FACULTY OF COMMERCE

DEPARTMENT OF INSURANCE AND RISK MANAGEMNT

RESEARCH PROJECT

AN INVESTIGATION OF THE EFFECTIVENESS OF RISK MANAGEMENT STRATEGIES IMPLEMENTED BY BANKS TO CURB CYBER RISK. A CASE OF CBZ BANK

BY

FRANCIS MBIRIMBINDO.

R1810382X

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF BACHELOR OF COMMERCE IN INSURANCE AND RISK MANAGEMENT HONOURS DEGREE OF MIDLANDS STATE UNIVERSITY

RELEASE FORM

Registration Number: R1810382X

Dissertation Title: An investigation of the effectiveness of risk management strategies implemented by banks to curb cyber risk. A case of CBZ Bank

Year granted: 2021

Permission is granted to Midlands State University library and the department of Insurance and Risk to produce copies of this dissertation in an effort it deems necessary for academic use only.

Signature of student……

Date signed……..

Permanent Address: 547 Southlea Park, Harare

APPROVAL FORM

Topic: An investigation of the effectiveness of risk management strategies implemented by banks to curb cyber risk. A case of CBZ Bank

TO BE COMPLETED BY THE STUDENT

I certify that the dissertation meets the preparation guidelines as presented in the faculty guide and instruction for preparing dissertations.

_____ _____

(Signature of Student) **Date**

TO BE COMPLETED BY THE SUPERVIOR

This dissertation is suitable for presentation to the faculty. It has been checked for conformity with the faculty guidelines.

_____ _____

(Signature of Supervisor) **(Date)**

TO BE COMPLETED BY THE DEPARTMENTAL CHAIRPERSON

I certify to the best of my knowledge that the required procedures have been fulfilled and the preparation criteria was met in this dissertation.

_____ _____

(Signature of Chairperson) **(Date)**

STUDENT DECLARATION

I, Francis Mbirimbindo, do hereby declare that this dissertation is the result of my own investigation and research, except to the extend indicated in the acknowledgements, references and my comments included in the body of the report, and that it has not been submitted in part or in full for any other degree to any other University.

_____ _____

(Signature of Student) (Date)

DEDICATIONS

This research is dedicated to my wife (Annia), my mother, kids and the Almighty God for their inspiration

ACKNOWLEDGEMENTS

I wish to express my utmost heartfelt gratitude to my Supervisor, Ms. F. Mariwi for tirelessly working with me in carrying out this research. The success of the project is centred on her guidance, inspiration and support. Furthermore, I am indebted to my Manager, Mr. T. Hamandishe who provided me with invaluable suggestions and indispensable contributions. My sincere appreciation further goes to L. Mukwenya, E. Matondo, T. Mutizwa, D. Chigwegwe and other friends who rendered me support in terms of ideas, prayers, and inspiration and material resources. Vote of thanks also goes to my parents and family members for the support they gave to me throughout the period of my research. Above all, deep-heartedly and sincere thanks go to the Almighty God for all the blessings and inspiration during my research and study periods**.**

ABSTRACT

Banks in Zimbabwe were greatly affected by cyber risk between 2015 and 2020. During this period, the trend had threatened much the viability and sustainability of financial institutions. Given this background, the study sought to ascertain the effectiveness of risk management strategies which were employed by these banks in curbing cyber risk and test the hypothesis that poor and inadequate technological infrastructure and internal control mechanisms, absence of legislation and bank-specific factors are the major drivers of cyber risk in Zimbabwe. A combination of causal, explorative and quantitative research designs was adopted for this study. The targeted selected population were seven (7) CBZ Bank Harare branches. Judgmental sampling method was used for selection of research respondents. Secondary data used in models was sourced from sources such as CBZ reports, journals, Reserve Bank of Zimbabwe (RBZ), internet and private websites. Primary data which was used to substantiate the model results was gathered using questionnaires. The failure by the government to enact cyber laws was exposed in this study as one of the contributory factors of cyber risk. Based on research findings, the study suggests that banks should put in place vibrant risk management strategies such as running automated vulnerability scanning tools against all networked devices at least weekly and remedy any vulnerability within an agreed time frame, police the network perimeter where banks should establish multi-layered boundary defences with firewalls and proxies deployed between the untrusted external network and the trusted internal network, user education and awareness as well as maintain the Board's engagement with information risk. The Reserve Bank should embark on proactive supervision and monitoring of bank rather than reactive approach.

LIST OF ABBREVATIONS

RBZ	Reserve Bank of Zimbabwe
BAZ	Bankers Association of Zimbabwe
NRA	National Risk Assessment
OTP	One time password
ATM	Automated Teller Machine
POS	Point of Sale
PIN	Personal Identification Number
ICT	Information Communications Technology

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.0 Introduction

It is critical for companies to recognize risks that are likely to affect their day to day operations and try to manage such threats successfully. While some risks have a minor influence on business, others can result in the loss of key services, complete closure of business or losses in revenue (Ashford, 2016). Effective risk management strategies ensures that the risk's impact is minimized. In Zimbabwe, Information Technology (IT) supports the majority of the banking industry's functions and banks are can now able to perform online transactions thereby reducing unnecessary costs to the organization at the same time increasing their revenue. The major goal of the study is to see how effective these financial institutions' risk management strategies are at dealing with cyber risk.

1.1 Background of study

The banking business is one of the most technologically reliant industries worldwide and it has been noted that the wide usage of Information Technology systems in the financial service sector has seen an increased in efficiency and success in its operations. However, this has brought challenges to the sector such as hacking, distributed denial of service (DDoS) assaults, phishing, card cloning, viruses and worms which have jeopardised the security of most banks Ashford, (2016). In 2008, confidential information of about nearly ten (10) million clients in South Korea, was stolen through hacked websites. In June 2005, hackers in the United States of America (USA) stole information of at least 200,000 credit card accounts and 40 million accounts containing personal information from Card Systems Solution. According to Stechyshyn, (2015), cybercriminals managed to launch malicious programs and stole critical information from JP Morgan Chase, the United States' largest bank sometime in June 2014. Another company, TJX Companies, Inc announced that hackers unlawfully gained access into the company’s networks and stole about 45.7 million of visa and debit card credentials (Brodkin, 2007). According to a recent poll conducted, a British security software and hardware company Sophos Group PLC, 86

percent of Nigerian businesses were victims of cyberattacks in 2019. It was observed that Nigerian banks such as Unity and Access Banks were victims of data breach in August and September 2020. It was revealed in the Annual Integrated Report (2017) that most financial institutions in South African were affected by crimes related to cyber (Binuyo et al 2014). This information was supported by the South African Banking Risk Information Centre which revealed that in 2017, banks like Standard Bank, Nedbank and First Rand Bank reported 13438 cyber cases with more than R250 million losses Smith, (2018). The financial services sector in Zimbabwe has not been spared from cyber-attacks. The RBZ and the NRA reports, indicated that cybercrime caused US$1.8 billion losses every year and in the same reports, one hundred and forty incidents of cybercrime cases between 2011 and 2015 were committed of which twenty cases were phishing incidents, thirteen card fraud, ten identity theft, twenty four unauthorised access, seventy two hacking and one telecommunications piracy. An increase of cybercrime cases are noted to be on the increase regardless of substantial investment done by banks trying to improve their information security Gordon et al (2005). Despite employing various risk management strategies such as self-protection in trying to eliminate the likelihood of cyber breaches and loss protection mechanisms to minimize loss cause, CBZ bank was among the banks that were greatly affected by cyber-attacks in Zimbabwe. This was caused by complexity and widespread use of Information Technology systems like internet banking, mobile banking, e-wallets and Automated Teller Machines. As a result, it is critical for banks to pay close attention to the growing threat of cybercrime Deloitte, (2018).

Table 1.1 an analysis of cases that were recorded in the books of CBZ Holdings in 2015 to 2020

THREATS	**Number of cases recorded in each year**					
	2015	**2016**	**2017**	**2018**	**2019**	**2020**
Account Compromise	**43**	**33**	**54**	**91**	**127**	**209**
Spam emails	6	**19**	**37**	**66**	**96**	**166**
Identity Theft	**28**	**16**	**49**	**86**	**222**	**255**
Card fraud (credit & debit)	**17**	**56**	**83**	**187**	**298**	**434**

1.2 Statement of the problem

After the banks had observed a surge in cybercrimes they implemented several risk management measures to combat the problem. However, the strategies seemed to be failing to control and mitigate the increase in the cases resulting in banks losing huge sums of money to the criminals causing alarm among Zimbabwean institutions especially CBZ Bank. From 2015 to 2020, the Zimbabwean financial services industry received more client claims related to cyber risk as well as high operational risk losses which were linked to cybercrime. As a result, it is important and necessary for banks to evaluate the implemented risk management strategies to see if they are effective in fighting or curbing the problem of cyber risk.

1.3 Research objectives

The following objectives had to be accomplished in order to meet the study's goal:

1. To investigate the effectiveness of risk management strategies employed by Banks in curbing cyber risk.
2. To find out why cyber risk has increased despite the use of various risk management strategies
3. To examine if financial institutions are making significant investments in cyber risk management
4. To suggest possible remedies or strategies to curb the problem of cyber risk affecting Zimbabwean banks.

1.4 Research questions

The researcher in this case should try to provide answer for the following questions:

1. What bank specific factors have contributed to the problem of cyber risk in Zimbabwean banks?
2. What caused an increase in cyber risk despite the implementation of risk management strategies by banks in fighting cyber risk?
3. What are the possible remedies and strategies that can be adopted by banks to control the problem of cyber risk in Zimbabwean?

1.5 Statement of hypothesis

In view of the increase in cyber cases, the contention that poor implementation of risk management strategies by banks contributed much in cybercrime.

1.6 Significance of study

This research will be beneficial to quite a number of stakeholders which comprises the researcher, the banking industry, the police and the university

To the Researcher.

The study will develop an in-depth knowledge of modern risk management strategies used to curb cybercrimes

To the Midlands State University

The research is going to add value to the university through new concepts that will be revealed during the study and these concepts will be coined in the programme.

To the banking industry.

The findings of the research will suggest some remedial actions which will assist the industry address issues related to cyber risk. This will go a long way in reducing crimes that had negative impact on its reputation.

To the Regulator

The study also identifies actual regulatory gaps and supervisory deficiencies between present regulatory measures and ideal regulatory measures that the Central Bank may implement to close the gap.

1.7 Delimitation of the study.

During the period of the research, the researcher was based in Harare and the study was restricted to CBZ Bank Harare branches alone.

1.8 Limitations to the study.

During the research, there were problems which were encountered by the researcher which had an impact on the credibility and objectivity of the area under investigation. This challenges included issues such as the research was limited to a period of five-years (2015 to 2020). Only information obtained during this period was used which means there was a possibility of omitting useful data which had a significant impact on addressing cybercrime.

It was difficult to have access to restricted and sensitive information of the bank due to bank confidentiality policies. To counter this challenge, the researcher used a letter obtained from Midlands State University which states that the information obtained was strictly for research purposes only.

The researcher used questionnaires to obtain the bulk of the information used in the research. The responses were 54/70 and 16 respondents did not return the completed the questionnaires. This had a negative impact on the quantity and quality of data that was to be collected and used in the research. The questionnaire was supposed to be simple and understandable for the respondents to easily complete without difficult. Due to Covid 19 it was a challenge to conduct face-to-face interviews so the respondents were interviewed telephonically which posed challenge of not knowing whether the respondents were responding giving genuine answers.

Time to conduct the research was so limited due to other commitments like work and other school related tasks which demanded time. The researcher found it difficult to conduct face to face interviews with the respondents due to Covid 19 restrictions as such the researcher used questionnaires which were left at the respondents' place of work and collection was done on later dates.

1.9 Organization of the Study

The study was designed in such a manner that the introductory chapter outlined the background of the need to carry out the study in cyber risk. The chapter explained the statement of the problem which happen to be the main agenda of the investigation. Certain issues such as research objectives, study questions and statement of hypothesis were highlighted to give a guideline to the researcher. Further sub topics like justification of the study, scope of the study and limitations were examined to give a clear picture of the study.

Chapter Two of the research looked at literature review which was relevant to risk management strategies which were implemented by banks in curbing cyber risk. Information on this chapter

was obtained from work which was done by other researchers on internet and related books. It was of paramount importance that after the researcher had obtained useful information which formed the basis of primary and secondary data the information was used for the selection of the best research methodology which become chapter three of this study. All the information that was gathered in chapter three was presented and analysed quiet well using charts and tables in chapter four and the fifth chapter then outlined the research findings, conclusions, recommendations as well as suggestions for future studies.

CHAPTER TWO

LITERATURE REVIEW

2.0 INTRODUCTION

It has been noted that due to the results of technological improvements, the banking industry has become more efficient and successful in their operations. According to Li, (2017), these improvements on the other triggered vulnerabilities like cyber risks. Information tend to suggest that cybercriminals have shifted their focus form other sectors from the industry and they have targeted the banking industry. As a result, most of the financial services sector players have seen the biggest number of cyberattacks, which are increasing at an alarming rate. Financial institutions information sharing is one of the key risk reduction technique that should be embraced Dzomira, (2014). In an endeavor to fight cyber risk, organizations are encouraged to exchange information to supplement security operations as banks can prevent such similar incidents to those that have occurred in the past. Researchers have observed that cybercriminals are taking advantage of lack of information sharing in developing, expanding and sale of their cybercrime tools and techniques Lagazio et al, (2014). A notable achievement was noted in Zimbabwe when the banks created the Security Managers interbank platform to share information and the platform has proved to be of use.

2.1 Definition of key terms

2.1.1 Cybercrime

Cybercrime is defined as malicious acts involving computers, such as the manipulation and destruction of electronic data, unauthorized access to computer systems, software piracy, and physical damage to computer systems (Lagazio et al., 2014). According to Shalaginov et al. (2017), cybercrime includes not only harmful conduct but also the misapplication of IT systems' intended purposes. Banking institutions are vulnerable to cybercrime as a result of malicious human attacks intent on ruining or defrauding the target victim (Brady, 2018). It has been identified as a banking-specific operational risk, and it is therefore suggested that it be treated as such.

2.1.2 Strategy

According to Summer, (2009) a strategy is long term business plan to a set of competitive moves that are designed to generate successful outcomes.

2.1.3 Effectiveness

Effectiveness, according to Wojtczak (2002), is a measure of how well a specific intervention, technique, regimen, or service works.

2.1.4 Risk

According to Peter (2005), risk is the perceived uncertainty associated with a particular event. The greater the amount of risk that an investor is willing to take on, the greater the potential return.

2.1.5 Phishing

Phishing is a common form of cybercrime. Phishing, like spamming, entails the distribution of deceptive emails and texts (Minniti, 2016). These emails and messages are designed to appear legitimate in the eyes of the victims to trick them into revealing personal information such as PIN combinations, account numbers and verification codes Rama, (2016).

2.1.6 Social engineering

According to Rama, (2016), social engineering is a type of cyber-attack in which criminals employ social skills and psychological influence to trick victims into divulging personal information. A cyber-criminal can use social engineering to get private information such as enterprise records, system admission IDs and account numbers and to some extent sensitive data they require. Social engineering tactics include phishing efforts, virus attacks, and password attacks. Sending an email to someone that appears to be from a genuine friend whom he trusts is one of the most typical ways to accomplish this (Van Den Bergh & Pretorius, 2017).

2.1.7 Malware

Uppal et al (2014), defined malware as an illegal application that is loaded onto a computer system with the goal of stealing information. The United Nations Office on Drug Crime (2013) stated that malware spasms are carried out by the culprit installing dangerous software on the victim's

computer that permits them to trick the hard drive for the information they require. Malware transmissions is between computer and network systems according to Magutu et al (2011). Malicious software in cases can be built on to the system to capture communication or log key board strokes, thus bagging the operator's admittance and go through the information for passwords. Roderic (2006), described viruses and worms under the transmittable group and Trojans under the oblique class. After an illegal virus contaminates a computer, it reproduces itself, tainting the complete system thereby causing service rejection. Worms are independent and they can spread through storage devices such as USB drives or emails, resulting in a space scarcity.

2.2 Bank specific factors which contributed to the problem of cyber risk in Zimbabwean banks

2.2.1 Deficiencies in governance and risk management

According to Galorath (2006), top management responsibility and support are critical in making sure the attainment of any initiative within a business. Thus, risk management plays necessary role in the recognition that risk is a reality and assurance from top senior executives to middle class workers to categorise and mitigate risks. The importance of top management commitment and support helps the successful decision-making process in order to manage risk because they have ultimate responsibility for the business operations. According to Marshall et al. (2006), the Board of Directors should identify, understand and categorize risks in terms of their impact on the organization. They should also ensure that frameworks are in place to effectively cover all of the different types of risks. Failure to put in effective risk governance strategies, makes it difficult for senior management to appreciate organization's risk exposures Suren, (2016). Board of directors should be convinced that risks are contained within acceptable limits. Rejda (2013), on the other hand claims that the governance aspect provides sound risk reporting frameworks, allowing risk to be reported immediately and providing responsible authorities time to alter and make changes as needed. Clear reporting structures, timely risk reporting, and strategy monitoring and review are all results of good governance. Ineffective policy execution also contributes to the rise of cyber risk. The corporate security policy is owned by the board of directors of a company. Without efficient risk management and governance instruments in place, the Board lack trust in the company's policies if they being followed consistently across the board (Straub & Welke, 1998). It is difficult to manage

risk management operations when an organisation lack good governance. As a result of senior management's frequent disregard for information security issues, many information systems are significantly less safe than they could be, and security breaches are far more often and damaging than they should be. IT experts have a hard time persuading top management to invest in security projects (Lindup, 1996). Top management often supports programs that can demonstrate their cost effectiveness.

2.2.2 Internal threats

An insider such as employees, ex-employees or clients who has or had access to the organization's assets wilfully misuses that access in a way that compromises the organization's information security (Kowalski et al 2008). Internal threat is a challenge that all businesses face since employees' actions or ignorance can result in incidents ranging in severity from a few missed staff hours to unfavourable financial loss causing the business to fail. Despite the fact that some academics argue that internal dangers are more dangerous than external threats, not every company considers its employees to be a serious threat source (Leach, 2003). Humans are usually terrified of the unfamiliar and do not suspect co-workers of being crooks. As a result, we fear hackers but not people we know well, such as IT support guys, which can cause us to behave incorrectly when dealing with information security issues (Mcllwrath, 2006). Insiders have additional possibilities to wreak havoc on the organization's data security Liu et al. (2009) also observed that businesses are grappling with the problem of how to protect information that is required to be shared with insiders in order to perform or support business processes.

2.2.3 Managing Risks Associated with Vendors

Current risk management systems frequently lack precise direction on how to manage organizational risks in a proactive manner. Because of the vendor's risk to the enterprise's data and infrastructure, most IT businesses are exposed to significant risk from their vendors Liu et al. (2009). For example, the enterprise's Zimbabwe Shared Services (ZSS) vendor will have access to confidential customer data. Another example is a development firm such as EFT or Zimswitch, which will have network connectivity to enterprise infrastructure as well as crucial server resources. These areas have not been accounted for in the organizational risk profile, despite the enormous risk introduced by the suppliers. A process framework that uses a

requirement engineering method to specify security needs in advance and utilize them to build SLAs, ensuring that the enterprise's sensitive data is safeguarded and the risk of these interactions to the e-business is minimized should be put in place to manage vendors Moore, (2003).

2.2.4 Lack of legislation.

Cyber laws are a key component is fighting cybercrimes because of the intangible nature of cyberspace. It has been proved beyond reasonable doubt that law enforcement agencies lack the technical knowhow with regards to cyber risk as well they do not have appropriate regulations, automated equipment to investigate and prosecute illegal cyber transactions Gercke, (2011). As a result, cyber criminals enjoy a safe harbor due to a lack of cyberspace legal legislation. Most organizations are hesitant to report cyber-criminal activities in order to safeguard their company reputation, investor and public confidence (Harry, 2002). PWC (2011) indicated that law enforcement agencies are not able to identify the perpetrators of cybercrime or arrest and prosecute those using traditional methods. Furthermore, it has been noted that current laws were insufficiently developed to effectively arraign cyber offenders. However, Williams (2007) pointed out that while organisations continue to lose money as a result of cyber fraud, there isn't enough law in place to completely eliminate the crime.

2.3 Causes of an increase in cyber risk despite the implementation of risk management strategies by banks in fighting cyber risk.

2.3.1 Lack of education and awareness of users

Gercke, (2011) states that all users of the system are responsible for managing threats to the organization's information assets and ICT. It is important for companies to encourage their employees to part in event of knowledge sharing with other counterparts from other institutions. Clients should receive appropriate cyber training and education which is current, relevant and upto date on a regular basis so that they do not operate in silos. Banking stakeholders must engage in cyber fraud awareness and education to keep abreast with the ever changing world in ICT advancements Harry, (2002). The other challenge faced by banks is the issue of the general public's lack of understanding of cyber risk and the need for them to how to maintain a negligible amount of security to protect individual info. It is worth noting that training and education should not be done to people who use ICT systems only but even to those that are involved in fighting crime Mwaita & Owor, (2013). Effective risk

communication allows all employees of the institution to get information about the institution's risks. The Basel Committee on Banking Supervision (2013) goes on to say that adopting uniform risk language across all business units will help with communication resulting in a better knowledge of risk and increased awareness. Carey (2001) was cited by Ranong and Phuenngam (2009) arguing that communication provides the staff with the opportunity to understand their roles and responsibilities as there are spelt out in the risk management process

2.3.2 No Secure Configuration

In order for companies to curb cyber risk, there is need for properly secured configurations of their ICT systems, Claessens et al. (2002). It is highly recommended that institutions put in place ICT policies and processes to cope with system configurations and improve system functionality. Apart from policies and processes, organisations should developing strategies to eliminate all the unneeded system functionalities on ICT systems as well as making sure that the systems patched against identified weaknesses is good organizational practice Maijala (2004). By failing to put in place a secure system can negatively affect the corporate by exposing it to more risks like privacy, integrity and information in danger. According to Sheridon (2008) corporates should establish and maintain a secure ICT systems as this is major security control. Unsecured, fortified, or patched ICT systems are particularly vulnerable to attacks that could be avoided. Unauthorized changes to ICT systems or information may occur if organizations put in place unsafe and implement corporate security policies to manage system functionality as well as mending the ICT systems Barker et al. (2008). Changes can be made from the system by attackers which can jeopardise the security. Patches are issued virtually every day and applying these patches in a timely manner can be of paramount importance in maintaining the integrity and availability of the system. The attackers of the system try to get unauthorised access to system by exploiting unpatched systems Prabovo, (2011). Many effective cyberattacks are successful because criminals exploit a system weaknesses that a patch was not released before being attacked. An attacker could take advantage of a system that has not been secured or hardened Sheridon (2008). It is good to know that without awareness of identified exposures or lack of patches and fixes, security incidents will continue to affect the business.

2.3.3 Information Risk Management Regime

According to Rama, (2016), Information Risk Management Regime it the way to go for organizations to examine their risks to information assets with the same level of rigor that it would apply to other risks like legal, regulatory, financial or operational risk. In order to achieve a positive result, all risk management programs should have Board of Directors support and they should actively participate in risk management. It is critical to define and communicate the organization's risk management mindset and approach Claessens et al. (2002). The board should make it mandatory that employees and service providers are taken through the organization's risk management profile and they should convey the corporate's risk appetite statement as well as risk management policies across the organization Rama, (2016). Companies are encouraged to effectively manage their risks regularly to eliminate chances of system intrusion at the same time operating within the parameters of the company's risk appetite. In most cases the failure of any corporate lies with business failing to manage its risks. Peter (2005) states that increased risk exposure, missed business opportunities, ineffective policy execution and poor security investment result from inadequate risk management and governance frameworks and structures.

2.3.4 Network Security

The fact that most businesses around the globe now use internet services, most of them connect to untrusted networks. This exposes a threat of cyber to business thereby compromising the integrity of data the hold and process. This can be avoided, according to Pandey et al., (2016), by developing guidelines and risk supervision practices to secure company webs, as well as adopting security controls that are proportional to the threats discovered and the organization's risk appetite. Internal and external threats must be safeguarded from corporate networks. The organization's risk appetite, risk assessment and corporate security policy should all be taken into account when determining how well networks are safeguarded Amanor, (2014). Businesses that fail to adequately defend their networks risk important company information being leaked, malware being imported and exported, denial of service, vulnerable systems being exploited and corporate resources being damaged or defaced Shackleford, (2015).

2.4 Possible remedies and strategies that can be adopted by banks to control the problem of cyber risk in Zimbabwean banks.

2.4.1 Incident Management

According to Lemieux (2015), every firm will face an information security issue at some point. Improving resilience, ensuring corporate continuity, raising customer and stakeholder confidence, and minimizing financial expenses can all be aided by establishing efficient event management rules and practices. Unavoidable security incidents may occur, and their commercial consequences will vary. All incidents which trigger organization's catastrophe recovery and business continuity plans should be properly managed. Certain instances may show more serious underlying issues when examined more closely Cox and Lahti (2017). If businesses fail to adopt an incident management system to identify, handle cybersecurity events, company cannot recover after an attack. Business sometimes fail to notice and address a problem quickly may worsen the problem's impact, resulting in a long-term outage, significant financial loss, a loss of client trust, and ongoing business disruption Greetings, Rama (2016). An organization that fails to rectify vulnerabilities in its corporate security architecture and address the root cause of events risks facing frequent and costly business disruption. Failure to disclose an incident that results in the compromise of sensitive information in line with legal and regulatory standards could result in Lagazio et al (2014). So an organisation should be in a position to identify certain incidents within the company and their impact. These dictated by the organization's business profile, incident management plans should be created using a risk-based strategy that considers all business activities Lagazio et al., (2014). The impact will be determined by the organization's business profile, so incident management plans should be designed using a risk-based strategy that examines all business activities. Furthermore, the effectiveness and quality of the organization's security policies and regulations will be critical in avoiding disasters. The Board of Directors of the organization must be informed of events as well as provide guide its implementation. The organization should set aside resources to maintain incident management capable of dealing with a wide range of potential issues. This ability could be outsourced to a reputable vendor, such as one that participates in the Cyber Incident Response program. Any legal or regulatory reporting or data accountability responsibilities should be met by risk-based policy processes and strategies. The incident response team according to Kopp et al (2017) requires discipline. The company must have reputable providers of incident management training. The organization must

identify and empower certain personnel (or vendors) to handle ICT problems, as well as provide them with clear terms of reference for dealing with every type of incident that may arise. While data loss is unavoidable, the company's data asset base should be backed up in a systematic manner. All security incident management strategies should be tested on a regular basis, including Disaster Recovery and Business Continuity Mclean (2013). The test results should be utilized to help create incident management plans and evaluate their effectiveness.

2.4.2 Managing User Privileges

Controlling user access credentials to ICT as well as the information and services a company provides is best practice Egwali, (2008). If user rights are not adequately managed, the number of malicious and unintended attacks may increase. Authorized users can contaminate ICT systems by abusing the powers that have been granted to them, either purposefully or unintentionally Cassim (2011). Corporate systems and procedures have a duty to account creation and deletion when a member of staff leaves Cassim (2011). It does not matter whether the user were created for part time or for testing purposes, unused dormant accounts should be cancelled or deactivated in compliance with business policy which guides sensitivity of the passwords according to Deloitte (2014). ICT systems should have added validation element that should be put in place in the risk assessment. Business requirements and the principle of least privilege should be used to apply access controls. Users should only have access to the systems to do their jobs Deloitte (2014). Limit the number of privileged accounts that have access to the system. There is need to evaluate users more frequently than the need to keep a regular user account. User activity should be monitored, particularly any procedures like creating, changing or deleting records. Records of network device activity must separate accounting or auditing system, according to Strauss (2017). The company must restrict log in access as well as all privileged user access must be documented to avoid issues of fraud and ensure the content's integrity and availability. Everyone should be informed of the proper account usage policy as well as their own responsibility to follow company security regulations and disciplinary procedures.

2.4.3 Malware Prevention

Any information exchange carries the danger of exposing the company to malicious code and content (malware), jeopardizing the confidentiality, integrity, and availability of the

organization's data Kesh et al (2002). Lowering the risk can be a simple process. Malware can cause business to come to a standstill. Due to obvious variety, data communicated by organizations, malware can be imported in a variety of ways. Email, for example, is still the most frequent method of exchanging internal and external information Pandey et al (2016) Malware can be delivered to a company's ICT system via removable media or a networked personal device. Develop and implement rules, standards, and processes that address malware-prone business processes while simultaneously achieving overall risk management goals. All electronic data supplied to or received by the company should be scanned for potentially hazardous content. To prohibit access to known hazardous websites, make sure your perimeter gateway implements blacklisting. Two antivirus solutions should be installed and stand-alone workstations (without network connectivity) should be provided. The workstation should be able to scan content from any type of media, with each scan preferably being traceable back to a specific person.

2.4.4 Monitoring

Monitoring information and communications technology activities, according to Weiss (2002), helps businesses better detect risks and respond efficiently, as well as serve as a platform for learning lessons to improve the company's overall security. Frequent monitoring is a necessary activity to meet cyber requirements, as well as to establish whether authorized users are using the system and whether it has been or is being attacked Beh (2001). An organization should be able to monitor and detect assaults from the outside as well as attacks generated by intentional or inadvertent insider activities and threats, in order to take appropriate and proportionate action to prevent or mitigate the consequences of a business attack Ogut (2006). Recent security incidents and attacks, as well as the company's incident management methods, should be taken into account when developing the strategy. Signature-based detection for known attacks, as well as empirical detection for potentially unknown assaults based on novel or unexpected system behaviour, should be included in these solutions. There is need for an organisation to monitor its network movement for odd activity that could indicate data compromise Ogut (2006). Monitoring capabilities should be able to generate audit logs that can detect illegal or unintentional input and data misuse. Create and install a centralized system for collecting and analyzing security appliances, systems Weiss (2002). For the reason that of

the large amount of data involved, most of this should be automated allowing analysts to swiftly discover and examine anomalies. Ensure that the centralised solution's design and implementation do not allow attackers to circumvent standard network security and access constraints.

2.4.5 User Education and Awareness

Unfortunately, employees' usage of an organization's information and communication technologies involves a variety of hazards Standard Chartered Bank (2017). Employees must be security conscience at all times and they have to adhere to the company policies. It has been noted that companies must create time for training their users regarding cyber risk affecting their organisation as well as measure that should be taken to address the challenges. If consumers are unaware of their obligations in fighting cyber risk they is a likely hood of a breach in security which may cause the company to face legal and regulatory consequences Mindell, (2000). It is necessary that Users receive training on cyber risk because they are a key target for a range of assaults since they have a higher possibility of success and are less expensive to launch than technology attacks Mindell, (2000). An employee's personal circumstances may drastically change, leaving them vulnerable to seduction and forcing them to expose personal or sensitive commercial information to strangers Cassim (2011). In most cases Users who are dissatisfied with their environment have a tendency of trying to persuade or steal other user’s credentials to gain access into the systems that they are not permitted to access. The company should create and publicize a user security policy that covers allowed use as part of their overall corporate security strategy. Security measures that are appropriate and relevant to all company functions and operations should be included in all ICT systems. Contracts (terms and conditions of employment) for contractors and third-party users should be archived for any future eventuality like disciplinary action. In an ideal world, the company's technological access controls would be tied to the original user registration process. ICT staff have to enrol in a recognized certification program to further their education and formalize their expertise. Create a system for assessing the effectiveness and use of all workers' security training. The organizations must establish a security culture that encourages employees to speak up to high management without fear of reprisal regarding poor security procedures and security incidents Lemieux (2015). Any violation of the law should be punishable.

2.5 Chapter Summary

The researcher looked at information from different authors in order to examine each of the bank's present measures in order to combat an increase in the number of cyber risk cases when plans are in place.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

According to Rajasekar et al. (2013) research is a rational and systematic quest for new and useful knowledge on a certain issue. When describing the resolution, management of data, and disseminating research findings it follows defined frameworks and follows laid down procedures Williams, (2007). Research design, target population and sample techniques as well as data collection methodologies and research tools, were all described to come up with a proper conclusion.

3.1 Research design

Research design is a set of methodical processes devised by a researcher conduct the research Kolbaek (2014). The research area, the population or sample size, and the variables to be assessed should all be included. There are three sorts of study designs, according to Creswell (2003) viz quantitative method, qualitative method and a combination of the two. The researcher used qualitative research designs during the research which is characterized as an inquiry approach that asks the inquirer to make knowledge claims based on constructivist viewpoints.

3.2 Study Population

Mugo (2002) defined study population as a collection of people, things, or things from whom measures are taken, such as academics. As a result of the aforementioned definitions, it can be inferred that in order to acquire the desired findings, a study population must meet the required requirements.

3.3 Sample Size

According to Mugo (2002), sampling is a methodology of selecting a suitable sample or a relevant part of a population with the goal of determining the demographic's features or characteristics. The survey was limited to seven CBZ Bank Harare branches out of 42 across the country and respondents were either interviewed or handed questionnaires at each location.

3.3.1 Sampling Techniques

3.3.1.1 Random Method

When every unit in the population under study has an equal gamble of being picked for the sample, random selection is used, and the likelihood of a unit being chosen is not affected by the selection of other units from open populace Hopkins (2009). Cluster sampling is a technique for dividing populations into groups that is typically used when the population is spread out over a vast area that can be separated into sections. It also recognizes and provides an equal opportunity for everyone in the population to be chosen.

3.3.1.2 Non Random Sampling

It allows you to choose from a range of sample selection methods based on your personal preferences Saunders, (2014). Quotas, Snowball sampling, judgemental sample are some of the techniques to non-random probability, Elder (2009). According to the researcher, certain subjects are better suited for investigation than others. An approach was used to select respondents from the 7 CBZ bank branches. Judgmental sampling is a non-probabilistic approach of selecting respondents based on specified characteristics or characteristics (Strauss& Corbin, 1998). This method generates parameters, making it easier to select only those responders who have an impact on the problem statement.

3.4 Data collection and Research instruments

To collect data that was used on this study, the researcher used a survey design that includes questionnaires and interviews.

3.4.1 Primary Data

Information that is obtained in this category is data from specific sources rather than from a previous study. To conduct this investigation, questionnaires and telephonic interviews carried out to gather the required data.

3.4.1.1 Questionnaires

A questionnaire, is a set of pre-designed questions used to collect data from people and it contains questions and other data collection elements for research purposes Briefs (2008). The researcher

created a standard number of question questionnaire and circulated it to seven CBZ Harare branches.

Table 3.4 Breakdown of Questionnaires sent to branches

	Number of Questionnaires	Percentage Contribution
Actual returned & used for the study	54	77%
Not returned	16	23%
Total	**70**	**100%**

3.4.1.1.1 Advantages of questionnaires

Although questionnaires are affordable, the researcher was able to save money on travel expenses. They provide respondents' anonymity while simultaneously ensuring their confidentiality. Questionnaires are a simple and quick way to obtain feedback. Questionnaires could be completed in a matter of seconds or collected over the course of a day. They are attempting to eliminate interview bias. For the reason that the responder is not in close proximity to the researcher, individual questions are typically answered with greater zeal.

3.4.1.1.2 Disadvantages of questionnaires

Inquiries should not be confused and should be simple and straightforward, the abundance of data that is sometimes acquired via various ways can be misplaced. There are chances that one may not get responses since it depends on respondents' reaction. Since there are high chances that requests can be discussed beforehand, responses can autonomous. A manager can assign his subordinates to complete the questionnaires.

3.4.1.2 Telephone interviews

During telephone interviews the researcher collects data via the phone Bryman and Bell (2015). The interview technique is less expensive and it does not consume time. In contrast, data gathering is biased since it eliminates persons who do not have access to a phone.

3.4.1.2.1 Interviews advantages

Interviews help the researcher in gaining better understanding of the topic under examination Saunders and Lewis (2014). Ambiguous question can be clarified by the researcher through nonverbal communication and can be tailored to the researcher's needs, allowing them to obtain additional information through visuals and gestures.

3.4.1.2.2 Disadvantages

Interviews have a disadvantage because respondents may offer the researcher the facts they assume or hearsay, interview results can be distorted. Respondents can opt out of receiving information that isn't beneficial to them.

3.4.1.3 Likert scale

This is one of the approaches to investigate viewpoints, according to Boone & Boone (2014). In every question on the Likert scale, the respondent expresses their level of agreement or disagreement. The scale is a measure of individual's opinions and attitudes, according to author. In a questionnaire issued to CBZ Bank units, the researcher employed the Likert scale

Table 3.4 below shows a Likert scale

Item	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**
Points	5	4	3	2	1

3.4.1.3.1 Likert scale Advantages

It is simple to comprehend and can be used anywhere. The data acquired using the Likert scale is easy to generate figures, according to Boone & Boone (2015). The data collected using the scale is simple to analyse. Responders on the Likert scale are not obligated to voice an opinion and the surveys are less time-consuming and cost-effective method to gather information.

3.4.1.3.2 Likert scale Disadvantages

There is possibility that responders can either select the extreme point or say nothing at all and this have an effect on the outcome of results in that they concentrate the results in the center.

3.4.2 Types of Questions

3.4.2.1 Open ended

These questions respondents' answers open ended questions in their own way Bryman and Bell (2015). The questions solicit responses from respondents and according to Brickmann (2014), it allow the respondents to freely express their opinions without fear of being influenced by the researcher. In order to gather more information, the researcher used open-ended questions in her interviews with bank employees.

3.4.2.2 Advantages

The respondents have the right to express their thoughts completely. There is no influence when they are asked open-ended questions. According to Flowler (2013), such questions inspire respondents to express their feelings without fear. More qualitative data regarding the problem under investigation can be obtained by the researcher.

3.4.2.3 Disadvantages of open ended questions

Flowler (2013) also pointed out that, despite the many advantages of open ended questions, respondents can react to the same topic in a variety of ways. It's difficult to compile statistics and compare data from open-ended inquiries.

3.4.2.6 Disadvantages of closed ended questions

According to Houghton et al (2013), closed-ended inquiries can reveal a belief that the respondent may not have. Closed-ended inquiries limit the student's ability to use his or her imagination. Closed-ended questions might lead to simple answers on more difficult topics.

3.4.3 Secondary data

Data obtained from sources other than the first source, such as information or data gathered in another researcher's own research and filed for future references or exhibited in a larger study. This was the most effective method, and it accounts for a significant portion of the researcher's work, mainly in the collected works review and inquiry sections of this study.

3.5 Data Validation

According to Lewis (2015 the research instrument used, as well as the research plan, determine the data's validity. Validity is a sign of how complete the investigation is, according to Rea and Parker (2014). This is the most important aspect of data validity. The researcher double-checked that the data he had gathered was correct and relevant to the subject at hand. The researcher conducts face-to-face interviews to ensure that the information gathered is accurate.

3.6 Data Presentation

This refers to how data is presented on graphs or charts Matthew and Ross (2014). The researcher obtained from the bank employees quantitative and qualitative data and the data was divided into groups. Pie charts, bar graphs and tables were used to show the data in an easily understandable manner.

3.7 Data Analysis

A process of analysing and interpreting usable data Silverman (2016).This is the critical component for collecting and presentation data. Other authors described the process as a systematic method for evaluating, describing, and illustrating data obtained through statistical testing, frequency distributions, and linear regression procedures.

3.9 Summary

The researcher used various methods to solicit information from 70 CBZ staff. 54 respondents completed the questionnaires and returned them for analysis to validate the research's main goal of evaluating the bank's risk management strategies for reducing cyber risk were all discussed in this chapter.

CHAPTER FOUR

DATA PRESENTATION AND ANALYISIS

4.0 Introduction

The findings relating to CBZ Bank's risk management measures for reducing cyber risk were tabulated and analysed. The researcher used the results obtained from returned questionnaires and interviews to form the basis for the study.

4.1 Response rate

This is the number of respondents who completed questionnaires divided by total number of people participated in the study. Size of the sample and number of the respondents are the two variables to get response rate and ranges from 0% to 100%. The higher the response rate, the more likely the results are representative of the population. Response rate formula is given by Babbie (2010) as:

$$\text{Response rate} = \frac{\text{Number of valid responses}}{\text{Total number approached}} * 100\ \%$$

The scholar chose seven CBZ branches to analyse out of 42. A total of 54 of the 70 surveys were completed giving a 77 percent response rate. The questionnaires were all be used in the study as well as results of three (3) telephonic interviews. As a result, the researcher can confidently assert that the study's findings are quite reliable.

Table 4.1 Respondents participants

Respondents	**Questionnaires dispatched**	**Questionnaires returned**	**Response rate**
Managers	21	17	81%
Officers	35	28	80%
Clerks	14	9	64%
Total	**70**	**54**	**77%**

Source: Primary data

The response rate of questionnaires given to seven CBZ branches is shown in table 4.1. The researcher was able to distribute 70 questionnaires, 54 of which were completed and returned to the researcher and 16 of which were not returned at all. The researcher received a (54/70) 77 percent response rate on the questionnaire. Follow-ups were used to attain the 77 percent response rate. A response rate of more than 50%, is deemed satisfactory Hagan (2014). The researcher came to the conclusion that the questionnaire responses were acceptable.

4.2 Telephone Interview Responses

Table 4.2 Interview Responses

Section	**Interviews**	**Interviews conducted**	**Response Rate**
Retail	3	3	100%
Total	**3**	**3**	**100%**

Source: Primary Data

Table 4.2 shows the response rate for researcher's telephone interviews. Three regional managers from the retail banking sector agreed to be interviewed by the researcher. Three interviews were conducted by the researcher, all of which were successful. The response rate to the interviews was satisfactory.

4.3 Data Presentation

The following are the outcomes of the study:

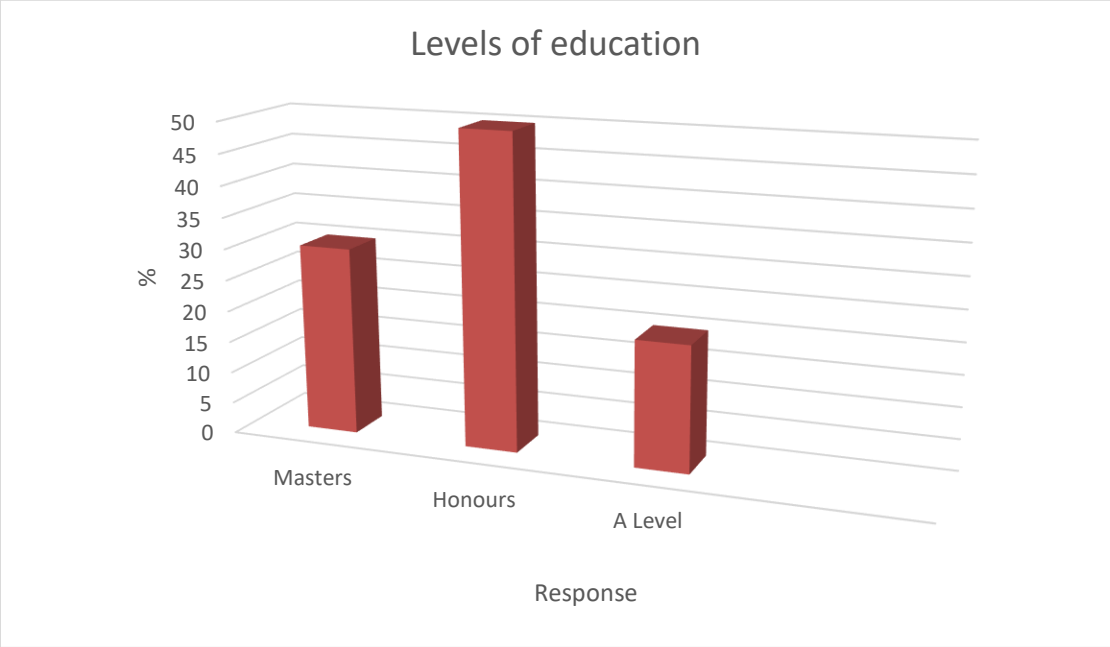
4.3.1 Level of education

This question was asked in to establish the level of education of the respondents. The level of education a person have an impact on the results. 30% respondents said they had a master's degree, 50% said they have honours degrees, and 20% said they have "A" level certificates. The table below has the statistics:

Table 4.3 Highest levels of education

Masters	**Honours**	**A Level**
30% =16	50% =27	20% =11

Figure 4.1 Highest levels of education

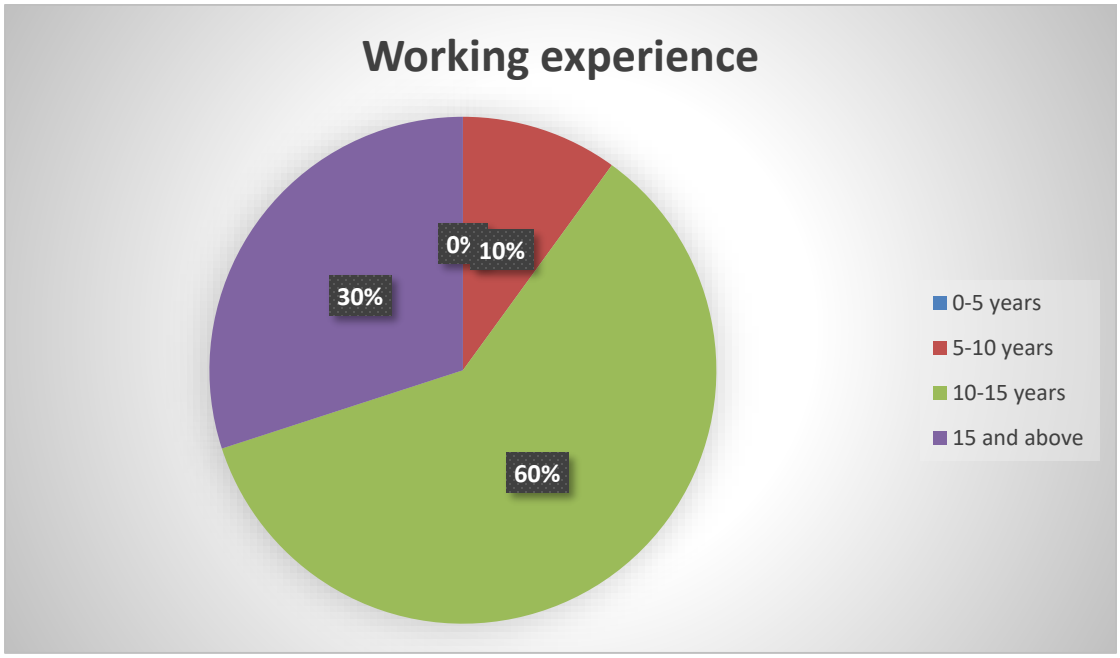


Source: Primary data

4.3.2 Work experience

The question was asked to get the level of knowledge the respondents has about their companies and cyber risk. According to the findings, 10% of the respondents were between the ages of 5 and 10, 60% were between the ages of 10 and 15, and 30% were 15 or older. The information that one has can be of use in answering the questions.

Figure 4.2 Working experience



Source: Primary data

4.3.3 Bank specific factors that have contributed to the problem of cyber risk in Zimbabwean banks.

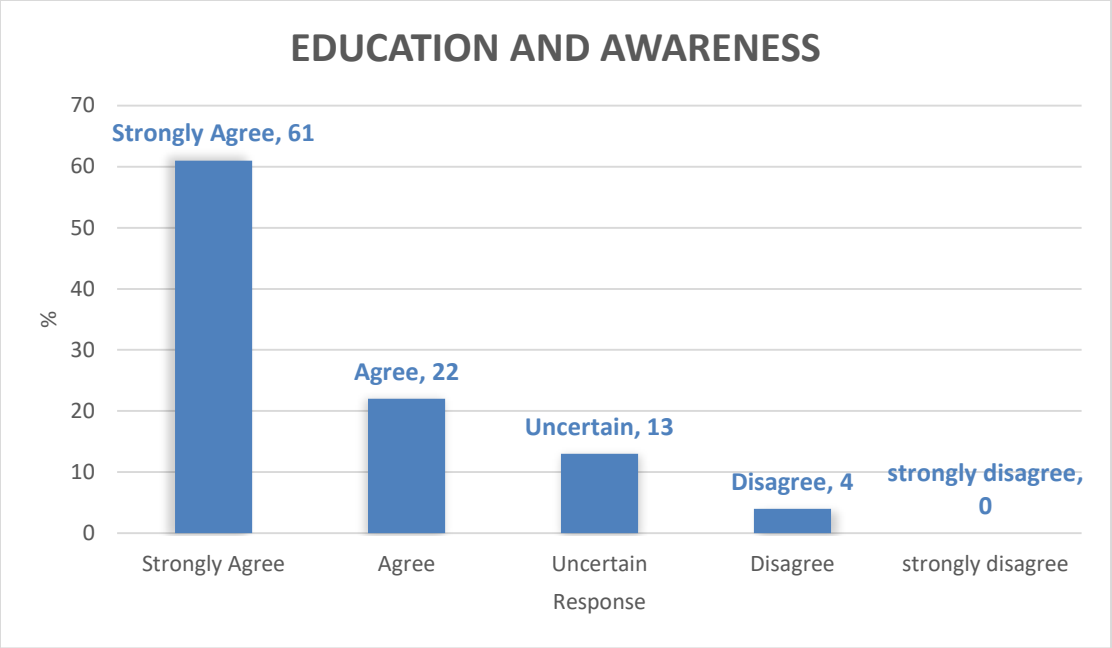
4.3.3.1 Level of education and awareness

Table 4.4 Education and awareness

Descriptions	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**	**Total**
Response	33	12	07	02	0	**54**
Percentage	61%	22%	13%	04%	0	**100%**

According to Table 4.4, 33/54 (61%) respondents strongly agreed, 12/54 (22%) agreed, 7/54 (13%) were unsure, 2/54 (4%) disagreed, and 0/30 (0%) strongly disagreed that education and training are critical in combating the rise in cybercrime instances. The researcher found that CBZ personnel and clients demand thorough cyber risk training and awareness based on the replies and findings of the interviews.

Figure 4.3 Education and Awareness



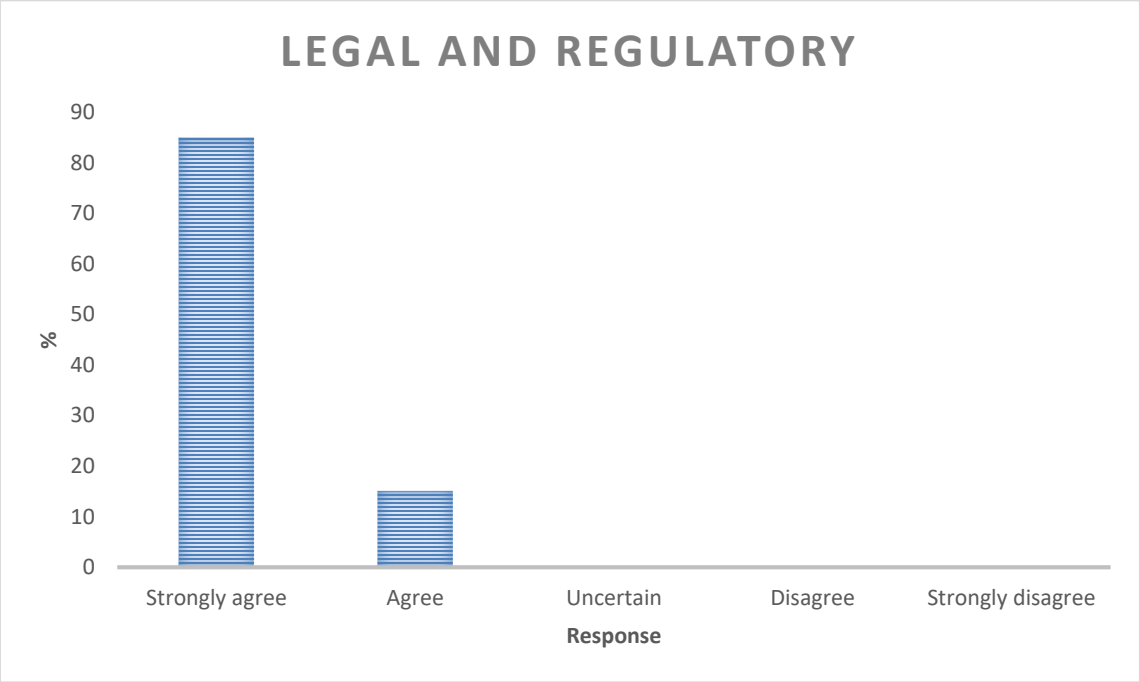
4.3.3.2 Legal and regulatory factors

The goal of the question was to see if the lack of a legal and regulatory framework at CBZ Bank is to blame for the increase in cybercrime. According to the findings, 85% strongly agreed and 15% agreed that the lack of cyber laws and regulations increases cyber risk. Due to the intangible nature of cyberspace, most law enforcement agencies lack the technological competence, regulatory authority, and automated equipment needed to investigate and prosecute cybercriminal transactions.

Table 4.5 Legal and regulatory factors

Descriptions	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**	**Total**
Response	46	08	0	0	0	**54**
Percentage	85%	15%	0	0	0	**100%**

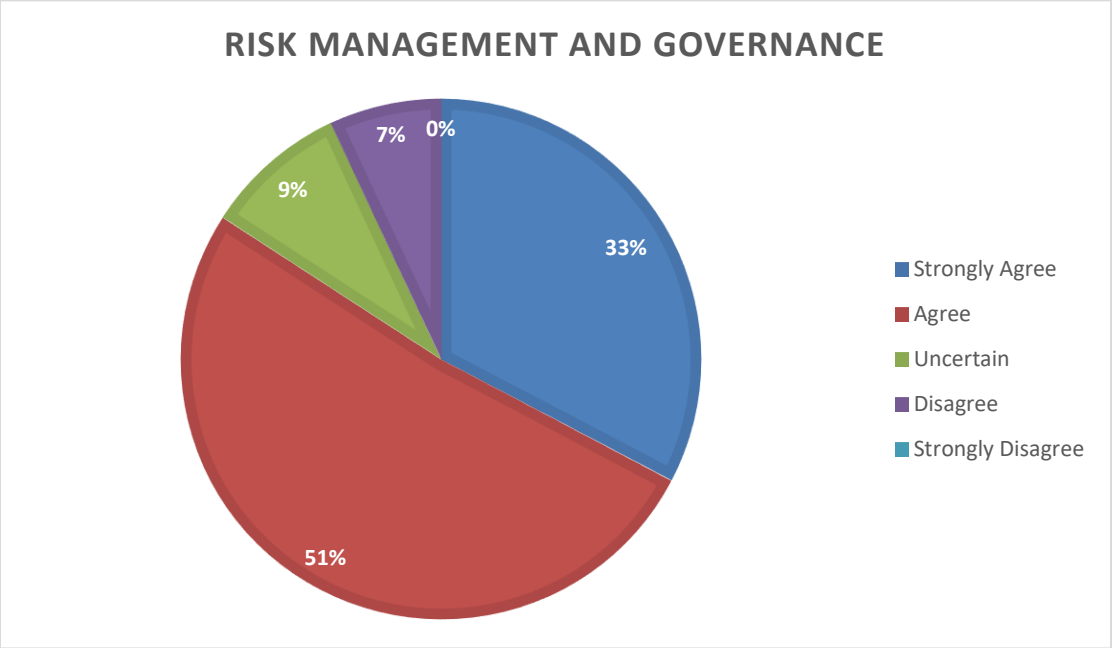
Figure 4.4 Legal and regulatory factors



4.3.3.3 Risk management and governance

According to the data collected from questionnaires, 17/54 (33%) respondents strongly agreed, 28/54 (52%) agreed, 5/54 (9%) were unsure, 4/54 (7%) disagreed, and 0/30 (0%) strongly disagreed that failing to have effective risk management and proper governance contributes to an increase in cyber risk. Top management commitment and support are critical in determining the success of any initiative within a company. According to three-thirds of respondents, failing to implement risk management and governance systems adds considerably to an increase in cyber risk.

Figure 4.5 Risk management and governance



4.3.3.4 Internal threats (staff)

According to survey results, 24/54 (44%) respondents strongly agreed, 29/54 (27%) agreed, 0/54 (0%) were unsure, 1/54 (2%) disagreed, and 0/54 (0%) strongly disagreed that insiders who have or have access to the organization's assets, such as employees, ex-employees, or clients, might intentionally misuse such access in a way that threatens the organization's assets. According to the results of the interviews, 2/3 (67%) of respondents agreed and 1/3 (37%) disagreed that staff contribute to the rise in cybercrime within the bank.

Table 4.6 Internal threats (staff)

Descriptions	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**	**Total**
Response	24	29	0	0 1	0	**54**
Percentage	44%	54%	0%	02%	0	**100%**

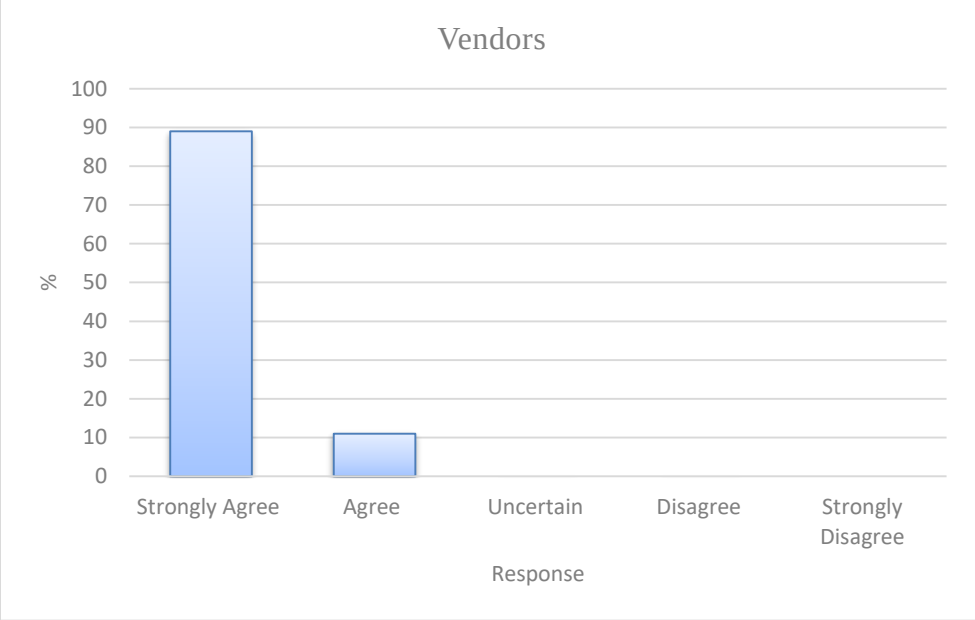
4.3.3.5 Vendor involvement

According to the table below, vendors were identified as the primary source of risk by 100% of the respondents. Vendor risk to the enterprise's data and infrastructure: Almost all of the respondents believed that the bank is vulnerable to vendors since they have access to confidential client information.

Table 4.6 Vendor involvement

Descriptions	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**	**Total**
Response	48	06	0	0	0	**54**
Percentage	89%	11%	0%	0	0	**100%**

Figure 4.5 Responses on Vendors



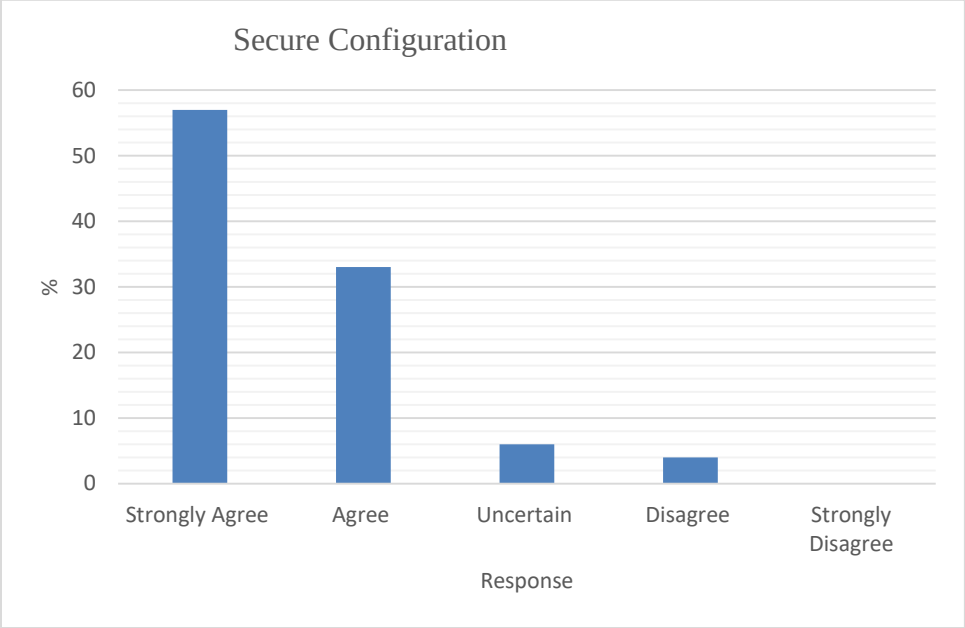
4.3.4 Causes of an increase in cyber risk despite the implementation of risk management strategies by banks in fighting cyber risk

4.3.4.1 Secure Configuration

According to survey results, 31/54 (57%) respondents strongly agreed, 18/54 (33%) agreed, 3/54 (6%) were unsure, 2/54 (4%) disagreed, and 0/54 (0%) strongly disagreed that despite the implementation of risk management measures to reduce cyber risk, there was an increase in cyber risk due to a lack of Secure Configuration. The respondents agreed that developing a plan to

eradicate unnecessary ICT systems, as well as keeping them patched against known vulnerabilities, is good organizational practice because failing to do so will almost certainly expose the business and its ICT to additional risks and vulnerabilities, jeopardizing the confidentiality, integrity, and availability of systems and data.

Figure Secure Configuration



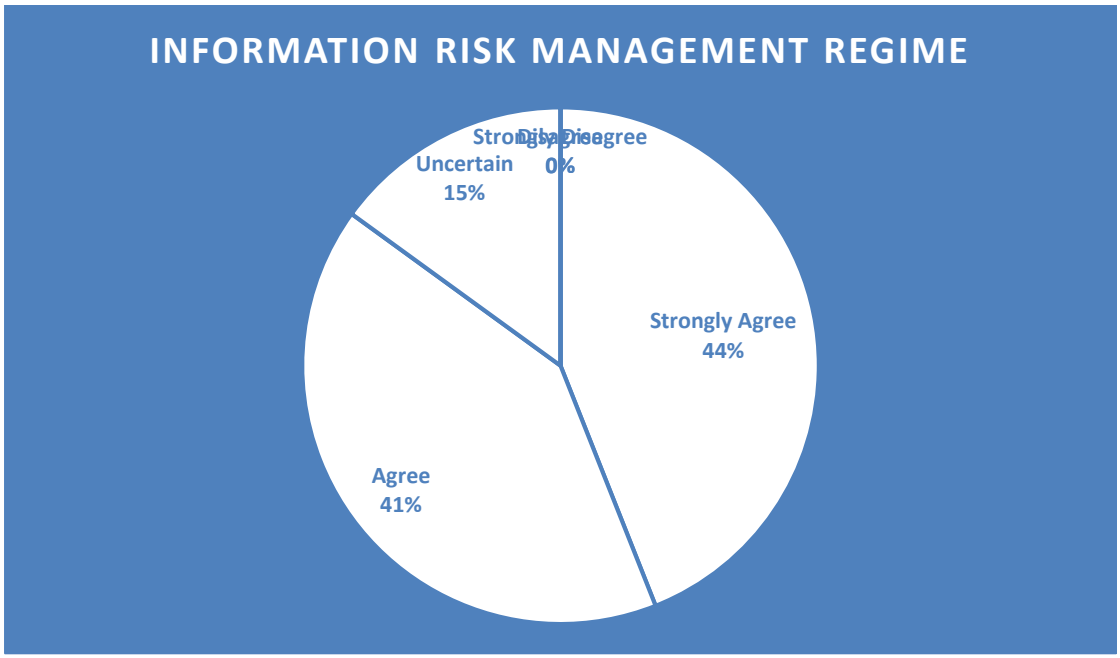
4.3.4.2 Information Risk Management Regime

Table 4.7 Information Risk Management Regime

Descriptions	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**	**Total**
Response	24	22	8	0	0	**54**
Percentage	44%	41%	15%	0	0	**100%**

According to the responses to the question on the Information Risk Management Regime attribute, 24/54 (44%) strongly agreed that it created an increase in cyber risk within the bank, 22/54 (41%) agreed, and 8/54 (15%) were unsure whether the element contributed to an increase or not. They agreed that in order to be effective, any firm must face danger and responsibly at level compatible with organizations risk appetite. The findings of the interview also revealed that neglecting to adopt effective risk management can exacerbate the surge in cybercrime.

Figure 4.5 Information Risk Management Regime



4.3.4.3 Responses on Network Security

Internal and external threats must be protected from business networks, according to the results of the interviews and questionnaires, as indicated by 46/54 (85 percent) respondents who strongly agreed and 8/54 (15 percent) who agreed that networks should be secured to reduce cyber risk.

Table 4.7 Responses on Network Security

Descriptions	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**	**Total**
Response	46	08	0	0	0	**54**
Percentage	85%	15%	0%	0	0	**100%**

4.3.5 Possible remedies and strategies that can be adopted by banks to control the problem of cyber risk in Zimbabwean.

4.3.5.1 Responses on Incident Management

Adopting good event management norms and practices, according to the results of interviews and questionnaires, can assist strengthen resilience, assure company continuity, increase customer and

stakeholder confidence, and minimize financial expenses. The findings are shown in the table below.

Table 4.7 Responses on Incident Management

Descriptions	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**	**Total**
Response	15	32	07	0	0	**54**
Percentage	28%	59%	13%	0	0	**100%**

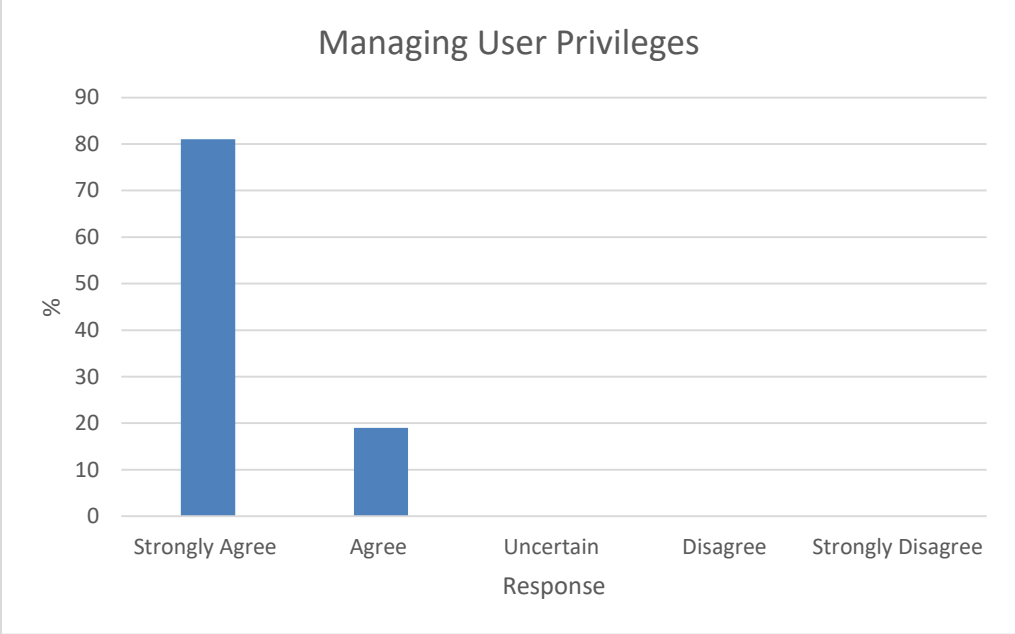
4.3.5.2 Responses on Managing User Privileges

According to the survey's findings, 44/54 (81%) strongly agreed that all users of ICT systems should only be given the privileges they need to do their responsibilities, and 10/54 (19%) agreed as well. The amount of harmful and unexpected assaults may increase if user permissions are not properly maintained.

Table 4.8 Managing User Privileges

Descriptions	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**	**Total**
Response	44	10	0	0	0	**54**
Percentage	81%	19%	0%	0	0	**100%**

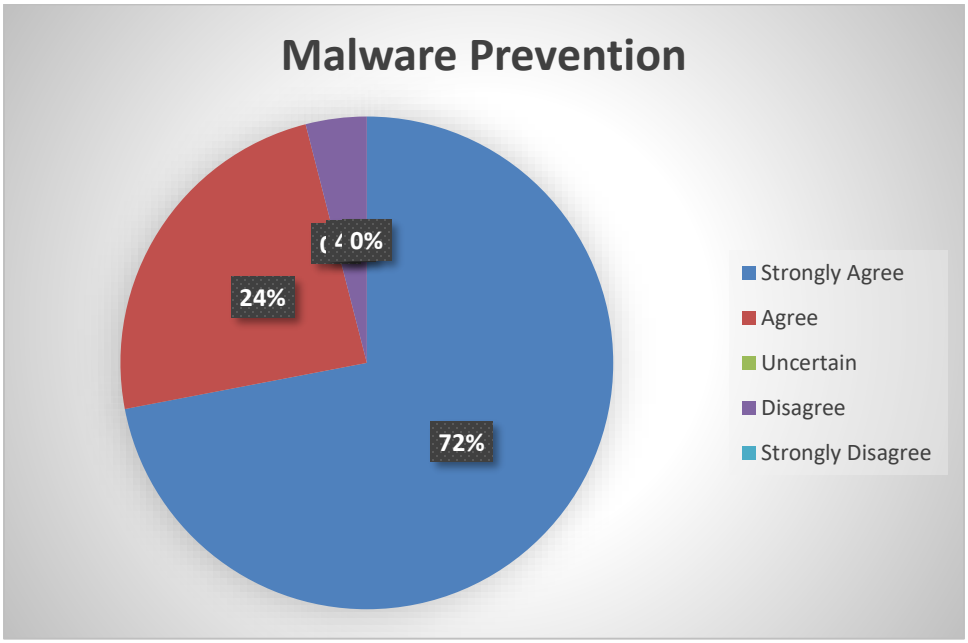
Figure 4.5 Managing User Privileges



4.3.5.3 Responses on Malware Prevention

According to the results of the questionnaires, 39/54 (72%) respondents strongly agreed, 13/54 (24%) agreed, 0/54 (0%) were doubtful, 2/54 (4%) disagreed, and 0/54 (0%) strongly disagreed that implementing security measures to decrease cyber risk can assist in lowering the organization's cyber risk.

Figure 4.6 Malware Prevention



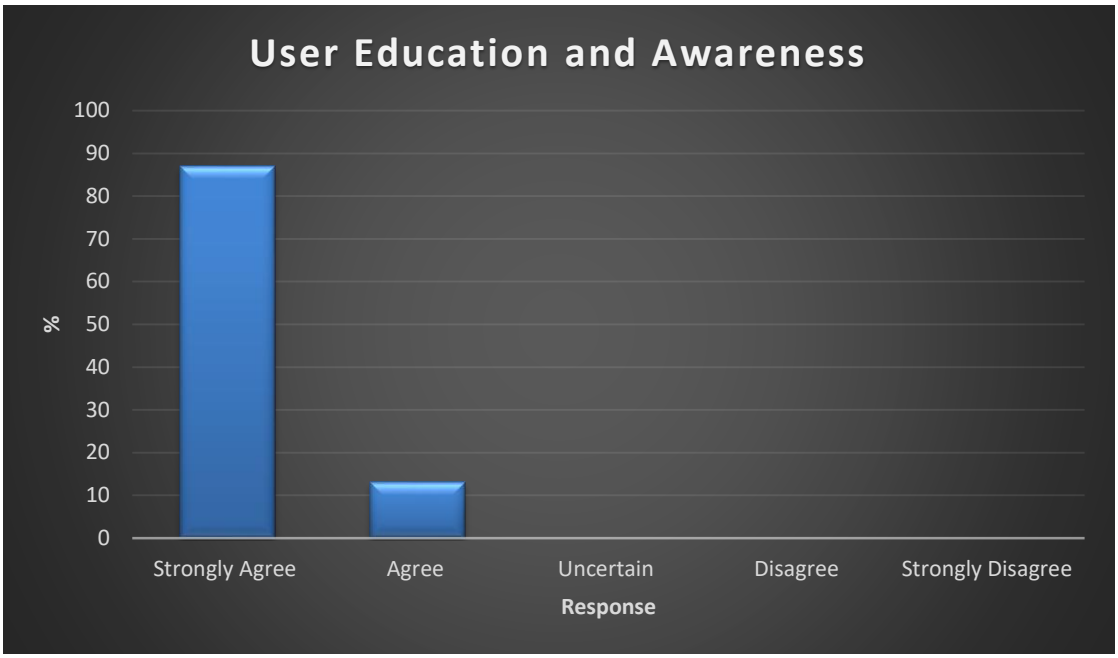
4.3.5.4 Responses on Monitoring

According to the comments from the interviews, monitoring information and communications technology (ICT) activities aids organizations in better detecting hazards and responding effectively to threats. The results of the questionnaires listed below corroborate this:

Table 4.9 Monitoring

Descriptions	**Strongly Agree**	**Agree**	**Uncertain**	**Disagree**	**Strongly Disagree**	**Total**
Response	47	07	0	0	0	**54**
Percentage	87%	13%	0%	0	0	**100%**

4.3.5.5 Responses on User Education and Awareness



According to the surveys, 36/54 (67 percent) strongly agreed and 18/54 (33 percent) agreed that user education and awareness is crucial in combating cyber risk. Users who have not been taught in the secure use of their organization's ICT systems or the operations of a security control may inadvertently compromise the security control as well as the confidentiality, integrity, and availability of data stored on the system.

4.3.6 Cyber security budget

The response to the question concerning cyber security budget revealed that the majority of employees are unaware if the company has a budget to address cyber risk, as demonstrated by 47/54 (87%) respondents who were unsure about the issue and just 7/54 (13%) who agreed that there is a budget for cyber risk.

4.4 Chapter Summary

The results of the research were analyzed and presented in this chapter in accordance with the questionnaires and interviews. The information gathered through interviews and questionnaires were processed and displayed in graphs, tables and charts. Chapter 5 included the summary of previous chapters and recommendations for the issue under study.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

Most of the information used in this chapter was primary and secondary data obtained from different sources and proposes solutions to the problems that an increase in cyber risk poses to the banking industry. The development of prospective solutions included the incorporation of reviews on the subject, as well as opinions from scholars and participants in the organization.

5.1 Chapter Summaries

The study's main purpose was to determine how effective risk management strategies are at decreasing cyber risk in the banking industry, employing CBZ Bank as a case study.

The first chapter explored how cybercrime is becoming more prevalent in the financial business. The study's background indicated that Zimbabwe's financial services sector has been hit hard by cyber-attacks, with an uptick in phishing, credit card fraud, identity theft, unauthorised access, hacking, and telecommunications piracy. The problem statement, research objectives generated from research questions, study importance, limits, and delimitations were also covered in this chapter.

The second chapter looked at the work of other authors on the factors that caused the problem of cyber risk in Banking institutions, the causes of an increase in cyber risk despite banks' implementation of management approaches in combating cybersecurity risks, and possible remedies and strategies that banks can use to deal with different situations of cyber risk in Zimbabwe. The researcher's research approach for obtaining data from CBZ Bank was outlined in the third chapter. This chapter focused on the researcher's study approach, sampling methodology, demographic, data presentation, and analysis methodologies.

The findings on CBZ Bank's risk management approaches for combating cyber risk were analysed and presented in the fourth chapter. Using the Likert scale in questionnaires, the researcher might better grasp and present the data obtained in graphs, tables, and charts. Out of 70 surveys delivered, 54 were completed and returned to the researcher.

5.2 Major Findings

It was determined that the bank's present procedures for reducing cyber risk are insufficient to provide 100 percent security. The study identified bank-specific issues such as level of education and awareness, legal and regulatory factors, risk management and governance, internal threats (employees) and security system suppliers as contributing to the problem of cyber risk. It is undeniable that the vast majority of respondents from all target audiences unanimously agreed that the bank's risk management techniques were effective, even if they were not perfect. The majority of respondents felt that the rise in cybercrime was due to a lack of secure configuration, information risk management, network security, and user education.

Human beings are the greatest threat to information technology, according to the study, and if they are not properly equipped, they can do harm to the organization. Despite having comprehensive precautions in place, staff employees' actions can create weaknesses in the system, allowing hackers to get access. The researcher discovered that the bank system was not properly protected due to a lack of secure configuration, which allowed criminals to gain access to the system and obtain information illegally, implying that more complex cyber security measures should be implemented to make the system less vulnerable to attacks. This demonstrates that the bank is reactive rather than proactive in terms of system security.

The bank's network security, according to the researcher, is critical and the bank has failed to implement a secure network that should identify, prevent and delete malware software before the system is penetrated. Continuous traffic load monitoring is required.

Effective risk management is seen as a critical component in reducing cyber risk, and management plays an oversight role in cyber risk management. Security structures should be under complete control of management, and risk assessments should be conducted to detect weaknesses in the bank's vulnerable areas. The researcher discovered that the bank has not implemented tools and models to help with efficient knowledge management from a variety of sources. Although the bank employs Basel III to control operational risk, it has been discovered that insufficient legislation contributed to the rise in cyber cases.

Vendors should be well-managed to ensure that no data is shared with third parties. The researcher also found out that the remedies and strategies which were implemented by the bank in fighting cybercrime as such incident management, managing user privileges, malware prevention monitoring information and communications technology (ICT) activities and user education and

awareness were not 100 % effective because despite them in place still the bank continued to experience an increase in cybercrime cases.

5.3 Conclusion

5.3.1 Bank preparedness to fight cybercrime

The researcher was able to conclude that the bank was caught off guard by cybercriminals. Preventive procedures, such as current and updated software and strong network security, should be implemented to reduce the danger of cybercrime. The bank should utilize access permission control mechanisms to authenticate people. There is no sufficient cyber expenditure in place to combat cyber dangers. There is no budget for cyber training and development, and the bank should prioritize cyber training for non-IT employees as well as consumers. The bank must implement invasion detection and cryptography techniques to secure data from unauthorised access. To aid in the fight against cyber risk, the bank must implement well documented cyber risk policies and processes

5.3.2 Effectiveness of existing risk management strategies

The bank is well aware of the surge in cybercrime, and current tactics have proven to be effective. However, there is a need for well-researched, well-articulated, and well-tested rules that detect and prevent unauthorized access and block it before it does harm. It is critical for the bank to ensure that procedures are in place to detect all failed log in attempts, reducing the likelihood of hackers gaining access to the system. Disgruntled employees and IT providers have been identified as a source of worry since the organization has failed to deal with them.

5.4 Recommendations

5.4.1 Effective Risk Management

The analysis uncovered a number of concerns that need to be addressed in order to combat cyber risk within the bank. As a strategy for reducing cyber risk, the bank should adopt a well-defined risk management framework. It is critical that the bank improves its preparedness to reduce the occurrence of cyber risk by implementing strong and often updated preventive systems. The system in existence should work on a two-step approval process, with a creator and a checker. In

order to reduce the cyber risk, invasion detection systems should be reinforced with control measures.

5.4.2 Effective security management system

It is advised that the bank report full compliance in terms of password protection and ongoing review of log in credentials. Any attempt to gain access to a system should be recognized and reported as soon as possible so that action can be taken. The bank should ensure that access control policies such as reactivation of individual profiles on a weekly or monthly basis, as well as automated password rests after a set amount of time, are fully implemented. Banks have to provide a robust ICT control environment, which comprises encryptions, access restrictions and ICT system configurations, among other things. The bank have a duty to set up a security operations centre to constantly observe and detect cyber threats in real intervals. Establish multi-layered detection controls for suspected cybercrime events that span procedures, expertise and persons, such as checking the physical surroundings, human actions, vendor activities, gadgets, infrastructure and programs. Data backups should be created, preserved and verified to warrant data reclamation in the event of an attack. To protect data from criminal invaders, the bank should implement encryption mechanisms.

5.4.3 Staff competency and awareness

The majority of cybercrimes were perpetrated by employees or ex-employees who revealed bank information to third parties. According to the report, employees should be properly investigated before being hired or promoted. It is also critical that personnel undergo sufficient training on a regular basis in order to remain relevant. Internal and external awareness campaigns should be conducted to ensure that everyone is aware of the hazards that exist. Although training does not produce instant observable benefits, it does have a favourable impact on the organization's ability to defend itself against external threats. The bank should decide who has overall responsibility for cyber risk management and describe the roles that each individual should play in cyber risk management. The board of directors should create a cyber risk management framework, approve it and regulate the bank's cyber risk appetite. The cyber risk management framework as well as the controls, strategies and performs that reinforce it, should be overseen by management. The government should establish legislation to assist banks in combating cybercrime.

5.5 Areas for further research

During the study, gaps were noted in the following areas which warrants future investigations

5.5.1 It is important to study the behaviour of the attackers or cybercriminals

5.5.2 It is necessary to look at the dissimilarity between policies implemented in technologically advanced and emerging economies.

5.6 Chapter Summary

The research study's primary findings, conclusion, and research problem recommendation were the emphasis of this final chapter, which integrated the prior chapters. This chapter also included a research topic for future investigation.

References

Ashford, W. (2016). Tesco Bank cyber-attack prompts security warning from Financial Conduct Authority. Computer Weekly. Available from: http://0 search.ebscohost.com.wam.city.ac.uk/login.aspx?direct=true&db=bth&AN=119484764&site=eh ost-live.

Acharya, B. (2010) Questionnaire design. Available from: The University of Tribhuvan. [06 August 2021]

Anderson, E. (2017). How to comply with the 5 functions of the NIST cybersecurity framework. Available from: https://www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework.

Ashford, W. (2016). Tesco Bank cyberattack prompts security warning from Financial Conduct Authority. Computer Weekly. Available from: http://0-search.ebscohost.com.wam.city.ac.uk/login.aspx?direct=true&db=bth&AN=119484764&site=eh ost-live (Accessed on 06 August 2021).

Brady, S. (2018). Banks lead the fight against cyber risk. Available from: http://0eds.b.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=5024671-6596-4ec3-9a6e-17d0b575c17a%40sessionmgr101 (Accessed on 06 August 2021).

Binuyo, A. O. & Aregbeshola, R. A. (2014). The impact of information and communication technology (ICT) on commercial bank performance: evidence from South Africa. Problems and Perspectives in Management,: 59-68. Availablefrom:https://www.researchgate.net/publication/268979895_The_impact_of_informatio n_and_communication_technology_ICT_on_commercial_bank_performance_Evidence_from_S outh_Africa (Accessed on 19 June 2021).

Brodkin, J. (2007). TJX breach may spur greater adoption of credit card security standards. Network World. Retrieved from http://www.networkworld.com/news/2007/032907-tjx-breach-adopt-standards.html

Creswell, J. (2003) Research design: Qualitative, quantitative and mixed methods approaches (2nd Ed). Thousand Oaks, CA: SAGE Publications.

Creswell, J. W. (2014) Research Design Qualitative, Quantitative and Mixed Methods Approach, (4th Ed).Lincoln: University of Nebraska

Deloitte. (2018). Cyber risk and regulation in Europe. A new paradigm for banks. Available from: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk /IE_FS_Cyber_risk_regulation_0218_draft32.pdf.

Elder, S. (2009) Sampling methodology. School to work transition survey: A methodological guide. International labour office. Geneva

Evaluation briefs, (2008) Data collection methods for program evaluation: questionnaires.

Evaluation briefs, (2010) Increasing questionnaire response rate.

Kgosana, R. (2018). Cybercrime costs SA almost R2.2bn a year. The Citizen. Available from:https://citizen.co.za/news/south-africa/crime/2047717/cybercrimecosts-sa-almost-r2-2bn-a-year/

Lata, P. (2016). Role of Information Technology in Banking Sector. Journal of Commerce and Management Thought, 7(1): 186-195. Available from: http://0 eds.a.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=2&sid=d09ae76e57fc-4bc4-bdf4-a780182c7ba3%40sessionmgr4007

Rama, P. (2016). An evaluation of information technology security threats: A case of the University of Johannesburg. (Mini Dissertation). Auckland Park, Johannesburg: University of Johannesburg. Available from: http://hdl.handle.net/10210/237303.(Accessed on 6 August 2021)

Sattar, S. (2014 09 June). Role of IT in banking sector. The Nation. Available from:https://nation.com.pk/09-Jun-2014/role-of-it-in-banking-sector (Accessed on 19 June2021).

Smith, C. (2018). Cybercrime now 55% of gross losses in SA banking industry – report. Fin24. Available from: https://www.fin24.com/Companies/Financial- Services/cybercrime-now-55-of-gross-losses-in-sa-banking-industry-report-20181004 (Accessed on 19 June 2021)

Shackleford, D. (2015). Combatting cyber risks in the supply chain. SANS institute. Availablefrom:https://www.raytheon.com/capabilities/rtnwcm/groups/cyber/documents/content/rtn273005.pdf.

Saunders, M., Lewis, P and Thornhill, A. (2009) Research methods for business students (5th Ed). London: Prentice Hall

Strauss, P. (2017). Cyber Threats and Responses in the Banking Sector. CSIR Conference.https://conference2017.csir.co.za/sites/default/files/Documents/Cyber%20Threats%20and%20Responses%20in%20the%20banking%20sector.pdf (Accessed on 06 July 2021)

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the Minds of Hackers. Information Systems Management, 24(4), 281 - 287.

APPENDICIES

APPENDIX A: INTRODUCTION LETTER

Midlands State University
P. Bag 9055

Gweru

16 January 2021

The Chief Human Resources Officer

CBZ Holdings

60 Kwame Nkrumah

Harare

Dear Sir/Madam

REF: PERMISSION TO CARRY OUT A RESEARCH

My name is Francis Mbirimbindo a final year student at the Midlands State University, pursing a Bachelor of Commerce in Insurance and Risk Management Honours. As part of the degree program, I am conducting a research entitled, "An investigation of the effectiveness of risk management strategies implemented by banks to curb cyber risk. A case of CBZ Bank". I am asking for your permission to conduct this research. All the information provided is guaranteed to remain confidential and will be used specifically for academic purposes.

Your assistance to this research will be greatly appreciated.

Yours faithfully

Francis Mbirimbindo R1810382X

MIDLANDS STATE UNIVERSITY

P.BAG 9055 1
Gweru
Zimbabwe

Telephone: (263)54260404/260337/260667
Fax: (263) 54 260233/260311

FACULTY OF COMMERCE

DEPARTMENT OF INSURANCE AND RISK MANAGEMENT

Date 16/01/2021

To whom it may concern

Dear Sir/Madam

Ref: Request for information for a research

My name is Francis Mbirimbindo (Registration Number-R1810382X), I am a male student at Midlands State University studying for a Bachelor of Commerce in Insurance and Risk Management Honours Degree. I am currently undertaking a research project for my final year entitled **"An investigation into the effectiveness of risk management strategies employed by banks to curb cyber risk. A case of CBZ bank."** To this end l intend to collect data by use of the attached questionnaire. I kindly ask you to complete the questionnaire. I assure you that all the information will be used for purely academic purposes only and confidentiality shall be maintained.

Should you require more information about the researcher, kindly get in touch with the chairperson of the Department of Insurance and Risk Management, Mr. F Makaza on his mobile number 0774620669.

Your co-operation will be greatly appreciated.

Yours sincerely

Mbirimbindo Francis (R1810382X)

(0772953828 fmbirimbindo@gmail.com)

APPENDIX B: QUESTIONNAIRE

Instructions

1. You are advised not to write your name on this questionnaire.

2. Please tick the appropriate answer box below for your honest answer.

Section A. Introductory questions

1. Section of operation?

   Retail Banking ☐ ICT ☐ E-Banking Service ☐

2. For how long have you been working in this company?

   0-5 Years ☐ 5-10 Years ☐ 10-15 Years ☐ 15 & above ☐

3. What is your highest academic qualification?

   A Level ☐ Degree ☐ Masters ☐ Other (specify)

State your position in the organization

Manager ☐ Officer ☐ Clerk ☐

Section B: Cyber security awareness

4. Are you aware of recent cyber-attacks in Zimbabwe? Either within your institution or others?

   Yes/No. If your answer is yes, please give an example?

5. The following factors have contributed to the problem of cyber risk in Zimbabwean banks?

	Strongly Agree	**Agree**	**Neutral**	**Strongly Disagree**	**Disagree**
Level of education and awareness					
Legal and regulatory factors					
risk management and governance					

Internal threats (staff)					
Vendors					
Secure Configuration					

6. Is the increased risk of cyber-attacks important to your institution, as the Zimbabwean banking industry moves more towards digital banking? Yes/No. If your answered is yes, please indicate if you are using tools to mitigate the risk?
7. Do you partake in any cyber-security events that address cyber-security (workshops, roadshows etc)? Yes/No

Section C: Compliance

8. Does your institution have a cyber-security risk policy? Yes/No. If your answer is yes, how often is this policy reviewed and updated to meet regulations? Does it need approval from the board? Yes/No
9. Is there sufficient collaboration between IT and Business functions to help limit cyber risk? Yes/No
10. Do you share information on cyber-attacks with other institutions or any regulatory bodies? Yes/No. Specify
11. **What are the possible remedies and strategies that can be adopted by banks to control the problem of cyber risk in Zimbabwean?**

	Strongly Agree	**Agree**	**Neutral**	**Strongly Disagree**	**Disagree**
Incident Management					
Managing User Privileges					

Malware Prevention					
Monitoring					
User Education and Awareness					

Section D: Cyber security prevention, policies and procedures

12. Do you have risk based policies, procedures and monitoring processes for the identification and reporting of suspicious activity? Yes/No

13. Do these policies and procedure need board approval? Yes/No

14. What do you think are the reasons for the increase in cybercrime despite the implementation of risk management strategies by banks in fighting cyber risk?

	Strongly Agree	**Agree**	**Neutral**	**Strongly Disagree**	**Disagree**
Lack of education and awareness of users					
No Secure Configuration					
Information Risk Management Regime					
Network Security					

15. What challenges are you currently facing as you are implementing the above named strategies?.....

.....

.....

Section E: Budget and training

16. Is there any mandatory cyber- security training provided to:

Board and Senior Committee Management	Yes/No
1st line of defence	Yes/No
2nd line of defence	Yes/No
3rd line of defence	Yes/No
Non-employed workers (contractors / consultants)	Yes/No

17. Does your institution have a cyber-security budget? Yes/No. Is the budget independent of the IT budget? Yes/No

Specify?.....

.....

.....

Your effort and time is greatly appreciated

Francis Mbirimbindo (R1810382X)

APPENDIX C: INTERVIEW GUIDELINE

1. What do you think are the reasons for the increase in cybercrime within CBZ Bank?
2. What strategies do you use as a bank in order to curb cyber risk?
3. What challenges are you currently facing as you are implementing the above named strategies?
4. What do you think makes your products so vulnerable to cyber risk than those of other banks?
5. Do you think information technology has an impact on the insurance industry and how?
6. What other strategies do you wish to use or recommend that may help decrease cyber risk within the banking industry?

Your effort and time is greatly appreciated

Francis Mbirimbindo (R1810382X)