds or disrupt operations (BlackFog, 2019).

The financial sector, being a critical infrastructure, is highly targeted by cybercriminals. This is evidenced by the Financial Conduct Authority's (FCA) report of an 80% increase in cyber-attacks against financial institutions in 2017. Furthermore, the 2017 Cost of Cybercrime Study by Accenture and the Ponemon Institute revealed that financial services had the highest cybercrime costs compared to any other sector. Cybercrime attacks are becoming increasingly frequent, dangerous, and sophisticated. In 2016, the Federal Bureau of Investigation (FBI) - Internet Crime Complaint Centre received one million four hundred eight thousand eight hundred forty-nine complaints, resulting in a reported loss of US $4.63 billion (Smith, 2017). There were fifty-five thousand and forty-three reported cases and a total loss of US $339,474,918 in 2016. The top cybercrime attack for that year was the Business Email Compromise/Email Account Compromise (BEC/EAC), resulting in a total loss of US $360,513,961. This was followed by identity theft, credit card fraud, phishing, and hacking, with losses of US $58,917,398, US $48,187,993, US $31,679,451, and US $55,500, respectively (Smith, 2017).

Financial institutions, such as banks and financial services, are attractive targets for cybercriminals because they possess valuable data and money that can be sold. They also have vulnerabilities that make it relatively easy to access the data. According to Ozarslan (2022), firms in the finance industry store critical and valuable data electronically, including credit card and deposit information, estates, wills, titles, and other sensitive data, and manage trillions of dollars. Additionally, their ongoing digital transformation, the complex regulatory environment, the intricate supply chain ecosystem, and the hybrid workspace practices accelerated by COVID-19 are creating more opportunities for cybercriminals to access and profit from that data. Consequently, cyber threat actors are increasingly focusing on the financial sector.

The way people bank has undergone significant changes in the past few years, according to The Fintech Times (2021). With the development of new technologies, individuals no longer solely access and generate data through ATMs or on-site banking. Instead, they use online banking, mobile applications, and e-commerce platforms. This has increased the vulnerability of financial

institutions, as services such as cashless payments have become more prevalent. Cybercriminals now infiltrate and manipulate data to imitate individuals, gain access to sensitive information, disable devices, and even sell sensitive data to competitors or marketing agencies through multiple channels (The Fintech Times, 2021).

According to statistics on major cybercrime trends, 67% of all data breaches involve advanced personally identifiable information like dates of birth and addresses. Due to the sensitive nature of this information, the financial industry has become a target for a series of cybercrime incidents, resulting in data breaches for millions of customers (Fintech Times, 2021). Despite the increasing sophistication of services available, the two major risk areas for the financial services industry continue to be email phishing and third-party unprotected services. A single breach can provide hackers with data that can be used to gain unauthorized access to other infrastructures through the reuse of passwords or social engineering attacks. This data is then traded on the Deep/Dark Web (Fintech Times, 2021). Additionally, aggregated data can be used to target enterprises and steal intellectual property, trade secrets, customer information, financial data, or corporate strategies. Therefore, data breaches can have far-reaching implications, not only affecting the individual customer whose data has been compromised (Fintech Times, 2021)."

As in many other countries, cybercrime is becoming a rising threat in Zimbabwe's financial industry (Smith, 2019). Due to their increased reliance on digital technologies, financial institutions in Zimbabwe, such as banks and other financial service providers, are more susceptible to cyberattacks. In other words, Jones and Lee (2018) discovered that Zimbabwean financial institutions are vulnerable to cyberattacks. According to a Reserve Bank of Zimbabwe report (2018) on several kinds of cyberattacks, including phishing, social engineering, malware and ransomware attacks, and cybercrime poses a serious threat to the nation's financial sector. Gumbo et al. (2018) discovered in their research of cybercrime in Zimbabwe, that social engineering and phishing were two of the most prevalent forms of cyberattacks used against financial institutions. Attacks like these have the potential to cause financial losses for both the institutions and their clients, as well as the theft of private financial data.

1.2 Problem Statement

According to a research report published by Accenture and the Ponemon Institute (2019), cybercrime targeting the financial sector increased by 67 percent in the last five years. Following the COVID-19 outbreak, the year 2020 experienced many changes. Taking Steward Bank as a case study, in the wake of stay-at-home orders and large-scale shutdowns, the bank had to change its terms of operation and with a lot of its employees now forced to work from home. Cybercriminals had the perfect opportunity to target systems and networks of individuals and businesses (Akimori, 2021). While cyberattacks are not new to the financial sector, the pandemic period further worsened the problem. The financial industry was one of the hardest hit by cyberattacks during the lockdown period. According to data from CrowdStrike Intelligence, a cyber-security service company, there were 86 attacks in the sector, placing it sixth among the most targeted industries globally.

According to Ozarslan (2022), financial institutions have long been concerned about cybersecurity breaches, but they are now even more worried because cyber threats present greater operational and reputational risks. The most common threats they face include ransomware, phishing, web application and vulnerability exploitation attacks, denial of service (DoS) attacks, and insider threats. As a result, banks need to assess their current operating practices. In this dissertation, the researcher studies the challenges of cybercrime in the financial sector and recommends further measures that can be taken to improve cyber security.

1.3 Research objectives

●To identify the cause of cybercrimes in the financial sector affecting institutions such as Steward Bank Limited for the specified period of 2020-2021.

●To assess the impact of cybercrime on Steward Bank Limited.

●To evaluate the current strategies utilised by Steward Bank Limited to deal with cybercrime in the financial sector.

●To make recommendations on the best strategies that can be implemented so as to curb cybercrimes in the financial sector.

1.4 Research questions

●What were the causes of cybercrimes in the financial sector affecting institutions such as Steward Bank Limited for the specified period of 2020-2021?

●What is the impact of cybercrime on Steward Bank Limited?

●Which current strategies are being used by Steward Bank to curb cybercrime in the financial sector?

●What other strategies can be recommended so as to curb cybercrimes in the financial sector?

1.5 Significance of the Study

The research seeks to determine the challenges of Cybercrime in the financial sector taking Steward bank as the case study of the research. Thus the findings of the study would be applied in implementing and improving Cyber Security by suppressing Cybercrime in the financial sector. The study would also be significant:

1.5.1To the Researcher

This research study is a partial accomplishment and requirement of the Bachelor's Honours Degree in Financial Intelligence of Bindura University. The study will serve to enrich the student's knowledge of cybercrime, its challenges in the financial sector, and how to combat cybercrime by practical application of the theories, concepts, strategies, and recommendations covered under the period of study.

1.5.2To the university

The finalised work shall contribute to literature and give insight for future research carried out by other researchers and banks in order to better understand the challenges of cybercrime in the financial sector and the importance of cyber security.

1.5.3 To Steward bank

The study shall give insight to financial institutions about the cyber security strategies to adopt as a way of combating cybercrime. As a result, this research work shall emphasize the proper implementation of measures to curb cybercrime in the financial sector by banks.

1.6 Assumptions

The assumptions of this research were that:

- The information gathered from primary data sources was accurate, and responses were given in good faith.

- The questions would be understandable to the respondents.

- The Steward Bank management would understand the impact of cybercrime on their business.

- Research material will be readily available and accessible

- Any financial institution will be a representative of the finance sector.

1.7 Delimitation of the Study

- The research is going to be focused on the financial sector, Steward bank limited in particular for the period 2020 to 2021.

1.8 Limitations of the Study

Due to the confidentiality policy, access to information will most likely be limited to some extent. As a result, the researcher will have to guarantee the respondents that ethical standards would guide the research and that their opinions would be treated in confidence and would not be exploited for any other purpose without their consent.

- The researcher had limited financial resources to carry out this study.

- The researcher has a limited amount of time to complete the study, she will make the most of every opportunity.

1.9 Definition of terms

1.9.1 Cybercrime

Thomas and Loader (2000) define cybercrime as "computer-mediated activities that can be conducted through global electronic networks and that are either illegal or considered illicit by certain parties." Another definition provided by Gordon and Ford (2006) describes cybercrime as "any crime that is facilitated or perpetrated utilizing a computer, network, or hardware device."

1.9.2 Financial Sector

According to Kenton's (2021) definition, the financial sector refers to the part of the economy comprising businesses and institutions that offer financial services to commercial and retail clients. This industry encompasses several businesses, including banks, investment organizations, insurance providers, and real estate companies.

1.10 Summary

The first chapter focused on building the groundwork for the research. It has established the foundation for the research, outlining the areas that will be addressed and how they will be covered. It has provided the background of the study, stating the problem statement and the significance of the study. The research objectives were outlined and the research questions were clearly stated. The chapter also emphasized the assumptions, delimitations, and limitations of the study. The chapter that follows will go through relevant literature to the study which is a theoretical framework, conceptual framework as well as empirical evidence. Chapter three is going to be centred on the methodology employed in the study and the chapters that follow will focus on data presentation, discussion, and finally the summary, conclusions, and recommendations.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

This Chapter discusses and analyses current information or prior (but significant) studies, including material from conference reports, financial gazettes, and business reports that provide the basis for the suggested study. The focus of a literature review is on the outcomes the researcher sought to explore in order to better comprehend the research topic and the research issues. Lambert (2012) describes a literature review as an in-depth analysis of what is known about the subject of the study, the concepts that are related to it, and the various viewpoints that have been expressed on the subject. Also according to Cooper (1998), the outcome of a literature review depends on the purpose and focus of the research study. Synthesis studies are literature reviews that aim to summarize and draw conclusions from prior empirical studies in order to identify any issues that have not yet been addressed.

2.1 Purposes of Literature Review

The goal of a literature review, according to Remeny (2001), is to create or define the field of study, develop a theoretical framework for the subject area of study, and find studies, models, and cases that support the research topic. Fink (2014) states that the purpose of literature reviews is to show readers how the research fits into a larger field of study while also giving an overview of the sources used in the research. A literature review discusses the relationship between each work and the others being considered in the context of how it contributes to understanding the research problem being addressed. (Fink and Arlene, 2005).

2.2 Conceptual Framework

2.2.1 Definition of Cybercrime

The definition of cybercrime has evolved over time and varies depending on the author's perspective. According to the United Nations Office on Drugs and Crime (UNODC, 2017), cybercrime encompasses a broad range of offenses against computer data and systems, including hacking, computer-related forgery and fraud (such as phishing), content offenses (such as child pornography), and copyright offenses (such as disseminating pirated content). Furthermore, the term "cybercrime" refers to all illegal and criminal activities carried out using computers, the Internet, and the World Wide Web (Nfuka, Sanga, and Mshangi, 2014).

Stallings and Brown (2015) define cybercrime as criminal activities that involve computers or computer networks as tools, targets, or places of criminal activity, which may or may not involve the internet. Other authors, such as Sarrab et al. (2013) and Broadhurst (2006), define cybercrime as unauthorized entry into a computer system with the intention of deleting, modifying, or damaging computer data. Cybercrime can also be seen as "computer-mediated activities that are illegal or considered illicit by certain parties and can be conducted through global electronic networks" (Douglas and Loader, 2000). Due to the varying definitions, cybercrime is a complicated form of crime with different forms and motives, according to Sarrab et al. (2013).

2.3 Nature of Cybercrime

In Zimbabwe, a piece of legislation known as the Criminal Codification and Reform Act regulates a wide range of criminal offenses, including technological and cybercrime-related offenses. According to Kashuwa (2021), there are various types of cybercrime, such as phishing, hacking, malware, and identity theft.

2.3.1 Phishing

Phishing, according to Kashuwa (2021), is a social engineering attack that deceives people into providing personal information, such as usernames, passwords, or credit card numbers, through a fake email or website. Vivek (2014) further defines phishing as a type of crime in which confidential information, including Debit/Credit Card numbers, Customer IDs, IPINs, CVV

numbers, Card expiration dates, and so on, is acquired via emails that appear to be sent from an authentic source. Instant messaging and email spoofing are used to conduct phishing attacks. According to Boateng and Amanor (2014), phishing is defined by Roger (2008) as an attack that targets individuals and organizations to acquire private information for fraudulent purposes. In their analysis of phishing attacks and countermeasures, Isaac, Chiong, and Jacob (2006) defined phishing as an act of deceiving people into providing personal information (involuntarily) through the use of forged emails or fake websites, which can result in identity theft (the fraudulent use of another person's name or personal information in order to gain a financial advantage).

Europol (2014) describes phishing as a form of fraud committed against businesses and financial institutions through the theft of customer identities. Identity theft, which involves the illegal use of sensitive information without the owner's knowledge, is another term for phishing (United Nations Office on Drugs and Crime, 2010). There are three types of phishing identified by Sarannia and Padma (2014) as spear, clone, and whaling. KPMG (2012) states that phishing is the most common type of identity theft. In order to safeguard themselves against phishing attempts, Kashuwa (2021) has underlined the necessity for both individuals and organizations to take preventative action.

2.3.2 Hacking

The act of hacking has been around for a long time and is considered one of the earliest forms of computer crime (Herselman and Warren, 2010). As defined by Mugume (2020), hacking is the unauthoritative access to or manipulation of computer systems or networks, frequently with the goal of stealing data or causing harm to the system. Paget (2007), who was cited by Hedayati (2012), articulated that hacking involves unauthorized access to computer systems or databases to acquire confidential information. With the increasing availability of personal information online, cybercriminals find it easier to steal from businesses and individuals (Magutu et al., 2011). Unauthorized access happens when somebody gets unauthorized access to various computer databases to which they don’t have legitimate access (Payne, 2013). Unauthorized access is defined in Section 163 of the Criminal Codification and Reform Act of Zimbabwe as using a computer or network without permission or in excess of such permission.

Bawane and Stelke (2014) identified various hacking techniques, including denial of service, spoofing, sniffing, viruses and worms, key loggers, social engineering, and fake messages. As highlighted by Broadhurst (2006), keylogging is a common tactic used by hackers. This involves installing software on a victim's computer that records the keystrokes entered by the user. The recorded information can then be used for various cybercrimes, including identity theft, internet fraud, telecommunication fraud, and economic espionage. Hackers often target computer systems with large databases to obtain identity-related data on a large scale. Magutu et al. (2011) also noted that the use of a single password for multiple accounts can exacerbate the consequences of a cyber-attack, leading to significant losses due to identity theft across multiple accounts.

2.3.3 Card Fraud

Section 165 of the Criminal Codification and Reform Act describes computer-related fraud. Card fraud is the use of stolen credit or debit card information to make unlawful transactions or withdrawals, frequently through the use of skimming devices or other types of cyberattacks, according to Feltoe (2019), a legal expert in Zimbabwe. Additionally, Sharma and Nanda (2006), further defined card fraud as the act of using unauthorized personal or account information in order to misrepresent account information. Sonepat and Sonepat (2014) support this definition, specifying that credit card fraud involves using an unauthorized account for unintended operations. KPMG (2012) adds that credit card fraud can only occur after the theft of relevant card and transaction information. There are two main types of card fraud: offline, which involves the theft of physical cards, and online, which occurs through the internet, phone, shopping, and web transactions (Sonepat and Sonepat 2014).

2.3.4 Malware

According to Kashuwa (2021), malware includes viruses, Trojan horses, and other malicious software that is intended to harm computer systems or networks. Malware also refers to the installation of unauthorized software into a computer system, typically done without the owner's permission, with the intent of stealing sensitive information. This is supported by the United Nations Office on Drug Crime, which notes that malware attacks involve the installation of malicious software that enables the collection of information such as credit cards and social security numbers. Malware can also move between computer and network systems to modify them

without the owner's consent. Malicious software can intercept communication or record keyboard strokes, allowing attackers to gather sensitive information. Uppal et al (2014) categorized malware into two types: contagious and masked. The contagious type includes viruses and worms, while the masked type includes Trojans. Viruses replicate themselves and infect the entire system, causing a denial of services, while worms pass-through storage devices and cause storage space shortages. Trojans behave like legitimate programs but are used to steal personal and confidential information. They are often downloaded from the internet. (Uppal et al, 2014; United Nations Office on Drug Crime, 2013; Magutu et al, 2011; Roderic, 2006).

2.3.5 Identity theft

Identity theft, regarded by Cole and Pontell (2006) as the fastest-growing form of cybercrime in America, is a crime that is difficult to define, as investigators do not agree on its definition and which crimes should be included under this broad concept (McNally and Newman, 2008; Cole and Pontell, 2006). However, McNally and Newman (2008) defined identity theft as the use of an individual's personal information for fraudulent purposes.

Online identity theft, which encompasses hacking, phishing, malware, and online fraud, and offline identity theft, which involves "trashing" and traditional theft, are two categories of identity theft (Hoofnagle, 2009). CIPPIC (2007), as cited in Hedayati (2012), identifies the personal information commonly stolen by identity thieves, including credit card numbers, social security numbers, dates of birth, passwords and PINs, home addresses, and phone numbers. The increased risk of identity theft in Zimbabwe was mentioned by Mugume (2020), who also emphasized the necessity for people to take precautions to secure their personal information, such as by using strong passwords and two factor authentication.

2.4 Criminology Theories in Cybercrime

In the realm of criminology, various theories have been developed to explain criminal behaviour, including cybercrime. Various theories, including the following, are used to inform Zimbabwe's criminal law regarding cybercrime.

2.4.1 Routine Activity Theory

The Routine Activity Theory posits that crime occurs when there is a convergence of a motivated offender, a suitable victim or target, and the absence of a capable guardian who can prevent the crime from happening. Hutching and Hayes (2009) applied this theory to phishing in financial institutions, attributing the increase in cybercrime to the rise in internet usage, which increases the pool of potential offenders and targets. The absence of capable guardianship, such as account holders, law enforcement, and financial institutions, also increases the risk of cyber-attacks. Zimbabwean criminal laws may aim to lessen potential targets' vulnerability by establishing cybersecurity regulations.

2.4.2 Rational Choice Theory

Rational Choice Theory proposes that offenders weigh the benefits of committing a crime against the risks of being caught and punished. According to Wittek (2003), the term "rational choice theory" (also known as the "choice theory" or "rational action theory") refers to an explanation of social phenomena involving the outcomes of individual action that can be in some manner regarded as rational. Strict punishment and deterrent measures, such as electronic mechanisms and surveillance cameras in financial institutions, can decrease the likelihood of cybercrime (Wada and Odulaja, 2012). However, the difficulty of detecting cybercrime and the potential for huge benefits entice rational cybercriminals to engage in such activities. Holt and Smirnova (2015) have used this theory to analyze the criminal law surrounding cybercrime.

2.4.3 Social Learning Theory

According to this theory, people pick up behavioral traits by watching and imitating others (Grabosky and Smith, 2001). People can develop the motivation and skills to commit a crime by associating with or being exposed to others who engage in criminal activities (Burruss, Holt and Bossler, 2012). In the case of cybercrime the internet, social media, and other online forums are common places where individuals might learn how to commit cybercrime. Zimbabwe's criminal laws aim to curb cybercrime by enforcing severe punishments and making successful convictions widely known to deter potential offenders from engaging in such behaviour.

2.5 Causes of Cybercrimes in the financial sector

The increasing use of technology and the internet has led to a surge in cybercrime, posing significant challenges to the financial sector. Cybercriminals use sophisticated techniques to gain unauthorized access to sensitive financial data, which can result in financial loss, reputational damage, and legal liabilities for financial institutions. To address these challenges, several studies have been conducted to identify the causes of cybercrime in the financial sector and propose effective strategies to prevent and mitigate cyber threats.

One of the key factors contributing to cybercrime in the financial sector is the lack of effective cybersecurity measures. Research suggests that financial institutions often struggle to keep up with the rapid pace of technological advancement, leaving them vulnerable to cyber-attacks (Muhumuza and Tumuheki, 2020). Furthermore, cybercriminals are constantly adapting their techniques to evade detection, making it difficult for financial institutions to stay ahead of the curve (Ahmed et al., 2021). Another factor contributing to cybercrime in the financial sector is the human element. Research suggests that employees are often the weakest link in an organization's cybersecurity posture, as they can inadvertently disclose sensitive information or fall victim to social engineering attacks (Kshetri, 2018). Furthermore, insider threats pose a significant risk to financial institutions, as employees with malicious intent can deliberately steal sensitive data or disrupt critical systems (Huang and Rustagi, 2019).

2.6 Impact of Cybercrime

The impact of cybercrime on the financial sector can be significant, both financially and reputationally. The impact of cybercrime on financial performance has been widely investigated in the literature. Mungai (2020) explored the impact of cybercrime on the performance of commercial banks in Kenya. The study found that cybercrime had a significant negative impact on the profitability, market share, and customer retention of commercial banks. Similarly, Gomes et al. (2021) found that cybercrime had a significant negative impact on the financial performance of financial institutions in Brazil.

A study by The International Business Machines Corporation (IBM) found that the cost of a data breach in the financial sector was $5.85 million per incident, the highest of any industry (IBM,

2021). The study also found that the financial sector had the longest time to identify and contain a data breach, with an average of 233 days.

In addition to financial losses, cybercrime can also damage the reputation of financial institutions. Cyber-based attacks damage a company's reputation since they result in the loss of commercially sensitive data, reactive costs incurred in response to data leaks, and possible legal repercussions, such as monetary fines (Wright, 2015). A study by Edelman found that the majority of consumers would consider switching to a competitor if their financial institution experienced a data breach (Edelman, 2021). The study also found that consumers were more likely to trust financial institutions that were transparent about their cybersecurity practices.

2.7 Ways to Mitigate Cybercrime in the financial sector

2.7.1 Use Anti-Virus Software and Firewalls

Antivirus software, often known as anti-malware software, is described by Laura (2022) as a security solution offered by businesses that ensure cyber security. It is a software program that runs on various digital devices and looks for programs or data that either shouldn't be on your devices or could be hazardous. Many PCs and organizations frequently employ antivirus software as a cybersecurity measure with the main goal of scanning, identifying, and preventing any dubious files and applications from entering the machine. (Meade, 2019).

Boudriga (2010) defines a firewall as a network security system that monitors and controls incoming and outgoing network traffic according to established security protocols. Firewalls can be software programs or hardware devices such as routers that filter and inspect information that comes in through the internet while browsing or surfing. By doing so, firewalls can direct the user to the relevant data and remove any irrelevant data that might pose a risk to online consumers. (Laudon, 2009).

2.7.2 Use of a Two-Step verification (Two-Factor Authentication) method

Is a technique for enhancing account security. The common password that is required for every account serves as the first "factor." A verification code obtained from an app on a computer or mobile device serves as the second "factor." According to Clickatell (2018), the two-step

verification approach adds an additional degree of security by requiring users to provide a one-time pin in addition to their password and log in. (OTP). After entering user credentials, an OTP is sent to the mobile device or email address of the account's legitimate user. An OTP changes or expires after at least one hour.

2.7.3 Data Encryption

Financial institutions can minimize the risk of fraud on their networks by encrypting all consumer data. This makes it harder for hackers to access the information without using complex decryption techniques. Encrypting data or communications sent over the internet will prevent any unauthorized users from accessing them, securing the data from all ends while yet remaining accessible to the parties involved in the conversation. (Symantec, 2015). Through this procedure, plain text is converted into encrypted text that can only be read by the sender and the recipient. (Laudon, 2009).

2.7.4 Employee Training/ Awareness

The best strategy to secure and safeguard your important corporate data is to provide your staff with in-depth training on cyber security dangers and methods for avoiding data breaches. Through this training, you can help your team members understand the value of cyber security and improve everyone's ability to safeguard company data from ransomware, phishing, business email compromise (BEC), and other online threats.

2.8 Empirical Evidence

Several studies have investigated the prevalence of cybercrime in the financial sector. A study by Junaid and Khan (2019) explored the challenges faced by banks in Pakistan due to cybercrime. This paper's objective was to outline the challenges that banks in Pakistan's banking sector were facing as a result of cybercrimes. Data from semi-structured interviews with bank personnel and IT specialists were gathered as part of the study's qualitative research methodology. According to the findings, banks in Pakistan experience a number of challenges as a result of cybercrimes, including monetary losses, damage to reputation, and a decline in client trust. The report also revealed that banks in Pakistan took a number of steps to address these issues, such as investing in cybersecurity tools and educating staff members on best practices.

Cybercrime: an emerging threat to the banking sector of Pakistan by Muhammad and Urooj (2019). This study aims to shed more light on the impact of cybercrime incidences on Pakistan's banking industry. This study examines how information security awareness affects the connection between cybercrimes and corporate performance. Design/methodology/approach. By examining the moderating impacts of information security awareness, the influence of cybercrime occurrences on organizational performance is further examined. Using a survey approach, a sample of 302 banking employees in Pakistan was investigated. The results showed that while information security awareness lessens the negative impact of cybercrime incidents on organizational performance, those incidents nonetheless have a negative impact.

Gomes, Oliveira and Gomes (2021) investigated the impact of cybercrime on financial institutions in Brazil. This study is based on a systematic literature review (SLR) that analysed articles published between 2010 and 2020. The study found that the primary challenges faced by these institutions were reputational damage, loss of customer trust, and financial loss.

Similarly, Mungai (2020) explored the impact of cybercrime on the performance of commercial banks in Kenya using Equity Bank Limited as a case study. The study used a descriptive research design and collected data through questionnaires administered to bank employees. Study findings were that cybercrime had a significant negative impact on the profitability, market share, and customer retention of commercial banks.

Also, a study by Alzahrani and Duan (2019) examined the challenges of cybersecurity in the Saudi Arabian banking sector. The study found that the primary challenges were the lack of cybersecurity regulations, the high cost of cybersecurity, and the lack of awareness and training for employees.

2.8.1 Empirical Evidence of Cybercrime in Zimbabwe's financial sector.

There are also several studies that have looked at cybercrime in the context of Zimbabwe's financial sector, including the following.

Mugari (2016) carried out a research on Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe. The study investigated the prevalence of cybercrime in the financial sector of Harare. The study focused on four financial institutions in the city and used stratified random sampling and purposive sampling techniques to select 48 respondents from commercial

banks. Questionnaires and in-depth interviews were the primary research tools used. The survey found that cybercrimes such as hacking, phishing, identity theft, and malware were prevalent in banks. Although financial institutions are implementing cybersecurity measures to address the issue, technical advancements are outpacing preventive efforts.

"Cybercrime in the Zimbabwean Banking Sector: A Case Study of CBZ Bank Limited" by Yvonne Tendai Mungwena and Farai Kwenda (2019) - This study examines the challenges of cybercrime in the banking sector in Zimbabwe, focusing on CBZ Bank Limited as a case study. The authors identify various types of cybercrime, such as phishing attacks and malware, and discuss the impact of these attacks on the bank and its customers.

Cybercrime and Security of Electronic Banking in Zimbabwe: A Case Study of Barclays Bank Zimbabwe Limited" by Tafirei Chigwata and Lovemore Mamvura (2017) - This study explores the challenges of cybercrime in the electronic banking sector in Zimbabwe, with a focus on Barclays Bank Zimbabwe Limited as a case study. The authors analyse the various types of cybercrime that can affect electronic banking, such as hacking and identity theft, and discuss the measures that banks can take to prevent and mitigate these attacks.

"An Analysis of Cybercrime in the Zimbabwean Financial Sector: A Case Study of Standard Chartered Bank Zimbabwe" by Prudence Chikwanda and Wendy Mahlangu (2019) - This study investigates the challenges of cybercrime in the financial sector in Zimbabwe, using Standard Chartered Bank Zimbabwe as a case study. The authors examine the various types of cybercrime that can affect banks, such as ransomware and insider threats, and discuss the importance of developing a comprehensive cybersecurity strategy.

"Cybersecurity in Zimbabwe's Banking Industry: A Review of Literature" by Andrew Makoni, Tendai Makoni, and Nyasha Musviba (2020) - This literature review examines the challenges of cybersecurity in Zimbabwe's banking industry, focusing on the various types of cybercrime that can affect banks. The authors analyse the existing literature on this topic and identify key areas for future research, such as the impact of cybercrime on financial stability and the role of regulatory bodies in preventing cybercrime.

2.9 Research Gap

While the literature provides extensive evidence of the impact of cybercrime on the financial sector, there is a research gap in understanding the specific challenges faced by individual financial institutions in mitigating the risk of cybercrime. Therefore, a potential research gap for this study could be to investigate the challenges faced by Steward Bank Limited in the period of 2020-2021 in addressing cybercrime threats, including the effectiveness of their cybersecurity measures, incident response plans, employee training, and other related factors. Specifically, the study could explore the factors that contributed to the bank's vulnerability to cyber-attacks, such as weaknesses in the security infrastructure, inadequate staff training, or lack of internal controls, and how these challenges were addressed. The findings of this study could provide insights into effective strategies to mitigate the risk of cybercrime for other financial institutions.

2.10 Chapter Summary

This chapter reviewed the theoretical and empirical literature on the challenges of cybercrime in the financial sector. The chapter also pointed to several natures of cybercrime and applied criminology theories to cybercrime. The empirical evidence reviewed showed that cybercrime had a significant negative impact on the financial performance of banks. The chapter that follows is centred on the research methodology that is used by the researcher.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

The research study's methodology is described in this chapter. It explains the method used to select the research subjects and the data collection techniques. The chapter begins by describing the research design chosen by the researcher, as well as the methods, instruments, sampling procedures, and data gathering techniques used.

3.1 Research Design

According to Kirshenblatt and Barbara (2006), research design refers to the overall approach selected to integrate various study components in a coherent and logical manner, ensuring that it effectively addresses the research problem. It guides the data collection, measurement, and analysis processes. Additionally, Claybaugh and Zach (2020) explain that research design is the overall method adopted to conduct a study, which establishes a clear and logical approach to address pre-established research questions through the collection, interpretation, analysis, and discussion of data. Cooper and Schindler (2003) define research design as the strategy and framework utilized to investigate data to find answers to research questions. The research design can be scientific, historical, descriptive, or a case study. In this research study, a case study methodology was used.

3.1.1 Justification of research design

To provide a more in-depth examination of the research problem, the study used a case study methodology and focused on Steward Bank Limited Head Office in Harare. A case study, according to Robson (2002), is a method for conducting research that entails an empirical investigation of a specific phenomenon within its actual context and the use of numerous sources

of data. Both primary and secondary sources of data were used to collect, critically analyse, and assess the information.

The researcher selected a case study approach because it was a cost-effective strategy that ensured a comprehensive analysis of documents and a long-term investigation of events. This approach enabled the researcher to understand the reasons, methods, and contexts related to a specific instance and provided a rationale for the need to conduct a more extensive examination in the future. Additionally, this research strategy was chosen since it made use of a variety of data collection techniques that aided in the study and confirmation of the facts provided. A case study describes actual occasions or circumstances, making it a true portrayal of the researcher's findings.

3.2 Target Population

A population, according to Wegner (1995), is a group of people who share one or more traits that are significant to the researcher. The entire collection of objects from which samples are taken is known as the population, according to Christiane (2005). The researcher used a target population comprising Steward Bank Limited head office employees in Harare.

3.3 Sample Population

According to King'oriah (2004) and Leary (2001), a sample is an accurate representation of the complete population being examined. Steward Bank Limited head office employees from four different departments, namely Finance, Risk, Auditing and IT served as the sample population for this study. The researcher used the Employee listing to compile a list of the personnel working in four different departments. According to the employee listing, 57 employees were from Finance department, 48 employees from IT, Risk had 13 employees and 8 employees from Auditing department making a total of 126 employees. So the researcher selected a sample from this demographic to gather information. Using the stratified random selection technique, the researcher then selected a sample of employees from the different departments.

3.4 Sampling Technique

According to Trachoma (2006), sampling refers to the procedure of selecting units, which could be individuals or organizations, from a population of interest. This can be done by applying one

of the following four major techniques: simple random sampling, systematic sampling, cluster sampling, or stratified sampling technique. To choose participants for the questionnaire and interviews, the researcher utilized stratified random sampling and purposive sampling procedures, respectively

3.4.1 Stratified Random Sampling

Craw Shaw and Chambers (2003) defines stratified random sampling as a strategy that divides the population into strata that are easily distinct from one another in order to sample the entire population. In this study, Steward Bank Limited's population was divided into four primary departments: finance, risk management, internal auditing, and IT. Due to the fact that there are several levels of employees in this research, stratified sampling was used. This strategy allows every person at every level to be included, preventing dominance by a single group. Due to the large number of stakeholders, the main goal of this sample technique is to reduce sampling errors.

3.4.2 Purposive Sampling

As defined by Crossman (2016), judgemental, selective, or subjective sampling are other names for purposeful sampling. Purposive sampling, according to Kothari (2004: 59), is a strategy used by researchers to choose individuals or groups as samples based on their objectives and viewpoints. In order to pick interview participants, the researcher employed the purposive sampling method. This strategy can quickly reach a targeted sample, meaning it is simple to obtain a sample of subjects with particular characteristics. Purposive sampling also saves time, money, and effort because it is adaptable, satisfies a variety of demands, and enables the researcher to choose a sample in accordance with the goal of the study and prior information of a population. As a result, the researcher had to select individuals from the risk management, internal audit, finance, and IT departments as they are the ones with full knowledge of the challenges of cybercrime in the financial sector.

3.5 Sample size

A good sample, according to Kothari (2004), should be genuinely representative of the population, have a minimal sampling error, and be feasible, affordable, and systematic. The number of objects to be chosen from the universe to form a sample was defined by Kothari (2004) as the sample size.

The sample size can be determined in a number of ways, including census, copying the sample size of related research, utilizing available tables, and applying formulas. The research's sample was skewed toward employees in the risk management, internal audit, finance, and IT departments. The sample size was determined using Slovin's sample size formula: n = N / (1 + N (e^2) where

n = required sample size

N = population size

e = the level of precision required (margin of error)

n = N / (1 + N (e^2)

n = 126 / (1 + 126(0.05^2)

n = 96.68

Rounding off to the nearest whole number, the sample size using Slovin formula was 97. The researcher then distributed a total of 87 questionnaires and planned 10 interviews.

3.6 Research Instruments

In order to acquire data, the researcher used questionnaires and interview techniques of data collection as the main research instruments.

3.6.1 Questionnaires

A questionnaire, in the words of Borg and Gall (2012), "is a research instrument used to gather data from respondents for the research topic under study." Questionnaires were the primary data gathering tool in this study by the researcher. As can be seen in the appendix, the questions were designed to elicit pertinent information from the respondents. The researcher delivered questionnaires with both open-ended and closed-ended questions to various target groups.

According to Kothari (2004), a questionnaire consists of a number of questions printed or typed in a specific order on a form or collection of forms. Respondents are given the questionnaire; they are responsible for reading, comprehending, and responding to the questions in the space provided on the actual questionnaire. The questions must be answered in the responders' own words. Structured and unstructured questionnaires are the two different categories of questionnaires,

according to Kothari (2004). Structured questionnaires are ones that have specific, pre-established questions. Each respondent receives the questions in the exact same format and sequence. The format of the question can be either closed or open (i.e., enabling free response), but it should be mentioned in advance and not formed during questioning.

3.6.2 Strengths of Questionnaires

Upon picking a tool for this research, the researcher was influenced by Kothari's (2004) analysis of the benefits of employing questionnaires. The questionnaires were really helpful for the research and the researcher because they collected data quickly and were cost-effective. Respondents' confidentiality and anonymity were upheld, which made it easier for them to respond to some delicate topics.

3.6.3 Limitations of Questionnaires

The low response rate presented some difficulties for the researcher, since some respondents found it challenging to find the time to complete the questionnaire because of busy work and social schedules. It was also time consuming since the questionnaire's open-ended questions took too long for responders to respond to. Additionally, respondents may have to expend a lot of effort on open-ended questions, which led to some respondents answering only to complete the detailed questions without contributing essential information.

In order to overcome these constraints, the researcher distributed questionnaires to people who expressed interest and then followed up on the questionnaires to gather pertinent data when it was appropriate.

3.6.4 Interviews

Ary (2010) states that interviews are a popular and fundamental method for collecting qualitative data. Additionally, Schostak (2006:54) defines an interview as a lengthy discussion between two individuals aimed at obtaining detailed information about a particular topic or subject. It also enables the interpretation of a phenomenon based on the interviewees' interpretations.

3.6.5 Strengths of Interviews

Blaxter et al. (2006) states that interviews are valuable because they provide researchers with the opportunity to obtain information that may not be obtainable through other techniques, such as questionnaires and observations. By conducting these interviews, the researcher was able to modify the interview questions' language to better meet the respondents' needs. Also the researcher's recording of nonverbal behaviour during the interview helped her to grasp some nonverbal expressions through observation. She made sure that all queries were addressed and pertinent data was gathered. Since it was a discussion, more responses were given and immediate feedback was gathered.

3.6.6 Weaknesses of Interviews

It was time-consuming because the researcher had to get to know the responders before beginning the interview. The extent of the interviews was also constrained by secrecy, confidentiality, and privacy.

The researcher had to first build a rapport with participants to make them feel more at ease in order to overcome these limitations, which led to more insightful responses and accurate data.

3.7 Data Collection Procedure

All questionnaires were self-administered by the researcher to Steward Bank employees with a focus on those in the departments that were chosen using stratified random sampling. Purposive sampling was used to pick interview subjects, and the researcher had to create an interview guide with all the relevant study-related questions in order for the research to be successful. Before being given to respondents, questionnaires and interview guides were created and approved by the research supervisor.

Prior to conducting the interview, the researcher had to schedule appointments with the respondents and ensure that they received a copy of the interview guide. This increased the reliability of the data by ensuring that each respondent was familiar with the questions before the interview day. Additionally, this made it possible for the participants to be well-prepared for the interviews, which increased the information's validity and decreased the likelihood that they would

be unprepared or unwilling to cooperate. The questionnaires were followed up on by the researcher on several occasions, and they were again collected in person a week later. After respondents had finished responding, the questionnaires were collected.

3.8 Validity and Reliability

3.8.1 Reliability

The degree to which a measurement yields consistent results is referred to as reliability. According to Myers (2009), reliability also has to do with how consistently a research study produces the same outcomes. The researcher had to ensure that the questionnaire was of reasonable lengths. Additionally, the researcher also took rigorous adherence to the study area very seriously, and questionnaires were distributed to employees in departments that were pertinent to the study.

3.8.2 Validity

The extent to which a measurement tool or technique is successful in describing or quantifying that which is intended to be measured, according to Weiner (2007), is referred to as validity. When creating the interview questions and questionnaire, the researcher was therefore directed by the study's goals, its research questions, and its main concepts to make sure the instrument would measure what it was intended to evaluate. By having the supervisor validate these instruments, the researcher was able to guarantee the content validity of the measuring tools, which were the interview schedule and questionnaire schedule.

Prior to distributing the questionnaires to the rest of the respondents, a pilot study was carried out to further strengthen the validity and reliability of the instruments, allowing any potential problems to be corrected before the study.

3.9 Data Presentation and Analysis

Both quantitative and qualitative analysis were performed on the study's data. Aakker (1998) asserts that data analysis entails using statistical methods on a database to draw conclusions about variables or a research.

The researcher used content analysis to analyse the qualitative data from the open-ended questions and interviews, counting the occurrences of particular facts to make it easier to draw conclusions. The completed questionnaires were edited for completeness and consistency prior to processing the responses. The information was then coded to make it possible to classify the responses into different groups. Before being coded for analysis, the primary data collected from the questionnaires was examined for inconsistencies, omissions, and readability. Statistical Package for Social Science (SPSS) computer software version 20 was used to analyse data. Pie charts, graphs, and tables were used to display the examined data. Tables are highly helpful for presenting survey results and formulating concise, sound conclusions. A bar graph displays discrete data in separate columns, whereas pie charts offer data as a proportion of the total.

3.10 Research Ethics: Key Considerations

The ethical considerations in research that were upheld throughout this study, included informed consent for data collection, anonymity (respondents' identities were concealed, so no personally identifiable information was collected), and voluntary participation, which allowed participants to join or leave the study at any time. Additionally, the researcher assured participants who contributed information to the study of anonymity and privacy.

3.11 Chapter Summary

The aforementioned chapter went in-depth on research designs, sample size and population, procedures used, validity and reliability, and sample instruments the researcher used to collect pertinent data for the study. The chapter that follows focuses on data presentation, analysis and discussion of the research findings.

CHAPTER IV

DATA PRESENTATION AND ANALYSIS

4.0 Introduction

This chapter analyses the data collected through questionnaires and interviews. The primary focus of this section is the presentation and interpretation of data, as well as discussing the outcomes and analysis. The data was analysed utilizing the Statistical Package for the Social Sciences (SPSS) computer software version 20 which aided in the generation of tables, graphs, pie charts, and descriptive summaries.

4.1 Response Rate

4.1.1 Questionnaire and Interview response rate

Table 1: Interview and questionnaire response rate

Instrument	Distribution	Response	Response Rate
Questionnaires	87	75	86.2%
Interviews	10	6	60%
TOTAL	97	81	100%

[Source: primary data]

According to the table above, the researcher distributed 87 questionnaires to four departments, namely Finance, Risk Management, Auditing, and IT. Out of the 87 questionnaires distributed, 75 were returned, giving a response rate of 86.2%. Additionally, out of the 10 interviews planned, only 6 people were interviewed, giving a response rate of 60%.

4.2 Demographic Data

4.2.1 Demographic Information of Respondents

The table below shows the demographic profile of the respondents in the study.

Table 2: Demographic Information of Respondents

Demographic	**Frequency**	**Percentage**
Gender		
Male	42	56%
Female	33	44%
Age Range		
< 18 years	0	
18-25	4	5.33%
26-35	29	38.67%
36-45	33	44%
46 years >	9	12%
Qualification		
O & A	1	1.33%
Certificate	3	4%
Diploma	12	16%
Undergraduate	46	61.33%
Postgraduate	13	17.33%
Position held		
Manager	8	10.67%
Analyst	20	26.67%
Officer	35	46.67%
Accountant	5	6.67%

Financial Controller	4	5.33%
Auditor	3	4%
Department		
Finance	35	46.67%
IT	31	41.33%
Risk	6	8%
Audit	3	4%
Period of Holding Office		
<2 years	19	25.33%
2-5 years	21	28%
6-10 years	30	40%
>10 years	5	6.67%

[Source: primary data]

As shown by the table above, most respondents were male (56%) whilst females comprised 44%. Respondents between the ages 36-45 occupied the majority of the sample under study with a percentage of 44%, followed by respondents between the ages 26-35 who had a total of 38.67%. The age range with the least percentages of 5.33% and 12% were 18-25 and 46 years and above respectively. This showed that the most vulnerable age groups to cyber risks greatly participated in the study.

Additionally, the table also shows the education level and the majority of the respondents in the research had undergraduate degrees as their highest educational level (61.33%), followed by 17.33% and 16% with post-graduate and diploma respectively. While the least of the respondents (1.33%) had secondary-level education as their highest form of educational qualification. This then indicated that the majority of respondents have knowledge enough to comprehend the various concepts covered in the study.

Table 2 also shows that the respondents were drawn from four departments, with 35 from Finance, 31 from IT, 6 from Risk, and 3 from Audit. The majority of the questionnaires were distributed to the Finance and IT departments, as they are the most frequently targeted by cybercriminals due to

their access to sensitive financial and confidential data. According to Verizon's (2020) research, fraudsters frequently employ phishing emails or other social engineering techniques to gain access to these departments' systems and data. Regarding the position held, the majority of respondents were officers (46.67%), followed by analysts (26.67%). In terms of the period of holding the office, the majority of respondents (40%) held their current position for six to ten years. This study revealed that respondents with work experience have a thorough understanding of the impact of cybercrime on the financial sector.

4.3 Understanding of Cybercrime

Table 3: Understanding of Cybercrime

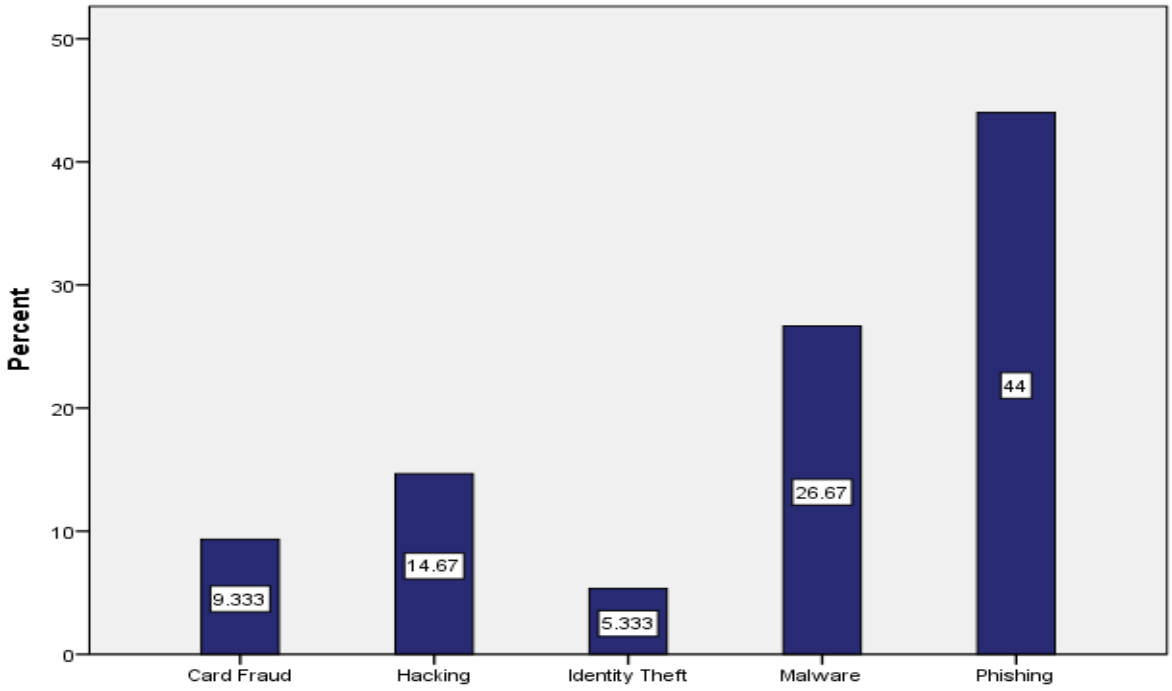
Understanding of Cybercrime	Frequency	Percentage
Comprehensive	19	25.33
Basic	53	70.67
None	3	4

[Source: primary data]

The majority of respondents had a basic understanding of cybercrime 70.67%, while 25.33% had a comprehensive understanding of cybercrime.

4.4 Cybercrime Encountered

Figure 1: Types of Cybercrime Encountered by Steward Bank Limited



[Source: primary data]

Figure 1 presents the types of cybercrime encountered by Steward Bank Limited, along with their frequencies and percentages. Phishing was recorded in the study as the cybercrime which is most encountered in the study whilst card fraud was the least encountered The findings provide valuable insights into the specific cyber-attacks faced by the bank, shedding light on the challenges it confronts in the financial sector. The study findings were supported by Mugari (2016), that is, in his research among the cybercrimes committed in banks are hacking, phishing, identity theft, and malware.

4.4.2 Phishing

The most prevalent type of cybercrime reported by Steward Bank Limited employees was phishing, with a percentage of 44%. Phishing involves the use of deceptive techniques, such as fraudulent emails or websites, to trick individuals into revealing sensitive information like passwords or financial details (Isaac, Chiong, and Jacob, 2006). The high incidence of phishing

attacks indicates a significant vulnerability within the bank's systems and highlights the need for robust security measures to protect against such threats.

4.4.3 Malware

Malware, a type of malicious software designed to harm or gain unauthorized access to computer systems, was reported as the second significant cybercrime encountered by Steward Bank Limited. The frequency of malware incidents constituted 26.67% of the reported cases. Malware can have severe consequences, including data theft, system disruption, and financial fraud (Magutu et al, 2011). The high occurrence of malware incidents emphasizes the need for effective cybersecurity measures, including robust antivirus software and regular system updates, to mitigate the risks associated with malware attacks.

4.4.4 Hacking

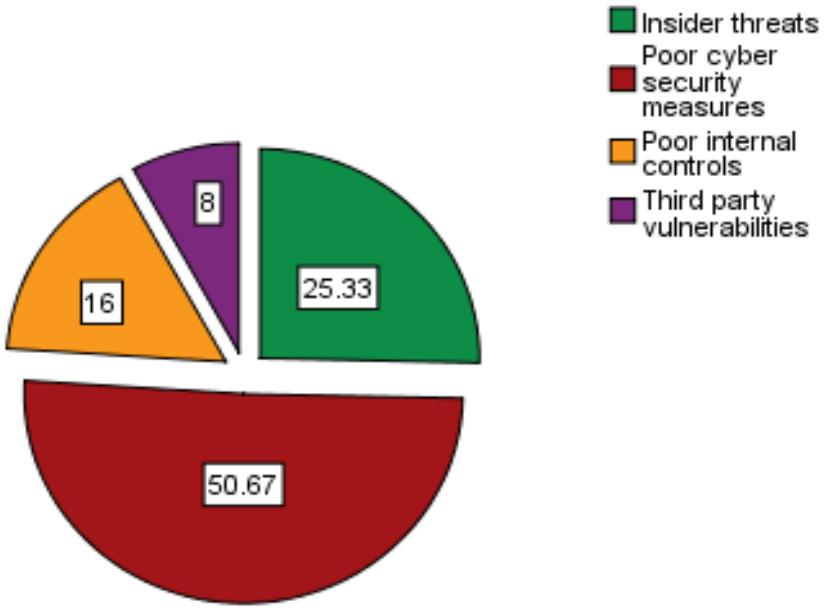
Hacking was another prevalent cybercrime encountered by Steward Bank Limited, with 14.67% reported incidents. According to Mugume (2020), hacking is the unauthoritative access to or manipulation of computer systems or networks, frequently with the goal of stealing data or causing harm to the system. The occurrence of hacking incidents highlights the potential weaknesses in the bank's cybersecurity infrastructure, which can lead to unauthorized access, data breaches, and financial losses.

4.4.5 Card fraud and identity theft

Card fraud and identity theft were also reported as notable cybercrimes faced by Steward Bank Limited. Card fraud incidents were reported at a frequency of 9.333 % while identity theft which was the least, were at a frequency of 5.333%. Card fraud involves the unauthorized use of credit or debit card information for fraudulent purposes, while identity theft refers to the fraudulent acquisition and use of personal information to impersonate individuals (Feltoe, 2019). These findings underscore the importance of robust authentication and verification mechanisms, as well as effective monitoring systems, to detect and prevent card fraud and identity theft.

4.5 Major Causes of Cybercrime in the financial sector

Figure 2: Major Causes of Cybercrime



[Source: primary data]

As shown in the figure above, the researcher asked respondents both on questionnaires and interviews about the causes of cybercrime in the financial sector. The distribution showed that poor cybersecurity measures are a major cause of cybercrimes in the financial sector with a percentage of 50.67 %. Alzahrani and Duan (2019) discovered similar results in their research on the cybersecurity challenges facing the banking sector in Saudi Arabia. The study revealed that the primary obstacles were the lack of cybersecurity regulations, the high costs associated with cybersecurity, and the lack of awareness and training for employees.

Additionally, insider threats accounted for 25.33%, which is consistent with the findings of Huang and Rustagi's (2019) study. Their research showed that insider threats pose a considerable risk to financial institutions as employees with malicious intentions may intentionally steal sensitive data or disrupt critical systems." Poor internal controls had 16% while third party vulnerabilities were the least with a percentage of 8%. Based on the findings, it was observed by the researcher that

poor cybersecurity policies and processes can potentially put financial institutions at risk of cyber threats and vulnerabilities. This may result in several unfavourable consequences, including but not limited to financial losses, damage to reputation, data breaches, and penalties from regulatory bodies.

Additionally, respondents were given the opportunity to lay out their perspectives on the various causes of cybercrime by submitting their responses in the space provided, as well as in the interview questions. Only a few respondents contributed to this question, as the majority had only experienced the causes listed in the questionnaire's closed-ended questions. Other causes stated by respondents included financial gain and high unemployment levels.

One of the interviewees stated that cybercriminals are motivated by financial gain, leading them to target financial institutions to steal either money or sensitive financial information. This statement is backed by the rational choice theory, which suggests that criminals weigh the potential benefits of committing a crime against the risks of getting caught and punished. As cybercrimes are quite challenging to detect and have the potential for significant gains, rational cybercriminals are attracted to such activities.

According to the social learning theory, people can develop the motivation and skills to commit a crime by associating with or being exposed to others who engage in criminal activities (Burruss, Holt and Bossler, 2012). This theory supports the research findings that high unemployment rates can lead individuals to turn to criminal activities like cybercrime as a way to earn money."

4.6 Cybercrime in the Bank's Operations

The respondents were asked to indicate the impact of cybercrime on the bank's operations. They were asked to rank the impact on a scale of 1 to 5, with 1 being very weak and 5 being very strong. The results are shown in Table 4.

Table 4: Impact of Cybercrime on the Bank's Operations

Variable	Frequency	Percent	Valid Percent	Cumulative %
Very Weak	3	4.0	4.0	85.3
Weak	11	14.7	14.7	100.0
Neutral	24	32.0	32.0	32.0

Strong	33	44.0	44.0	76.0
Very Strong	4	5.3	5.3	81.3
Total	75	100.0	100.0	

[Source: primary data]

As shown in Table 4, the majority of respondents 33 ranked the impact of cybercrime on the bank's operations as strong (4), followed by 24 respondents who ranked it as neutral (3). Only 4 respondents ranked the impact as very strong (5), while 11 ranked it as weak (2) and 3 ranked it as very weak (1). In the interviews conducted 4 people also ranked the impact as strong (4) and neutral (3). The research findings indicated that cybercrime causes a significant threat to the security and stability of the bank's operations.

4.7 Impact of Cybercrime on Steward Bank Limited

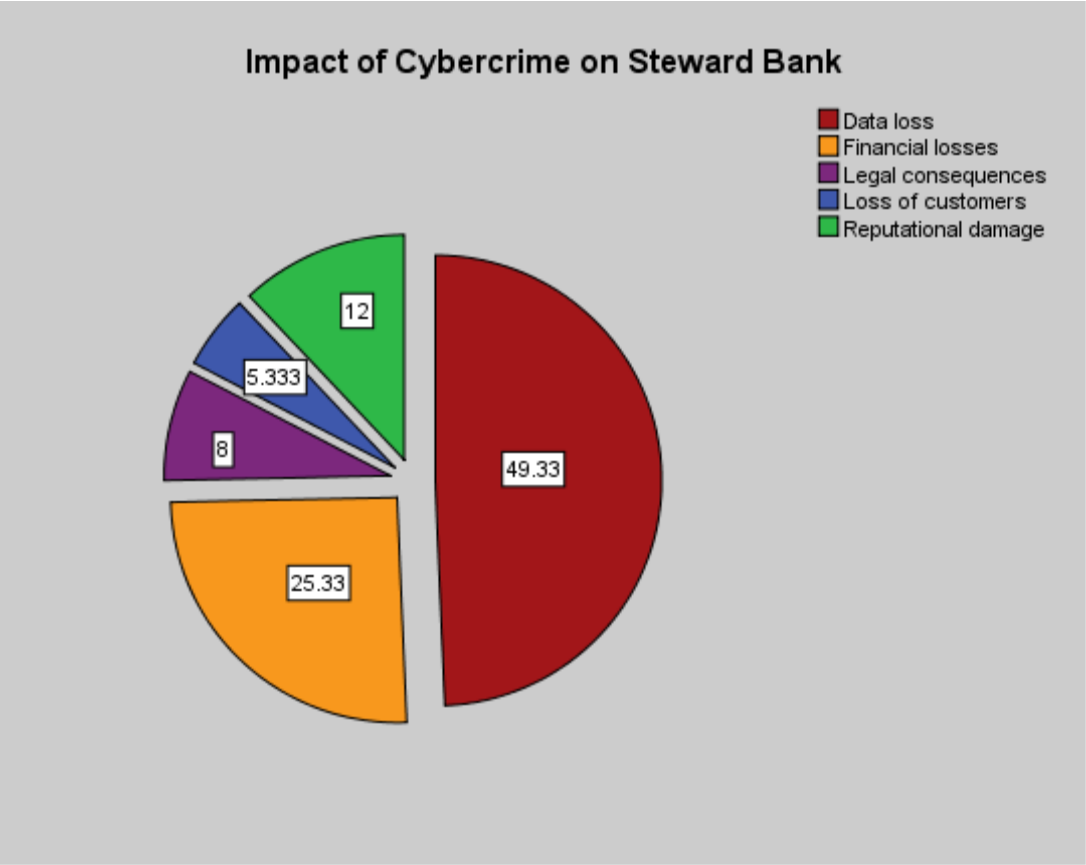
The respondents were asked to indicate which impact of cybercrime they considered to be the most significant at Steward Bank. They were asked to choose from the following options: financial losses, reputational damage, loss of customers, legal consequences, and data loss. The results are shown in Table 5.

Table 5: Most Significant Impact of Cybercrime on Steward Bank Limited

Impact	**Frequency**
Financial losses	19
Reputational damage	9
Loss of customers	4
Legal consequences	6
Data loss	37

[Source: primary data]

Figure 3: Most Significant Impact of Cybercrime on Steward Bank Limited



[Source: primary data]

From the fig above, the respondents ranked loss of data with 49.33% as the most significant impact of cybercrime at Steward Bank Limited. This was revealed by The Herald (2020), which showed that Steward Bank Limited was vulnerable to cyber-attacks, as evidenced by a data breach that occurred in 2020, which resulted in the loss of sensitive customer data. The research findings indicate that data loss is the most significant consequence of cybercrime for financial institutions. This is because these institutions hold significant amounts of sensitive customer data, including account numbers, payment details, and personally identifiable information. Losing such data may result in financial losses, harm to reputation, and legal penalties from regulators (Ponemon Institute, 2020).

Additionally financial losses was also significant with 25.33%. This was supported by Junaid and Khan (2019) in their study which explored the challenges faced by banks in Pakistan due to cybercrime. According to their findings, banks in Pakistan experience a number of challenges as

a result of cybercrimes, including monetary losses, damage to reputation, and a decline in client trust. Similarly, Mungai (2020) explored the impact of cybercrime on the performance of commercial banks in Kenya using Equity Bank Limited as a case study. Study findings were that cybercrime had a significant negative impact on the profitability, market share, and customer retention of commercial banks. Reputational damage and Legal consequences recorded 12% and 8% respectively. Loss of customers (5.333) was ranked as the least significant impact.

In interviews, some of the respondents mentioned loss of customer trust as a significant impact of cybercrime on Steward Bank Limited. These research findings can be supported by Gomes, Oliveira and Gomes (2021) in their investigation on the impact of cybercrime on financial institutions in Brazil, their findings showed that the primary challenges faced by these institutions were reputational damage, loss of customer trust, and financial loss

4.8 Measures put in place to combat Cybercrime

Table 6: Measures in place

Measures	Frequency	Percentage	Valid Percentage	Cumulative
Anti-Virus software	16	21.3	21.3	21.3
Employee training	23	30.7	30.7	52.0
Firewalls	8	10.7	10.7	62.7
Intrusion Detective Systems	10	13.3	13.3	76.0
Security policies and procedures	18	24	24	100.0
Total	75	100.0	100.0	

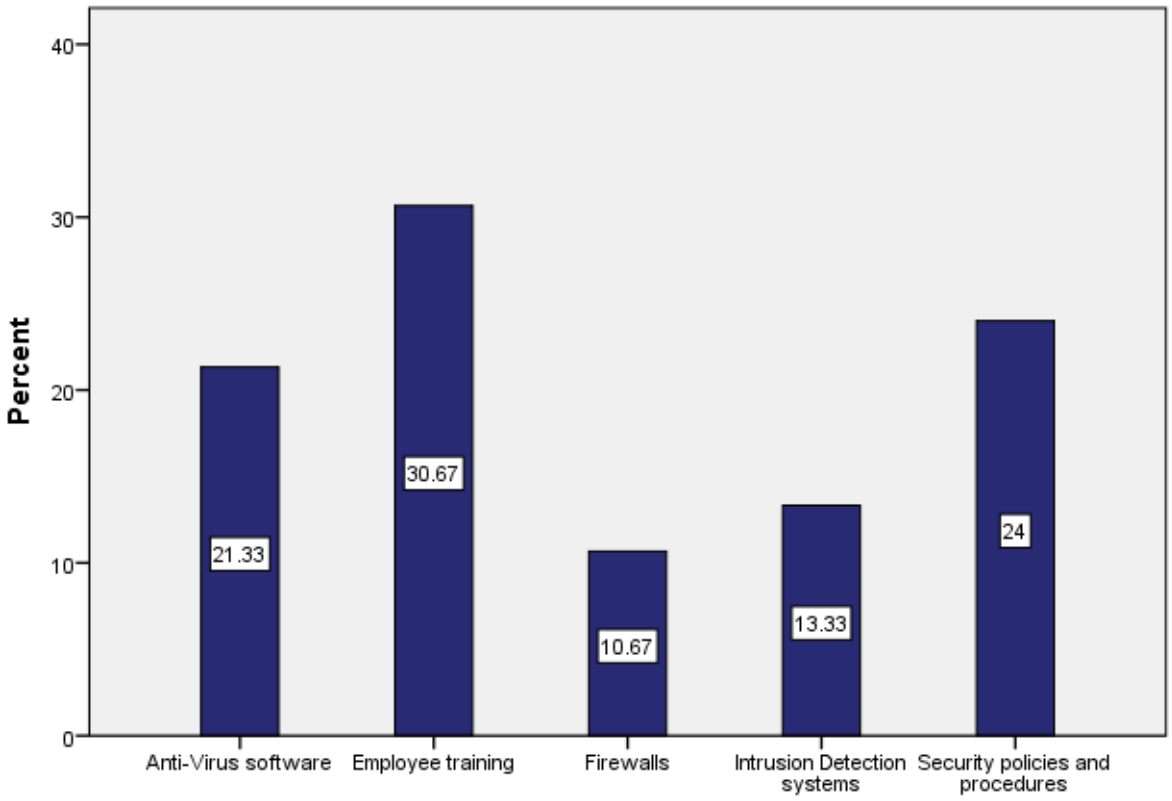
[Source: primary data]

Table 6 above shows the measures put in place by Steward Bank to combat cybercrime that were mentioned by the respondents during interviews.

4.9 Effectiveness of Measures Put in Place to Combat Cybercrime

The respondents were asked to rate the effectiveness of the measures put in place by Steward Bank to combat cybercrime. The results are presented in Figure 4 below.

Figure 4: Effectiveness of Measures to Combat Cybercrime



[Source: primary data]

Figure 4 presents the effectiveness of measures to combat cybercrime. The measures that were analysed included firewalls, intrusion detection systems, anti-virus software, security policies and procedures, and employee training. The majority of respondents rated all the measures as effective or very effective in combating cybercrime. In particular, employee training and security policies and procedures were rated the highest, with 30.67% and 24% respectively rating them as effective. The research findings indicate that the respondents believe that having well-defined security policies and procedures, as well as providing adequate training to employees, is critical in preventing cybercrime.

In terms of other measures, firewalls were rated as effective or very effective by 10.67%, while intrusion detection systems were rated as effective or very effective by 13.33%. Anti-virus software was also highly rated, with respondents rating it as effective or very effective. These

results show that the respondents consider these measures to be important in preventing cybercrime.

It is worth noting that there were a small number of respondents who rated the measures as not effective or somewhat effective. For example, one respondent during interviews rated intrusion detection systems as not effective, while two respondents rated security policies and procedures as somewhat effective. While these numbers are relatively small, they suggest that there may be some room for improvement in implementing these measures.

Overall, figure 4 provides useful insights into the perceived effectiveness of measures to combat cybercrime at Steward Bank, and suggests that the bank has implemented a range of measures that are generally seen as effective in preventing cybercrime.

4.10 Discussion of Results

The results of the study provide valuable insights into the demography of the respondents, their understanding of cybercrime, cybercrime encountered at the bank, its impact on bank operations, and the effectiveness of measures put in place to combat it. From the analysis of the demography, it can be seen that the majority of the respondents were from the finance and IT departments, as these departments are the most vulnerable to cyber threats. Also, the analysis of the understanding of cybercrime revealed that the respondents had a good understanding of cybercrime, with the majority correctly identifying the different types of cybercrime.

Additionally, the cybercrime encountered showed that phishing and malware attacks were the most prevalent types of cybercrime encountered at Steward Bank Limited. The impact of cybercrime on bank operations was found to be primarily in terms of data loss and financial losses. Analysis of the measures put in place to combat cybercrime showed that they are generally considered to be effective, with employee training and security policies and procedures, being most effective measures.

Overall, the results of the study highlight the importance of cybersecurity in the financial sector and the need for continuous efforts to combat cybercrime

4.11 Summary

This chapter analysed the data collected from the case study of Steward Bank Limited employees on the research on the challenges of cybercrime in the financial sector. The analysis covered the demography of the respondents, their understanding of cybercrime, cybercrime encountered at the bank, its impact on bank operations, the effectiveness of measures put in place to combat it, and a discussion of the results. The findings revealed that phishing and malware attacks are the most prevalent types of cybercrime encountered at Steward Bank and that the impact of cybercrime is primarily in terms of data loss and financial losses. The measures put in place to combat cybercrime are generally considered to be effective, with employee training and security policies being the most effective measures. The next chapter presents the conclusions and recommendations of the study.

CHAPTER V

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

The research focused on the challenges of cybercrime in the financial sector from 2020 to 2021, taking Steward Bank Limited as a case study. This chapter provides a summary of the research findings, conclusions, and recommendations based on the data collected throughout the study period.

5.1 Summary of the Study

This research study presented a comprehensive overview of various aspects associated with the research. Chapter One provided the background, problem statement, research objectives, questions, delimitations, and limitations. The literature review in chapter two included a theoretical and conceptual framework with relevant previous studies and an evaluation of the literature. Additionally, chapter three methodology discussed the research design, data collection tools, sample selection techniques, population studied, and the strengths and weaknesses of the instruments used. The data collected was presented in both graphical, tabular and textual formats. The final chapter provided a summary of the research findings, conclusions, and critical recommendations for all stakeholders in the financial sector.

5.2 Summary of the Major Findings

The study focused on various aspects of the challenges posed by cybercrime in the financial sector. To conduct the research, Steward Bank Limited was selected as the case study. The primary goals of the study were to identify the causes of cybercrime in the financial sector, assess the impact of cybercrime on Steward Bank, evaluate the current strategies implemented by the bank to deal with

cybercrime and provide recommendations on the best strategies that can be implemented to curb cybercrime in the financial sector.

According to the research findings, cybercrime poses a significant threat to the financial sector in Zimbabwe. That is, the research showed that respondents had a good understanding of cybercrime, with the majority correctly identifying the different types of cybercrime prevalent in the financial sector. The study revealed that phishing attacks were the most prevalent type of cybercrime encountered at Steward Bank as they recorded the highest percentage followed by malware.

The research aimed at identifying the causes of cybercrime in the financial sector and the research revealed that poor cybersecurity measures and insider threats were the major causes of cyberattacks in the financial sector. The absence of adequate cyber security measures can leave financial institutions vulnerable to cyberattacks. That is without proper security protocols, financial institutions are at risk of data breaches, ransomware attacks, and other types of cyberattacks. Also due to the human element, employees can intentionally or unintentionally expose sensitive data, steal intellectual property, or sabotage systems.

In addition, the study findings showed that the most significant impact of cybercrime on Steward Bank Limited was data loss, followed by financial losses. Financial institutions are responsible for the protection of their clients' information, and any violation of this responsibility can result in loss of trust, damage to reputation and potential legal implications. Additionally, financial institutions may suffer financial losses due to the interruption of crucial operations or embezzlement of funds.

The other objective was to evaluate the strategies utilized by Steward Bank Limited to curb cybercrime in the financial sector and the research study showed that the current measures utilized by Steward Bank Limited are generally considered to be effective, with employee training and security policies and procedures, being the most effective measures. Finally, the identification of the challenges of cybercrime in the financial sector gave way for some effective measures to be crafted which may assist in mitigating the prevalent cybercrimes affecting financial institutions. Developing a comprehensive cybersecurity strategy, use of multi-factor authentication for all critical systems and data, regularly updating software and systems, conducting regular vulnerability assessments, penetration testing, partnering with cybersecurity experts and also to stay informed about emerging cyber threats and trends in the cybersecurity landscape. All these are suggested as potential solutions that will act as a barrier in minimizing phishing and other

related cyber threats that may be done through the network. Also, internal controls are as well an effective method of enforcing stricter systems and policies.

5.3 Conclusion

Based on the research undertaken on the challenges of cybercrime in the financial sector, the researcher concludes that although there are many types of cybercrimes in the financial sector, phishing was considered the most prevalent followed by malware, hacking, identity theft then card fraud. The major cause of cybercrime in the financial sector was poor cybersecurity measures. Also, data loss was the most intense that affected the bank's operations. Financial losses, reputational damage, legal consequences and loss of customers were other recorded impacts.

The financial sector is a prime target for cyberattacks, and due to the increased pace of technological advancements, it is crucial for financial institutions to take proactive measures to prevent and mitigate cyber threats. This includes implementing strong cybersecurity measures, training employees on cybersecurity best practices and constantly evaluating and updating the cyber security policies as well as strategies.

5.4 Recommendations

In light of the above conclusions, this study came up with critical recommendations for all stakeholders in the financial sector.

5.4.1 To Financial Institutions

Based on conclusions drawn from the study, financial institutions must establish a thorough cybersecurity strategy that encompasses policies, procedures, and controls to handle cyber risks throughout the organization. It is also essential to train employees on cybersecurity and employ multi-factor authentication for all critical systems and data. Updating software and systems regularly to safeguard against known vulnerabilities is a must. Conducting regular vulnerability assessments, penetration testing, and having a robust incident plan are also crucial in financial institutions. Finally, partnering with cybersecurity experts, staying informed about emerging cyber threats, and monitoring trends in the cybersecurity landscape is essential. By adhering to these recommendations, financial institutions can improve their cybersecurity posture and better defend

themselves against cyber threats. It is important to keep in mind that cybersecurity is a continuous process that necessitates ongoing vigilance and attention to stay ahead of evolving threats.

5.4.2 To Customers

To safeguard against cyber threats, customers should create strong and distinct passwords and activate multi-factor authentication for all online accounts that offer this feature. This will offer an additional level of security in case a password is exposed. Furthermore, they should be wary of suspicious emails, phone calls, or text messages that ask for personal or financial information. It is also recommended that they regularly check bank and credit card statements for unauthorized transactions and utilize secure websites for all online transactions.

5.4.3 To the Government

Governments should allocate resources towards cybersecurity research and development to enhance cybersecurity technologies and solutions and keep up with emerging threats in the cybersecurity landscape. They must also create a cyber-incident response plan, regularly assess cybersecurity, and establish awareness campaigns that will educate the public on cybersecurity risks and best practices. Additionally, they should promote international cooperation on cybersecurity to share threat intelligence and best practices and to collaborate on joint cybersecurity initiatives. By implementing these measures, governments can help safeguard the financial sector against cybercrime.

5.5 Recommendations for Further Study

As technology continues to progress and more facets of our lives become linked to the internet, cybercriminals are expected to become more advanced in their techniques, making it increasingly challenging for individuals, organizations, and governments to combat them. As a result, it is crucial for organizations to continually assess and keep their cybersecurity measures up to date. Future research should concentrate on evaluating the effectiveness of cybersecurity measures implemented by financial institutions and identifying areas for enhancement. Additionally, an analysis of cybersecurity measures across various nations to identify best practices and areas for improvement would be beneficial.

REFERENCES

Ahmed, S., Islam, M. M. and Al-Sayed, A. (2021) *Cybersecurity challenges and mitigation strategies for financial institutions: A review*, Journal of Financial Crime, 28(1), 1-20.

Akimori, S. (2021) *Cybercriminals had the perfect opportunity to target systems and networks of individuals and businesses*. Available at: https// ulyaoth.com/security/cybercrime-in-the-financial-sector. Accessed: 12 April 2022.

Alzahrani, A. I. and Duan, Y. (2019) *Cybersecurity challenges faced by banks in Saudi Arabia*, Journal of Financial Crime, 26(3), 773-785.

Accenture and Ponemon Institute. (2017) *The cost of cybercrime study*. Ponemon Institute. Available at: <https://www.accenture.com/_acnmedia/PDF-62/Accenture-2017 CostCybercrime. Accessed: 15 August 2022.

Aakker, K. (1998) *Survey Methods*. MacMillan.

Ary, D., Jacobs, L.C., Sorensen, C. K. and Walker, D. A. (2010) *Introduction to Research in Education*. Cengage Learning.

Bawane, J. and Stelke, R. (2014) *Hacking techniques and preventive measures: A detailed study*, International Journal of Advanced Research in Computer Science and Software Engineering, 4(10), 1031-1038.

Boateng, R. and Amanor, C. (2014) *Phishing and Vishing: A growing threat to e-commerce*, International Journal of Advanced Research in Computer Science and Software Engineering, 4(8), 578-584.

Bollen, L. and Delaney, K. (2018) *Cybersecurity and financial institutions: A survey of the literature*, Journal of Financial Crime, 25(1), 92-105.

BlackFog. (2019) *The Business of Cybercrime.* Available at: https://www.blackfog.com/the-business-of-cybercrime/. Accessed: 15 August 2022.

Broadhurst, R. (2006) *Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime*. Surveillance & Society, 3(3), 1-19.

Broadhurst, R. (2006) *Cybercrime: The challenge for the criminal law,* Journal of International Commercial Law and Technology, 1(1), 1-12.

Borg, J. and Gall, T. (2012) *Does Organizational Structure Influence the Success of Its Electronic Banking Systems,* Business Process Management Journal.

Boudriga, N. (2010) *Firewall. In The Handbook of Information Security* (pp. 469-480). John Wiley & Sons.

Blaxter, L., Hughes, C. and Tight, M. (2006) *How to Research*. (3rd Ed.) New York: McGraw-Hill Education.

Burruss, G.W., Holt, T. J. and Bossler, A. M. (2012) *Learning to hack: Criminological characteristics of offenders in juvenile hacker networks,* Deviant Behavior, 33(1), 1-20.

Chandhary, H. (2014) *An overview of phishing and pharming attacks*, International Journal of Advanced Research in Computer Science and Software Engineering, 4(11), 123-126.

Claybaugh, Zach (2020) *"Research Guides; Organising Academic Research Papers; Types of Research Designs"*. Available at: library.sacredheart.edu. Accessed: 20 March 2023.

Cooper, D. R. and Schindler, P. S. (2003) *Business Research Methods.* 8th Edition Irwin, Boston: McGrawHill.

Cole, G. F. and Pontell, H. N. (2006) *Cybercrime and society.* Los Angeles, CA: Sage Publications.

Cooper, H. M. (1998) *"Synthesizing research: A guide for literature reviews."* Sage Publications.

Council of Europe. (2013) *Convention on cybercrime. United Nations Office on Drugs and Crime.*Availableat:https://www.unodc.org/documents/cybercrime/UN_Convention_Against_Cybercrime.pdf. Accessed: 15 February 2023.

Christiane, F. (2005) *WordNet and WordNet's. In: Brown, Keith et al*. (eds.). 2nd Edition, Oxford: Encyclopedia of Language and Linguistics.

Criminal Codification and Reform Act. (2018) Revised edition. Section 163. Zimbabwe.

Crawshaw, J. and Chambers, J. (2003) *A concise course on advanced level statistics.*4thEdition UK: Stanley Thormes (Publishers) ltd.

CrowdStrike Intelligence. (2022) Global Threat Report. Available at: https://www.crowdstrike.com/resources/reports/global-threat-report/ Accessed: 19 August 2022.

Crossman, A. (2016) *Purposeful Sampling in Qualitative Research*. ThoughtCo. Available at: https://www.thoughtco.com/purposeful-sampling-373318. Accessed: 07 April 2023.

Chikwati, E. and Mahere, S. (2021) *Insider threat management: A panacea for cybercrime in the financial sector,* Journal of Cybersecurity Research, 6(1), 1-10.

Clickatell. (2018) *Two-factor authentication (2FA) and one-time PIN (OTP) verification solutions.* Available at:https://www.clickatell.com/articles/mobile-marketing/two-factor-authentication-2fa-and-one-time-pin-otp-verification-solutions/ Accessed: 12 July 2022.

Douglas, M. and Loader, B. (2000) *Cybercrime: The new face of deviance*. In M. Douglas & B. Loader (Eds.), Inventing Criminology (pp. 161-184). Sage Publications.

Europol. (2014) *Phishing.* European Cybercrime Centre. Available at: https://www.europol.europa.eu/activities-services/main-reports/phishing. Accessed: 08 July 2022.

Edelman. (2021). *Edelman Trust Barometer 2021*. Available at: https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021-edelman-trust-barometer.pdf. Accessed: 19 March 2023.

Feltoe, G. (2019) *Credit Card Fraud: A Legal Perspective,* Journal of Internet Banking and Commerce, 24(1), 1-16.

Fink, A. (2014) *Conducting research literature reviews: From paper to the internet*. Sage publications.

Fink, A. and Arlene. (2005) *The survey handbook*. Sage publications.

Gomes, A. C., Souza, R. M., de Paula, T. A. and Monteiro, F. C. (2021) *Cybersecurity in the Brazilian financial sector: Perceptions of risk and preparedness,* Journal of Financial Crime, 28(2), 406-418.

Gomes, E. S., Cruz, J. B. D., Sousa, P. V. D. and Albuquerque, J. P. D. (2021) *Challenges and opportunities of cybersecurity in financial institutions in Brazil*, Journal of Financial Crime, 28(1), 159-173.

Gordon, S. E. and Ford, R. C. (2006) *Cybercrime: The transformation of crime in the information age.* Crime and Justice, 34(1), 1-52.

Gumbo, T., Chisango, F. and Musodza, K. (2018) *Cybercrime in Zimbabwe: Trends, challenges and recommendations,* International Journal of Cyber Criminology, 12(2), 569-583.

Grabosky, P. and Smith, R. (2001) *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities.* Transaction Publishers.

Hedayati, H. (2012) *Social engineering and its impact on computer security*, International Journal of Computer Applications, 52(2), 1-7.

Herselman, M. and Warren, M. (2010) *Securing the cloud: Security concerns for cloud computing,* In Proceedings of the International Conference on Computer Security and Applications (pp. 372-378).

Hoofnagle, C. J. (2009) *Big Brother's little helpers: How choicepoint and other commercial data brokers collect and use personal information*. University of Illinois Law Review, 2009(1), 77-108.

Holt, T.J. and Smirnova, O.V. (2015) *'The Rational Choice Theory and Its Application to Cybercrime', in Jaishankar, K. (ed.) Cyber Criminology: Exploring Internet Crimes and Criminal Behavior.* Boca Raton, FL: CRC Press, pp. 53-68.

Huang, Y. and Rustagi, N. (2019) *Insider threats in financial institutions*, Journal of Financial Crime, 26(3), 641-654.

Hutchings, A. and Hayes, N. (2009) *Exploring the relationship between phishing and identity theft: A comparative analysis of financial institutions and web-based e-commerce businesses,* Information Management & Computer Security, 17(1), 5-30.

Isaac, B., Chiong, R. and Jacob, S. M. (2006) *Analysis of Phishing Attacks and Countermeasures.* Information Security Researching. Kuching, Malaysia.

IBM. (2021) *Cost of a Data Breach Report 2021*. IBM Security. Available at: https://www.ibm.com/security/data-breach. Accessed: 20 March 2023.

Jaishankar, K. (2007) *Cyber criminology: Evolving a novel discipline,* International Journal of Cyber Criminology, 1(1), 1-4.

Jaishankar, K. (2008) *Understanding lone wolf terrorism: Global patterns, motivations and prevention.* Springer Science & Business Media.

Jones, A. and Lee, B. (2018) *'Zimbabwean financial institutions are vulnerable to cyberattacks'*, Journal of Cybersecurity, 3(2), pp. 87-103.

Junaid, M. and Khan, M. A. (2019) *Cybercrime and challenges faced by banking sector in Pakistan*, Journal of Financial Crime, 26(4), 1074-1090.

Kashuwa, A. (2021) *Types of Cybercrime*. Available at: <https://www.ictcatalogue.com/types-of-cybercrime/> Accessed: 17 March 2023.

Kenton,W.(2021)*Financialsector*.Investopedia.Availableat:https://www.investopedia.com/terms/f/financialsector.asp.on. Accessed: 20 October 2022.

Kirshenblatt- Gimblett, Barbara. (2006) *Part 1, What is Research Design? The Context of Design.* Performance Studies Methods Coirse syllabus. New York University: Spring.

King'oriah, J.E. (2004) *Research methodology: A step-by-step guide for beginners.* Nairobi: Kenya Literature Bureau.

Kothari, C.R. (2004) *Research methodology; methods and techniques.* 2nd Edition. . New Delhi: New age international publishers.

KPMG. (2011) *Global report on the cost of cybercrime.* Available at: https://assets.kpmg/content/dam/kpmg/pdf/2011/11/Global-Cyber-Crime-Survey-Report-2011.pdf. Accessed: 09 March 2023.

KPMG. (2012) *Credit card fraud*. Available at: https://assets.kpmg/content/dam/kpmg/pdf/2012/12/Credit-card-fraud.pdf. Accessed: 12 March 2023.

Kshetri, N. (2018) *Blockchain's roles in meeting key supply chain management objectives*, International Journal of Information Management, 39, 80-89.

Lambert, M. (2012) *"A beginner's guide to conducting a literature review."* .Nursing Times, 108(23), 20-23.

Laudon, K. C. (2009) *E-Commerce 5th Edition*. New York University: Pearson.

Laura. (2022) *What is Antivirus Software? How Does it Work?* Norton Life Lock .Available at: https://us.norton.com/internetsecurity-malware-what-is-antivirus.html. Accessed: 17 March 2023.

Leary, M. R. (2001) *Introduction to Behavioral Research Methods*. Boston, MA: Pearson Education.

Magutu, O., Njenga, K. and Kariuki, S. (2011) *Cybercrime in the banking sector: A review of the threats and vulnerabilities,* International Journal of Information and Communication Technology Research, 1(8), 417-426.

Meade, T. (2019) *Cyber Security News: what is an Antivirus Software.* Coloration America. Available at: https://www.colocationamerica.com/blog/differences-between-firewall-andantivirus Accessed: 13 February 2023.

Mugume,R.(2020)*Cybercrime:Hacking*.Availableat:<https://www.urcs.or.ug/2020/06/10/cybercrime-hacking/> Accessed: 15 March 2023.

Muhumuza, R. and Tumuheki, P. (2020) *Cyber security threats in Uganda's financial institutions,* Journal of Financial Crime, 27(1), 201-213.

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. Vol. 7, No 3 S1.

Myers, M. D. (2009) *Quantitative Research in Business and Management*. London: SAGE Publications Ltd.

McNally, R. J. and Newman, J. P. (2008) *The psychology of cybercrime*. In R. C. Davis, A. J. Lurigio, & S. Herman (Eds.), Victims of crime (4th ed., pp. 231-244). Thousand Oaks, CA: Sage Publications.

Ncube, M. (2020) *Cybercrime challenges facing the financial sector in Zimbabwe*, International Journal of Advanced Research in Computer Science and Software Engineering, 10(5), 314-321.

Nfuka, E. N., Sanga, C. and Mshangi, K. A. (2014) *Cybercrime: A Review of the Evolving Definition of the Term,* Journal of Computer Science & Systems Biology, 7(1), 27-32.

Ozarslan, S. (2022) *Cybersecurity in Financial Services: A Review,* Journal of Financial Crime, 29(1), 235-246. Available at: doi: 10.1108/JFC-11-2020-0205. Accessed: 20 June 2022.

Paget, T. (2007) *The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy.* Syngress.

Payne, B. (2013) *Crime and punishment in cyberspace: An unauthorized access theory of hacking.* American University Law Review, 62(4), 889-934.

Ponemon Institute. (2021) *Cost of a data breach report 2021*. Available at: https://www.ibm.com/security/data-breach. Accessed: 19 April 2023.

Robson. (2002) *A Resource for Social Scientists and Practitioners-Researchers*. London: Blackwill Publishers.

Remeny, E. (2001) *Literature reviews and research: A review*, Journal of the Academy of Marketing Science, 29(4), pp.436-453.

Roger, A. (2008) *'Phishing: A New Cybercrime'*, International Journal of Cyber Criminology, 2(2), pp. 339-347.

Reserve Bank of Zimbabwe. (2018) *Cybercrime in Zimbabwe and Globally*. Available at: RBZ Web site: www.rbz.co.zw/assets/cybercrime-globally-and-in-zimbabwe.pdf. Accessed: 20 May 2022.

Sarannia, A. R. and Padma, K. R. (2014) *A survey of phishing detection techniques*, International Journal.

Sarrab, M., Sibai, F., Serhrouchni, A. and Ferrag, M. A. (2013*) A survey of cybercrime in Lebanon,* Journal of Information Security, 4(4), 248-261.

Sonepat, S. and Sonepat, M. (2014) *Credit Card Fraud: A Review*, Journal of Indian Research, 2(4), 45-50.

Schostak, J. F. (2006) *Understanding Interviews*. SAGE Publications.

Sharma, P. and Nanda, S. (2006) *Credit card frauds: A critical review of the literature*, Global Business Review, 7(2), 195-217.

Stallings, W. and Brown, L. (2015*) Computer security: principles and practice*. Pearson

Smith, J. (2017) *The growth of cybercrime and its impact on the financial sector*, Journal of Financial Crime, 24(2), 215-223. Available at doi: 10.1108/JFC-01-2017-0004. Accessed: 20 June 2022.

Smith, M. (2019) *Cybercrime a rising threat in Zimbabwe's financial industry*. Available at: https://www.iol.co.za/business-report/international/cybercrime-a-rising-threat-in-zimbabwes-financial-industry-34745405. Accessed: 09 August 2022.

Symantec. (2015) *Encryption: A necessary step towards data security*. Available at: https://www.symantec.com/content/dam/symantec/docs/white-papers/encryption-a-necessary-step-towards-data-security-en.pdf. Accessed: 12 March 2023.

The Fintech Times. (2021) *Wipro: Why are Financial Services a prime target for Cybercrime.* Available at: https// the fintechtimes.com/wipro/why are financial services a prime target for cybercrime. Accessed: 15 July 2022.

The Herald. (2020, 29 September) *Steward Bank data breach raises cyberattack fears*. The Herald. Available at: https://www.herald.co.zw/steward-bank-data-breach-raises-cyberattack-fears/. Accessed: 24 March 2023.

Thomas, P. and Loader, B. D. (2000) *Cybercrime: law enforcement, security and surveillance in the information age.* Routledge.

Trachoma, W. M. K. (2006) *Sampling.* Available at: http://www.socialresearchmethods.net/kb/sampling.php. Accessed: 17 February 2023.

United Nations Office on Drugs and Crime. (2017) *Comprehensive Study on Cybercrime*. United Nations Publications.

United Nations Office on Drugs and Crime. (2010) *Comprehensive study on cybercrime*. Available at:https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2010/CYBERCRIME_STUDY_2010_small_.pdf. Accessed 10 March 2023.

Uppal, M., Chhabra, P. and Singh, S. (2014) *An analysis of different types of malware and their classification,* International Journal of Advanced Research in Computer Science and Software Engineering, 4(10), 356-359.

Vivek, Kumar and Verma. (2014) *Phishing.* Available at: < https://indiancaselaw.in/phishing/> Accessed: 7 March 2023.

Wada, F. and Odulaja, A. (2012) *The impact of rational choice theory on cybercrime research: A theoretical analysis,* International Journal of Cyber Criminology, 6(2), 773-788.

Wegner, E. C. (1995) *Morale in old age: Redefining the model:* Oxford, UK

Weiner, J. (2007) *Measurement: Reliability and Validity Measures*. Bloomberg: John Hopkins University.

Wittek, R. (2003) *The rational choice theory.* In G. Ritzer (ed.), Handbook of social theory (pp. 81-100). Sage Publications.

Wright, A. (2015) *Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime,* International Journal of Cyber Criminology, 9(1), 1-21.

Yar, M. (2005) *Cybercrime and society*. Sage.

APPENDICES

APPENDIX 1: INFORMED CONSENT LETTER

Bindura University of Science Education
Department of Financial Intelligence
P. Bag 1020
Bindura
May 2023

RE: RESEARCH PROJECT ASSISTANCE

Dear Respondent

I am a final year student at the abovementioned University pursuing a Bachelor of Commerce (Honours) in Financial Intelligence. I'm conducting research on; **Challenges of Cybercrime in the financial sector: A case study of Steward Bank Limited from 2020-2021**. I sincerely request your assistance in completing the following questionnaire so that this research can be effective in gathering pertinent data. Prior approval to conduct this study with the school as a case in point has been attained from the administration.

The researcher consequently requests you to voluntarily participate in this study and to be as honest as possible in answering the questions. Should you wish not to participate, then you should not respond to the questionnaire. The researcher wishes to assure you that your identity will not be revealed to any person(s) and your responses will be regarded as confidential. The information you provide will not be used outside its intended purpose.

In order to do justice to the said investigation, please complete the questionnaire to the best of your knowledge and ability. Please do not write your name on any part of the questionnaire. The questionnaire takes about ten minutes to complete.

Instructions

For your answers, you are kindly asked to tick in the box resembling your response or simply fill in the spaces provided.

Disclaimer: I hereby consent to participate in this research and I confirm that I have read the above information and agree with it.

Place: …….

Date: …….

Sign: …….

Please feel free to contact the following for further information about this:

+263 783 936 677, or email

chimbwandachelsea@gmail.com

Yours faithfully
Chelsea Chimbwanda

APPENDIX 2: QUESTIONNAIRE

SECTION A: PERSONAL BACKGROUND

Please put a tick [□] on the appropriate box, and where possible, include an explanation

1. PLEASE INDICATE YOUR GENDER:

a. Male [ ]

b. Female [ ]

2. PLEASE INDICATE YOUR AGE RANGE:

a. < 18 years [ ]

b.18 – 25 [ ]

c.26 – 35 [ ]

d.36 – 45 [ ]

e. 46 years > [ ]

3. CAN YOU SPECIFY YOUR ACADEMIC QUALIFICATION(S)?

a. O & A [ ]

b. Certificate [ ]

c. Diploma [ ]

d. Undergraduate [ ]

e. Postgraduate [ ]

OTHER (please specify) ……....

……

4. POSITION HELD IN THE COMPANY:

……

5. PERIOD OF HOLDING SUCH OFFICE:

a. 2 years and below [ ]

b. 2 – 5 years [ ]

c. 6 – 10 years [ ]

d. 10 years and above [ ]

6. IN WHICH DEPARTMENT ARE YOU EMPLOYED?

a. Risk Management [ ]

b. Internal Audit [ ]

c. Finance Operations [ ]

d. IT department [ ]

SECTION B

7. WHAT DO YOU UNDERSTAND BY THE TERM CYBERCRIME?

……

……

……

……

8. WHICH TYPES OF CYBERCRIME HAS STEWARD BANK LIMITED ENCOUNTERED?

a. Phishing [ ]

b. Hacking [ ]

c. Malware [ ]

d. Card Fraud [ ]

e. Identify Theft [ ]

9. OUTLINE ANY OTHER TYPES OF CYBERCRIME STEWARD BANK LIMITED HAS ENCOUNTERED IN THE PAST APART FROM THE ONES MENTIONED ABOVE?

……

……

……

……

10. AMONG THE FOLLOWING, WHAT WOULD YOU CONSIDER TO BE THE MAJOR CAUSES OF CYBERCRIME IN THE FINANCIAL SECTOR?

a. Poor cybersecurity measures [ ]

b. Third-party vulnerabilities [ ]

c. Poor internal controls [ ]

d. Insider threats [ ]

11. APART FROM THE ABOVE, WHAT WOULD YOU CONSIDER TO BE THE OTHER MAJOR CAUSES OF CYBERCRIME IN THE FINANCIAL SECTOR?

……

……

……

……

12. WHAT IMPACT DO YOU THINK CYBERCRIME HAS ON THE BANK'S OPERATIONS?

Please give a ranking below by use of a tick (□)

Very Weak **(1)**	**Weak** **(2)**	**Neutral** **(3)**	**Strong** **(4)**	**Very Strong** **(5)**

13. AMONG THE FOLLOWING, WHICH ONES WOULD YOU CONSIDER TO BE THE MOST SIGNIFICANT IMPACT OF CYBERCRIME ON STEWARD BANK LIMITED?

a. Financial losses [ ]

b. Reputational damage [ ]

c. Loss of Customers [ ]

d. Legal Consequences [ ]

e. Data Loss [ ]

14. APART FROM THE ABOVE, WHAT WOULD YOU CONSIDER TO BE THE OTHER IMPACT OF CYBERCRIME ON STEWARD BANK?

……

……

……

……

15. WHAT MEASURES HAVE BEEN PUT IN PLACE BY STEWARD BANK LIMITED TO DEAL WITH CYBERCRIME?

……

……

……

……

16. HOW EFFECTIVE ARE THE MEASURES YOU MENTIONED ABOVE?

Please give a ranking below by use of a tick (□)

Not Effective (1)	**Somewhat Effective (2)**	**Effective (3)**	**Very Effective (4)**

17. WHAT OTHER STRATEGIES WOULD YOU SUGGEST TO DEAL WITH CYBERCRIME IN THE FINANCIAL SECTOR?

……

……

……

……

Thank you for your time!

Your participation it is greatly appreciated

APPENDIX 3: INTERVIEW GUIDE

Challenges of Cybercrime in the financial sector: A Case study of Steward Bank Limited from 2020 – 2021.

1. What position are you currently holding at Steward Bank Limited?

2. Which cybercrimes do you think are prevalent in the financial sector?

3. What would you consider to be the major causes of cybercrime in the financial sector?

4. What impact do you think cybercrime has on the bank's operations?

5. What do you consider to be the most significant impact of cybercrime on Steward Bank Limited?

6. What strategies have been put by Steward Bank Limited to deal with cybercrime?

7. How effective have these strategies been?

8. What do you think can be done by the financial sector players to curb cybercrime?

Thank you