BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

CYBERCRIMES AND THEIR IMPACTS ON NATIONAL SECURITY A CASE STUDY OF ZB BANK

BY

LEON KUDZAISHE GUMBO

(B201877B)

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

APPROVAL FORM

The undersigned confirms that they have read and recommended this research project entitled,

"Cybercrimes and their impacts on national security" in partial

Fulfilment of the Bachelor of Commerce Honours Degree in Financial Intelligence.

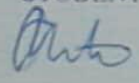
I certify that I have supervised LEON KUDZAISHE GUMBO B201877B for this research titled,

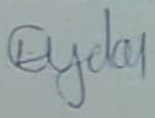
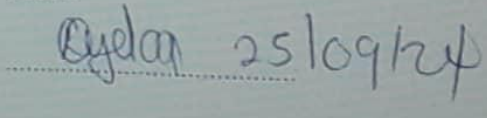
"Cybercrimes and their impacts on national security ", in partial

Fulfilment of the Bachelor of Commerce Honours Degree in Financial Intelligence, and

recommends that it proceed for examination.

SUPERVISOR  DATE 25/09/2024

STUDENT  DATE 25/09/2024

CHAIRPESON  DATE 

ABSTRACT

This dissertation examines the impact of cybercrime on national security, with a particular focus on ZB Bank in Zimbabwe. The study reviews existing literature on the types of cybercrimes, their global trends, and the countermeasures against them. The research identifies the types of cybercrime that ZB Bank is vulnerable to and assesses their impact on the bank's national security. The study proposes countermeasures that the bank can undertake to prevent and mitigate the impact of cybercrime. The research used a qualitative method that relied on secondary data sources such as journals, reports, and other published materials, and analyzed them using thematic content analysis. The study was guided by the following objectives: to investigate the nature of cybercrimes impacting the banking industry, to establish the extent of cybercrimes' impact on the banking industry and national security, to explore the measures that ZB Bank has put in place to mitigate the impact of cybercrimes on national security and to make recommendations for the improvement of cybersecurity measures in ZB Bank to strengthen national security. The findings of the study indicate that cybercrime poses a significant threat to national security and can lead to severe harm to critical infrastructure, such as financial systems, power grids, and emergency services. The study recommends that ZB Bank should implement various countermeasures such as investing in cybersecurity infrastructure, providing cybersecurity training to employees, and enhancing international cooperation to combat cybercrime. The research contributes to existing literature on cybersecurity and cybercrime and is significant to policymakers, financial institutions, and other stakeholders interested in the impact of cybercrime on national security.

ACKNOWLEDGMENTS

Undertaking this research project was a challenging and demanding task, and I am deeply grateful to have had the support and guidance of Mr Chitima, my lecturer and supervisor, throughout the entire process. Mr Chitima provided me with an invaluable opportunity to engage in this research, and I am grateful for his belief and confidence in me. Despite facing moments of self-doubt and frustration, Mr Chitima consistently encouraged and motivated me to keep going, providing me with the necessary guidance and direction to steer me back on track. His patience and wisdom was remarkable and I felt reassured and supported at every stage of the research project. I am truly grateful for the exceptional guidance and support that Mr Chitima provided me throughout this journey.

I also want to extend my gratitude to my mother and big sister for their maximum support throughout the whole journey

DEDICATION

I dedicate this dissertation to my mother and sister, who have been my pillars of support throughout my academic journey. Their unwavering love, guidance, and encouragement have been invaluable in helping me to achieve my educational goals. They also have been my source of inspiration and motivation, thank you for your unwavering support and for always pushing me to be my best self.

Table of Contents

Contents

CHAPTER I

Introduction.

Chapter one provides information on the nature of cybercrimes and their impacts on national security in banking sector. This chapter focused on the study's background, problem statement, objectives, research questions, significance, assumptions, delimitations, limitation, definition of key terms and summary of the study.

1.1 Background of the study

The rise of technology has brought about a significant increase in cybercrime, posing a threat to national security and the global economy. Cybercrime refers to criminal activities committed using digital devices, networks, and other forms of technology (Mackenzie & McNicholas, 2019). Cybercriminals take advantage of the interconnectedness of the internet and technology to carry out their malicious activities. These activities include hacking, phishing, identity theft, and malware attacks, among others.

With the growing digitization of financial services, banks have become prime targets for cybercriminals (Debabi, 2019). The banking industry is particularly vulnerable to cyberattacks due to its reliance on technology and the sensitive financial information it holds. Financial institutions are always a prime target for cybercriminals as they hold vast amounts of confidential and valuable data. Banks hold sensitive information such as personal identification information, account numbers, and transaction data that cybercriminals seek to exploit.

ZB Bank, one of the leading banks in Zimbabwe, has been a target for cybercrimes and cyber threats, experiencing several cyber-attacks over the years (Tarisayi & Mwanza, 2021). Cybercriminals target banks for multiple reasons, including financial gain, ransomware attacks,

and political motivations. The attacks can be internal or external and can come from individuals, criminal organizations, and state-sponsored entities.

ZB Bank has implemented various strategies to mitigate the risks associated with cybercrime. These include enhancing the bank's security protocols, establishing a cybersecurity framework,

and providing continuous employee training. Additionally, the bank has established a dedicated cybersecurity team responsible for the implementation and management of the bank's cybersecurity program and policies.

1.2 Statement of the problem

The rise of cybercrime has brought about significant challenges for financial institutions, including ZB Bank. Cybercriminals have found innovative ways to exploit loopholes in security systems, resulting in financial losses to organizations, reputational damage, and damage to customer confidence (Akhtar, Sattar & Bakht, 2018). The high rate of cybercrime in the banking industry poses a considerable threat to national security, which can lead to individual and institutional financial losses, affect the country's economic stability, among other factors (Ahmad, 2016).The primary problem, therefore, is how cybercrimes impact national security, with ZB Bank as a case study.

1.3 Research objectives

The overall objective of the study is to examine the impact of cybercrime on national security. The specific objectives include:

i. To investigate the nature of cybercrimes impacting the banking industry.
ii. To establish the extent of cybercrimes' impact on the banking industry and national security.
iii. To explore the measures that ZB Bank has put in place to mitigate the impact of cybercrimes on national security.
iv. To make recommendations for the improvement of cybersecurity measures in ZB Bank to strengthen national security.

1.4 Research questions

The research intended to answer the following questions

i. What are the types of cybercrimes that have impacted the banking industry, particularly in Zimbabwe, and how have they affected national security?
ii. To what extent have cybercrimes impacted the banking industry and national security in Zimbabwe, and what are the associated risks?
iii. What measures are banks, including ZB Bank, putting in place to mitigate the impact of cybercrimes on national security?
iv. Are there gaps in the cybersecurity measures put in place by ZB Bank, and how can they be addressed to improve national security?

1.5 Justification of the study

The research results will contribute to the body of knowledge on cybersecurity and cybercrimes and provide insights into their impact on national security to the student, banking sector, nation and university,

1.5.1 to the student

The student will gain a thorough comprehension of research methodology and gain valuable research skills through conducting this study, serving as both a training ground and an opportunity for growth.

1.5.2 to the banking sector

The findings of this study can be utilized by the banking sector in Zimbabwe to modify their operations and combat cybercrime.

1.5.3 to the nation

The study's findings will be helpful to policymakers and relevant authorities in Zimbabwe and other countries grappling with cybersecurity threats. The research will shed light on the implications of cybercrime on national security and the economy, providing guidelines for improving cybersecurity measures

1.5.4 to the university

The study's results can serve as a reference for future works by students at Bindura University of Science Education who may conduct related research. Additionally, the research is expected to provide insights into the effects of cybercrime on financial institutions in Zimbabwe.

1.6 Assumptions of the study

This study was guided by the following assumptions;

- The researcher assumes that the progress in technology leads to a rise in cybercrimes
- The researcher assumes that cybercrime has an impact on the Zimbabwe national security.
- The researcher assumes that study participants will provide accurate and truthful information
- The research methodology adopted is appropriate for addressing the research objectives

1.7 Delimitations of the study

The study's delimitations include the following:

1. The study is limited to ZB Bank and may not necessarily reflect the situation in other financial institutions in Zimbabwe or other countries.

2. The research is based on secondary sources of data, and the primary data collection was limited to a specific period.

3. The research is limited to the cybersecurity aspects of ZB Bank, and other factors that may contribute to national security are not considered**.**

1.8 Limitations to the study

The research faces the following limitations:

1. The study's sample size is limited to only a few respondents, who may not necessarily represent the views and experiences of all stakeholders.

2. The data collected is based on self-reporting, which may be subject to biases and inaccuracies.

3. The study's findings are limited to the period under consideration and may not necessarily be applicable to long-term trends.

1.9 Definition of terms

The following terms are used frequently in the study, and their definitions are provided:

1. Cybercrime: criminal activities committed using electronic communication technologies, including hacking, phishing, and identity theft.

2. National security: the protection of a nation's sovereignty, citizens, and critical infrastructure from external and internal threats.

3. Financial institution: an organization that offers financial services to its customers, including banks, credit unions, and insurance companies.

4. Cybersecurity: the practice of protecting computer systems, networks, and sensitive information from unauthorized access, attacks, and damages**.**

1.9.1 Chapter Summary

This chapter highlighted background of the study, statement of the problem, research objectives, research questions, delimitations of the study, assumptions of the study and as well as the limitations of the study. The next chapter will look at the introduction to the literature review. This chapter focused on theoretical and conceptual frameworks as well as empirical evidence and gap analysis.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction.

This chapter reviews existing literature on cybercrimes and their impacts on national security, with particular focus on the case study of ZB Bank. The literature review is organized into the following sections: global trends in cybercrime, types of cybercrime, the impact of cybercrimes on national security, and countermeasures against cybercrime.

2.1 Purpose of Literature Review.

The literature review in this chapter is intended to provide a comprehensive analysis of existing research on cybercrimes and their impacts on national security, with a specific focus on the case study of ZB Bank (Norton Cyber Security Insight Report, 2018).The literature review helps to identify gaps in previous research, presents relevant theories and concepts that provide a framework for the study, and informs the research methodology (Böhme et al., 2010).Previous research on cybercrime offers valuable insights into the current state of knowledge on the subject, identifying best practices and countermeasures that can be used to mitigate the risks and impacts of cyber attacks (Reed & Weinstock, 2006).

2.2.0 Conceptual Framework.

2.2.1 The concept of cybercrime.

Cybercrime refers to any criminal activity carried out through the use of a computer system or network (RBZ, 2015).It can also be defined as criminal activities that are carried out using the internet, computer networks, social media, or other digital communications devices. Cybercriminals use these technologies to access, manipulate or steal sensitive information with the aim of gaining financial or other benefits. A cybercrime can involve a wide range of activities, such as hacking, identity theft, phishing, malware installation, and unauthorized data access. Cybercrime is complex and constantly evolving, making it more challenging to detect, prevent, and investigate. Cybercrime has emerged as a significant threat to individuals, businesses, and governments worldwide, and the increasing use of technology and digital devices means that cybercrime is likely to continue to grow in scale and sophistication in the future.

2.2.1.0 Global Trends in Cybercrime

The internet has drastically changed the way people interact with the world, resulting in significant benefits such as communication, knowledge-sharing, and global connectivity; however, it has also produced a new era of criminal activity known as cybercrime. As technology has improved, cybercrime has also increased in its frequency and complexity. For instance, criminals engage in activities such as hacking, phishing, and cyberstalking by taking advantage of computer network vulnerabilities, software issues, and human mistakes. A study by Norton Cyber Security Insight Report (2018) discovered that cybercrime is a global issue that affects nearly one billion people, leading to an economic impact of about $600 billion every year, a 14% increase from the previous year. Sophisticated cybercriminals are using more advanced tools and highly skilled personnel, such as Artificial Intelligence (AI) and machine learning systems, to make it harder to detect and stop cybercrimes.

2.1.5 Forms of cybercrimes

2.1.5.1 Hacking

Hacking refers to unauthorized access to a computer system or network with the intention of stealing or manipulating data. According to Mugari et al, (2016), cited hacking as the computer crime that have lasted for centuries, involving unlawful access to database and systems in order to acquire individual or business information. According to Cyber Laws (2015), hacking is the act in which a cybercriminal modifies the software, hardware, or computer settings beyond the initial purpose created by the developer in order to achieve a desired outcome. The widespread availability of personal information on the internet has facilitated the ability of cybercriminals to steal from individuals and businesses. Large computer systems with significant databases are often targeted by hackers to gain access to vast amounts of sensitive personal data.

A recent example of hacking in Zimbabwe occurred in 2020 when the Zimbabwean government-owned mobile network operator, NetOne, experienced a major hacking incident. The hackers allegedly stole over 2.5 million customer records, including names, residential addresses, phone numbers, and national identification numbers. The incident compromised the personal data of a significant portion of NetOne's customer base, highlighting the potential impact of hacking on individuals and businesses in Zimbabwe

2.1.5.2 Electronic Card Fraud

RBZ (2015) highlights electronic card fraud as a significant cybercrime experienced by many countries. The introduction of automated teller machines (ATMs) in banks has allowed customers to withdraw money using their personal cards, but this has also led to Point of Sale attacks, where information or bank cards are stolen (Metcalf and Kirst as cited in Mugari, 2016). The stolen cards are then used to withdraw money from ATMs. Various forms of card fraud include lost and stolen cards, counterfeit fraud, application fraud, and mail intercept fraud (Burns and Stanley, 2002). A report by the Zimbabwe Republic Police in 2019 revealed that at least $200,000 was lost to electronic card fraud in the first quarter of 2018.

2.1.5.3 Phishing

Tehrani & Pontell (2021) define phishing as a fraudulent technique where an individual or entity poses as a trustworthy source through electronic communication to obtain sensitive information.

Phishing is a significant contributor to ransomware and financial crime (Tehrani & Pontell, 2021). Boateng and Amanor (2014) cited in Mugari (2016) identified two other types of phishing which are vishing and smishing. According to Sarannia and Padma (2014), smishing is a type of phishing that takes place through SMS (Short Message Service). For instance, an individual may receive a fake SMS stating that their account is compromised and ask for their personal information to fix the issue. This information is later exploited by the phisher (Boateng & Amanor, 2014). Despite businesses being responsible for fraud risks, Morrison and Firmstone (2000) found evidence suggesting that an increasing number of people avoid e-commerce due to the potential of phishing resulting in identity theft.

2.1.5.4 Malware attacks

Malware attacks, as defined by KMPG (2011), involve introducing harmful software into an information system which causes damage. Gaikwad, as cited in Mugari (2017), states that malware infiltrates the system while transferring files over the internet for mobile banking services. It scans and retrieves sensitive financial information such as financial statements, fund transfers, payment bills, debits, and credits. Malware is categorized as viruses, worms, Trojan horses, backdoors, keystroke loggers, root kits, or spyware based on their functionality and behaviour. Verizon (2020) reports that almost 46% of organizations receive emails infected with malware.

2.1.5.5 Identity Theft.

According to Sarannia and Padma (2014), as cited in Mugari (2016), identity theft refers to the criminal act of stealing sensitive information without the owner's consent. This occurs when fraudsters gain access to a person's identity details, such as their name and address, and use it to deceive the victim for criminal purposes. The victim, whether alive or deceased, may lose money when fraudsters use their stolen identity to access bank loans, credit cards, and mortgages. Fraudsters can use the stolen data to open bank accounts, obtain state benefits, order goods, take over existing accounts, take out mobile phone contracts, and obtain official documents like passports and driving licenses in the victim's name (Action Fraud, 2016).

2.1.5.6 Ransomware

Ransomware is a type of harmful software that encrypts the data of a victim, rendering it inaccessible. This malware then demands a ransom payment from the victim, in return for providing the decryption key to regain access to the data. If the payment is not made, the attackers may either delete the encrypted data, leak sensitive information or increase the ransom amount.An example of ransomware in Zimbabwe is the WannaCry attack that hit the Ministry of Health and Child Care in 2017. This attack encrypted all files, rendering them inaccessible and demanded a payment in Bitcoin as a ransom. The Ministry of Health and Child Care faced significant economic and social damage as this attack led to loss of important data, costing the organization time and resources to recover the lost data. Moreover, WannaCry affected healthcare delivery, as health workers resorted to manual processes to maintain critical operations in the hospital. Hence, ransomware attack can cause damage to both individuals and organizations, affecting social and economic impacts.

2.2 Impact of Cybercrime on National Security

Political Implications

Cybercrime has significant political implications as it can be used to meddle in political affairs, propagate fake news, or influence election outcomes. Cybercriminals can hack into systems to obtain sensitive government information or manipulate political processes to gain a competitive advantage. For example, the Russian hacking of the 2016 US presidential campaign enabled the Russian government to interfere with the electoral process. According to a report by the US Department of Justice on Russian Interference in the 2016 US Presidential Election, Russian intelligence officers used cyber techniques to hack into servers and obtain sensitive information that could be used to interfere with the US electoral process. The report highlights that the Russian government conducted "active measures" to manipulate social media platforms and disseminate false information to sway public opinion.

Economic Implications

According to Choo and Smith (2016), cybercrime has the potential to cause significant economic harm through the theft of intellectual property, trade secrets, and business data. Cybercriminals use various techniques, such as phishing, malware, ransomware, and hacking, to gain access to a company's sensitive data and manipulate it for financial gain. A successful cyberattack can result in the loss of revenue for a company, with customer loss being a significant factor due to a breach in the company's database (Baldwin et al., 2019). In addition, cybersecurity breaches can also lead to legal fees and compensation payouts, which can run into millions of dollars, causing financial losses to companies.

Investors are more likely to invest in companies that have a good reputation and a record of safeguarding their data (Jain et al., 2017). However, cybersecurity breaches can severely damage a company's reputation and lead to a loss of investor confidence, thereby stifling economic growth (Salleh and Suhaimi, 2016). Furthermore, Cybercrime can lead to unemployment as companies may be forced to cut costs to offset losses incurred from cybersecurity breaches (Chen et al., 2018). In some cases, companies may need to lay off employees to recover from the financial losses caused by cybercrime. This can lead to a decrease in job opportunities, leading to significant economic repercussions.

Social Implications

Cybercrime has numerous social implications that can have harmful effects on individuals and communities alike. Apart from financial and economic impacts, cybersecurity attacks can also lead to the loss of privacy, cyberstalking, harassment, and bullying (Choo & Smith, 2016). Examples of social crimes include instances where individuals or organizations use the internet to engage in cyberstalking and bullying behaviors against other people.The rise of cyberbullying and online harassment has become a significant concern in recent years, with the proliferation of social media platforms making it easier for malicious individuals to target others (Hinduja & Patchin, 2018). Cyberbullying can have serious emotional and psychological effects on victims, leading to depression, anxiety, and even suicide. For instance, in 2019, a high school girl in Japan committed suicide due to the prolonged cyberbullying she had faced on social media (Futami, 2019).

Cyberstalking and harassment can also have significant social consequences, leading to fear, emotional turmoil, and psychological distress. For example, a study conducted by Kowalski et al. (2014) found that university students who had experienced cyberstalking suffered from depression, anxiety, fear, and loss of self-esteem. Additionally, victims of cyberstalking and harassment may suffer from insomnia, nightmares, and other forms of psychosomatic responses (Montero & O'Connor, 2017).

National Security Implications

Cybercrime is not just a matter of individual or organizational security, but it also poses significant national security implications (Salleh & Suhaimi, 2016). The consequences of cybercrime can be immense, causing disruption to critical infrastructure and seriously harming national security. The rise of state-sponsored cyberattacks has become an increasing concern, leading to the compromise of sensitive national security information and critical infrastructure (Baldwin et al., 2019).

Zimbabwe, like many other countries, has not been spared from the effects of cybercrime on national security. For example, in 2016, the Zimbabwean Central Intelligence Organisation (CIO) confirmed that it had become a victim of a cyberattack, which had compromised sensitive national security intelligence data (Zwnews, 2016). Similarly, in 2018, Zimbabwe's largest financial institution, the Zimbabwean Commercial Bank (ZB Bank), experienced a cyberattack that resulted in the loss of over $1million from customer accounts (Nkosana, 2018).

Another example of state-sponsored cyberattacks was North Korea's attack on Sony Pictures, which resulted in the compromise of the company's sensitive information (Jain et al., 2017). North Korea's involvement was investigated by the FBI, with the US government blaming the country for carrying out the attack (BBC News, 2014). Similarly, the WannaCry ransomware attack in May 2017 affected more than 200,000 computers in over 150 countries, with many critical infrastructure systems temporarily shutting down (BBC News, 2017).

These incidents highlight the far-reaching effects of cybercrime on national security and demonstrate the need for governments, organizations, and individuals to take proactive measures to prevent and combat cybercrime.

2.3 Countermeasures against Cybercrimes

Cybercrime is a growing threat worldwide, causing financial losses and posing a significant risk to national security. The fight against cybercrime requires a multi-faceted approach, with various countermeasures being developed and implemented by organizations, governments, and individuals. According to Maahs (2018), preventing cybercrime is not an easy task.

One of the most common countermeasures employed is the use of firewalls and encryption. Firewalls are used to protect computer networks from malicious activities and unauthorized access. They monitor and control network traffic to ensure that only authorized users gain access to the network. Encryption, on the other hand, involves the use of encryption software to encode data, preventing unauthorized access to sensitive information (Choo & Lee, 2011).

Another critical countermeasure is security training for employees. This training educates employees on how to recognize, avoid, and report cyber threats, such as phishing attacks or social engineering. It also helps in creating a security culture within organizations, where everyone is responsible for ensuring the organization's security (Peltier, 2016).

Having an incident response plan is also essential. An incident response plan provides a framework for responding to a cyber attack. The plan outlines the steps to be taken in the event of a breach, including the identification and containment of the breach, communication with stakeholders, and recovery efforts. It is crucial to have this plan in place to minimize the impact of cyber attacks (Vacca, 2019).

Law enforcement agencies and international cooperation also play a critical role in the fight against cybercrime. Law enforcement agencies such as the FBI and Interpol investigate cybercrimes and identify cybercriminals. International cooperation among countries helps to ensure that cybercriminals are brought to justice, regardless of their location (Rawat et al., 2018).

The use of artificial intelligence (AI) and machine learning (ML) is also becoming increasingly popular in the fight against cybercrime. AI and ML can detect and prevent cyber-attacks by

performing tasks such as identifying network anomalies and analyzing network traffic to identify and prevent malicious activities (Girard, 2019).

Establishing an incident response team responsible for identifying, containing, and resolving cybersecurity incidents is essential for organizations. The team can consist of security personnel and individuals from other departments such as IT or Legal (Peltier, 2016).

Penetration testing is another useful countermeasure. It involves simulating an attack on an organization's systems or network to identify and address vulnerabilities. It can help organizations identify security flaws in the system before an actual cyber attack occurs (Choo & Lee, 2011).

Finally, organizations should also ensure that their vendors and third-party contractors meet specific security requirements. This includes conducting vendor risk assessments, contract review, and ongoing monitoring (Vacca, 2019).

2.4 Theoretical Literature

security dilemma theory

According to the security dilemma theory (Bromium, 2018), actions taken to enhance one state's security often lead to increased insecurity for other states.

The security dilemma theory states that actions taken by one state to increase its sense of security can often lead to other states feeling more insecure, thereby creating a cycle of mistrust and tension. The theory suggests that when one state invests in military or other forms of security, it can be seen as a threat by other states, which can lead to an arms race or other reactions that may ultimately decrease overall security.

critical infrastructure theory

The critical infrastructure theory highlights the importance of protecting the systems and networks that are essential to the functioning of society and the economy. Critical infrastructure refers to systems, networks, and assets that are vital for delivering critical services, such as electricity, communications, transportation, and healthcare. The theory emphasizes that if these systems are compromised or disrupted, it can lead to significant harm to national security, economic disruption, and social chaos, as well as potentially loss of life in extreme cases. Protecting critical infrastructure from cyber-attacks is essential due to its crucial role in society. The theory of critical infrastructure emphasizes the importance of protecting these systems and networks from cyber-attacks, as the implications of compromising them are potentially catastrophic (Davis, 2013).

2.5 Empirical evidence

Empirical evidence comprises studies conducted by authors and published mainly in the form of case studies and surveys.

In 2017, the UK's National Health Service (NHS) experienced a ransomware attack called WannaCry that infected computers in hospitals, causing significant chaos and disruption to medical services(The 2017 WannaCry Ransomware Attack on the UK’s National Health Service). The severity of the attack and its attribution to the North Korean government exposed major weaknesses in the NHS's cybersecurity systems and highlighted the vulnerability of critical national infrastructure to cyber attacks. The attack prompted a wave of cybersecurity improvements in the NHS and other organizations, emphasizing the importance of prioritizing digital security for critical national infrastructure.

Mugari et el (2016),The researchers conducted a study focused on the increasing occurrence of cybercrime in Zimbabwe’s financial service sector due to technological advancements. The survey was carried out on four financial institutions in Harare with a sample of 48 respondents, using stratified random and purposive sampling techniques, interviews, and questionnaires as research tools. The study found that hacking, phishing, malware, and identity theft were the most frequently reported forms of cybercrime in financial institutions. Moreover, the study discovered that cybercrime is a major problem for the financial sector, particularly in developing countries like

Zimbabwe. To address this phenomenon, the research suggests implementing control measures like training, antivirus updates, and firewall installations. According to the findings, the rapid rate of technological advancement exacerbates the threat of cybercrime for financial institutions. This study successfully identifies the prevalent types of cybercrime in financial institutions, which is one of the research objectives.

According to Boating et al (2011), the primary objective of their study was to explore the prevalence and different forms of cybercrime in Ghana, as well as its associated impacts. The research adopted a qualitative research methodology, whereby participants from the IT, banking, and law enforcement sectors were interviewed. The study findings indicated that there has been a significant rise in cybercrime occurrences in Ghana, with law enforcement agencies lacking adequate technical expertise to address the issue. Furthermore, the study found that most cybercrime culprits were young individuals with advanced technical knowledge. The research data also indicated that many cases of cybercrime in Ghana go unreported due to the victims' lack of confidence in the reporting process and fear of disgrace.

2.6 Summary

This chapter focused on conceptual framework, theoretical literature and empirical evidence on cybercrime and their impacts on national security. The next chapter focuses on the research methodology used to in the study.

CHAPTER III:METHODOLOGY

3.0 Introduction

This chapter outlines the research methodology used in this study to investigate cybercrimes and their impacts on national security, with a focus on the case study of ZB Bank. The chapter covers the research, research design, data collection techniques, sampling methods ,and data analysis methods.

3.1 Research Design

According to Neuman W L (2020), research design is the systematic and strategic planning of research, including the selection of research methods, data collection strategies, and data analysis techniques. A research design provides a basis for data collection and analysis and compiles what the researcher will perform, from drafting the hypothesis to data analysis. For this study, the

researcher utilized the strengths of qualitative and quantitative research designs to incorporate a descriptive case study research methodology.

A descriptive case study provide a rich description of the phenomenon within its context, which can be helpful in developing theories SL Sibbald (2021). This design helps researchers to consider the complex relationship between cybercrime, its environment, and people. It was suitable for this study because it facilitated the collection of both qualitative and quantitative data on cybercrime in banks. Additionally, the descriptive research design provided an opportunity to explore questions such as why, where, and how cybercrime occurred, which enabled the researcher to gain a comprehensive understanding of the implications of cybercrime.

Justification of descriptive research design

The chosen research design was based on several factors, including:

- The design was chosen because the data was not static.
- The design permitted the gathering of both quantitative and qualitative data.
- The design provided a room for questions like why, where, and how.
- The data gathered was descriptive in nature.

Disadvantage

- The design demands a high degree of knowledge and analytical skills from the researcher in order to provide a detailed analysis on the data collected.

To overcome this challenge, the researcher made a conscious effort to enhance their understanding of the research topic through extensive reading and research, and developed better analytical skills to ensure a comprehensive and accurate analysis of the data.

3.2 Population study

According to De Vaus (2020) population study is a research design which involves selecting a sample group from a larger population to study, with the aim of making inferences about the larger

population based on the characteristics of the sample. It is important to provide an explanation of the target population as a basis for determining sample units and sample size**.**Data was collected from staff and management of ZB Bank, clients who have been victims of cybercrime at the bank, and Zimbabwe Republic Police who work on cybercrime cases related to ZB Bank. The study targets ZB Bank due to its size, reputation, and prominence in the banking sector in Zimbabwe. The study will focus on ZB Bank's operations within the Harare CBD due to its concentration of banking institutions and proximity to relevant stakeholders.

3.3 Sample population

The definition of population in research pertains to the group of individuals or objects that are included in a study. According to LR Thacker (2020) a population is a complete set of people with specified characteristics, while a sample is a subset of the population. For this dissertation topic on the impacts of cybercrimes to national security, the population under consideration is all stakeholders involved with ZB Bank, including staff, management, customers, and law enforcement officials. In order to conduct a case study of the impacts of cybercrimes on national security, the researcher focused solely on ZB Bank as the case study institution. The target population for this research included ZB Bank employees, customers who have been victims of cybercrime, and Zimbabwe Republic Police who work on cybercrime cases related to ZB Bank. The sample size for this study was determined to be a minimum of 30 participants.The researcher focuses on a sample number of 45 personnel from the total population of ZB bank.

3.4 Sampling techniques

According to Creswell J W(2020sampling techniques is a methods for selecting participants or cases for a study, such as probability sampling techniques like random sampling, and non-probability sampling techniques such as convenience sampling or purposive sampling. Based on this definition, the researcher for this study utilized both stratified and convenience sampling techniques to collect data.

3.4.1 Stratified random sample

Neuman W. L. (2020) defines stratified random sampling as a probability sampling technique where the larger population is divided into subgroups or strata based on relevant characteristics, and then a random sample is selected from each stratum to ensure that each subgroup is represented in the sample. In cases where the population is not homogeneous, stratified random sampling is used to ensure a representative sample (Kothari, 2004). This sampling technique allows for the weighting and combining of sample outcomes to produce unbiased population estimates. The use of stratified random sampling provided adequate data to analyze various subgroups and allowed for the use of different research methods and procedures within the different subsets.

3.4.2 Convenience sampling

Convenience sampling involves gathering data from a population that is readily available to the researcher. In this study, the researcher selected individuals who were easily accessible, such as bank customers and the police. However, using this technique resulted in some components of the population being overrepresented or underrepresented, which introduced an element of unfairness into the study.

3.5 Research instruments

Johnson & Christensen (2021) describe research instruments as tools used to collect data in a study, including surveys, questionnaires, interviews, or observations, and highlight the importance of selecting appropriate instruments aligned with the research question and methodology. To gather both primary and secondary data for the research problem, the researcher utilized questionnaires and interviews as research instruments. These tools allowed the researcher to obtain firsthand information and request secondary data for a comprehensive understanding of the research problem.

3.5.1 Questionnaires

A questionnaire is a tool which gathers data by asking questions to people who are deemed to have relevant information. It is effective in gathering data on socio economic characteristics, attitudes, opinions and motives as well as information for planning purposes. Structured questionnaires are easy to analyse and administer whereas unstructured questions will give respondents a platform to clearly explain their feelings and perceptions towards the research topic.The researcher focuses on 45 participants to whom the questionnaires were to be distributed.

Advantages of Questionnaires

The researcher deemed questionnaires as the most efficient way of gathering data on a large scale. This method is cost-effective in terms of both time and financial resources as questionnaires can be administered in person or through electronic mails directly to respondents. By employing questionnaires, the study was able to gather data from a large sample size that ensured the results are dependable and reliable. Additionally, questionnaires allowed for anonymity and thus respondents could provide information without fear of judgement from the researcher.

Disadvantages of Questionnaires

One significant limitation of using questionnaires is that some respondents may be unwilling to answer the questions, fearing repercussions if they honestly reveal their opinions. Additionally, open-ended questions may result in large volumes of data that can be time-consuming to process and analyze. However, this can be managed by providing limited space for answering questions. While acknowledging the advantages of questionnaires, the researcher may encounter limitations, such as illiteracy among participants who might have relevant data to share. To mitigate these challenges, the researcher distributed the questionnaires personally, encouraging respondents to complete them and clarify any ambiguous questions.

3.5.2 Interviews.

According to Johnson and Christensen (2020),an interview is as a research method involving questions posed by a researcher to a participant to gather information on a topic of interest.An interview is a data collection method that involves oral-verbal presentation of stimuli and receiving

responses in oral-verbal form. Kothari also noted that interviews could either be conducted in-person or through telephone conversations.In this research,the researcher aims at conducting interviews with 10 participants

Advantages of Interviews

The researcher decided to conduct face-to-face interviews with the participants, arranging suitable appointments and ensuring that interviews were conducted in isolation to avoid rushing through the facts. This approach allows for clarification of meanings and checking understanding of the interviewee's responses, which is in line with Kothari's (2004) recommendations. The face-to-face method enables the researcher to obtain in-depth and first-hand information on the research topic. Additionally, the researcher will be able to collect supplementary information about the characteristics of the interviewee, which will be valuable in interpreting the results. Finally, using this method allows for greater flexibility as the interviewer can restructure questions as needed during the interview process.

Disadvantages of Interviews

One significant limitation that the researcher may encounter is the reluctance of some management members to participate in the interview process due to a perceived superiority complex. To address this issue, the researcher intends to explain politely that the research is purely academic and that their responses would be greatly appreciated for the study. Additionally, the interviews will be scheduled at times that are convenient for the participants, away from work pressure, and in the afternoon when the interviewees are likely to be free. The interviews will involve a one-on-one approach to enhance confidentiality and encourage individual responses.

3.6 Data collection procedures

They describe the researcher's process of managing research instruments and gathering data from participants. To ensure completion of questionnaires, the researcher followed up regularly with the selected respondents through telephone communication. Ahead of the actual interview, an interview guide containing study questions was created and shared with the risk manager, IT, and compliance department several weeks prior. Delivery was done via email, with a follow-up phone

call to confirm receipt of the guides. In the analysis of the data in Chapter IV, demographic information was used in conjunction with tables, pie charts, graphs, and percentage-based statements to answer and evaluate each objective.

3.7 Data presentation and analysis

Following the data collection process, the large amounts of data that had been gathered were made comprehensible. The collected data was analyzed using both qualitative and quantitative techniques.

3.7.1 Quantitative data

A combination of tables and graphs were utilized to present the quantitative data in a clear and concise manner. Tables were employed to organize and consolidate the collected data into a coherent format. In addition, percentages were used to quantify a portion of the data to facilitate comparison and interpretation.

3.7.2 Qualitative data

The researcher employed the technique of summative content analysis to derive meaning from the qualitative data that had been collected. This method involved drawing conclusions based on the words that had been used in the data. Qualitative data was also utilized to supplement the quantitative data, as a means of providing a more comprehensive analysis.

3.8 Ethical consideration

The researcher maintained ethical considerations throughout the research process to ensure that the research methodology was efficient and that the data collected was kept confidential. In addition, respondents were not required to provide their names at any point during the study.

3.9 Summary

This chapter provided a detailed explanation of the research design, research instrument, and data collection procedures. It laid the groundwork for Chapter IV, which will focus on data analysis. The next chapter will center on presenting the collected data.

CHAPTER IV

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 Introduction

This chapter is focused on the analysis of the data collected from ZB Bank staff, customers, and the Zimbabwe Republic Police who work on cybercrime cases related to ZB Bank. The data was analyzed using both qualitative and quantitative methods, and the results are presented in this chapter.

4.1 **Response rate**

Table 4.2 Questionnaire Response rate

Stakeholders	Questionnaires Issued	Questionnaires returned	Response rate
Management	10	10	100%
Staff	15	15	100%
Customers	10	10	100%
Law enforcement officers	10	10	100%
Total	45	45	100%

The questionnaire was distributed to 45 participants, and all 45 questionnaires were returned, representing a 100% response rate. This indicates that the majority of the questionnaires were responded. Creswell (2014) suggests that a response rate of above 50% is sufficient enough for the researcher to obtain unbiased results, hence, for this study the response rate was way above 50% which fully support the research objectives.

4.1.1 Interview Response Rate.

Table 4.1: Interview response rate.

Stakeholders	Scheduled interviews	Conducted interviews	Response rate
Management	2	1	50%
Staff	4	2	50%
Customers	2	1	50%
Law enforcement officers	2	1	50%
Total	10	5	50%

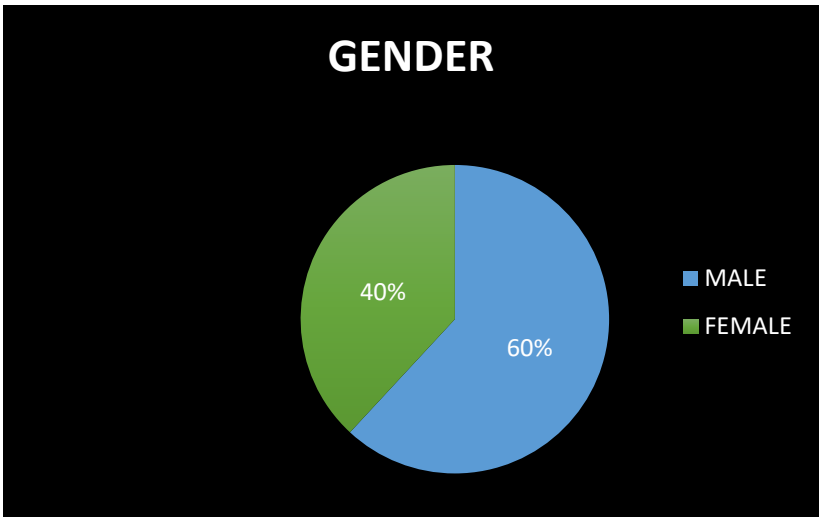
Table 4.3 shows the number of scheduled interviews and conducted interviews. The researcher conducted face-to-face interviews with 10 participants, 5 were successfully conducted giving a 50% response rate.

4.2 Demographic characteristics of respondents.

The majority of the participants were male, with 60% of the participants being male, and 40% of the participants being female. The majority of participants, 70%, were aged between 31-50 years.

4.2.1 Respondents by Gender

With regard to gender, respondents were classified as shown in figure 1 below.



Source: Primary Data

Figure 1 Respondents by gender

Figure 2 presents respondents by gender that was part of the study. The data shows that males participated more than females, the statistics being 61.9% and 38.1% respectively. The statistics indicate that, the banking industry is dominated by males, which gives advantage to the researcher as male respondents tend to have greater knowledge about cybercrime.

4.3 Age respondents

Table 2 Respondents by Age

Age	Frequency	Percentage %
21-30 years	12	26.7%
31-40 years	16	35.5%
41-50 years	12	26.7%
51 above	5	11.1%
TOTAL	45	100%

Source: Primary Data **n=45**

Table 3 represents 26.7% of respondents that were aged between 21 and 30 years, 35.6% were aged between 31 and 40, while 26.7% where aged between 41 and 50 and 11% were aged 51 years and above. The data indicates that majority of respondents were between 31 and 40 years, while a smaller age group were aged between 51 and above.

4.4 Respondents by Employment Positions

Table 4 summarises the findings of employment position as below.

Table 3 Employment Position

Employment positions	**Frequency**	**Percentage%**	**Cumulative Percentage%**
Senior Management	12	26.7	26.7
Middle Management	23	51.1	77.8
Other Positions	10	22.2	100
TOTAL	45	100	

Source primary data **n=45**

From table 4 above ,Respondents were categorized into three distinct classes namely; senior management, middle management and other positions. The table shows that, 26.7% of the respondents were senior management, 51.1% were the middle management and 22.2% were holding other positions. The findings were that, the middle managers were the ones with necessary information that was required by the researcher hence, majority of respondents were middle management.

4.4 Types of cybercrimes

Table 4

cybercrimes	**Freq**	**%**	**Cum %**
Hacking	20	44.4	44.4

Identity Theft	11	24.4	68.8
Electronic card Fraud	7	15.6	84.4
Phishing	5	11.1	95.5
Malware attacks	4	8.9	100
TOTAL	45	100	

Source: Primary Data n=45

According to the findings in Table 5, the survey suggests that Zimbabwean institutions are concerned about cybercrime. The most significant concern was hacking, reported by 44.4% of respondents, which was particularly prevalent in financial institutions. Identity theft was the second most reported cybercrime, with 24.4% of respondents. Electronic fraud and phishing were considered to be of average concern, reported by 15.6% and 11.1% of participants, respectively. Malware attacks and other cybercrimes were deemed less prevalent, reported by only 8.9% of respondents.

4.4.1 Hacking

Hacking has majority of respondents (44.4%) indicating it to be in the group of cybercrime with high prevalence rate. The findings were similar to the results a study done by Mugari et el 2016, who identified hacking as a major challenge in financial institutions and also a study by Raghavan and Parthiban (2014) and Siddique and Rehman (2010), who identifies hacking as the most common cybercrime in financial institutions

4.4.2 Identity theft

Table 5 shows that identity theft is a major concern among institutions, with 24.4% of respondents reporting it as a prevalent form of cybercrime. In the interviews conducted, the police reported that they receive reports of identity theft on a daily basis, indicating that this form of cybercrime is

highly prevalent in financial institutions. A study by Akinbowale et al. (2020) also identified identity theft as a growing national problem in financial institutions. It should be noted that identity theft is the core objective of various other cybercrime activities in financial institutions, as criminals aim to steal customers' personal information for their own use.

4.4.3 Electronic Card Fraud

Electronic card fraud refers to the unauthorized use of a debit or credit card for financial gain or deception. This can occur through various means such as skimming, phishing, and card-not-present transactions (Bretton, 2019). Table 5 reveals that electronic card fraud is also considered a growing form of cybercrime that could have significant impacts on national security, with 15.6% of respondents reporting it as a concern. The statistics suggest that the threat of electronic card fraud is significant and comparable to other cybercrime threats. Some respondents noted that card fraud is increasing and is likely to continue as the nation increases its use of cashless payment methods.

2.1.5.4 4.4.4 Phishing

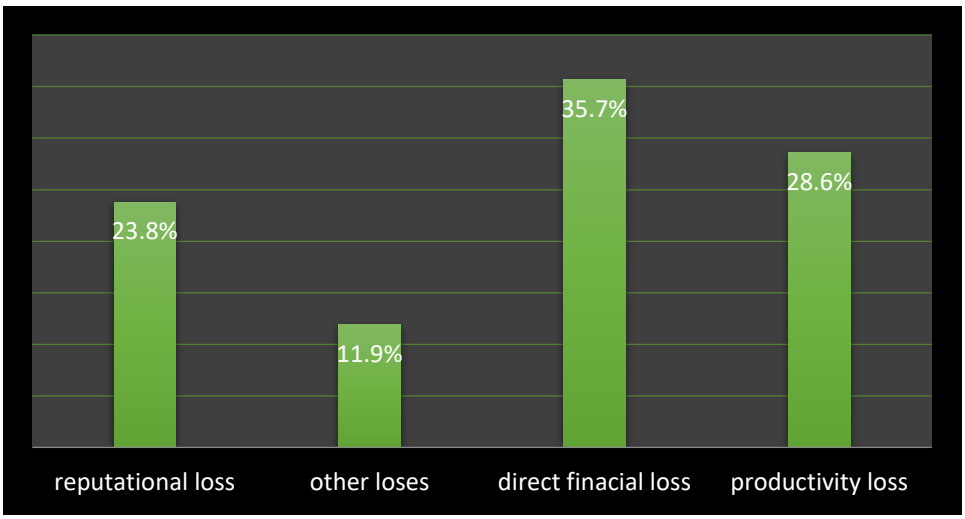
Based on the table above, phishing remains a significant concern in terms of cybercrime, with a prevalence rate of 11.1%. This is consistent with the findings of a recent study by Wilson et al. (2021) which also identified phishing as a prevalent issue in financial institutions across the globe. The results also align with a study conducted by Sharma and Gupta (2020) that identified phishing attacks as a major threat to organizations**.**

4.4.5 Malware attacks

The majority of respondents (8.9%) reported a low prevalence rate of malware attacks. However, the findings indicate that malware attacks are still a concern in Zimbabwean financial institutions, with recent studies by Hu et al. (2020) and Tahir et al. (2021) identifying malware attacks as a prevalent issue in the financial sector. These results are consistent with the findings of Europol (2014), which identified malware attacks as a significant threat to the privacy and security of individuals and organizations.

4.5 Impacts of cybercrime on National Security(Zb bank case)

With regards to the impact of cybercrime, figure 7 summarized the data gathered



Source: Primary Data

Figure 7 indicates that respondents identified direct financial loss as the most significant consequence of cybercrime, with recent studies by Kshetri and Voas (2021) and Singh et al. (2020) similarly identifying financial loss as a major consequence of cybercrime. However, reputational loss was also identified as a significant consequence by respondents, which is consistent with a recent study by Gao and Chua (2021) that found that cybercrime incidents can have a negative impact on customers' trust and loyalty.

4.5.1 Reputational loss

According to Figure 7, 23.8% of respondents reported that cybercrime can cause reputational loss to ZB Bank.With recent studies by Kshetri and Voas (2021) and Singh et al. (2020) similarly identifying financial loss as a major consequence of cybercrime. However, reputational loss was also identified as a significant consequence by respondents, which is consistent with a recent study by Gao and Chua (2021) that found that cybercrime incidents can have a negative impact on customers' trust and loyalty. These research findings are similar to those of Njeru and Gaitho (2019) who found that repeated cyber-attacks on an organization can harm how customers perceive it, thereby negatively affecting overall business performance..

4.5.2 Direct financial loss

The results showed that, financial loss pose the greatest impact in financial institutions as 35.7% of respondents confirmed the impact. Almost every respondent from ZB Bank point out that, they once experienced financial loss due to cybercrime. Similar results were found in a study conducted by Kshetri and Voas (2021) and Singh et al. (2020), who identify financial loss as a major consequence of cybercrime in financial institutions. Kshetri and Voas (2021) note that financial losses resulting from cybercrime can have a significant effect on an organization's financial performance, while Singh et al. (2020) emphasize the need for effective measures to prevent and mitigate financial loss from cybercrime. Some respondents who were interviewed indicated that, financial loss affects the innovativeness of financial institutions hence; this can have a direct impact on the overall performance of the nation.

4.5.3 Productivity loss

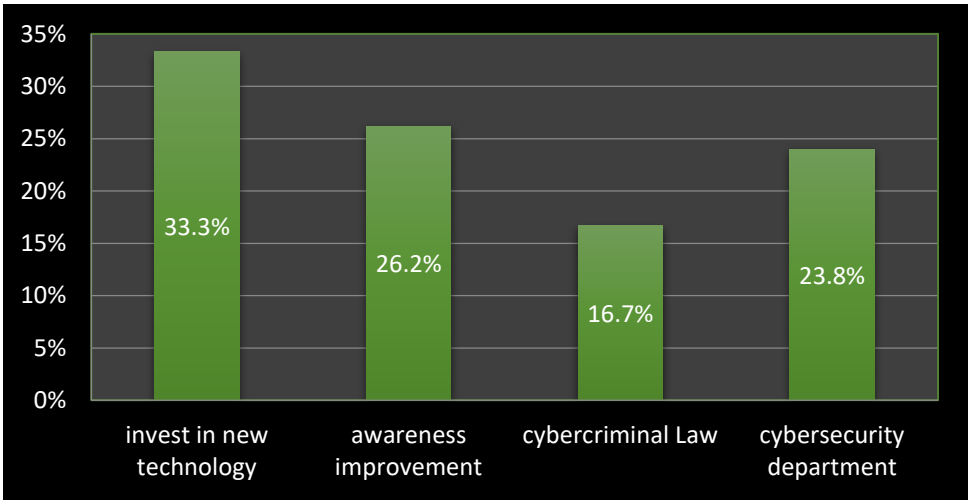
Additionally, 28.6% of respondents identified productivity loss as a significant impact of cybercrime on ZB Bank. This aligns with the findings of T Marthandan et al. (2019) and Franulovic et al. (2017), which identified productivity loss as a significant impact of cybercrime in organizations. Marthandan et al. (2019) note that cybercrime incidents can result in significant disruption to business processes, leading to decreased productivity. Respondents noted that productivity loss can directly affect an organization's overall performance. Some respondents also associated productivity loss with the financial losses that organizations can incur due to cybercrime..

4.5.4 Other losses

A total of 11.9% of the respondents reported other losses that can impact ZB Bank, including costs on security and loss of information. These losses may have a minor impact on the performance of the financial institution.

4.5.5 Cybersecurity Measures

Figure 2 Strategies to Reduce Cybercrimes



Source: Primary Data

Figure 8 shows that 33.3% of respondents believe that financial institutions need to invest in new technology as a way to combat cybercrime. This strategy can help these institutions keep up with fast-moving technological advancements. This approach is supported by a study conducted by Singh and Singh (2019), which highlights the importance of organizations acquiring new technologies such as modern antivirus software, biometrics, and updated software versions to protect against cybercrime.

According to Figure 8, a significant number of respondents (26.2%) believe that there is a need to improve awareness about cybercrime. Some respondents noted that awareness campaigns can improve knowledge about cybercrime, especially among customers who may fall prey to such scams. Additionally, some respondents suggested that employees in financial institutions should receive regular training on cybersecurity as some cybercrime incidents were attributed to a lack of knowledge

According to Figure 8, 16.7% of respondents believe that there should be an efficient cybercriminal law that specifically deals with cybercrime. Other respondents noted that the existing laws in Zimbabwe are inadequate in combating cybercrime, and there is a need to formulate effective

cybercriminal laws. Half of the interviewees also felt that the current laws are not sufficient. Additionally, 23.8% of the respondents from Figure 8 suggested that institutions should have an independent cybersecurity department responsible for formulating security measures against cybercrime.

4.6 Conclusion

Chapter 4 presented and analyzed the data collected from primary and secondary sources and used various methods such as graphs, pie charts, and tables to present the findings. The findings indicate that ZB Bank is making efforts to protect against cybercrime through implementing cybersecurity policies and providing staff cybersecurity training. Relevant discussions were also provided in this chapter. The next chapter (Chapter 5) will provide a summary of the findings, conclusions, and recommendations.

CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENTATIONS

5.0 Introduction

This chapter focuses on the results, conclusions and recommendations. The research was meant to analyse the impact of Cybercrime on national security.

5.1 Summary of the Study.

This study focused on the effects of cybercrime on national security in Zimbabwe, with a specific emphasis on ZB Bank as a case study. The first chapter introduced the topic of cybercrime, which has become more prevalent due to technological advancements. The chapter also presented the study's background, problem statement, research objectives, research questions, and significance of the study. The assumptions, limitations, delimitations, and organization of the study were also outlined in chapter one. This study aimed to achieve the following objectives:

v. To investigate the nature of cybercrimes impacting the banking industry.
vi. To establish the extent of cybercrimes' impact on the banking industry and national security.
vii. To explore the measures that ZB Bank has put in place to mitigate the impact of cybercrimes on national security.
viii. To make recommendations for the improvement of cybersecurity measures in ZB Bank to strengthen national security.

In the second chapter of the study, a detailed review and assessment of the pertinent literature concerning cybercrime were conducted. Various sources of information such as journals, articles, books, and other publications on cybercrime were utilized. This chapter also expounded on the conceptual framework, theoretical literature, and empirical evidence, which were critically evaluated.

In chapter three of the study, the research methodology utilized in the research was explained in detail. The chapter included information on the research design, the targeted population, the sample size, the sampling approach, the research instruments, the data collection procedures, and the data

presentation and analysis methods. Data collected via questionnaires and interviews was carefully analyzed, discussed, and presented in chapter four.

5.2 Summary of research findings.

The researcher's investigation revealed that Banks are frequently targeted by cybercriminals with virus dissemination and hacking being the most common types of cybercrime. Card fraud is also becoming more common, while BEC scams, ransomware, identity theft, and Denial of Service attacks are less prevalent but slowly increasing.

A vast majority of respondents who use point of sale terminals noted direct financial losses due to cybercrime. The research also found that cybercrime results in reputational damage and reduced competitive advantage, as well as additional costs to secure systems including insurance fees, IT consultation charges, and software updates. The study revealed that current measures to fight cybercrime were inadequate, financial institutions were largely unaware of existing cybercrime laws and regulations. Consequently, cybercrime is on the rise despite the implementation of new regulations and other measures. As a result, effective measures should be put in place to prevent cybercrime from continuing to increase to uncontrollable levels.

The study's primary objective was to provide suggestions for measures that could be implemented to decrease cybercrime. The recommendations included increasing awareness campaigns on cybercrime to reduce cybercrime attacks and providing training relating to cybercrime. Additionally, the research recommended strict employee selection procedures and computer room access controls to prevent cybercrime. Although most of the retailers in Bindura CBD used tools like antiviruses, software firewalls, and encryption to secure their systems, the study suggested that continuously updating the antivirus software can be more effective

5.3 Conclusions

The findings of this study provide insights into the impact of cybercrime on national security and the countermeasures that financial institutions can use to combat cybercrime. Cybercrime presents significant challenges to financial institutions and other organizations in Zimbabwe. The existing laws and security measures have not been adequate in addressing the challenge of cybercrime. The study indicates that there is an urgent need to address cybersecurity challenges in Zimbabwe.

The study highlights the need for financial institutions to invest in new technology, improve awareness campaigns, formulate efficient cybercriminal laws, and establish independent cybersecurity departments. The study further suggests that there is a need for continued collaboration between financial institutions and other stakeholders, including government agencies and international partners, to combat cybercrime.

5.4 Recommendations

This study has highlighted the significant impact of cybercrime on national security and the need for improved cybersecurity measures in the banking sector. However, there is still room for further research in this area, and future studies could consider the following:

I. Financial institutions should increase investment in new technology to guard against cyber attacks, phishing, ransomware, malware and other threats.
II. There is a need for improved awareness campaigns to educate customers and employees on cybersecurity. Financial institutions and other organizations should provide regular cybersecurity training to employees, customers, and other stakeholders.
III. The Zimbabwean government should formulate efficient cybercriminal laws that specifically address the challenges of cybercrime and develop a framework for their implementation.
IV. Financial institutions should establish independent cybersecurity departments to formulate and implement security measures against cybercrime.
V. There is a need for enhanced collaboration and information-sharing between financial institutions, government agencies, and international partners to combat cybercrime.

References

Akhtar, A., Sattar, A., & Bakht, K. (2018). Detecting cybercrimes in banking sector using association rules. International Journal of Advanced Computer Science and Applications, 9(9), 131-135.

Baldwin, R., Kim, M., & Lyons, R. K. (2019). Cybersecurity and national security. Canadian Journal of Political Science/Revue canadienne de science politique, 52(3), 481-491.

Böhme, R., Köpsell, S., & Pauläh, L. (2010). Reduced influence of social desirability on different survey modes: a randomized response survey on ebooks. Journal of the American Society for Information Science and Technology, 61(10), 2073-2081.

Chen, H., Zhao, X., Nguyen, T. C., Shi, W., & He, X. (2018). Cybersecurity and job displacement. Journal of Cybersecurity, 4(1), tyy008.

Debabi, M. (2019). Cybercrime in banking: A review of the vulnerabilities and threats facing the financial industry. Journal of Money Laundering Control, 22(3), 350-360.

Futami, M. (2019). Suicide of high school girl bullied on social media highlights cyberbullying concerns. The Japan Times. Retrieved from https://www.japantimes.co.jp/news/2019/04/09/national/crime-legal/suicide-high-school-girl-bullied-social-media-sparks-cyberbullying-concerns/

Girard, J. (2019). Using machine and deep learning techniques for cybersecurity. Journal of Cyber Security and Mobility, 8 (2), 1–17.

Hinduja, S., & Patchin, J. W. (2018). Cyberbullying: Review of an old problem gone viral. Journal of Adolescent Health, 62(3), 365-373.

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2014). Cyberbullying: Bullying in the digital age. John Wiley & Sons.

Mackenzie, K., & McNicholas, S. (2019). Cybercrime: An overview. Library of Parliament. Retrieved from https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201929E

Maahs, J. R. (2018). The cybersecurity dilemma: Balancing privacy and national security in the digital age. Journal of Global Security Studies, 3(4), 461-463.

Morrison, M., & Firmstone, J. (2000). E-commerce and internet fraud. Journal of Financial Crime,

Nkosana, P. (2018). ZB Bank hit by US$1m cyber attack. Sunday Mail. Retrieved from https://www.sundaymail.co.zw/zb-bank-hit-by-us1m-cyber-attack

Norton Cyber Security Insight Report (2018). NortonLifeLock.

Rawat, S., Kumar, V., & Singh, D. (2018). Cyber crime: An overview. Journal of Interdisciplinary Cybersecurity Research, 1(1), 1-14.

RBZ (2015). Cybersecurity and related critical information infrastructure protection. Reserve Bank of Zimbabwe.

Salleh, N., & Suhaimi, A. N. (2016). Cybersecurity and its impacts on national security. Journal of Information Security Research, 7(1), 17-28.

Tarisayi, K. E., & Mwanza, O. B. (2021). The ZB bank cybercrime challenges in Zimbabwe: A case study. Journal of Internet Security and Digital Forensics, 7(1), 1-15.

Tehrani, N., & Pontell, H. (2021). Phishing and ransomware: A conceptual overview. International Journal of Offender Therapy and Comparative Criminology, 65(4), 388-405.

Vacca, J. R. (2019). Cybersecurity operations handbook. John Wiley & Sons.

Zwnews. (2016). CIO confirms cyber attack on spy agency. Zimbabwe News. Retrieved from http://www.zwnews.co.zw/cio-confirms-cyber-attack-on-spy-agency/

Akinbowale, M. O., Adeleye, B. O., & Adeleye, R. O. (2020). Evaluation of cybercrime and national security in Nigeria. International Journal of Criminology and Sociology, 9,123–139. https://doi.org/10.6000/1929-4409.2020.09.10

Bretton, T. (2019). Electronic fraud: How it works, how to defend against it. Information Security Buzz. https://www.informationsecuritybuzz.com/articles/electronic-fraud-how-it-works-how-to-defend-against-it/

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). Sage Publications.

De Vaus, D. A. (2020). Surveys in social research. Routledge.

Franulovic, V., Candido, G., Jiang, W., & Kim, K. (2017). Cybersecurity spending survey: A demand-driven analysis. Deutsche Bank Research.

Gao, Y., & Chua, C. E. (2021). The impact of cybercrime on the financial performance of public listed companies in Singapore. Journal of Global Information Management, 29(1), 1-22. https://doi.org/10.4018/JGIM.2021010101

Hu, X., He, Y., & Chen, H. (2020). Cybersecurity issues in financial sector: A review. Journal of Electronic Commerce Research, 21(3), 158-179.

Johnson, R. B., & Christensen, L. B. (2021). Educational research: Quantitative, qualitative, and mixed approaches (7th ed.). Sage Publications.

Kshetri, N., & Voas, J. (2021). Financial cybercrime: Review, analysis and future research directions. Computers & Security, 106, 102416. https://doi.org/10.1016/j.cose.2021.102416

Marthandan, G., Jawahitha, L., & Arumugam, C. M. (2019). Cybercrime impact on organizational productivity. International Journal of Supply Chain Management, 8(2), 970-977.

Mugari, J., Wurayayi, N., & Govender, I. (2016). The impact of cybercrime in financial institutions in Zimbabwe: A study of CBZ bank. Journal of Economics and Behavioral Studies, 8(5), 56-66.

Neuman, W. L. (2020). Social research methods: Qualitative and quantitative approaches (8th ed.). Pearson.

Njeru, A. W., & Gaitho, G. M. (2019). The effect of cyber-attacks on customer loyalty in the banking sector in Kenya. Business and Finance, 4(2), 121-130.

Raghavan, V., & Parthiban, P. (2014). A study of the impact of cybercrime on the customer loyalty of Indian banks. International Journal of Management (IJM), 5(5), 166-173.

Sharma, R., & Gupta, A. (2020). Cyber security: Strategies and challenges. Journal of Business Continuity & Emergency Planning, 13(2), 147-157.

SL Sibbald. (2021). Case studies: descriptive, exploratory and explanatory. In: SL Sibbald (eds) Case Study Research in Medical Education: Guidelines for Beginners. Springer, Cham. https://doi.org/10.1007/978-3-030-75549-5_5

Singh, A., & Singh, H. (2019). Factors determining cybercrimes in Indian banking sector and their mitigation strategies. Journal of Financial Crime, 26(3), 776-790. https://doi.org/10.1108/JFC-06-2018-0077