BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

EMERGING CYBERSECURITY TRENDS IN ELECTRONIC BANKING TRANSACTIONS IN THE BANKING SECTOR. A CASE STUDY OF ZB BANK

BY

RUFARO MAPOSA

(B202102B)

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

Title: Emerging cybersecurity trends in electronic banking transactions in the banking sector.

To be completed by the student

I certify that this dissertation meets the preparation guidelines as presented in the Faculty guideline and instructions for typing dissertations

.... …………/………/……..

(Signature of student) Date

To be completed by the supervisor

This dissertation is suitable for submission to the Faculty

This dissertation has been checked for conformity with the Faculty guidelines

………………………………. …………./ …………/……..

(Signature of Supervisor) Date

To be completed by the department chairperson

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

……………………………. ………../……./………

(Signature of Supervisor) Date

RELEASE FORM

NAME OF STUDENT: RUFARO MAPOSA

DISSERTATION TITLE: Emerging cyber security trends in electronic banking transactions in the banking sector.

DEGREE TITLE: Bachelor of Commerce (Honours) degree in Financial Intelligence

YEAR GRANTED: 2022

Permission is hereby given to the Bindura University of Science Education Library to produce single copy of this dissertation and to lend or sell copy for private, scholarly or scientific research purpose. Only the author reserves the other publication rights and; neither the dissertation nor extensive extracts from it may be printed or otherwise reproduced without the author's permission.

SIGNED …………………………………………………….

PERMANENT ADDRESS: 216/12 MBIZO KWEKWE

TELEPHONE: +263779897415

EMAIL: maposarufaro97@gmail.com

DATE: /……. /……….

DEDICATION FORM

This dissertation is dedicated to my parents, who were always supported and encouraged me in my academic pursuits. Without their love and support, I would not have been able to complete this work. I also dedicate this work to my advisor Mr F Chituma, who has been a source of guidance and inspiration through my studies. In addition, I dedicate this work to my love, close friends and fellow students, who have been a source of friendship and support during my time in graduate school. Above all, I thank the Almighty God for the knowledge, wisdom, faith, love, opportunity and for his presence in my life and supporting me through the academic terrain.

ABSTRACT

The growth of electronic banking has led to increased security risks and challenges. This research therefore explores the emerging trends in cybersecurity for electronic banking transactions. It starts by providing an overview of the current landscape of cyber security threats, focusing on the rise of mobile banking and the increased use of cloud-based services. The study was guided by the following objectives; to study the nature of cybersecurity in the banking sector, determine the impacts of emerging cybersecurity trends in the banking sector, evaluating the effectiveness of the emerging cybersecurity trends to deal with cybercrime in the banking sector, recommendation on emerging trends of cybersecurity in electronic banking transactions. The research also discusses the emerging trends in cybersecurity including artificial intelligence and machine learning, biometrics, block chain technology. Finally, the study explores the challenges and opportunities for improving cybersecurity in the context of electronic banking.

ACKNOWLEDGMENTS

Strong thanks to my lecturer and supervisor, Mr F Chituma for giving me the opportunity to carry out this research. I lost hope along the way , sometimes became lazy but he would not allow me to quit, thank you very much for your able guidance, encouragement, wisdom and patience; for I would not have completed this project within the required time without an understanding and kind-hearted supervisor like you.

I also extend my gratitude to my placement workmates at Kwekwe Polytechnic for encouraging, supporting and mentoring during my attachment. I would also like to appreciate the support and commitment I witnessed from the staff at different banks in Kwekwe for their ideas, feedback and advice during the data collection process.

To Mrs Musemisi, in whose house I found a home throughout the duration of my studies, to my parents Mr and Mrs Maposa, my little brother Tinashe Maposa, my closest friends and colleague Pauline, Thelma and Dephine. I’m much grateful and appreciative.

Table of contents

CHAPTER 1

INTRODUCTION

1.0 Introduction.

Chapter one provides information on the nature of cyber security trends in electronic banking transactions. It gives a general overview of the existence and how electronic banking transactions are being made. This chapter addresses the study's background, problem statement, objective, research questions, assumptions, significance, delimitations and limitations.

1.1 Background of the study

Banking security has been challenged over times. The banking system is one of the major aspects driving the economy of a country. The internet has played a key role in changing how we interact with other people and how we do business today. Due to internet electronic commerce has emerged. Technology has advanced dramatically over the past two decades, and among the advances are computers, mobile phones, as well as the internet, which have revolutionized corporate communications (Holt and Bossler 2016). The banking sector has adopted the usage of internet electronic commerce, allowing business with their customers and other corporations to happen more effectively using the internet. Electronic banking transaction can be best defined by (Wikipedia) as an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website.

At the same time online transactions volumes have significantly increased (Mugari2016). The electronic banking system addresses several emerging trends: customers' demand for anytime, anywhere service, product time to market imperative and increasingly complex back-office integration challenges. The challenges that oppose electronic banking are the concerns of security and privacy of information. The arrangement of technologies, protocols and methods referred to as cybersecurity is meant to guard against attacks, damage, malware, viruses, hacking, data theft and unauthorized access to networks, devices, programs and data

(Chaum & David August 1992). Trends are latest technology innovations in security solutions for the digital banking industry are set to improve customer experience and safety.

Emerging cyber security in electronic banking transaction are due to increase of cybercrime threats globally and criminals concentrating on stealing information exchanged between customers and merchants particularly the cardholder information (Deloitee 2016). With the increasing use of the internet for financial transactions, there was a corresponding increase in cybercrime and fraud. As a result, financial institutions and governments began to recognize the need for improved cybersecurity to protect consumers and businesses. The emergence of new technology Data encryption.log in protection, certification, artificial intelligence, digital account opening, and API deployment are some of the emerging cybersecurity trends.

The banking sector in Zimbabwe has experienced a rapid evolution in its mode of operation, with a notable increase in electronic banking transactions. This transformation has been facilitated by advancements in technology and the growing preference for digital financial services (Smith, 2017). However, the transition to electronic banking has introduced new challenges related to cybersecurity, as the sector is now exposed to a range of emerging threats and risks associated with digital transactions (Brown, 2019).

According to recent research, the shift towards electronic banking in Zimbabwe has led to a surge in cyber-attacks targeting financial institutions, highlighting the need for heightened vigilance and improved security measures (Jones & Moyo, 2020). Moreover, the vulnerabilities inherent in existing electronic banking systems have been underscored by the increasing sophistication of cybercriminal tactics, necessitating a proactive approach to cybersecurity (Reserve Bank of Zimbabwe, 2018).

The absence of comprehensive studies focusing on the specific cybersecurity challenges within the Zimbabwean electronic banking landscape emphasizes the significance of conducting a dedicated investigation into this critical area. Previous research primarily focused on global trends and did not address the unique challenges faced by the banking sector in Zimbabwe (Chikwava & Kamujoma, 2016). Therefore, there is an urgent need to fill this research gap by examining the evolving cybersecurity trends specific to electronic banking transactions within the Zimbabwean context. This will enable the development of tailored strategies to mitigate risks and enhance the security of electronic banking systems in the country.

The aforementioned studies underscore the importance of exploring emerging cybersecurity trends within the electronic banking landscape in Zimbabwe, thereby providing the rationale for conducting a comprehensive investigation into this area.

1.2 Statement of the problem

The increasing adoption of online electronic banking transactions in Zimbabwe's banking sector has been coupled by increases in cybercrimes. Thereby the need to emerge cybersecurity trends in electronic banking transactions. Security is simply the protection of interests (Dr David Chaum, CEO of Digi Cash). The exponential growth of electronic banking transactions has revolutionized the global banking sector, offering customers unparalleled convenience and accessibility. In the recent years, the banking sector in Zimbabwe has witnessed a significant shift towards electronic banking transactions, driven by technological advancements and changing customer preferences. While this shift presents numerous benefits such as convenience and efficiency, it also brings about new challenges, particularly in the realm of cybersecurity. The increasing reliance on electronic banking systems and digital platforms has exposed the sector to a myriad of cybersecurity threats and risks that have the potential to compromise the integrity, confidentiality and availability of sensitive financial and personal information.

The problem at hand revolves around the need to identify, understand and address the emerging cybersecurity trends within electronic banking transactions specifically within the Zimbabwean banking sector. This includes an exploration of the evolving tactics employed by cybercriminals, vulnerabilities within existing banking systems and the corresponding cybersecurity measures being adopted within the sector. This is crucial given the potential impact of security breaches on customer trust, financial stability and the overall reputation of the banking industry in Zimbabwe.

In addressing this problem, this dissertation aims to shed light on the dynamic cybersecurity landscape within electronic banking transactions in Zimbabwe and contribute valuable knowledge that can inform policy makers, banking institutions and cybersecurity professions in their efforts to mitigate risks fortify the security7 of electronic banking transactions.

1.3 Research objectives

This study's goal was to look into the nature and effects of emerging cybersecurity on the banking sector. It also sought to curb concerns about electronic banking transactions from different perspectives: business to business (B2B) where by one business makes a commercial transaction with another. Customer to customer (C2C) e-commerce online platform where customers can buy and sell their products or services to each other, in the case of electronic banking transactions customers transfer money to each other. Another perspective will be that of business to customer (B2C) where businesses sell their product to customers via an online platform. The study was guided by the following objectives to accomplish the above goal;

1. To study the nature of cybersecurity in the banking sector in ZB Bank
2. Determine the impacts of emerging cybersecurity trends on ZB Bank under the banking sector
3. Evaluating the effectiveness of the emerging cybersecurity trends to deal with cybercrime in the banking sector looking at ZB Bank
4. Recommendation on emerging trends of cybersecurity in electronic banking transactions

1.4 Research questions

The research intended to answer the following questions

1. What is the nature of cybersecurity in the banking sector?
2. To what extend is cybersecurity trends impacting the banking sector?
3. How effective are the emerging cybersecurity trends in fighting concerns about electronic banking transactions such as cybercrimes?
4. How best can the banking sector implement the cybersecurity trends?

1.5 Justification of the study

The purpose of the study was to compile data on how emerging cybersecurity trends has affected positively the banking sector.

1.5.1 to the student

The researcher given the opportunity to contribute towards the topic of cybersecurity which has become a national significance, it gives her a stronger insight of cybersecurity and the emerging trends. The opportunity allowed the researcher to complete the prerequisites for the Bachelor of Commerce with Honours in Financial Intelligence.

1.5.2 to the banking sector

The project was worthwhile since it made ZB Bank employees that the researcher got to speak with aware of how vulnerable they are to the threat of cybercrime if they do not implement new cybersecurity trends. This research would help the banking sectors to develop other strategies to cope with cybercrimes and attacks.

1.5.3 to the nation

Research on emerging cybersecurity trends on electronic banking transactions can be a key source of information for policymakers, the public, and security professionals on how cybersecurity trends help to avoid cybercrime.

1.5.4 to the university

Researchers in the future looking into the same problem of cybersecurity since technology is always advancing in terms of electronic banking transactions with the aim to remove paper in businesses, the future researcher should find the study to be interesting. The study can be used as a source of literature if the university decides to publish it.

1.6 Assumptions of the study

The research was guided by the following assumptions

- Emerging cybersecurity trends can curb the concern of electronic banking transactions
- Already placed cybersecurity on electronic banking transactions are inadequate

1.7 Delimitations of the study

The study’s goal was to look into the nature and effects of emerging cybersecurity trends on the electronic banking transaction in the banking sector using ZB Bank as a case study. The purpose of the study was to determine the types of cybersecurity trends that are emerging in the banking sector and how they are helping with the concern of using electronic banking transactions. The study was restricted to the banking sector, ZB Bank in particular. Surveys were given to a sample of 10 respondents that work at ZB Bank Kwekwe as supervisors, managers and tellers. ZB Bank was selected as the site of the investigation because of the researcher residing in Kwekwe.

1.8 Limitations to the study

The major setback to this study was difficulty in obtaining comprehensive and up to date on the emerging cybersecurity trends in the banking industry. There was limitation of literature on the topic, which did not cover all relevant aspects of cybersecurity for electronic banking transactions. The researcher put up the necessary effort, perseverance accomplish the study's goal.

Another difficulty the researcher encountered was information confidentiality. Many respondents were hesitant to share information out of concern of their work contracts they sign that indicates the important of confidentiality. To conquer the issue, the researcher did not ask for identities of the respondents to maintain privacy and confidentiality.

2.0 Chapter Summary

Chapter one outlined purpose, background, statement problem and significance of the study. The chapter also highlighted on the assumptions, delimitations and limitations to the study including definitions of terms. Subsequent to this chapter is Chapter Two which focused on literature review. Empirical literature, conceptual and theoretical framework on emerging cybersecurity trends on electronic banking transaction were discussed in Chapter Two.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction.

The chapter scrutinized relevant literature from other cybersecurity researchers. Reviewing emerging cybersecurity trends on electronic banking transactions from sources such as journals, articles, books and newspapers, literature review can provide comprehensive understanding of the research objectives. Theoretical literature, conceptual framework and empirical evidence relative to trends of cybersecurity on electronic banking transactions in the banking sector were highlighted in this chapter.

2.1 Purpose of Literature Review

Literature review is critical analysis on the existing research on a particular topic (Smith, 2016). Literature review is vital in research since it provides the foundation on which the research is based (Saunders, Lewis, Thornhill, 2016:74). A literature review on emerging cybersecurity trends will examine the latest research on the evolution of cyber threats and security measures. It includes research on new types of cyber-attacks and new methods of defense. The following section of the literature review focused on the conceptual framework.

2.2.0 Conceptual Framework

2.2.1 The concept of emerging cybersecurity trends

Cybersecurity is a process of protecting information by preventing, detecting and responding to attacks (NIST; 2018). Alternatively, cybersecurity refers to the technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access (ENISA, 2013). One thing all d   definitions have in common is that cybersecurity involves the protection of attacks. As such, it is crucial to comprehend various manifestation and modus operandi of cyber-attacks and threats. Some of the types of cyber threats were explored in the section that follows.

2.2.2 Forms of Cybersecurity in electronic banking transactions

2.2.2.1 Firewall

Firewalls play a crucial role in protecting sensitive financial data exchanged during electronic banking transactions. They examine network traffic, inspecting packets for suspicious patterns, unauthorized access attempts, or malicious activities (Sarangi et al., 2019). A firewall serves as a protective barrier between the internal network of a financial institution and the external internet, controlling and filtering network traffic to prevent unauthorized access and potential cyber threats. By analyzing incoming and outgoing data packets, firewalls enforce security policies and rules to ensure the confidentiality and integrity of electronic banking systems. Firewalls allow only authorized connections and block potentially harmful traffic, such as malware or hacking attempts, this prevents unauthorized individuals from gaining access to customer accounts, transaction data, or other sensitive information. Firewalls help safeguard electronic banking systems from Distributed Denial of Service (DDoS) attacks. These attacks aim to overwhelm network resources, making systems inaccessible to legitimate users. Firewalls can detect and mitigate DDoS attacks by filtering out malicious traffic, preventing disruptions to electronic banking services (Tamilselvan et al., 2020).

2.2.2.2 Encryption

Encryption is a fundamental form of cybersecurity in electronic banking transactions, providing a strong layer of defense to protect sensitive data from unauthorized access and interception. In electronic banking transactions, encryption plays a crucial role in safeguarding the confidentiality and integrity of customer data, financial details, and transaction information. By encrypting this data during transmission and storage, financial institutions ensure that even if it is intercepted by unauthorized individuals, it remains unreadable and unusable (Kshetri, 2019). Modern encryption algorithms, such as Advanced Encryption Standard (AES) are widely employed in electronic banking systems. These algorithms provide strong cryptographic protection, making it extremely difficult for attackers to decipher the encrypted data without the corresponding decryption key (Bhunia et al., 2020). The use of encryption in electronic banking transactions not only protects customer data but also helps maintain the trust and confidence of customers in the security of online banking services. It demonstrates the commitment of financial institutions to safeguarding sensitive information and complying with industry regulations.

2.2.2.3 Multi-factor authentication (MFA)

In electronic banking, MFA typically involves the combination of two or more authentication factors, such as something the user knows (e.g., password or PIN), something the user has (e.g., a physical token or mobile device), or something the user is (e.g., biometric characteristics like fingerprints or facial recognition). By requiring multiple factors, MFA significantly reduces the risk of account compromise even if one factor is compromised (Moustafa, 2020). Multi-factor authentication (MFA) is a crucial form of cybersecurity in electronic banking transactions, providing an additional layer of protection by requiring users to provide multiple forms of identification to verify their identity. It helps mitigate the risk of unauthorized access and strengthens the security of customer accounts and transactions. Research has shown that MFA can effectively reduce the risk of account compromise and unauthorized transactions. A study by Campagna et al. (2019) found that financial institutions that implemented MFA experienced significantly lower rates of account takeover compared to those that relied solely on passwords.

2.2.2.4 Secure payment gateway

Secure payment gateways provide a secure and encrypted channel for the exchange of sensitive financial information between customers, financial institutions, and merchants. They play a vital role in ensuring the confidentiality and integrity of payment data during online transactions. Secure payment gateways employ various security measures to protect sensitive financial information. One key aspect is the use of encryption protocols such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to establish a secure connection between the customer's device and the payment gateway (Choudhury et al., 2021). Secure payment gateways often utilize tokenization techniques. Instead of transmitting actual credit card information, a unique token is generated and used for the transaction. This tokenization process ensures that even if the transaction data is intercepted, it is meaningless to an attacker without the corresponding tokenization system (Bhunia et al., 2020). The use of encryption, tokenization, and strong authentication mechanisms ensures that electronic banking transactions are conducted securely, reducing the risk of data breaches or unauthorized access to sensitive financial information.

2.2.2.5 Transport Layer Security (TLS)

Transport Layer Security (TLS) is a critical form of cybersecurity in electronic banking transactions, providing secure communication channels over the internet. It is a cryptographic protocol that ensures the confidentiality, integrity, and authenticity of data exchanged between clients and servers during online banking transactions. TLS incorporates mechanisms for server authentication, ensuring that clients are communicating with legitimate servers. It uses digital certificates, issued by trusted certificate authorities (CAs), to verify the authenticity of the server's identity (Dierks & Rescorla, 2008). This prevents man-in-the-middle attacks and protects against phishing or spoofing attempts.

2.2.2.6 Data loss prevention (DLP)

Data Loss Prevention (DLP) focuses on safeguarding sensitive information from unauthorized disclosure, leakage, or loss. It involves implementing policies, technologies, and controls to prevent the accidental or intentional exposure of sensitive data, ensuring its confidentiality and preventing financial and reputational damage. In the context of electronic banking transactions, DLP encompasses various measures to protect customer data, transaction details, and other sensitive information. It involves identifying and classifying sensitive data, such as personally identifiable information (PII), financial account numbers, or authentication credentials (Kabay et al., 2020). By encrypting sensitive data during transmission and storage, financial institutions ensure that even if it is intercepted or compromised, it remains protected and unusable.

2.2.3 Impacts of cybersecurity on electronic banking transactions

2.2.3.1 Data privacy

In the digital era, where vast amounts of sensitive customer information are transmitted and stored electronically, maintaining the privacy of this data is of utmost importance. Data privacy is an impact of cybersecurity in electronic banking transactions. Cybersecurity measure such as secure communication protocols and encryption techniques are employed by financial institutions to safeguard customer information and protect it from unauthorized access or interception (Smith, 2019). Encryption converts data into unreadable code, ensuring that even if intercepted it remains incomprehensible to malicious actors. Secure communication protocols such as Transport Layer Security (TLS) establish encrypted connections between user’s devices and banking servers, ensuring that data exchanged during electronic transactions is protected (Jones, 2020). This prevents attackers from eavesdropping on sensitive information such as account numbers, passwords and transaction details. Banks must ensure data privacy to avoid legal consequences and maintain the trust of their customers (Brown, 2018). Individuals need assurances that their personal and financial information is secure promoting confidence in conducting online banking activities. When customers trust that their data is protected, they are more likely to engage in electronic transactions, contributing to the growth and success of digital banking services (Peltier, 2020).

2.2.3.2 Secure Authentication

With the increasing prevalence of online banking, ensuring the identity of users is paramount to prevent unauthorized access and protest sensitive financial information. Two-factor authentication (2FA) and multi-factor authentication (MFA), play a vital role in enhancing the security of electronic banking transactions (Wang, 2018). Authentication methods require users to provide additional evidence off their identity beyond traditional username and password credentials. One-time passwords (OTP) is a commonly used form of secure authentication. OTPs are temporary codes generated from each login attempt and are typically sent to the user’s registered mobile device. It adds an extra layer of security by requiring users to possess both their password and the unique OTP to gain access (Khan, 2021). Financial institutions employed the biometric authentication such as fingerprint and facial recognition. Biometric data is unique to each individual, making it difficult for unauthorized parties to replicate or forge (Lin, 2019). When users are assured that their accounts are protected by robust authentication measures, they are more likely to trust the platform and engage in online banking activities (Lau, 2018). In turn, contributes to the growth and adoption of digital banking services.

2.2.3.3 Fraud Prevention

Financial institutions face increasing threats from various types of fraud such as identity theft, unauthorized transactions and account takeover because online banking continues to evolve and expand. Cybersecurity measures play a vital role in detecting and preventing fraudulent activities, safeguard both the financial institution and its customers. Fraud detection systems utilize sophisticated algorithms and machine learning techniques to analyze patterns, trends and anomalies in transaction data (Bishop, 2019). Monitoring and evaluating transactional behaviour, these systems can identity unusual or suspicious activities, flagging them for further investigation. This enables early detection and prevention of fraudulent transactions, protecting both the financial institution and its customers from financial losses (Chen, 2020).

Anomaly detection techniques help identity deviations from normal user behaviour, such as sudden large transactions or login attempts from unfamiliar locations (Hoffman, 2021). This not only protects the institutions assets but also safeguards the trust and confidence of customers. Customers feel secure in their online banking activities, they are more likely to engage in electronic transactions and maintain long-term relationships with the financial institution (Laureani, 2021).

2.2.3.4 Transaction Integrity

Maintaining the integrity of transactions is essential to ensure that funds are transferred accurately and securely without any unauthorized modifications and tampering. Transaction integrity is an impact of cybersecurity in electronic banking transactions. Digital signatures is an aspect of transaction integrity, by applying unique digital signatures to transactions, financial institutions can ensure that the transactions, details remain tamper proof and that any modifications can be detected even alterations. It provides an additional layer of security and trust in the electronic banking process. Digital signatures employ cryptographic techniques to verity the authenticity and integrity of electronic documents and transactions (Aloul, Zahidi, & Al-Sharhan, 2018). Transaction verification mechanisms, such as transaction reconciliation and audit trails, contribute to transaction integrity. Reconciliation involves comparing different transaction records to ensure consistency and accuracy (Chen, 2019). Audit trails provide a record of all transactions and associated activities, enabling traceability and accountability (Bash, 2020). These mechanisms help identify discrepancies or anomalies in transactions allowing for prompt investigation and resolution of any integrity issues.

2.2.3.5 Customer trust and confidence

In an increasingly digitalized banking environment customers rely on financial institutions to safe guard their personal and financial information. Cybersecurity measures play a vital role in fostering customer trust and confidence, ensuring the security and privacy of their electronic banking transactions. When customers perceive that their financial institution has implemented strong cybersecurity measures, they feel more confident in conducting electronic banking transactions (Lau, 2018). Encryption, secure authentication and fraud prevention mechanisms demonstrate the commitment of the institution to protect customer data and prevent unauthorized access. This instills a sense of trust and reassurance, encouraging customers to engage in online banking activities. When financial institutions are transparent about their cybersecurity policies, procedures and compliance with industry standards, customers have a clearer understanding of the security measures in place (Lau, 2018). Regular communication about cybersecurity updates, awareness campaigns and guidance on safe online banking practices further enhance customer confidence in the institution's commitment to their security.

2.2.4 Forms of Electronic Banking Provided by ZB Bank.

2.2.4.1 Internet (online) banking

Yibin, (2003), defined internet banking as the endowment of retail and low value banking products and services through the internet. Chang and Hamid (2010), also defined internet banking as the process were customers conduct banking transactions electronically or online without the need to visit the bank. According to Postal and Telecommunications Regulatory authority of Zimbabwe (2015), there has been an increase in the penetration of internet, statistics showing a penetration rate of 50% in 2015. The introduction of broadband internet by Powertel, Africom and Econet has enhanced the growth of internet banking in Zimbabwe.

2.2.4.2 Mobile banking

Arcand, Promiene, Brun and Rajaobelina (2017), defined mobile banking as service offered by banks to customers to enables them to conduct financial transactions using mobile devices without visiting the banks. Similarly, mobile banking was defined by Okiro (2013), as endowment of financial and banking services via gadget such as mobile phones. It is usually done via SMS or the internet. According to Haris, (2010), postulated that, mobile banking enables customers to access financial services from even at the comfort of their home. MPS (2012) posits that, mobile phone adoption in Africa has raised abruptly, Zimbabwe being one of it. Mobile money in Zimbabwe provides payment and financial service that are easier to access and quicker. Almost every bank in Zimbabwe has adopted mobile banking services.

2.2.4.3 Smart Cards

A smart card can be described as an embedded integrated circuit that can be a microcontroller with a security token (Shuabi, 2010). Amedu (2005) defined smart card as a plastic device containing an embedded integrated circuit that is used to resolve financial obligation. A smart card can be either a debit card or a credit card.

2.2.4.4 Credit Cards

A credit card is issued by banking institutions that permits holders to borrow funds, usually at the point of sale (Deitel et al, 2001). Essinger (1999) defined credit card as a card provided by a bank that allows the owner to access their account through the bank's website. Visa and MasterCard are two examples of credit cards.

2.2.4.5 Debit cards

Shuabi (2010) described a debit card as a plastic card that enables cardholder to have access to bank accounts electronically and to make payments. It is a type of payment card in which the amount is deducted for every transaction made by the cardholder (Nwaolisa and Kasie, 2012). In some cases, a debit card can also be used as an ATM to withdraw cash and check bank balance.

2.3 Theoretical Literature

This study was mainly influenced by the Routine activity theory as advocated by Cohen and Felson. However, other theories relevant to the study were also considered.

2.3.1 Routine activity theory

It assumes rational decision-making offender, the theory is part of the Classical school framework. Routine activity theory was developed by Lawrence Cohen and Felson. The theory recognized the components of crime Felson (1998) identified the mechanisms of crime that must be combined, specifically, the motivated offender, appropriate targets, and a lack of guardianship. This theory is premised on that, many crimes are committed in the daily routines of people who identify the inviting opportunity to commit crime. The usage of online and mobile banking systems on a daily basis creates an opportunity for crime to be committed. The theory can be applicable in this research study, as the rise of cybercrime risk can be attributed to technological advancement in the banking sector which has increased a number of motivated offenders.

2.3.2 Space transition theory

This theory was currently put forward by Jaishankar (2008). It describes the nature of people behaviour in both physical space and cyberspace. The theory involves the movement of people from one space to another, for instance, from physical space to cyberspace and vice versa. People with suppressed criminal behaviour in the physical space have a higher tendency to commit crime in the cyberspace. Jaishankar (2008), poses that, identity flexibility and lack of a deterrent factor in cyberspace give the offender options to commit cybercrime. However, the theory can point the rapid increase in cybercrime in financial institutions.

2.3.3 The Theory of Technology-Enabled Crime

This integrates numerous groups of criminological theories to help in having a better understanding on why crimes co-evolved with computer and telecommunications technologies became the most complex types of crimes to avoid and control. When criminals invent something new and innovative, the law enforcement agencies should step up to control, deter as well as to counter new forms of crime. Technology-enabled crimes are those crimes committed directly against computers and networks. The activities that falls into this category are referred to as high technological crimes, cybercrimes or computer crimes. The theory postulates that the utilization of technology facilitates the commission of crimes. The theory provide a platform for understanding contemporary threats that are posed by emerging forms of cybercrime and security measures and ways of preventing and controlling crime. The theory is useful to this study as it gives an understanding of the new methods and tools being utilized by cyber criminals in committing crimes.

2.4 Empirical Evidence

2.4.1 The Emerging Threat to the Financial Services Sector in Zimbabwe

The study was conducted by Mugari, Gona, Maunga and Chiyambiro (2016). The study ought to single out the types of cybercrime prevalent in the financial sector in Zimbabwe and to identify how effective the current measures for reducing cybercrime in the financial sector in Zimbabwe were. The study also aimed at identifying what would be done to prevent and control cybercrime in financial institutions in Zimbabwe. The study was confined to Harare metropolitan area. The research results shown that hacking was a challenge in the financial institutions in Zimbabwe with an average of 75% respondents saying it happens at their work places while identity theft and malicious software were also prevalent. Mugari et al (2016) concluded that cybercrime is prevalent in the financial institutions, with hacking, identity theft and malicious software as the most prevalent cyber threats. Control measures such as training, updating software's and firewalls topped up the list of strategies to curb cybercrime.

2.4.2 Study of the Impact of Cybercrime on Business in Canada

The study was done by the International Cyber Security Protection Alliance (ICSPA) in Canada. The study researched on the prevalence of cybercrime and its effect on their business operations. The survey of business was conducted across 520 small, medium and large businesses in the finance, airline/shipping, telecommunications, utilities, retail sector and defense and aerospace. The study revealed that cybercrime was fairly prevalent among Canadian business with 69% reporting some kind of attack within a twelve month period. The types and frequency of attack varied depending on the nature and size of business. Malware and virus attacks indicated to be the most prevalent with phishing and social engineering coming second. The cybercrime conducted resulted in total losses of approximately $5.3 million or 14 000 per affected organisation on average. Malware and virus attacks were the most common form of cybercrime and over a period of 12 months, 51% of organisations experienced them. Respondents reported 1 701 malware and virus attacks and represented 6.6 attacks per affected business. A summary of attacks showed that financial and retail sector experienced most attacks. The study will bring a broader perspectives of cybercrime being faced by business. The same theory and findings can also be used to explain the impacts of cybercrime in emerging cybersecurity trends in electronic banking transactions in the banking sector in Zimbabwe.

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

The aim of the study was to investigate the extent to which cybercrime influences performance of commercial banks in Kenya. The study used explanatory research design and targeted the tier one bank of Kenya since it serves the highest number of customers. The study results showed that, average respondents agreed that the insurance cost of protection against cybercrime is affecting the performance of the bank which in turn affects the innovativeness of banks. Banks expend at least 2% of its revenue in paying the victims whose information has been hacked and the reputational cost is huge. Many respondents were of the view that, repeated cyberattacks tend to damage the status of the bank and in return affecting the overall operations. The results of this study made the researcher to find out if it is the same case in Zimbabwe’s banking sector.

2.4.4 Frank and Odunayo, (2013). – Approach to cyber security issues in Nigeria, challenges and solutions.

The study was carried out in Nigeria. The aim of the study was to assist people and businesses in reducing the exposure of their information and networks as helping them in nurturing a cyber-security culture. The sample size was obtained from the Nigerian commercial businesses and individual and the data was gathered using interview and online questionnaires. The study findings noted that, cybercrime is causing institutions to nearly face collapse. The researchers noted that lack of consciousness and training is one of the down sides of fighting cybercrime. The study advocated that institutions and individuals should always ensure that their information is protected and they employ all necessary measure to fight cybercrime.

2.4.5 International Journal of Computer application Issue 4, Volume 1 (2014) – Cybercrime changing everything; an empirical study.

This study looked at an overview of cybercrime, cybercrime perpetrators, and their motivations, as well as a detailed study of various cybercrimes, as well as exceptional encounters that may be met in the process of prevention, detection and investigation. The growth of internet technology has come with a rise in cybercrime opportunities. Computer crimes have stretched including cyber extortion, cyber laundering, and software piracy among others. Law administrators have been unsatisfied by legislators' incapacity to keep cyber-crime legislation up to date with the fast-moving technological curve. Simultaneously, legislators must strike a balance between competing interests. The nexus of this study with the one being conducted is that, it factored in the issue of internet technology growth, which was the cause of cybercrime.

2.5 Summary of previous studies and identifying the research gap

Njeru and Gaitho (2019) conducted the study on examining degree to which cybercrime impacts performances of commercial banks in Kenya. The findings showed that, average respondents agreed that insurance cost against cybercrime has an overall effect on the overall performance of banks. Due to time and geographical factors, the results of this study may differ with where the researcher is undertaking his research, hence, creating a research gap.

The ICSPA in Canada conducted the research. The research looked into the commonness of cybercrime and how it affected their business operations. According to the research, malware and virus attacks were found to be the furthermost common, followed by phishing. This study created a research gap as it only looked at the 19 prevalence of cybercrime in general business set-up, hence, the researcher will be specific on financial institutions domiciled in Kwekwe, ZB Bank in particular.

The nature of ICT changes every day and it varies with place and level of development within a country, this means that, opportunities and threats arise each and every day. This research however, concentrated on emerging cybersecurity trends in electronic banking transaction. There have been limited researches that were done to explore the emerging cybersecurity trends in electronic banking transactions performance of financial institutions in Zimbabwe and also, differences in time and geographical locations motivated this research to be conducted, therefore, creating the foundation for the study.

While previous studies have shed light on the importance of emerging cybersecurity trends in electronic banking transactions, there is a research gap in terms of comprehensive investigations that consider the collective impact and practical implementation of these trends. Bridging this gap would provide valuable insights for financial institutions, policymakers, and researchers to develop effective strategies and solutions to enhance the security of electronic banking transactions.

2.6 Summary

This chapter focused on conceptual framework, theoretical literature and empirical evidence on the emerging cybersecurity trends on electronic banking transaction. The next chapter focuses on the research methodology used to in the study.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

This chapter presents the research methodology employed to investigate and analyze emerging cybersecurity trends in electronic transactions in the banking sector. The methodology section is crucial for understanding the systematic approach employed to address the research objectives and answer the research questions. By outlining the research design, data collection methods, sampling strategy, data analysis techniques, ethical considerations, and limitations, this chapter provides a comprehensive framework for conducting the study.

3.1 Research Design

Research design refers to the overall plan or framework that guides the collection, analysis, and interpretation of data in a research study (Creswell & Creswell, 2017). It outlines the specific steps and procedures that researchers undertake to address their research questions and achieve their research objectives. . In this research a descriptive survey research design was used with the aim of providing a clear and accurate picture on the emerging cybersecurity trends in electronic banking transactions in the banking sector.

3.1.1 Descriptive Research Design

Descriptive research design is defined as a design that describes the events, tabulates, depicts and describe data (William et al (2013).The descriptive case research design allows the researcher to collect data with techniques such as comparison, measurement, classification and evaluation. The use of descriptive case method allows use of an array of instruments for data collection and analysis such as questionnaires, interviews and observations are used and this in-turn enhances reliability and validity of the research findings. The design was of the advantage to the researcher as it used both primary and secondary data. The design provided for the transformation of qualitative data into numerical guides.

3.1.2 Justification of descriptive research design

The researcher adopted research design because of the following reasons;

- The design helps gain insights into the variables of interest and identify patterns, trends, or relationships that may exist.
- The design is suitable for collecting data from large populations or diverse groups.
- The design employs quantitative analysis techniques, such as descriptive statistics and frequencies, to summarize and analyze the collected data.
- The design provided a chance for questions like why, where, and how to be answered.
- The design permitted the gathering of both quantitative and qualitative data.

3.1.3 Disadvantages

- The design demanded the researcher to present high degree of knowledge an analytical skills so as to give a detailed analysis on data collected

In order to overcome the challenge, the researcher showed high degree understanding and developed better skills through reading to make detailed analysis

3.2 Research Population

The term "population" refers to the entire group of things or people who are the subject of the study and about whom the researcher wishes to learn more (Kothari,2004). Wegner (2003), defined population study as a set of people and items of interest from which sample are drawn for measurement. Explanation of the target population was needed in order to give a base for calculating sample units and sample size. The population under study is the banking sector. Respondents will be drawn from banking sectors that operates in Kwekwe CBD.

The study population was 10 commercial banks registered with the RBZ and bank customers. The target population was chosen basing on the complexity, highly professional employees, and use of ICT systems, these institutions are implementing emerging cybersecurity trends in electronic banking to mitigate cybersecurity since they are easy targets to cybercrimes activities.

3.3 Population Sample

A sample is a subgroup, a part of a larger population. Sampling allows the researcher to make a generalization of the entire population but only if the sample is a representative of the greater population (Leedy and Omrad, 2001). A total of ten banks were chosen at random in

Kwekwe, selecting thirty-four respondents. In addition, six respondents were chosen from customers, making a total of 40 respondents.

The sample consisted a total of ten e-banking personnel from the selected ten banks, six respondents from compliance department, twelve ICT personnel, six risk management personnel and six Security Operations Center (SOC) personnel. All in all, the sample constituted of forty respondents.

3.4 Sampling Techniques

Sampling techniques are fundamental to the research process as they determine how a subset of the population will be selected for study. According to Cochran (1977), sampling techniques can be classified into two main categories: probability sampling which includes methods such as simple random sampling and stratified sampling, and non-probability sampling; encompasses approaches like convenience sampling and snowball sampling. Hence, in this study the researcher will use stratified random sampling and judgmental sampling.

3.4.1 Stratified Random Sampling

Stratified random sampling is a technique used in statistical research to ensure that the sample drawn is representative of the entire population by dividing the population into distinct subgroups, or strata and then selecting samples from each stratum. This method is particularly useful when dealing with diverse demographic characteristics, ensuring that each sub group is adequately represented in the sample (Gupta, 2018).

3.4.2 Judgmental Sampling

According to Patton (1990), judgmental sampling offers researchers the flexibility to select participants based on specific criteria aligned with the research objectives. Judgmental sampling was used to select all 40 respondents. This was the most effective way for the researcher to determine which respondents in a given source had the most expertise about emerging cybersecurity trends. By analyzing the roles of individuals at the banking sector, the researcher simply chose respondents based on professional judgment. To select the interview respondents, judgmental sampling was used.

3.5 Research Instruments

According to Hair et al (2019), research instruments encompass a wide range of tools and methods employed in data collection, including questionnaires, surveys, interviews, observations, tests, scales or existing database. Research instruments are the tools that are used to collect the data and information needed to solve a problem that is being examined. The researcher used questionnaires and interviews as research tools, allowing to gather first-hand information while also requesting secondary data to fully understand the research problem.

3.5.1 Questionnaires

Questionnaires are research instruments that involve a set of structured questions administered to participants to gather information about their opinions, attitudes, behaviors, or other relevant data (Smith et al., 2018). They are widely used in research studies to collect data from a large number of individuals in a standardized manner. The questionnaire is made up of a group of questions that are printed or typed in a specific order on a form or set of forms (Kothari, 2004). The questionnaire was the primary research tool utilized to collect data from the banking sector in Kwekwe CBD for this study. The questionnaire was deemed perfect for data collection because it was flexible and could be used to collect data from a large or small number of people.

The researcher utilized an open ended and close ended questionnaire to collect data. Open ended inquires allow the respondents to express himself or herself. The researcher capitalized on the higher level of privacy and flexibility offered by the questionnaire since participants felt more secure because they could complete the questionnaire at their own pace. The questions on the questionnaire were all closed ended. Respondents can only react to the options presented in closed-ended questions, therefore their responses are limited.

The number of responses was limited, there were fewer errors and the data presented could be trusted. The researcher was able to obtain a huge amount of data in a short amount of time by using a questionnaire. Respondents were able to complete the questionnaire at their leisure and without feeling rushed. In addition, one of the most important advantages the researcher enjoyed with self-administered questionnaires was no-response bias.

The response rate was much slower than the researcher had anticipated. The number of respondents was lowered since some of the questionnaires provided were never returned. The respondents stated that they did not understand the question such that certain questions were left unanswered. The handwriting of other respondents was difficult to read, therefore the researcher had to find many people to read the handwriting.

3.5.2 Interviews

According to Kothari (2004), the interview method of data collection entails presenting oral-verbal stimuli and responding terms of overall verbal responses. Interviews are conversations between two or more persons in which one person asks questions of the respondents while the other takes notes to be considered and analyzed afterwards (Zikmund, 2005). The researcher obtained permission to conduct interviews from the banks' management. Respondents were interviewed in semi structured and unstructured interviews. A semi structured interview is one of the methods for gathering data by establishing a dialogue that gives the targeted respondents the time and space to express their thoughts on a certain topic.

The response rate of the interview was excellent. All of the scheduled interviews took place. The interview were held in private to avoid the risk of being victimized, and all interview records were treated with confidentiality. Conducting an interview during the research was beneficial because it allowed the researcher to collect specific information and explanations that were not possible to obtain through the questionnaires. The interviews allowed the researcher to reply to the interviewees' responses, more questions were asked during the interviews, resulting in additional relevant information.

Despite many benefits of interviews, several respondents were unable to express themselves openly due to confidentiality and privacy concerns, which limited the breadth of the interview. Conducting interviews took time, a single interview could take a long time to complete. Due to other commitments, several respondents had to reschedule their interviews, but the researcher had to wait patiently. To overcome these obstacles, the researcher established a positive rapport with the interviewees and assure them that the material acquired would be kept confidential and used only for the study purpose.

3.6 Data collection procedures

Questionnaires were self-administered, directly handed in to verify that the intended participants received them. Personal distribution of the questionnaires had the benefit of establishing a positive relation with the respondents and aided in achieving a high response rate. The questionnaire was delivered to the various departments of the 5 departments selected in a total of 40 copies. Respondents were given one week to complete the questionnaire, after which the researcher collected the questionnaires personally from each individual. Using judgmental sampling, twenty respondents were selected for the interviews. Of the 20 interview respondents: 4 were ICT personnel, 4 e-banking personnel, 4 compliance department, 4 risk management and 4 from the security operation center personnel.

3.7 Validity and Reliability of instruments

Validity, as defined by Zikmund (2005), is the precision with which a measure or degree to which a source accurately portrays a concept. Reliability was also defined by Zikmund (2005) as the ability of the measuring instrument to produce repeatable results. The study's use of diverse information gathering methodologies ensures that information gathered is accurate and consistent. To verify validity and reliability, the researcher will use a test-retest approach as well as a pilot study. A pilot test provided assurance that the target population was properly specified and provided guidance on how to modify data collection instruments I order to meet the research objectives. The interview guide and the questionnaires were pre-tested first in order to get a gauge of time and resources required to do the examination and to uncover sampling problems. These tests and pilot studies will be conducted to see if a certain method produces the same results when performed repeatedly to the same object, as well as to ensure that the questions are clear and the questionnaire is of an appropriate length.

3.8 Data presentation, analysis and interpretation of data

The data that was acquired from the survey was subjected to both quantitative and qualitative examination. To make the data more understandable, it was displayed using visuals, tables, charts and diagrams. SPSS software was used to analyze data acquired through questionnaires while the Microsoft Excel software was used to supplement with tabular and graphical displays. The researcher gathered responses, examined the responses for meaning and insights, compared and contrasted the various responses from the respondents and then interpreted the meaning to produce helpful information.

3.9 Ethical considerations

Saunders et al., (2016) defined ethics as the appropriateness of the researcher's behavior in relation to the rights of those who become the subject of the survey. Permission to conduct interviews was sought from the banks' management. Ethical issues were considered throughout the whole process of this research that is before and after data collection. The respondents were informed of all ethical criteria such as confidentiality and honesty, participation was voluntary and participants could withdraw from the exercise at their choice. Importantly, all participants were treated with dignity, fairness and respect.

3.10 Chapter Summary

This chapter looks at research methodology, research design, target population, sample size, sampling techniques, research instruments, date collection procedures and data presentation, analyses and procedures. The next chapter (Chapter 4) concentrated on gathering, analyzing and presenting data.

CHAPTER IV

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 Introduction

The major factors of this chapter was on the discussion, presentation and analysis the major findings of the survey. Questionnaire and interview response rates were presented and analyzed in this chapter.

4.1 Response Rate

4.1.1Questionnaire response rate

Departments	Questionnaire Issued	Questionnaire Returned	Response Rate
E-banking personnel	10	10	100%
Compliance	6	6	100%
ICT	12	12	100%
Risk Management	6	6	100%
SOC personnel	6	4	67%
Total	40	38	95%

[Source: Primary Source, 2024]

Table 4.1 shows that 40 questionnaires were distributed to different departments of the banking sector. According to the table above, 38 of 40 questionnaires issued to respondents were returned, indicating a 95 percent 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. The response rate of 95% fully support the research objectives.

4.1.2 Interview Response Rate

Table 4.2 Interview response rate

Departments	**Scheduled Interviews**	**Conducted Interviews**	**Response Rate**
E-banking personnel	4	4	100%
Compliance	4	4	100%
ICT	4	4	100%
Risk Management	4	4	100%
SOC personnel	4	4	100%
Total	20	20	100%

[Source: Primary Source, 2024]

Out of the 20 scheduled interviews, all were conducted, translating to a 100% response rate, as shown by table 4.2. The researcher had planned to interview 20 participants, choosing 4 from each chosen department.

4.2 Demographic characteristics of respondents

The data gathered from the responders to the questionnaire provided their demographic variables such as gender, age, employment history, job category, academic qualifications and period of employment. Therefore, these facts aid in confirming the information that would have been gained from the questionnaires. As a result, the respondents' demographic information is shown below.

4.2.1 Gender

N=38

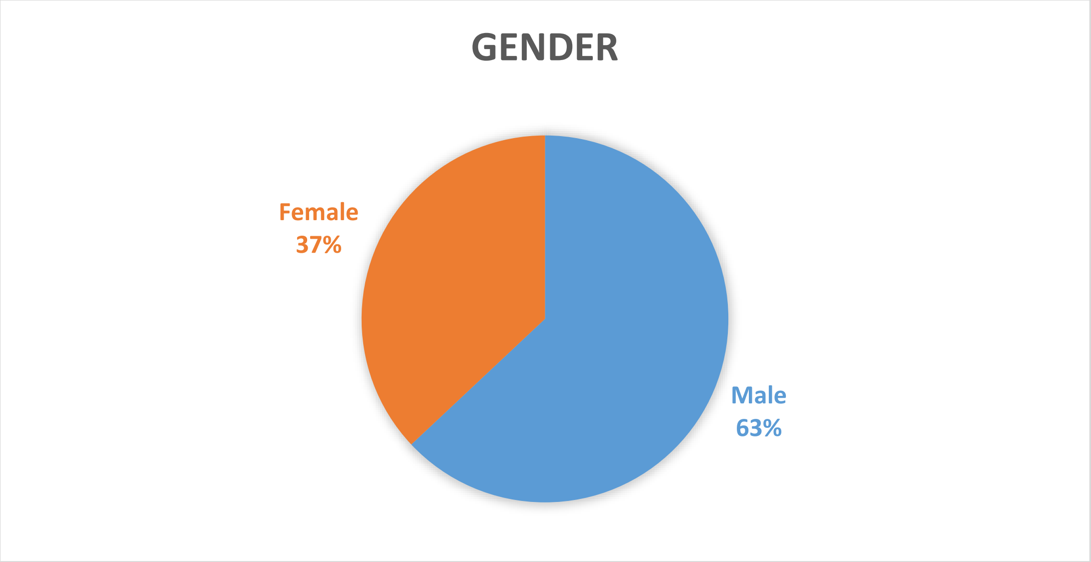

Figure 4.1 Gender distribution of respondents'

[Source: Primary Source, 2024]

According to figure 4.1 this depicts the respondents' gender distribution, men made up the bulk of respondents with 63% with respect to gender whilst women constituted only 37%. This was due to the fact that women were reluctant to complete the questionnaires which men had superior knowledge of technological concerns. Questionnaire distribution was based on gender sensitivity and no bias in all sorts was shown.

4.2.2 Age

The age ranges of the respondents are displayed in table 4.3 below. The age range was divided into five categories: under 25, 25-29, 30-34 and 35 years and over. The study's findings were as follows

Table 4.3: Age of respondents.

Variables	Demographic Variable	Frequency	Percentage %
Age Distribution	Below 25 years	5	13.2
	25-29 years	14	36.8
	30-34 years	11	28.9
	35 years and above	8	21.1
	Total	38	100

[Source: Primary Source, 2024]

The table indicates the age range of all the respondents who participated in the research study. The interval of 25-29 years had the highest frequency in the age distribution as denoted by 36.8% while range 30-34 years constituted 28.9% of the respondents. Respondents above 34 years constituted 21.1% and those below 25 years of age were only 13.2% of the total research population. This distribution in age shows that mainly the young people are more into information technology (ICT) and cyber activities participated in the survey.

4.2.3 Period of employment

Respondents were asked how long they had worked for their current employer. These were the outcomes that were attained:

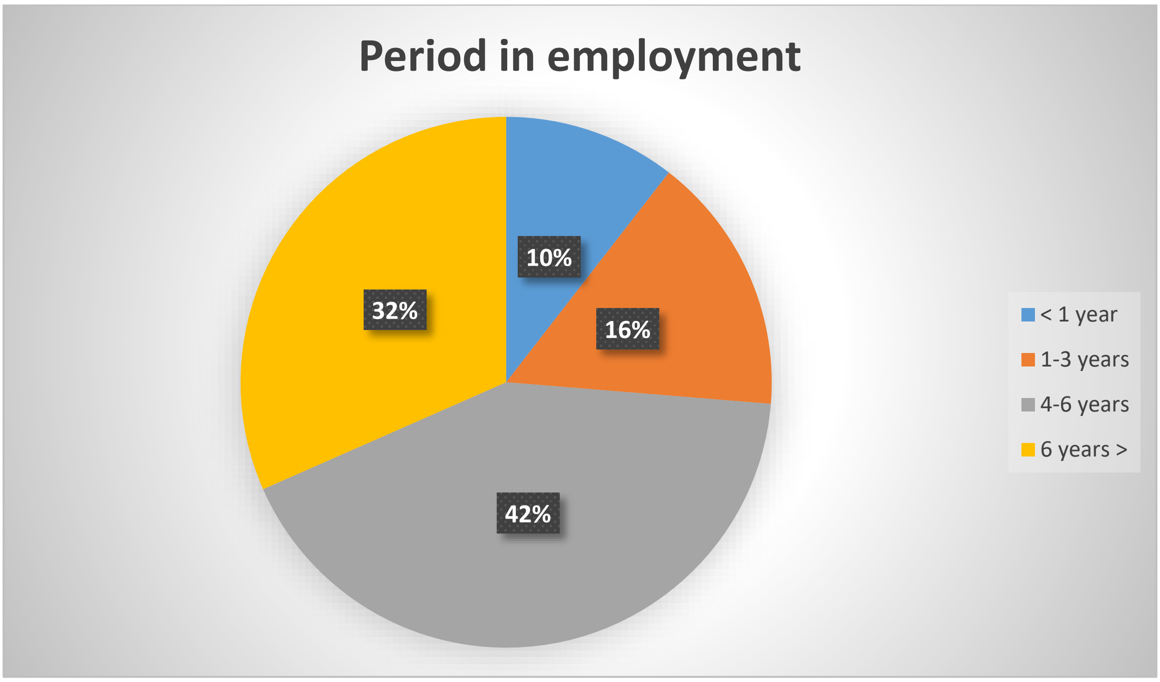

Figure 4.2 Period of employment

[Source: Primary Source, 2024]

Figure 4.2 shows that most of the employees had spent around 4-6 years with their departments as depicted by the highest percentage of 42% on the period interval 4-6 years. This was followed by a 32% of respondents who confirmed that they had spent more than 6 years with their respective departments. This reveals that the respondents of the research were well informed about challenges the banking sector is facing that include cyber threats. Employees who had spent just less than a year with their departments constituted only 10% of the respondents. The respondents that worked for 1-3 years constituted 16% of the respondents.

4.2.4 Employment category

The survey asked respondents to choose their employment category that best described their currents position in the company. The research results were as follows.

Table 4.4 Employment category of respondents

Variable	**Variable description**	**Frequency**	**Percentage**
Employment category	E-banking personnel	10	26.3
	ICT	12	31.6
	Risk management	6	15.8
	Compliance	6	15.8
	SOC personnel	4	10.5
	Total	38	100

ICT expects constituted a large proportion of the respondents with a 31.6% followed by E-banking personnel who constituted 26.3% of the respondents. Risk management and compliance both constituted 15.8% of the respondents. Also considered in the demographic distribution was the security operation center personnel with 10.55% of the respondents.

4.2.5 Nature of business

Table 4.5: Respondents nature of business

Variable	**Variable description**	**Frequency**	**Percentage %**
	Security	4	10.5
	Technology	22	57.9
	Risk	6	15.8
	Compliance	6	15.8
	Total	38	100

Table 4.5 shows that 57.9% of respondents was constituted by technological nature of business that is e-banking personnel and ICT. The type of business that include risk and

compliance both constituted 15.8% of the respondents. The security nature of the banking sector constituted only 10.5% of the respondents.

4.2.6 Academic qualifications

N=38

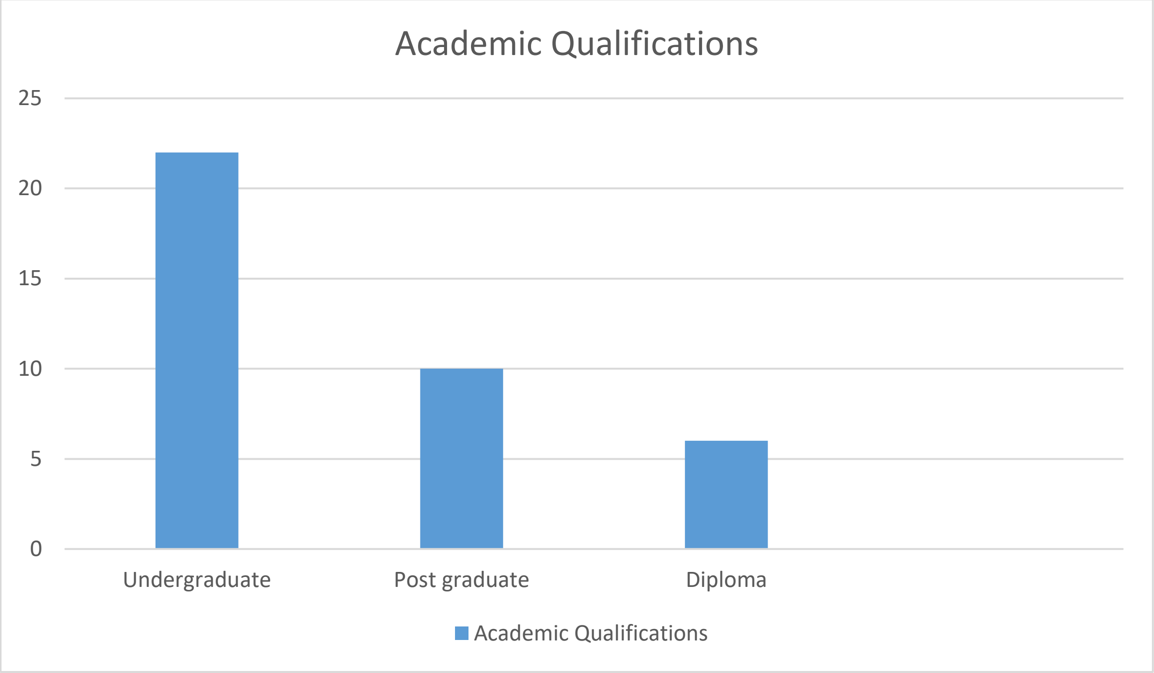

Figure 4.3 respondents' highest level of education (Source: Primary source)

The academic qualifications of the respondents ranged from diploma, undergraduate and postgraduate. Figure 4.3 reveals that, overall, 22 (57.9%) of the respondents had undergraduates degrees, followed by 10 (26.3%) with post graduate degrees and lastly 6(15.8%) with diploma certificates. The figure implies that a large proportion of the respondents were mature enough and well knowledgeable to comprehend matters relating to emerging cyber security trends in electronic banking transactions in the banking sector.

4.3 Research Findings

4.3.1 Level of knowledge on cybersecurity.

The respondents were asked to demonstrate their level of understanding towards cybersecurity. Below is a summary of the responses.

Table 4.6: Respondents level of knowledge on cybersecurity

Variable	No knowledge	Little knowledge	Moderate knowledge	Vast knowledge
Level of knowledge on cybersecurity	15.8%	31.6%	36.8%	15.8%

Source: Primary Source

According to table 4.6, 36.8% of respondents had a moderate understanding of cyber threats. The majority of these respondents worked in ICT, e-banking personnel, SOC and risk management and had a basic understanding of cybersecurity in the banking sector. 15.8% of the population were highly knowledgeable people. Only 31.6% of the respondents said they knew little about cybersecurity. Many respondents had learned about cybersecurity because of the type of departments they work that require the knowledge of cybersecurity that protects the banking sector and need to put and implement emerging cyber security trends in electronic banking transactions in the banking sector.

4.3.2 Types of cybersecurity

The respondents were asked to indicate the types of cybersecurity which were prevalent in the banking sector and summarized in the table overleaf are the results.

Table 4.7: Frequency of main types of cybersecurity in ZB Bank

Cyber Threats	**Doesn't occur %**	**Rarely occur %**	**Common %**	**Very common %**
Firewall	0	0	5.3	94.7
Encryption	0	0	0	100
Multi-factor authentication	0	0	21.1	789
Secure payment getways	0	0	23.7	76.3
Transport Layer Security	0	0	0	100
Data Loss Prevention	0	68.4	31.6	0

Table 4.7 shows that none of the respondents reported that firewalls does not occur or rarely occur. Firewall were reported as common by 5.3% of respondents and very common by 94.7% of respondents. This emphasizes the widespread recognition of firewalls as a fundamental cybersecurity measure to protect networks and systems from unauthorized access and threats.

Encryption according to table 4.7 was reported as very common by 100.0% of respondents. None of the respondents indicated that encryption does not occur or rarely occurs. This underscores the critical role of encryption in safeguarding sensitive data during transmission and storage, ensuring its confidentiality and protection from unauthorized entities.

None of the respondents indicated that multi-factor authentication does not occur or rarely occurs. 21.1% of the respondents confirmed that it is very common. This highlights the increasing recognition of the importance of multi factor authentication in mitigating the risk of unauthorized access and enhancing the security of unauthorized access and enhancing the security of electronic banking transactions.

The findings show that secure payment gateways are commonly implemented with 23.7% of respondents considering them common and 76.3% considering them very common. Of the respondents none stated that secure payment getways do not occur or rarely occur. Table 4.7 on secure payment getways underscores the significance of secure payment ensuring to secure transmission of financial information during online transactions.

As indicated in table 4.7, respondents reported transport layer security as very common by 100.0%. It shows the crucial role of transport layer security protocols, such as TLS, in establishing secure connections and protecting the confidentiality and integrity of data during electronic banking transactions

Data loss prevention was reported as rarely occurring by 68.4% of respondents and as common by 31.6% of respondents. This suggests that a relatively lower adoption rate of data loss prevention strategies in the in the surveyed population, highlighting the need for increased awareness and implementation of measures to prevent the unauthorized disclosure and loss of sensitive data.

4.4 Impacts of cybersecurity on the performance of financial institutions.

4.4.1 Data Privacy

The responses of a yes/no question asking respondents to decode the effects of cybercrime on the loss of sensitive data are as follows.

N=38

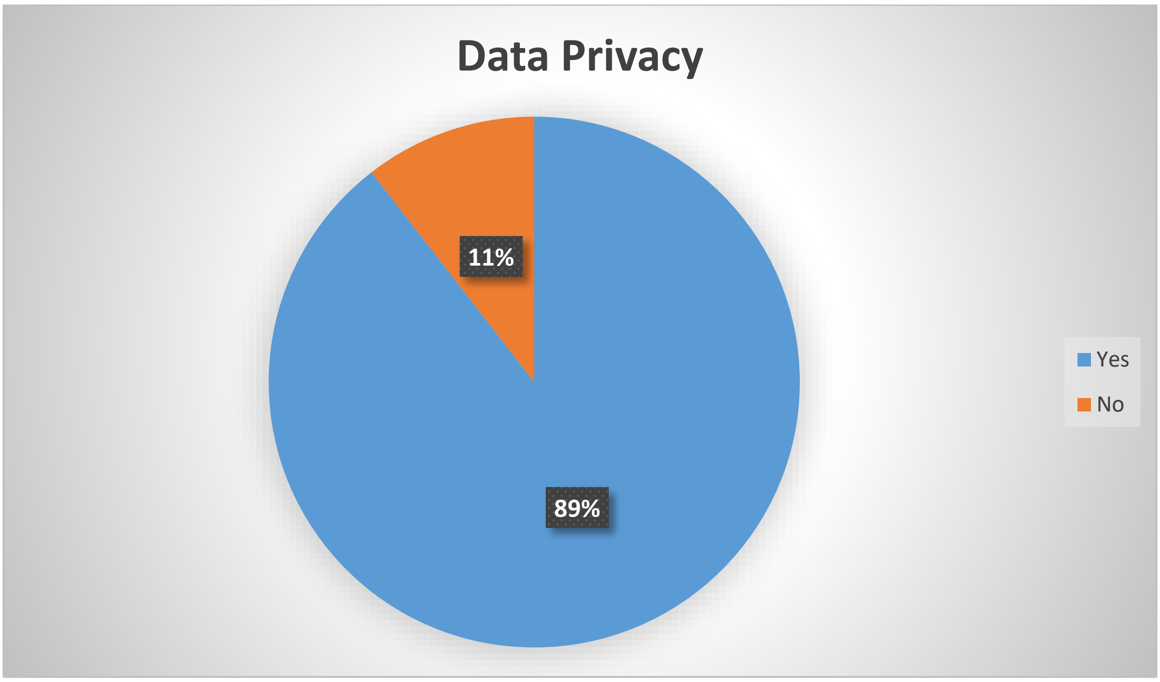

Figure 4.4

According to figure 4.4, 89% of the respondents perceived data privacy as an impact of cybersecurity in electronic banking transactions. Data privacy is crucial in electronic banking as it involves protecting sensitive user data such as account numbers. Acknowledging the impact of data privacy suggests that respondents understand the potential risks associated with data breaches and the need to maintain confidentiality.Recognizing the importance of data privacy, respondents likely appreciate the regulatory requirements and ethical considerations surrounding the handling of personal information. This finding underscores the significance of implementing robust security measures, encryption protocols, and access controls to protect user data. It also reflects an understanding of the potential consequences of data breaches, such as financial loss, identity theft, and damage to the reputation of both the financial institution and the customers involved.

4.4.2 Fraud Prevention

N=38

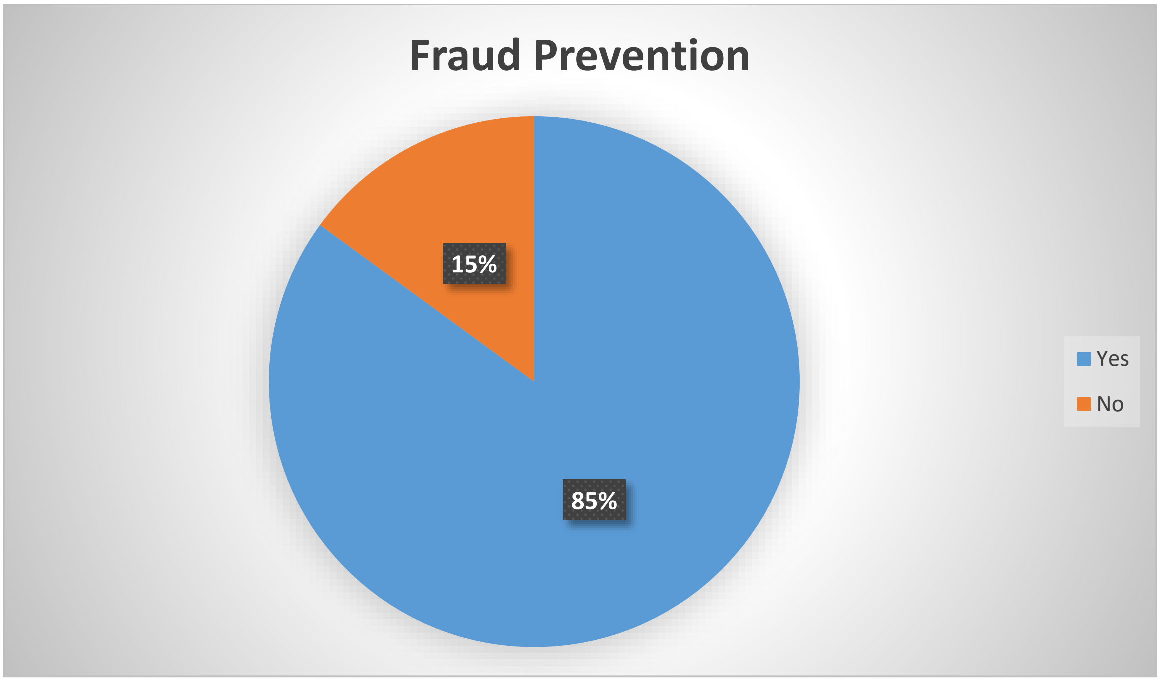

Figure4.5

Figure 4.5 indicates that 85% of respondents recognized the impact of fraud prevention whilst 15% did not. Recognizing the impact of fraud prevention on electronic banking transactions indicates a significate understanding of the risks associated with fraudulent activities. Fraud prevention aims to detect and mitigate fraudulent behaviour, protecting users from financial losses and maintaining the integrity of the banking system mentioned one of the respondents. The high percentage of respondents suggests an awareness of various forms of electronic banking fraud such as phishing and identity theft.

4.4.3 Secure authentication

N=38

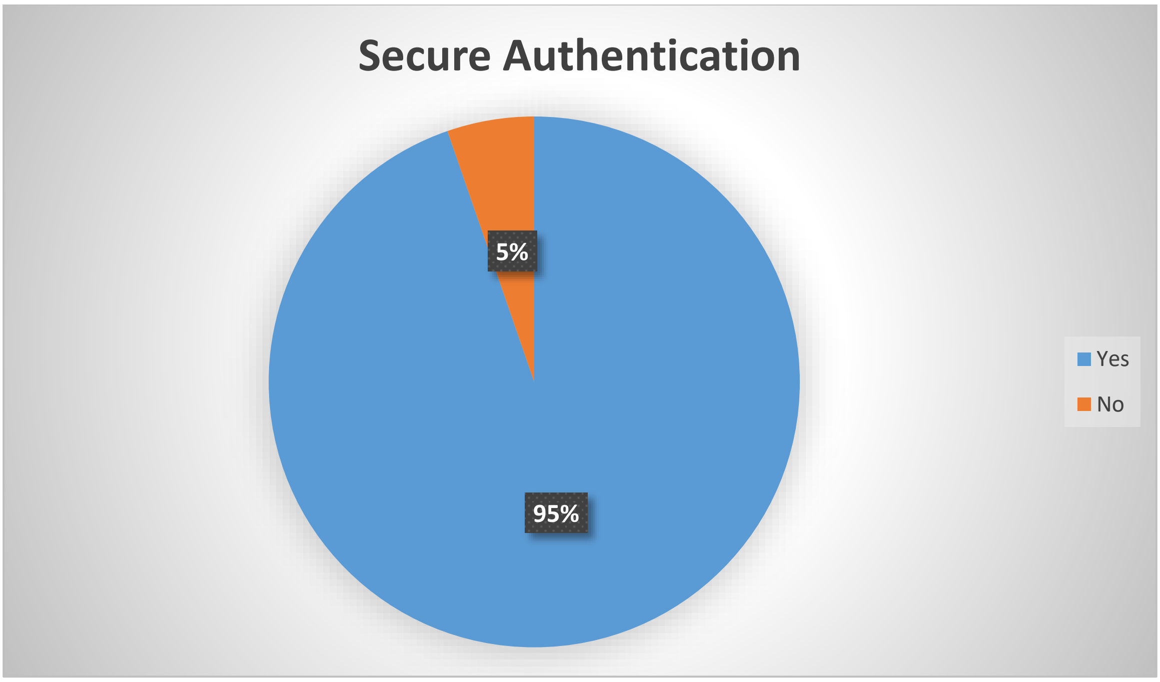

Figure 4.6

Secure authentication is essential in electronic banking to verify the identity of users and protest against unauthorized access. According to figure 4.7, 95% of the respondents know the impact of secure authentication on electronic banking transactions. Respondents mentioned that the bank should be aware of the vulnerabilities associated with weak authentication mechanisms. The importance of secure authentication highlights on understanding of the potential risks of unauthorized access and account compromise. Acknowledging the impact of secure authentication, respondents understand the value of robust security measures to protect user accounts, maintain customer trust and ensure the confidentiality and security of electronic banking transactions. The high percentage indicates a proactive approach to enhancing authentication mechanisms and reinforcing the overall cybersecurity of electronic banking systems.

4.4.4 Transaction integrity

N=38

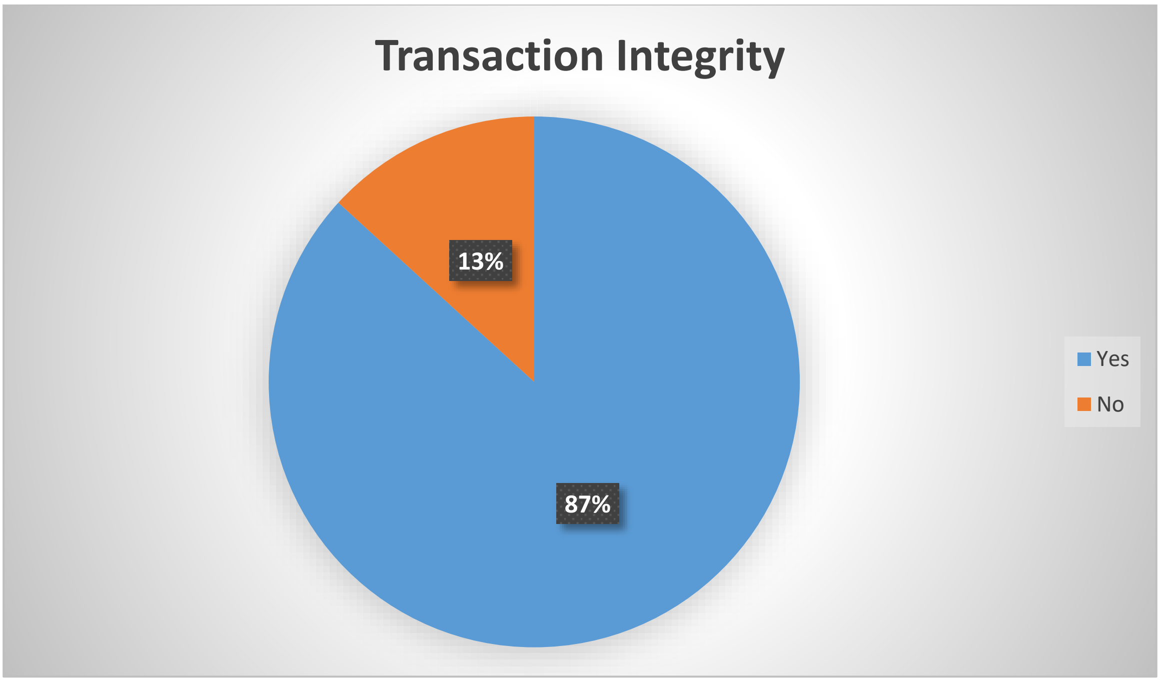

Figure 4.7

Figure 4.7, indicates that 87% of the respondents acknowledge the impact of transaction integrity on electronic banking transactions whilst 13% of the respondents does not acknowledge. Transaction integrity ensures that electronic banking transactions are not tampered with or altered during the process. Respondents mentioned that potential risks associated with unauthorized modification or disruptions to transactions are curbed by transaction integrity. Robust security measures need to be put to protect the integrity of electronic banking transaction. It indicates a proactive approach toward implementing safeguards to prevent transaction tampering or unauthorized modification. 87% of the respondents acknowledge the importance of implementing measures to ensure the accuracy and reliability of transactions, thereby safeguarding the financial interests of customers and maintaining the integrity of the electronic banking system as a whole.

4.4.5 Customer trust and confidence

N=38

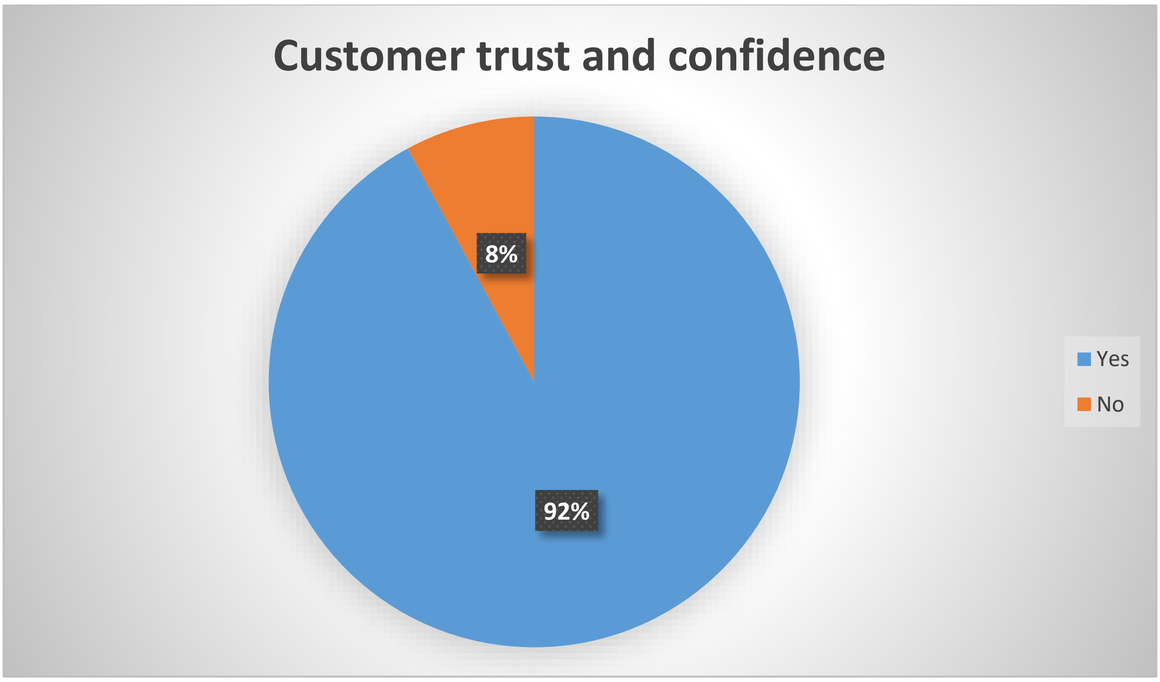

Figure 4.8

Customer trust and confidence refer to the belief and assurance customers have in the security, reliability and confidentiality of their electronic banking transactions. As shown by figure 4.8, 92% of the respondents recognize the impacts of customer trust and confidence on electronic banking transactions. It plays a crucial role in the success and acceptance of electronic banking services by customers one of the interviewed respondents mentioned. Customer trust and confidence reflects an appreciation for the role that trust plays in fostering relationships with customers and promoting the adoption of electronic banking services.

4.5 Emerging cyber security trends

N=38

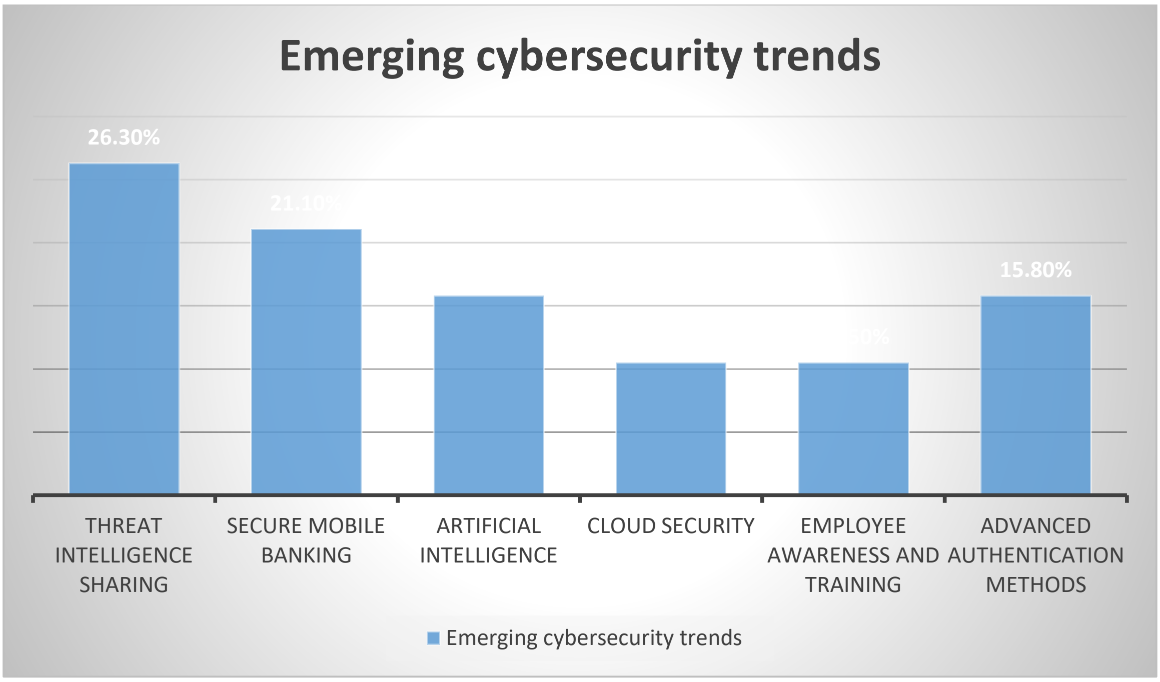

Figure 4.5

4.5.1 Threat intelligence sharing

Threat intelligence sharing is emerging as a crucial cybersecurity trend in electronic banking transactions, as it enables financial institutions to proactively defend against evolving cyber threats. Figure 4.5 indicates that 26.3% of the employees at ZB Bank approve of threat intelligence sharing as a crucial emerging cyber security trend in electronic banking transactions. By collaborating and sharing information with industry peers, government agencies, and cybersecurity organizations, financial institutions can gain valuable insights into emerging threats, indicators of compromise, and attack techniques. This collective knowledge empowers institutions to enhance their defensive capabilities, identify potential vulnerabilities, and strengthen their security posture. Effective threat intelligence sharing enables financial institutions to stay ahead of cybercriminals by leveraging shared experiences and expertise. It facilitates the timely identification and mitigation of emerging threats, reducing the risk of successful attacks on electronic banking transactions. By receiving real-time threat intelligence, financial institutions can proactively adjust their security measures, update their detection systems, and implement appropriate countermeasures. Threat intelligence sharing fosters a collaborative ecosystem where stakeholders work together to protect the entire banking sector. Through trusted relationships and secure channels, financial institutions can exchange anonymized threat data, share best practices, and collaborate on incident response. This cooperative approach helps in identifying patterns, uncovering sophisticated attack campaigns, and developing effective mitigation strategies.

4.5.2 Secure mobile banking

According to figure 4.5 21.1% of the respondents viewed that secure mobile banking is an emerging cyber security trend. As mobile banking continues to gain popularity, it becomes crucial for financial institutions to ensure the security and integrity of customer transactions conducted through mobile applications. This trend focuses on implementing robust security measures to protect sensitive data and prevent unauthorized access to mobile banking systems. ZB Bank is adopting various security practices to enhance secure mobile banking one of the respondents indicated. These include secure coding practices, encryption, multi-factor authentication, and secure communication protocols. Secure coding practices ensure that mobile banking applications are developed with security in mind, minimizing vulnerabilities and potential entry points for attackers. Encryption techniques, such as Transport Layer Security (TLS), are used to protect data transmitted between mobile devices and banking servers, safeguarding it from eavesdropping or tampering.

Multi-factor authentication adds an extra layer of security by requiring users to provide multiple pieces of evidence to verify their identity, such as passwords, biometrics, or one-time passwords. This helps prevent unauthorized access to mobile banking accounts even if one factor is compromised. Additionally, secure communication protocols, such as HTTPS, are used to establish encrypted connections between mobile devices and banking servers, ensuring the privacy and integrity of data exchanged. These security measures aim to protect mobile banking transactions from threats such as malware, phishing attacks, and data breaches. By implementing secure mobile banking practices, financial institutions enhance customer trust and confidence in conducting financial transactions through mobile applications.

4.5.3 Artificial intelligence

Of the respondents 15.8% acknowledge Artificial intelligence in the electronic banking transactions as an emerging cybersecurity trend in ZB Bank. AI-powered solutions are being increasingly adopted by financial institutions to enhance their security measures and safeguard electronic banking transactions. Artificial intelligence (AI) is an emerging cybersecurity trend in electronic banking transactions, offering advanced capabilities to detect, prevent, and respond to cyber threats more effectively. AI algorithms can analyze vast amounts of data in real-time, enabling financial institutions to identify patterns, anomalies, and potential threats that may go unnoticed by traditional security systems. Machine learning algorithms can learn from historical data and continuously improve their threat detection capabilities, adapting to evolving attack techniques. One application of AI in electronic banking transactions indicated by the ICT department is anomaly detection. AI systems can establish a baseline of normal user behavior and identify deviations that may indicate fraudulent activities or unauthorized access attempts. By leveraging behavioral analytics, AI can detect anomalies in transaction patterns, login activities, or account behaviors, enabling early detection and prevention of fraudulent transactions. AI can assist in automating threat intelligence analysis. AI-powered systems can analyze vast amounts of threat data, including indicators of compromise (IOCs) and threat intelligence feeds, to identify emerging threats and potential attack campaigns. This helps financial institutions stay ahead of cybercriminals and proactively implement mitigation strategies. AI can also enhance incident response capabilities. AI algorithms can aid in the analysis of security incidents, rapidly identifying the nature and severity of an attack, and suggesting appropriate response actions. This enables faster incident containment, reducing the impact of cyber threats on electronic banking transactions.

4.5.4 Cloud Security

As financial institutions leverage the cloud for cost-effective and scalable infrastructure, ZB Bank implemented this trend to ensuring robust security measures becomes crucial to protect sensitive data and maintain the integrity of electronic banking transactions. Financial institutions need to ensure that only authorized personnel can access sensitive data and systems hosted in the cloud. 10.5% of the respondents indicated that cloud security ensures robust security measures against cyber threats .This includes implementing strong authentication mechanisms, such as multi-factor authentication, and employing role-based access controls to restrict access privileges based on job responsibilities. Financial institutions need to encrypt data both at rest and in transit to protect it from unauthorized access or interception. Encryption technologies, such as Transport Layer Security (TLS) for data in transit and encryption protocols for data at rest, help ensure the confidentiality and integrity of electronic banking transactions. According to RBZ (2015), organizations can have reliable IT systems that can access top-notch databases and keep track of transactions coming from the internet. Financial institutions need to have robust monitoring systems in place to detect and respond to any security incidents or potential threats in real-time. This includes monitoring network traffic, user activities, and system logs to identify any suspicious or unauthorized activities that may impact electronic banking transactions.

4.5.5 Employee awareness and training

Figure 4.5, indicates 10.5% of the respondents agreeing to employee awareness and training as an emerging trend of cybersecurity in their electronic banking transactions at ZB Bank. In order to inform employees in the financial institutions about the risks associated with implementing electronic banking transactions, Mugari (2016) argued for the organization of workshops and seminars. Effective employee awareness and training programs help employees understand the various types of cyber threats, such as phishing, social engineering, malware attacks, and the importance of adhering to security policies and procedures. By raising awareness about these threats, employees become more vigilant and can identify and report potential security incidents promptly. Training is essential in preventing cybercrime, according to research done by Boateng et al. (2011), who found that cybercrime was spreading because Ghanaian agencies lacked the technical, investigative, and controlling know-how to combat it. Training programs often include simulated phishing exercises, where employees receive mock phishing emails to test their ability to recognize and avoid such attacks. These exercises create a hands-on learning experience and help in strengthening employees' ability to identify and respond appropriately to phishing attempts.

4.5.6 Advanced authentication methods

Traditional methods such as passwords and PINs are increasingly being supplemented or replaced by more robust authentication techniques to mitigate the risks associated with credential theft and account hacking. According to figure 4.5 15.8% of the respondents indicated that advanced authentication methods reduce cyber threats therefore being an emerging trend of cyber security. One of the emerging authentication methods is biometrics, which involves using unique biological characteristics such as fingerprints, iris scans, or facial recognition to verify a user's identity. Biometric authentication offers a higher level of security as these characteristics are difficult to replicate or steal, providing a more reliable means of identity verification. Another advanced authentication method is the use of hardware tokens or security keys. These physical devices generate unique codes that are used as a second factor of authentication. Hardware tokens are resistant to phishing attacks and provide an additional layer of security, ensuring that only authorized users can access electronic banking transactions. These advanced authentication methods are designed to enhance the security of electronic banking transactions by providing more robust and reliable means of user identification. By implementing these methods, financial institutions can mitigate the risks of credential theft, account takeover, and fraud, ensuring a safer banking experience for their customers.

4.6 Summary

The information gathered during the research was provided and covered in this chapter. Tables, bar graphs, and pie charts were used to illustrate the data. Interviews and questionnaires were used to collect the data. The summary, conclusions, and recommendations are covered in the next chapter.

CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter focuses on the results, conclusions and recommendations. The research was to analyse the emerging cyber security trends in electronic banking transactions.

5.1 Summary of research findings

The main thrust of the research was to analyse emerging cybersecurity trends in electronic banking transactions looking at ZB Bank as a case study. The information was gathered from ZB Bank, books, newspapers and journals. The research findings' key aim which was to assess the emerging cyber security trends in electronic banking transactions based on the following research questions:

What is the nature of cybersecurity in the banking sector?

The nature of cybersecurity in the banking sector is comprehensive involving multiple layers of protection. The research findings indicate that the banking sector recognizes the importance of addressing various aspects of cybersecurity to ensure the integrity, confidentiality and reliability of electronic banking transactions. The approach involves implementing measures across different fronts such as data protection, fraud detection, authentication, transaction integrity and customer trust. According to the findings, the nature of cybersecurity is also characterized by strong awareness of risks and proactive measures to mitigate them. The findings suggest that the sector understands the potential consequences of cyber threats and take proactive stances towards implementing security measures.

To what extend is cybersecurity impacting the banking sector?

Cybersecurity trends are significantly impacting the banking sector. The high recognition of the impacts of data privacy, fraud prevention, secure authentication, transaction integrity and customer trust and confidence shown by research findings indicates the profound influence of cybersecurity trends. The banking sector is impacted by cybersecurity trends driven by technological advancements such as artificial intelligence, bringing both opportunities and challenges for cybersecurity. ZB Bank leverage these technologies to enhance security measures while also addressing potential vulnerabilities and risks. Research findings indicate that cybersecurity trends have a substantial impact on the banking sector.

How effective are the emerging cybersecurity trends in fighting concerns about electronic banking transaction such as cybercrime?

Research findings on the effectiveness of emerging cybersecurity trends in fighting concerns about cybercrimes in electronic banking transactions are inferred based on the recognition of their impacts. Threat intelligence which involves gathering and analysing information about potential cyber threats, can enhance the ability of financial institutions to detect and respond to cybercrimes. Staying informed about emerging threats, organisations can proactively implement appropriate security measures and mitigate risks.

The impact of secure authentication suggests that emerging cybersecurity trends insecure mobile banking can be effective in combating cybercrimes. Technologies such as biometrics, strong encryption and secure mobile applications can enhance the security of mobile banking transactions and protect against unauthorized access or data breaches

Artificial intelligence play a significant role in cybersecurity by automating threat detection and response, identifying patterns of suspicious activities and enhancing anomaly detection. Leveraging AI technologies, financial institutions can strengthen their defence mechanisms and mitigate cyber threats more effectively.

Research finding show that the impacts of data privacy suggest that emerging trends in cloud security can help address concerns about cybercrimes. Cloud security measures such as robust encryption and access controls can protect sensitive data stored in the cloud and reduce the risk of unauthorized access and data breaches.

Investing in comprehensive cybersecurity training programs can expose employees to recognize and respond to potential cyber threats effectively. Educating employees about best practices, phishing attacks, safe computing habits can significantly reduce the risk of cybercrimes caused by human error. This shows the effectiveness of employee awareness and training as an emerging cybersecurity trend in fighting concerns about electronic banking transactions such as cybercrime.

How best can the banking sector implement the cybersecurity trends?

- Develop a comprehensive cybersecurity strategy that encompasses all relevant areas, including data privacy, fraud prevention, secure authentication, transaction integrity, and customer trust and confidence.
- Conduct regular risk assessments to identify potential vulnerabilities and threats specific to the banking sector. This will help prioritize cybersecurity initiatives and allocate resources effectively.
- Keep abreast of emerging cybersecurity trends, technologies, and regulatory changes. Stay informed about the latest threats and vulnerabilities to ensure that security measures remain current and effective.
- Conduct regular cybersecurity awareness and training programs for employees at all levels. Educate them about cyber threats, safe computing practices, and the importance of following security protocols. Encourage a culture of cybersecurity awareness and responsibility throughout the organization.

5.2 Conclusion

The study findings show that the advent of emerging cybersecurity trends in ZB Bank and banking sector brought about trust and confidence in electronic banking transactions such as internet banking. Technology is ever changing therefore, there is also need to introduce emerging cybersecurity trends continuously since there is a link between technology and cybercrime, as level of cyber security trends increase so as new cybercrimes. From the research findings, emerging cyber security trends have a positive impact on the performance of financial institutions in terms of electronic transactions. Threat intelligence sharing has the most positive impact.

5.3 Recommendations

Below are the recommendations made by the researcher on each finding related to the impacts of cybersecurity:

- Data Privacy
    - Develop and enforce strict access controls to ensure that only authorized personnel can access sensitive data.
- Fraud prevention
    - Deploy advanced fraud detection systems that utilize machine learning algorithms to identify suspicious activities and patterns
- Secure Authentication
    - Implementing multi-factor authentication (MFA) methods, combining elements like passwords, biometrics and one-time passcodes
- Transaction integrity
    - Establish secure communication channels with external patterns and financial networks to maintain transaction integrity
- Customer trust and confidence
    - Offer customer education programs on cybersecurity best practices and how to identify potential threats

For the emerging cybersecurity trends, the recommendations include:

- Threat intelligence
    - Regularly analyze and share threat intelligence within the organization to strengthen defenses against emerging threats.
- Secure Mobile Banking
    - Educate customers about the importance of securing their mobile devices and using official banking apps from trusted sources.
- Artificial Intelligence
    - Leverage AI technologies to automate threat detection, incident response, and vulnerability assessments.
- Cloud Security

    - Continuously monitor and audit cloud infrastructure for any security vulnerabilities or unauthorized access.
- Employee Awareness and Training
    - Develop a comprehensive cybersecurity training program for employees at all levels.

These recommendations aim to address the research findings and promote a proactive and comprehensive approach to cybersecurity in the banking sector. If the fore mentioned recommendations are implemented, the preventive approaches implementation may advance from effective to a much more effective.

List of references.

Aloul, F., Zahidi, A., & Al-Sharhan, S. (2018). A review of digital signature: Types, techniques, and challenges. International Journal of Advanced Computer Science and Applications, 9(7), 226-234.

Bash, C. (2020). Audit trail security and integrity. Journal of Information Security and Applications, 51, 1-14.

Bishop, M. (2019). Fraud detection in electronic banking transactions using machine learning techniques. Journal of Financial Crime, 26(2), 468-486.

Bhunia, S., Roy, S., Bhattacharya, A., & Chakraborty, S. (2020). Cryptography and Network Security: Principles and Practice. CRC Press.

Boateng, R., Budu, J., Isabalija, R., and Olumide, L., (2011).' Sakawa- Cybercrime and Criminality in Ghana': Journal of Information Technology Impact, Volume (11): 85-100.

Brown, A. (2018). GDPR compliance: What it means for US banks. Journal of Digital Banking, 2(1), 4-13.

Brown, R. (2019). "Emerging Cybersecurity Threats in Electronic Banking Transactions." Journal of Banking Security, 5(2), 123-135

Brown, J., & Adams, C. (2018). Cybersecurity and banking: Electronic threats and countermeasures. Journal of Internet Banking and Commerce, 23(3), 1-18.

Campagna, G., Culnane, C., & Rubinstein, B. (2019). The Effectiveness of Multi-Factor Authentication: An Empirical Study. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 1149-1163).hen, S. (2019). Transaction reconciliation in electronic banking: A comprehensive survey. Journal of Computer Science and Technology, 34(2), 355-376.

Choudhury, P., Biswas, G. P., & Chaki, N. (2021). Security Issues and Countermeasures in E-commerce. In Security and Privacy in Cyber-Physical Systems (pp. 319-340). Springer

Chen, J. (2020). A survey of fraud detection techniques in electronic banking transactions. International Journal of Information Security, 19(2), 195-211.

Chikwava, T., & Kamujoma, P. (2016). "Cybersecurity in the Banking Sector: A Review of Global Perspectives." International Journal of Cybersecurity, 3(1), 45-58.

Cochran, W. G. (1977). Sampling Techniques (3rd ed.). New York, NY: Wiley.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage Publications.

Dierks, T., & Rescorla, E. (2008). The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246.

Deloitee, 2016. Retail- Cyber Executive Briefing, retrieved from https://www2.deloitecom/nz/en/pages/risk/articles/Manufacuting.html on 15/02/2022

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis (8th ed.). Cengage Learning.

Hoffman, D. (2021). Anomaly detection for fraud prevention in electronic banking transactions. Journal of Cybersecurity, 7(1), 35-52.

Holt, T. J. & Bossler, A.M.2016. Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Crime Sciences Series. New York: Routledge

Johnson, R., Smith, K., & Anderson, L. (2020). Survey Research Methods. Oxford University Press.

Jones, R. (2020). Cybersecurity in banking: An evolving landscape. Journal of Banking Regulation, 21(1), 22-40.

Jones, A., & Moyo, K. (2020). "Cyber-Attacks on Financial Institutions: Implications for the Zimbabwean Banking Sector." Banking Trends, 8(4), 287-301

Kabay, M., Desai, A., & Slay, J. (2020). Data Loss Prevention. In Computer Security Handbook (pp. 1105-1135). Wiley.

Khan, M. (2021). Enhancing the security of online banking using one-time password. International Journal of Computer Science and Information Security, 19(1), 26-34.

Kshetri, N. (2019). Encryption. In The Global Cybercrime Industry (pp. 81-97). Springers

Kshetri, N. (2017). Cybersecurity in the financial sector: Innovations and challenges in the 21st century. Journal of Cyber Policy, 2(3), 331-348.

Kothari, C. R. 2004. Research Methodology, Methods and Techniques, Second Edition. New Delhi: New Age International Publishers.

Lau, W. (2018). The role of trust in mobile banking adoption: An empirical analysis. Journal of Electronic Banking Systems, 2018(1), 1-10.

Laureani, A. (2021). Trust and online banking adoption: The moderating role of cybersecurity. Journal of Financial Services Marketing, 25(2), 92-103.

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

Li, Q., Zhou, L., & Zhang, Y. (2018). Cybersecurity and its impact on financial stability. China Finance Review International, 8(2), 174-195

Liu, Y. (2019). Biometric authentication: A secure approach for mobile banking applications. International Journal of Information Management, 48, 12-22.

Liu, D., & Chen, Z. (2017). Cybersecurity in the banking sector: The Chinese practice and legal framework. Computer Law & Security Review, 33(4), 635-647.

Moustafa, N. (2020). User Authentication in Online Banking: A Review. In Cybersecurity for Industry 4.0 (pp. 79-96). Springer.

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

Mugari, I. 2016. Perspectives on Cyber-Threats to the Retail Sector. A Case Study of Eastgate Shopping Mal. International Journal Of Innovative Research and Development Vol 5 (3), 180-187.

Patton, M. Q. (1990). Qualitative Evaluation and Research Methods. Thousand Oaks, CA: Sage Publications

Peltier, J. (2020). Building trust in digital banking. Journal of Electronic Banking Systems, 2020(1), 1-5.

Reserve Bank of Zimbabwe (RBZ). (2016). *Cybercrime in Zimbabwe and Globally*. Retrieved from http://www.rbz.co.zw/assets/cybercrime-globally-and-in-zimbabwe.pdf on 02/03/2016.

Reserve Bank of Zimbabwe. (2018). "Cybersecurity Guidelines for Banking Institutions." Available at: https://www.rbz.co.zw/cybersecurity-guidelines (Accessed: 15 May 2021).

Reserve Bank of Zimbabwe. (2019). Cyber Attacks and the Imperative for Enhanced IT Security Strategies in the Banking Sector. Annual Report on Banking and Finance, 2019, 45-52

Sarangi, S., Tripathy, S. K., & Panda, S. K. (2019). Intelligent Intrusion Detection System Using Data Mining and Machine Learning Techniques. In Data Science and Big Data Analytics (pp. 63-80). Springer.

Smith, T. (2019). Cybersecurity in the banking sector: Challenges and solutions. International Journal of Economics, Commerce, and Management, 7(3), 128-136.

Smith, J. (2017). Cybersecurity and Banking: Ensuring Safe Electronic Transactions. Harare: Zimbabwe Publishing House.

Smith, A. (2019). The impact of cybersecurity on electronic banking: A case study of customer trust and confidence. International Journal of Electronic Commerce, 23(3), 1-22

Smith, J. (2020). Impact of Cyber Threats on IT Security Spending in Zimbabwean Banks. Journal of Cybersecurity, 5(2), 112-125.

Tamilselvan, M., Kumar, S. A., & Anand, K. (2020). A Comprehensive Analysis of Denial of Service (DoS) Attacks in Cloud Computing Environments. In Block chain and Machine Learning for Cybersecurity (pp. 125-144). IGI Global.

Wang, C. (2018). Two-factor authentication for online banking: A systematic literature review. Computers & Security, 76, 1-13.

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

QUESTIONNAIRE

Instructions to respondents

1. Read each question and answer each question truthfully and honestly

2. Do not inscribe any of your personal information in the questionnaire

3. Please tick where applicable in the space provided

Section A: Demographic Data

1. What is your gender?

   a. Male [ ]

   b. Female [ ]

   c. Other [ ]

2. Indicate your age group

   a. Below 25 [ ]

   b. 25-29 years [ ]

   c. 30-34 years [ ]

   d. 35 years and above [ ]

3. For how long have you been working at this institution?

   a. Less than 1 year [ ]

   b. 1-3 years [ ]

   c. 4-6 years [ ]

   d. 6 years [ ]

4. Employment category

   a. E-banking personnel [ ]

   b. ICT [ ]

c. Risk management [ ]

d. Compliance [ ]

e. Security Operation Center [ ]

5. Nature of Business

a. Security [ ]

b. Technological [ ]

c. Risk [ ]

d. Compliance [ ]

6. What is your highest level of education?

a. Diploma [ ]

b. Undergraduate [ ]

c. Postgraduate [ ]

Section B: Types of cybersecurity

7. Below are some of the common forms of cybersecurity in the electronic banking transactions. Please indicate their prevalence rates in your institution.

Types of Cybersecurity	**Doesn't Occur**	**Rarely Occur**	**Common**	**Very Common**
Firewalls				
Encryption				
Multi-factor authentication				
Secure payment gateways				
Transport Layer Security				
Data Loss Prevention (DLP)				

8. What other cybersecurity are prevalent in your institution. Please indicate below if there are any

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
………………

Section C: Impact of cybersecurity

9. Has your institution faced the impact of the following cybersecurity?

Impact	**YES**	**NO**
Data privacy		
Secure Authentication		
Fraud Prevention		
Transaction Integrity		
Customer trust and confidence		

10. What other effects have your institution faced due to cybersecurity

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
………………

Section D: Effectiveness of the emerging cybersecurity trends

11. Below are some of the strategies that the banking institution adopt as emerging cybersecurity trends to curb cyber threats. Please indicate whether the measure are available in your organization.

Measure	**YES**	**NO**	**Don’t know**

Threat intelligence sharing			
Secure mobile banking			
Artificial intelligence			
Cloud security			
Employee awareness and training			
Advanced authentication methods			

12. In addition to the measures above, what other measures has the institution put as emerging cybersecurity?

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
………………

13. What is your overall comment on the emerging cybersecurity trends in the electronic banking transactions?

a. Very ineffective [ ]

b. Not effective [ ]

c. Effective [ ]

d. Very effective [ ]

Section E: Measures that can be adopted to implement the cyber security trends

14. What tactics can your institution use to implement cybersecurity trends in the banking sector?

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
………………

15. In your own opinion, how can the government assist in the implementing of cyber security trends?

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
……………….

INTERVIEW GUIDE

1. What is the nature of cybersecurity affecting the ZB Bank?

2. How does ZB Bank assess and mange cybersecurity risks within the organization?

3. Have there been any notable instances where emerging cybersecurity trends positively impacted ZB Bank's security posture?

4. Can you discuss any challenges or obstacles faced by ZB Bank in adopting and integrating emerging cybersecurity trends?

5. How has the implementing of emerging cybersecurity trends contributed to the prevention or mitigation of cybercrime incidents at ZB Bank?

6. Are there any specific challenges or risks associated with the adoption of recommended emerging cybersecurity trends that should be addressed?

7. How can ZB Bank ensure a smooth integration of the recommended trends with its existing systems and processes?