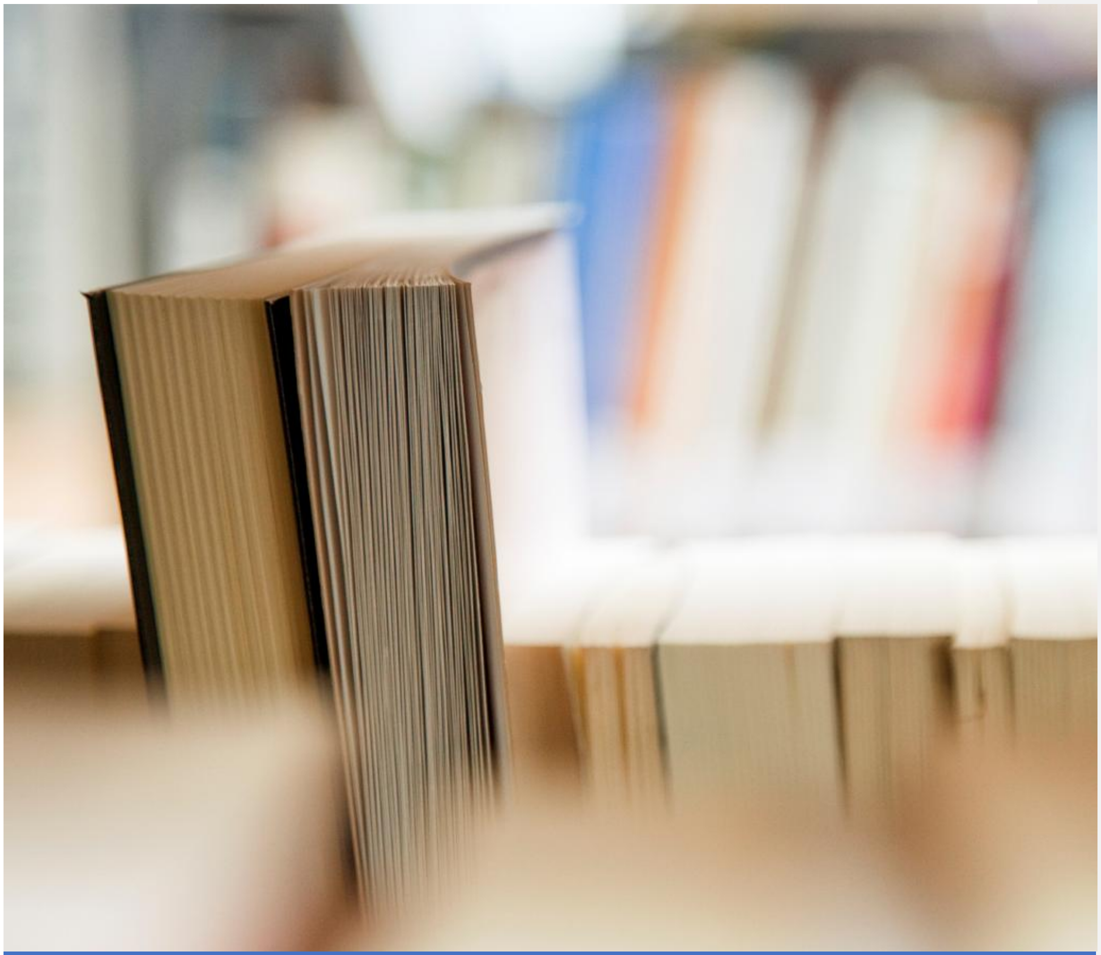


EFFECTIVENESS OF CYBERSECURITY INVESTMENT IN LOSS PREVENTION IN NIGERIAN BANKS

BUSINESS PROJECT SUPERVISOR: LAMIN FATTY

Oluwatobi Adewoye 9/20/23 BUSINESS PROJECT

A SYSTEMATIC REVIEW OF THE EFFECTIVENESS OF CYBERSECURITY INVESTMENT IN LOSS PREVENTION IN NIGERIAN BANKS

CANDIDATE NUMBER	C2064087
MODULE NAME	Business Project
WORD COUNT	9352
SUBMISSION DATE	**29 September, 2023**

DECLARATION
I declare that:

- This is my own unaided work.Yes ☒
  No ☐
- The word count stated by me is correct.Yes ☒
  No ☐
- I'm happy for my work to be retained on the Elite repository andmade available to staff and future students**
  Yes ☒
  No ☐

SUPERVISED BY: LAMIN FATTY

DEDICATION

I dedicate this project to my family, my dad, my mum, and my sister. You are the basis on which I have created not only this project, but also the dreams that inspire my path. This accomplishment is both yours and mine.

ACKNOWLEDGEMENT

As I reflect on my Masters path, I am overwhelmed with gratitude for the consistent support and direction that have helped turn this academic endeavor into a rewarding one.

First and foremost, I would like to thank God Almighty for His grace and guidance throughout this trip. His continual presence has provided me with strength and inspiration.

Mr. Lamin Fatty, my project supervisor, deserves my heartfelt gratitude for his excellent counsel, knowledge, and continuous support. His guidance has been critical in defining the course of my research.

I am grateful to the distinguished teaching members of the University of Law, Birmingham campus, whose commitment to knowledge transfer has provided me with the skills and insights required for academic and professional success. Thank you to all of my tutors for your persistent work.

During the academic year, I was extremely grateful to my friends, colleagues, and course mates, especially those in the Cybersecurity Management course 2022/2023. This goal has become a communal reality thanks to your companionship and persistent support.

To my friends in Birmingham and around the United Kingdom, your ongoing love, encouragement, and support have been a constant source of motivation. I am very glad for the ties we've formed and the triumphs we've shared.

Last but not least, I want to thank my parents Mr. & Mrs. Adewoye, my sister Tomilore Adewoye, my Uncles Engr. Raji and Dr. Raji, my aunty Pharm. Adenike Rufai, The Daniyans, The Akanbis, The Isholas, Family friends and members and my grandparents, both near and far. Your counsel, support, and encouragement have been pillars of strength for me. This accomplishment is both yours and mine.

I'd like to express my heartfelt gratitude to everyone who has been a part of this adventure. Your donations, no matter how large or small, have been critical in achieving this milestone.

Each of you, may the future bring you continued success and fulfilment.

Thank you very much.

Table of Contents

DEDICATION 2
ACKNOWLEDGEMENT 3
ABSTRACT 6
Chapter 1 7
Introduction 7
1.1 Background of the Study 7
1.2 Research Aim 8
1.3 Research Questions 8
1.4 Research Objectives 9
1.5 Research Hypotheses 9
1.6 Research Rationale 9
1.7 Scope of the Study 9
Chapter 2 10
Literature Review 10
2.1 Nature of investment in cybersecurity in Nigerian banks 10
2.1.1 Current state of cybersecurity and challenges in Nigerian banks 10
2.1.2 Best practices and strategies for effective cybersecurity for banks 11
2.2 Concept of loss prevention in Nigerian banks 13
2.3 Theoretical Review 14
2.3.1 Institutional Theory 14
2.3.2 Innovation Diffusion Theory 15
2.3.3 Deterrence Theory 15
2.4 Empirical Review 16
2.5 Gaps in the Literature 17
Chapter 3 18
Research Methodology 18
3.1 Introduction 18
3.2 Research Philosophy 19
3.3 Research Approach 19
3.4 Research Method 19
3.5 Data Sources 19

3.6 Data Analysis 20
3.6.1 Model Specification 20
3.6.2 Apriori Expectations 20
3.6.3 Explanation of Variables 21
3.6.4 Justification of Methods 21
3.7 Ethical Considerations 21
Chapter Four 22
Data Presentation, Analysis and Discussion of Findings 22
4.1 Introduction 22
4.2 Descriptive Analysis 22
4.3 Panel Data Estimation 25
4.4 Diagnostics 26
4.5 Summary of Findings 28
Chapter Five 29
Summary, Conclusions and Recommendations 29
5.1. Introduction 29
5.2. Summary of the Study 29
5.3. Conclusions of the Study 29
5.4. Contribution to Knowledge 29
5.5 Limitations of the Study 30
5.6 Areas for Further Research 30
5.7 Recommendations of the Study 30
References 31

ABSTRACT

This study investigated the effectiveness of Nigerian deposit banks' cybersecurity investment in preventing bank losses for the period 2016 to 2022. Bank losses was proxied by resolved claims of customers (as reported by customers and investigated and resolved by the banks) and bank gross earnings was used as a scale variable. Three research objectives and questions guided the study. The research used secondary data from banks annual financial reports in the form of panel data. A total of 11 banks were sampled and the panel data estimation technique of fixed effect estimation technique was employed for the regression instead of the random effects model as it was found to be more robust as our independent variables explained 71% of variation in bank losses due to cyber theft. The result from the study showed that banks investment in cybersecurity reduced bank loses, though statistically significant its effect was very minimal and losses due to Nigerian banks grows by 25% yearly. The study recommend that banks should massively increase their investments in cybersecurity in order to have a significant effect in reducing bank losses. The CBN and Financial Reporting Council of Nigeria should urgently draw up new financial reporting codes and standards that mandate banks to include their expenditures on cybersecurity and the actual losses due to cyber theft in their yearly financial reports as necessary information to the public.

Chapter 1

Introduction

1.1 Background of the Study

In recent years, Nigerian banking system has undergone significant transformations driven by advancements in technology and the widespread adoption of digital banking services. These developments have brought about numerous benefits, including improved efficiency, convenience, and expanded financial services. However, they have also introduced new risks and vulnerabilities, particularly in relation to cybersecurity (Kola-Oyeneyin, et al., 2020).

Nigeria's banking sector plays a critical role in the country's economy, serving as a catalyst for economic growth, financial inclusion, and trade facilitation. With a large and rapidly growing population, the demand for banking services has increased, leading to the expansion and diversification of the banking industry. As a result, Nigerian banks have become attractive targets for cybercriminals due to the potential financial gains associated with successful attacks. In recent years, there has been an increasing incidence of cyberattacks on Nigerian banks. According to Jaiyeola (2023), the Nigerian Bankers' Association reported that there were over 1,000 cyberattacks on Nigerian banks in 2020 alone. These cyberattacks have resulted in the loss of millions of naira, as well as the exposure of sensitive customer data.

The rise of cyber threats in Nigerian banks has been fuelled by several factors. Firstly, the increasing digitization and interconnectedness of banking systems have provided cybercriminals with more avenues for exploiting vulnerabilities. Secondly, the proliferation of mobile banking and electronic payment platforms has created new entry points for attacks, with criminals targeting both individual customers and the banks themselves. Additionally, the casualization of bank workers which leads to constant churn greatly compromises bank security systems and architecture.

Banks that suffer data breach stand to lose more than just the money that has been siphoned but their clientele and reputation that took years to build (Ekran, 2022). A review cited by Baur-Yazbeck et al. (2019) points that globally, “Africa’s financial institutions are the most vulnerable to cyberattacks due to weak system safeguards and protections”. According to Aladenusi and Odumuboni (2022), Nigeria has been in the top 16th most affected country for cybercrime in the past five years. Agusto & Co. credit rating agency in their 2022 Consumer Digital Banking Satisfaction Index reported that 59% of Nigerians have fallen victim to cyberattack in recent years (Olowole, 2022). Orji (2019) submits that because Nigeria has the largest population of internet users in Africa with over 100 million subscribers, the potential cost of cybercrime to the Nigerian economy is over 13 billion US dollars yearly.

Cybersecurity breaches and financial fraud in Nigerian banks range from unauthorized fund transfers, ATM skimming, phishing attacks, and data breaches leading to identity theft. The impact of these attacks extends beyond the banks themselves, affecting the overall stability of the financial system and the confidence of both domestic and international stakeholders. Hence, the regulatory environment in Nigeria has recognized the importance of cybersecurity in the banking sector. The Central Bank of Nigeria (CBN) issued guidelines and regulations to enhance cybersecurity practices in banks, such as the CBN 2018 Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers. However, despite these efforts, there are ongoing challenges in effectively implementing and enforcing cybersecurity measures across the banking industry.

According to a Deloitte (2022) report, banks on their part have tried to modernize their cybersecurity systems with many using zero trust architecture and multifactor authentication to manage their stored data on cloud services. Still the industry has suffered new forms of attack like corporate espionage whereby banks hire hackers to steal trading information of competitor banks. This kind of motive complicates cybersecurity as every bank belongs to the interbank settlements system. On the other hand, as many financial institutions migrate to cloud host services, care must be taken to avoid Distributed Denial of Service attacks (DDoS). Imperva (2022) states that DDoS attack involves "multiple connected online devices, collectively known as Botnet, which are used to overwhelm a target website with fake traffics". Most corporate espionage in the financial sector come in form of DDoS attacks where a competitor aims at disrupting another's business platform with the aim of stealing frustrated customers.

Other known forms are hacktivism is when people express displeasure at big businesses and try to bring their website down as seen during the end SARS protest. A well-known hacktivist is the Anonymous group. Another form is via extortion, when a cybercriminal demands money to stop a DDoS attack often known as ransomware. A mode of attack very common in Nigeria is phishing, which is a method of cloning emails and domains into tricking users to give away personal information or unknowingly download malware (Partida, 2022).

The nature of remote work by employees have made phishing even on the rise. A Gallup poll in late 2021 has shown that 54% of employees want hybrid work arrangements while 37% exclusively want to continue working remotely as they did during Covid19 (Partida, 2022). This complicates the fight against phishing as a bank employee that works from a coffee shop may use a public WIFI that lacks the needed protection. Another method that is popular in developing countries like Nigeria, similar to phishing is spoofing. A popular spoof in Nigeria is when "a hacker 'spoofs' a financial institution's phone number to call or text customers to trick them into disclosing personal account details. The bank's correct caller ID will show up on the customer's phone, making it difficult for customers to ascertain its legitimacy. Spoofing attacks is known to decrease customer's trust (Partida, 2022).

1.2 Research Aim

The research aim is to evaluate effectiveness of cybersecurity investment in loss prevention in Nigerian banks.

1.3 Research Questions

The study aims to provide answers to the following research questions:

I. What is the extent of banks' investment in cybersecurity systems?

II. Does banks' investment on cybersecurity systems deter fraud losses?

III. What is the average yearly growth rate of losses due to cyber fraud in Nigerian banks?

1.4 Research Objectives

The broad objective of this study is to investigate the nexus between banks' cybersecurity investments and bank losses, in order words if the deployed cybersecurity infrastructure by banks have been able to prevent incidences of theft. This is further narrowed down to the following specific objectives which are:

I. To investigate the yearly size of investments in cybersecurity in Nigerian banking sector.

II. To determine the impact of bank's cybersecurity investment on losses.

III. To ascertain the average yearly growth rate of losses due to cyber fraud in banks.

1.5 Research Hypotheses

The following null hypothesis is formulated to guide the study.

H_0; Banks' investments in cybersecurity does not have any significant influence on losses.

1.6 Research Rationale

The rationale for this research lies in the increasing importance of cybersecurity in Nigerian banks and the critical need for effective loss prevention measures. Nigerian banks play a crucial role in the country's economy, but they face significant challenges in safeguarding their assets and protecting customer information from cyber threats. With the rapid digitization of banking services and the rise of cybercriminal activities, there is a pressing need to assess the effectiveness of existing cybersecurity practices in mitigating financial losses and ensuring the security of customer assets.

1.7 Scope of the Study

In the financial world, losses refer to negative financial outcomes experienced by individuals, companies, or financial institutions. A loss occurs when the value of an asset or investment decreases, resulting in a financial setback or decrease in net worth. Losses can occur in various financial contexts, including investments, trading activities, business operations, and lending. However, this study will limit losses to theft of money by a third party from a bank's customers account.

The Nigerian banking sphere is made up of merchant banks, commercial banks, microfinance banks and development banks. This study will only use evidence from sampled commercial banks. This study will analyse 11 banks and the time period of analysis will be from 2016 to 2022.

Chapter 2

Literature Review

2.1 Nature of investment in cybersecurity in Nigerian banks

Investments in cybersecurity can be classified into two main categories; hardware investments which include investments in security appliances such as firewalls, intrusion detection systems, and antivirus software (Ojeka, et al., 2017). The second is software investments which include investments in security software such as anti-malware software, data loss prevention software, and identity and access management software. This software is typically installed on a bank's computer systems. In addition to hardware and software investments, Nigerian banks also invest in cybersecurity through employee trainings. Employees are trained on how to identify and avoid cyberattacks. Trainings cover topics such as phishing, malware, and data breaches.

The nature of investment in cybersecurity in Nigerian banks is constantly evolving as new threats emerge and new technologies are developed. For example, in recent years, there has been a growing focus on investments in cloud security and artificial intelligence (AI)-powered cybersecurity solutions. In most cases, investments in cybersecurity are imported into Nigeria because there is limited local production of cybersecurity products and services (Akintoye, et al., 2022). However, there are a growing number of Nigerian cybersecurity companies that are developing and providing local solutions.

Investment in cybersecurity is often treated as an operating expense in Nigerian banks. This includes costs associated with implementing and maintaining cybersecurity measures such as firewalls, antivirus software, intrusion detection systems, employee training programs, and security audits. These expenses are incurred on an ongoing basis to ensure the effectiveness and continuity of cybersecurity practices within the bank.

2.1.1 Current state of cybersecurity and challenges in Nigerian banks

The current state of cybersecurity in Nigerian banks is mixed. There have been some improvements in recent years, but there are still significant challenges and vulnerabilities. One of the biggest challenges is the lack of awareness of cybersecurity risks among bank employees. Employees are often the weakest link in a bank's cybersecurity defences, as they may not be aware of the latest threats or how to protect themselves (Rufus Akintoye & Joshua, 2022). Another challenge is the lack of investment in cybersecurity. Nigerian banks have traditionally not invested heavily in cybersecurity, and this has left them vulnerable to attacks.

In Nigeria there has been a couple of advancements in cybersecurity namely increased awareness, regulatory guidance and technology adoption. Nigerian banks have become more aware of the importance of cybersecurity and the potential risks they face. They have recognized the need for proactive measures to protect their systems, customer data, and financial transactions. The CBN has issued guidelines and regulations to enhance cybersecurity practices in banks. These include the CBN Cybersecurity Guidelines for Deposit Money Banks and Payment Service Providers, which provide a framework for implementing robust security measures. Nigerian banks have adopted advanced technologies and solutions to strengthen their cybersecurity posture. This includes implementing firewalls, intrusion detection systems, encryption mechanisms, multi-factor authentication, and security information and event management (SIEM) tools.

However, challenges still remain namely sophisticated cyber threats, insider threats, lack of skilled professionals and legacy systems and infrastructure (Deloitte, 2022). Nigerian banks face a constant and evolving threat landscape, with cybercriminals employing sophisticated techniques such as phishing, social engineering, ransomware attacks, and advanced persistent threats (APTs). Insider threats, whether intentional or unintentional, pose significant challenges. This includes employees with access to sensitive data who may engage in unauthorized activities or inadvertently compromise security through negligence or lack of awareness (Makeri Ajiji, 2017). The shortage of skilled cybersecurity professionals especially from the massive emigration from Nigeria is a major challenge for banks. There is a need to recruit and retain talent with specialized cybersecurity skills to effectively manage and respond to cyber threats. Many Nigerian banks still rely on legacy systems that may have vulnerabilities or limitations in terms of security. Updating and securing these systems can be challenging due to compatibility issues, cost considerations, and the need for extensive testing (Garba & Musa Bade, 2021).

2.1.2 Best practices and strategies for effective cybersecurity for banks

Scofield (2022) and Saracino (2022) listed some of the major steps for effective cybersecurity management which are;

i. Risk Assessment and Management:

Conduct regular risk assessments to identify potential vulnerabilities and threats specific to the bank's systems, infrastructure, and operations.

Develop a risk management framework that includes risk identification, analysis, evaluation, and mitigation strategies.

Prioritize risks based on their potential impact and likelihood of occurrence to allocate resources effectively.

ii. Robust Security Infrastructure:

Implement multi-layered security measures, including firewalls, intrusion detection and prevention systems, secure network architecture, and encryption protocols.

Deploy advanced authentication mechanisms, such as multi-factor authentication (MFA), to enhance the security of user access and transactions.

Regularly update and patch software, operating systems, and firmware to address known vulnerabilities and protect against emerging threats.

iii. Employee Awareness and Training:

Conduct regular cybersecurity awareness and training programs for all employees to educate them about common threats, safe online practices, and their roles and responsibilities in maintaining security.

Promote a culture of security consciousness by encouraging employees to report suspicious activities, phishing attempts, or any potential security incidents.

Establish clear policies and procedures for handling sensitive data, password management, and acceptable use of technology resources.

iv. Incident Response and Recovery:

Develop an incident response plan to ensure a swift and coordinated response to security incidents. This includes identifying key personnel, establishing communication channels, and defining escalation procedures.

Regularly test and update the incident response plan to align with emerging threats and changing technologies.

Implement backup and recovery mechanisms to ensure the availability and integrity of critical data in the event of a cybersecurity incident.

v. Vendor and Third-Party Management:

Establish strict security requirements for third-party vendors and conduct due diligence assessments before engaging in partnerships or outsourcing services.

Monitor and enforce compliance with security standards and contractual obligations by third-party vendors.

Regularly review and update vendor contracts to include provisions for cybersecurity, incident reporting, and data protection.

vi. Continuous Monitoring and Threat Intelligence:

Implement a Security Operations Centre (SOC) or utilize managed security services to monitor network traffic, detect anomalies, and respond to security incidents in real-time.

Stay updated on the latest cybersecurity threats, trends, and best practices through information sharing platforms, industry collaborations, and partnerships with security vendors.

Leverage threat intelligence sources to proactively identify potential threats, vulnerabilities, and attack vectors.

vii. Regulatory Compliance:

Ensure compliance with applicable regulatory requirements, such as the Central Bank of Nigeria's cybersecurity guidelines and other relevant data protection regulations.

Regularly assess the bank's cybersecurity practices against regulatory frameworks and guidelines to identify gaps and implement necessary improvements.

viii. Collaboration and Information Sharing:

Participate in industry forums, information sharing platforms, and collaborations with other banks and financial institutions to exchange insights, experiences, and best practices.

Engage with law enforcement agencies and industry-specific cybersecurity organizations to report incidents, share threat intelligence, and contribute to collective efforts in combating cyber threats.

2.2 Concept of loss prevention in Nigerian banks

Adetiloye, Olokoyo and Taiwo (2016) submit that loss prevention in Nigerian banks encompasses various strategies and measures aimed at identifying, mitigating, and preventing financial losses resulting from fraud, embezzlement, theft, and other forms of misconduct. The concept of loss prevention in Nigerian banks evolved over time, with one influential component being the introduction of forensic accounting practices. Forensic accounting emerged as a specialized field within accounting that focuses on investigating financial crimes, detecting irregularities, and providing evidence for legal proceedings.

In the Nigerian banking sector, forensic accounting played a pivotal role in uncovering fraudulent activities and establishing controls to prevent similar occurrences. The use of forensic accounting techniques helped banks identify loopholes in internal systems, enhance internal controls, and develop fraud prevention mechanisms. The adoption of forensic accounting in Nigerian banks was influenced by several factors. Firstly, there was a growing recognition of the need to combat financial crimes and protect the integrity of the banking system. This led to increased demand for professionals with expertise in forensic accounting to address the rising incidents of fraud and embezzlement. Secondly, regulatory bodies, such as the CBN, emphasized the importance of internal control mechanisms and compliance with anti-money laundering and anti-fraud regulations (Kawugana & Faruna, 2018).

According to Uniamikogbo (2019), as forensic accounting gained traction in Nigerian banks, it became an integral part of loss prevention strategies. The role of forensic accountants expanded to include proactive measures such as risk assessment, fraud detection, and the development of fraud prevention policies. Forensic accountants worked closely with internal audit departments and law enforcement agencies to investigate suspicious transactions, trace illicit funds, and prosecute offenders. However, as technology advanced and banking operations became increasingly digitized, traditional forensic accounting methods alone proved insufficient to address the evolving landscape of financial crimes. This necessitated the integration of cybersecurity measures into the concept of loss prevention in Nigerian banks.

Today, loss prevention in Nigerian banks encompasses a comprehensive approach that combines traditional forensic accounting practices with robust cybersecurity measures. Banks have invested in sophisticated technological solutions to protect their systems, detect and prevent cyber threats, and ensure the integrity of financial transactions. This includes the implementation of firewalls, intrusion detection systems, encryption mechanisms, user authentication protocols, and continuous monitoring of network activities. Furthermore, loss prevention in Nigerian banks extends beyond internal measures and incorporates customer awareness programs, staff training on fraud detection, and collaborations with regulatory bodies and law enforcement agencies to share intelligence and combat financial crimes effectively (Adeyemo, 2012).

2.3 Theoretical Review

Theoretical review in research work provides a comprehensive and critical analysis of the existing theoretical literature relevant to the research topic or problem. The theoretical review aims to identify and evaluate the key concepts, ideas, and theories that have been developed by previous researchers in the field. It helps to ensure that the research is grounded in the relevant theoretical literature and that the research design is appropriate for addressing the research questions or hypotheses. Below is a list of relevant theories that will guide this study.

2.3.1 Institutional Theory

Institutional theory is a sociological theory that examines how social and organizational structures influence individual and organizational behaviour. It was initially developed by two prominent scholars, John W. Meyer and Brian Rowan, in 1977 (Robert J. David & Boghossian, 2019). Meyer and Rowan's work laid the foundation for institutional theory, which has since evolved and expanded into various fields, including sociology, organizational studies, and management. The central premise of institutional theory is that institutions, which include formal and informal rules, norms, and values, shape the behaviour of individuals and organizations. Guth (2016) explains that institutions exert influence through three primary mechanisms: coercive, normative, and mimetic.

Coercive Mechanism: Coercive influences are based on formal regulations, laws, and rules. Organizations comply with these regulations to avoid penalties, sanctions, or legal consequences. In the context of cybersecurity in Nigerian banks, the coercive mechanism of institutional theory can be observed through compliance with regulatory guidelines issued by the Central Bank of Nigeria (CBN) and other governing bodies.

Normative Mechanism: Normative influences refer to social norms, values, and expectations that guide behaviour. Organizations conform to these norms to gain legitimacy and acceptance within their social environment. In the context of cybersecurity, normative pressures can be seen in the adoption of industry best practices, adherence to international standards, and the establishment of ethical codes of conduct.

Mimetic Mechanism: Mimetic influences occur when organizations imitate or emulate the practices of others, particularly those considered successful or prestigious. In the cybersecurity context, Nigerian banks may adopt cybersecurity measures and practices observed in other reputable financial institutions to maintain competitiveness and legitimacy in the industry.

Institutional theory suggests that organizations strive for legitimacy by conforming to institutional pressures. Thus, the effectiveness of cybersecurity measures in Nigerian banks can be influenced by the regulatory environment, industry norms, and practices, as well as the social expectations and pressures faced by these institutions. Over time, Institutional Theory has expanded to include concepts such as institutional isomorphism (the tendency for organizations to become more similar to each other over time) and institutional logics (the dominant values, beliefs, and assumptions that shape organizational behaviour). These concepts further enhance our understanding of how institutions shape cybersecurity practices in Nigerian banks and their impact on loss prevention outcomes.

2.3.2 Innovation Diffusion Theory

This theory developed by sociologist Everett M. Rogers in 1962, explores how new ideas, practices, or technologies spread within a social system. It provides insights into the adoption and acceptance of innovations by individuals, organizations, or communities (Surry & Farquhar, 1997). The theory has been widely applied across various fields, including technology, healthcare, and organizational studies.

Rogers (1995) discusses key components of the diffusion of innovation theory to include:

Innovation: An innovation refers to a new idea, practice, or technology that is perceived as new or different by the individuals or organizations adopting it. In the context of cybersecurity in Nigerian banks, innovations can include new security technologies, processes, or strategies aimed at preventing losses due to cyber threats.

Adoption: Adoption refers to the decision of individuals or organizations to implement and use the innovation. It involves the acceptance, assimilation, and integration of the innovation into existing systems or practices. Adoption can be influenced by factors such as perceived benefits, compatibility with existing processes, complexity, trialability, and observability.

Diffusion: Diffusion is the process by which an innovation spreads through a social system. It involves the communication, dissemination, and adoption of the innovation across different individuals, organizations, or communities. Diffusion can occur through various channels, including interpersonal networks, mass media, and organizational communication.

Adopter Categories: The Diffusion of Innovation Theory categorizes adopters into different groups based on their timing of adoption relative to others. These categories include innovators, early adopters, early majority, late majority, and laggards. Innovators and early adopters are typically more open to adopting new innovations and play a crucial role in driving the diffusion process.

Kang and Westskytte (2018) suggest that applying the Diffusion of Innovation Theory to cybersecurity in banks, researchers can examine factors influencing the adoption and diffusion of cybersecurity practices. This includes understanding the characteristics of the innovation, identifying opinion leaders and influential individuals within the banking sector, assessing organizational readiness for change, and analysing communication channels and networks that facilitate the spread of cybersecurity practices.

2.3.3 Deterrence Theory

Deterrence theory is a criminological theory that focuses on how the threat of punishment or negative consequences influences individuals' decision-making and behaviour. Howe and Pelser (2020) note that it was originally developed within the field of criminology in the mid-20th century and has since been applied to various contexts, including cybersecurity. it is important to complement the analysis with other theories and frameworks to gain a comprehensive understanding of the effectiveness of cybersecurity in loss prevention. The concept of deterrence is based on the assumption that individuals are rational decision-makers who weigh the potential costs and benefits of their actions. it proposes that the fear of punishment or negative outcomes acts as a deterrent, influencing individuals to refrain from engaging in illegal or undesirable behaviours (D'Arcy & Herath, 2011).

In the context of cybersecurity and loss prevention in Nigerian banks, Deterrence Theory can be applied to understand how the implementation of cybersecurity measures can deter potential cybercriminals and reduce the likelihood of security breaches. Ghandi (2012) list key components of deterrence theory include:

Severity: the severity of punishment or negative consequences plays a crucial role in deterrence. In the cybersecurity context, this can include legal penalties, financial liabilities, damage to reputation, or loss of trust. The more severe the potential consequences, the greater the deterrence effect.

Certainty: Deterrence theory emphasizes the importance of the perceived certainty of punishment. If potential cybercriminals believe that they are likely to be caught and face consequences for their actions, they are more likely to be deterred. Therefore, the presence of robust cybersecurity measures, effective monitoring systems, and timely incident response mechanisms can enhance the perceived certainty of being caught, thus strengthening the deterrence effect.

Swiftness: The swiftness of punishment or negative consequences is another factor in deterrence. Prompt and efficient responses to cybersecurity incidents can increase the perception that the likelihood of being caught and punished is high, further deterring potential cybercriminals.

By examining Deterrence Theory in the context of cybersecurity, researchers can assess the effectiveness of cybersecurity measures in deterring cybercriminal activities in Nigerian banks. This includes analysing the perceived severity, certainty, and swiftness of the consequences associated with cybersecurity breaches, as well as exploring the role of regulatory frameworks, law enforcement efforts, and incident response capabilities in strengthening deterrence.

2.4 Empirical Review

Khalil et al. (2021) in thier study surveyed managerial cadre employees of various electronic banks (e-banks) working in Pakistan to analyze the association between cybersecurity costs and e-banking product innovation performance (PIP) and financial performance (FP). The collected data were estimated via multivariate statistical techniques after which they found that prevention and detection costs (PDC), response costs (RC), and development costs (DC) have a statistically significant effect on PIP and FP, while indirect costs (IC) have a negative significant influence on PIP and FP. The study also found that PIP has a statistically significant effect on e-banking FP. Additionally, the study found that PIP partially mediates an association between PDC, RC, DC, and FP, while PIP insignificantly mediates in a relationship amongst IC and e-banking FP. The study's findings suggest that cybersecurity costs can have a significant impact on e-banking PIP and FP. The study also found that PIP can mediate the association between cybersecurity costs and FP. The findings are applicable to the modern electronic banking (e-banking) systematic risk control and information security solution. The study is novel in the context of cyber security costs, including (PDC, RC, DC, IC) by measuring its influence on PI and e-banking FP.

Bouveret (2018) analyzed cyber risk around the world for financial institutions by analyzing a variety of datasets, including data from financial institutions, government agencies, and cybersecurity firms. The collected data were used to create a novel standard VaR type framework "to assess various types of stability risk and can be easily applied at the individual country level". The study found that data breaches, fraud, and business disruption are the most common types of cyber incidents that financial institutions face. The study also found that cyber risk can have a significant impact on financial institutions, with losses ranging from 10 to 30 percent of net income. The study's findings suggest that cyber risk is a significant threat to financial institutions and that financial institutions need to take steps to mitigate this risk.

Wang, Nnaji and Jung (n.d.) in their study analyze cyber security in the Nigerian Internet banking industry using an online survey with 100 experienced professionals working in both the Nigerian banking and banking security service sectors. The study found that the Nigerian cybercrime industry has transformed from low-tech cyber-enabled crimes to high-tech sophisticated breaches. The top three most experienced breaches are viruses, worms or Trojan infections; electronic spam mails; and hacking. The study also found that banking professionals have received adequate management in both support and training. However, the lack of advanced technologies to prevent and address cyber security breaches and the unsatisfactory level of legislative compliance are the primary factors that have reduced cyber security capability in Nigerian banks.

2.5 Gaps in the Literature

A thorough online search by this author showed that there is paucity of research on the relationship between Nigerian banks' investment in cybersecurity systems and losses using secondary data. This is so because a lot of researchers cannot untangle the classification issues in cybersecurity investment which is a major part of intangible assets and their obliviousness to the availability of fraud loss secondary data. To this end, this study aims to fill this void with empirically analysed data, using a sophisticated technique of panel data estimation.

Chapter 3

Research Methodology

3.1 Introduction

This study uses the Onion Model of research methodology proposed by Saunders, Lewis and Thornhill (2016), which emphasizes the iterative and cyclical nature of the research process. According to this model as shown in figure 1, the research process involves several layers or stages, with each layer building upon the previous one. The outermost layer is the philosophical paradigm, which informs the researcher's worldview and influences their research design and methods. The next layer is the research strategy, which includes the overall approach to the research and the specific methods used to collect and analyse data.

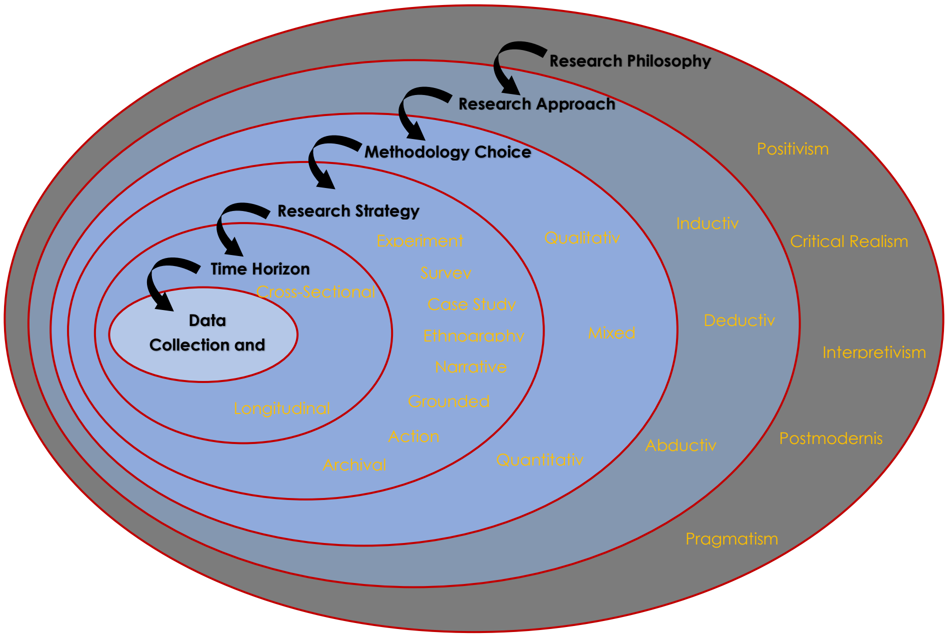


Figure 1: Research Onion Model (Adapted from Saunders, Lewis and Thornhill, 2016)

The third layer is the research choices, which involves decisions about the type of data to collect, the sampling method, and the data collection instruments. The fourth layer is the time horizon, which refers to the time frame over which data is collected and analysed. The fifth layer is the data collection and analysis methods, which includes techniques such as surveys, interviews, and statistical analysis. Finally, the innermost layer is the research findings, which are used to draw conclusions and make recommendations. Saunders, Lewis and Thornhill (2016) recommend that researchers move back and forth between these layers as they refine their research questions and design. This iterative process helps to ensure that the research is rigorous and valid, and that the findings are meaningful and useful.

3.2 Research Philosophy

Research philosophy reflects the underlying beliefs about the nature of knowledge and reality. For panel data analysis research, this study will use the positivist research philosophy. Positivism is an epistemological stance that emphasizes the objectivity of knowledge and the use of scientific methods to understand and explain phenomena (Saunders, Lewis & Thornhill, 2016). It assumes that there is an objective reality that can be observed, measured, and analysed. In the context of panel data analysis, a positivist research philosophy aligns well with the quantitative nature of the approach, where data is collected, analysed, and interpreted using statistical methods.

3.3 Research Approach

According to the Onion Research Model by Saunders, Lewis and Thornhill (2016), the research approach is the second layer of the research onion and defines the overall strategy or plan for conducting the research. The appropriate research approach for panel data analysis would be the deductive approach. The deductive approach is commonly associated with positivist research philosophy and involves testing hypotheses derived from existing theories or conceptual frameworks.

3.4 Research Method

The research method for our study would be quantitative research. Quantitative research involves the systematic collection, analysis, and interpretation of numerical data to answer research questions and test hypotheses. It emphasizes the use of statistical methods and large sample sizes to provide objective and generalizable results. Bryman and Bell (2015) enumarated the steps to include data collection, quantitative analysis by employing statistical techniques to analyze the collected data. In the context of panel data analysis, we will later find out whether it is fixed effects or random effects models that best fits our data. To examine the relationships between variables we will need to use a statistical software package.

3.5 Data Sources

This study uses firm level panel data gotten from the yearly audited financial statements published on the relevant banks' website and on the Nigeria Stock Exchange website. Panel data combines time series and cross-sectional data. It is imperative to add that for this study, we will use a balanced panel data meaning that each entity (or bank) will contribute the same number of data, in other words there will not be any missing data also called unbalanced panel. The number of banks used for this study is more than the time period, our panel data can also be called a short panel.

3.6 Data Analysis

Panel data regression method will be used and it comprises of fixed effect estimator and random effect estimator. For the properties of the two estimators, econometric theory shows that the fixed effect estimator is always consistent even if the underlying model is random effects (Gujarati & Porter, 2009). Normally in conducting a panel data estimation, both estimators are estimated together and another test called the Hausman test is conducted to choose between the two estimators.

3.6.1 Model Specification

The implicit (functional) representation of the model is expressed as:

$$BL = f\ (ICS, GE, Trend) \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ (3.1)$$

Where;

BL = Bank Losses

ICS = Investments in Cybersecurity

GE = Gross Earnings

Trend = Time trend is a vector of year dummies to measure the yearly average growth rate of bank loses

The explicit (econometric) form of the model in equation (3.1) is expressed as;

$$BL_{it} = \beta_{1i} + \beta_2\ ICS_{it} + \beta_3\ GE_{it} + \beta_4\ Trend_i + \mu_{it} \ \ldots\ldots\ldots\ldots\ldots\ldots\ (3.2)$$

3.6.2 Apriori Expectations

This refers to the supposed relationship between the dependent and independent variables of the model as determined by theoretical postulation. The result or parameter estimates of the model will be interpreted on the basis of the supposed signs of the parameters as established by theory.

Differentiating partially with respect to each of the variables to obtain apriori expectation of equation (3.2) will result as follows;

$$B2 < 0,\ B3 > 0\ B4 < 0 \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ (3.3)$$

For the apriori expectations, both parameters or coefficients of B2 and B3 is expected to be positive and negative respectively because it is expected that as investments in cybersecurity increases, bank losses due to cyber theft will reduce and as gross earnings increases, hackers will be attracted to steal from the banks. While negative B4 indicates decrease in BL with the time Trend assuming banks adopt latest cybersecurity systems. In sum, based on apriori bank losses is expected to decrease when CSI increases and as time passes on (via Time Trend). All the negative relationships could be as a result of adopting modern cybersecurity technologies by banks.

3.6.3 Explanation of Variables

The functional model in relation (3.1) is a multivariate equation. Bank losses is our dependent variable. On the right-hand side of equation (3.2) are the independent variables made up of investment in cybersecurity (ICS) and gross earnings (GE) which proxy revenue. Gross earnings will serve as our scale variable. In line with Central Bank of Nigeria (CBN) requirement, banks are mandated to publish complaints by customers of irregular debits on their accounts, usually from cyber theft. The banks have two choices, either to resolve it or escalate it to CBN for intervention. In some cases, when banks claim to resolve it (after their investigation), they refund the total amount claimed from the customer, when this is the case under the resolved complaint, we use the total amounts claimed as a proxy for bank losses.

But in many cases banks do not refunds the whole monies claimed in a financial year even when the complaints have been thoroughly investigated and resolved. Banks may not want to refund all monies resolve probably because it overstretches their loss provision for a given financial year. When this is the case, we take the difference between amounts claimed (which is larger) and amounts refunded as a proxy for losses. The difference is that in the first case the incidence of loss falls on the bank, while in the latter it falls on the customers.

3.6.4 Justification of Methods

Apart from the fact that panel regression model is widely used in measuring the effects of investments and operational efficiency among firms, the superiority of panel regression model is in the fact that it gives "more informative data, more variability, less collinearity among variables, more degrees of freedom and more efficiency (Gujarati & Porter, 2009).

3.7 Ethical Considerations

Research ethics are crucial to ensure the reliability and credibility of the research work (Saunders, Lewis & Thornhill, 2016). However, in this given study, all the secondary data are extracted from reliable and credible sources and properly acknowledged to ensure ethical research work. Overall, there are no significant research ethical issues in this research as human participants are not involved and the data is publicly available.

Chapter Four

Data Presentation, Analysis and Discussion of Findings

Commented [LF1]: Great work. It is observed that you have identified your data and starting analyzing using econometrics and other statistical tools. This is where you contributes to the subject area. I have captured all the points we discussed in our last meetings.

4.1 Introduction

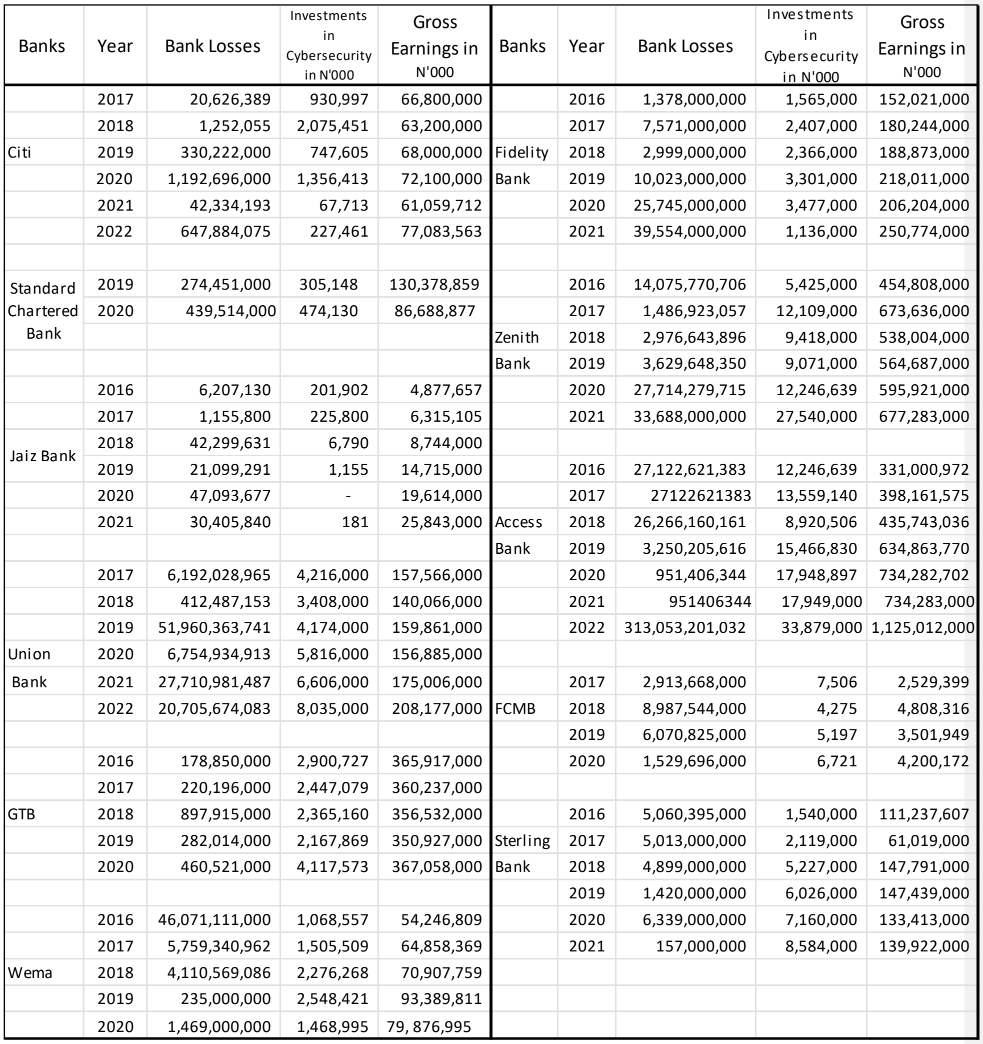
In this chapter, the sourced data was analysed, and results discussed with respect to the research question and hypothesis of the study.

4.2 Descriptive Analysis

The data from Table 4.1 below shows that bank revenue proxied by gross earnings (in N' thousands) were not continuously rising, there were periods it fell especially due to the Covid19 impact in 2019 and 2020 as can be seen from the results of Wema bank, Fidelity bank, Zenith bank, UBA and FCMB. The composition of the deposit money banks ranges from Jaiz bank (an Islamic bank) while Citi bank and Standard Chartered bank (are foreign owned banks with subsidiary in Nigeria). The other remaining banks are Nigerian owned and headquartered. It is important to note that some of the systematically important bank otherwise known as tier 1 banks made it into our sample. They include GTB, Access bank and Zenith bank.

Furthermore, from Figure 4.2 we can deduce that the type of panel data used for our analysis is unbalanced panel in that not all the banks had data from the same years. Only Jaiz, GTB, Wema, Fidelity, Zenith, Access and Sterling banks posted data from 2016. Citi, Access, and Union banks were the only banks that posted data for 2022. The rest of the banks had data from 2017 to 2020. Our panel data can also be said to be a short panel because the number of entities in this case, 11 banks are more than the number of years involved which is seven (2016-2022). The benefit of short panel is that we do not need to bother about the stationarity of the variables which is a necessary condition for parameter estimation.

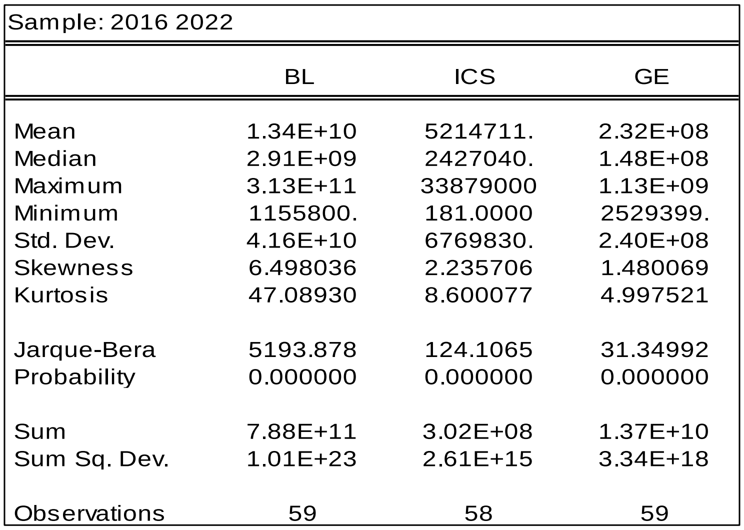
Table 4.1 Panel data for the 11 sampled banks



Banks	Year	Bank Losses	Investments in Cybersecurity in N'000	Gross Earnings in N'000	Banks	Year	Bank Losses	Investments in Cybersecurity in N'000	Gross Earnings in N'000
	2017	20,626,389	930,997	66,800,000		2016	1,378,000,000	1,565,000	152,021,000
	2018	1,252,055	2,075,451	63,200,000		2017	7,571,000,000	2,407,000	180,244,000
Citi	2019	330,222,000	747,605	68,000,000	Fidelity	2018	2,999,000,000	2,366,000	188,873,000
	2020	1,192,696,000	1,356,413	72,100,000	Bank	2019	10,023,000,000	3,301,000	218,011,000
	2021	42,334,193	67,713	61,059,712		2020	25,745,000,000	3,477,000	206,204,000
	2022	647,884,075	227,461	77,083,563		2021	39,554,000,000	1,136,000	250,774,000
Standard Chartered Bank	2019	274,451,000	305,148	130,378,859		2016	14,075,770,706	5,425,000	454,808,000
	2020	439,514,000	474,130	86,688,877		2017	1,486,923,057	12,109,000	673,636,000
					Zenith	2018	2,976,643,896	9,418,000	538,004,000
					Bank	2019	3,629,648,350	9,071,000	564,687,000
	2016	6,207,130	201,902	4,877,657		2020	27,714,279,715	12,246,639	595,921,000
	2017	1,155,800	225,800	6,315,105		2021	33,688,000,000	27,540,000	677,283,000
Jaiz Bank	2018	42,299,631	6,790	8,744,000					
	2019	21,099,291	1,155	14,715,000		2016	27,122,621,383	12,246,639	331,000,972
	2020	47,093,677	-	19,614,000		2017	27122621383	13,559,140	398,161,575
	2021	30,405,840	181	25,843,000	Access	2018	26,266,160,161	8,920,506	435,743,036
					Bank	2019	3,250,205,616	15,466,830	634,863,770
	2017	6,192,028,965	4,216,000	157,566,000		2020	951,406,344	17,948,897	734,282,702
	2018	412,487,153	3,408,000	140,066,000		2021	951406344	17,949,000	734,283,000
	2019	51,960,363,741	4,174,000	159,861,000		2022	313,053,201,032	33,879,000	1,125,012,000
Union	2020	6,754,934,913	5,816,000	156,885,000					
Bank	2021	27,710,981,487	6,606,000	175,006,000		2017	2,913,668,000	7,506	2,529,399
	2022	20,705,674,083	8,035,000	208,177,000	FCMB	2018	8,987,544,000	4,275	4,808,316
						2019	6,070,825,000	5,197	3,501,949
	2016	178,850,000	2,900,727	365,917,000		2020	1,529,696,000	6,721	4,200,172
	2017	220,196,000	2,447,079	360,237,000					
GTB	2018	897,915,000	2,365,160	356,532,000		2016	5,060,395,000	1,540,000	111,237,607
	2019	282,014,000	2,167,869	350,927,000	Sterling	2017	5,013,000,000	2,119,000	61,019,000
	2020	460,521,000	4,117,573	367,058,000	Bank	2018	4,899,000,000	5,227,000	147,791,000
						2019	1,420,000,000	6,026,000	147,439,000
	2016	46,071,111,000	1,068,557	54,246,809		2020	6,339,000,000	7,160,000	133,413,000
	2017	5,759,340,962	1,505,509	64,858,369		2021	157,000,000	8,584,000	139,922,000
Wema	2018	4,110,569,086	2,276,268	70,907,759					
	2019	235,000,000	2,548,421	93,389,811					
	2020	1,469,000,000	1,468,995	79, 876,995					

Source: Published yearly financial reports of various banks

Table 4.2 Descriptive results of the variables



Sample: 2016 2022

	BL	ICS	GE
Mean	1.34E+10	5214711.	2.32E+08
Median	2.91E+09	2427040.	1.48E+08
Maximum	3.13E+11	33879000	1.13E+09
Minimum	1155800.	181.0000	2529399.
Std. Dev.	4.16E+10	6769830.	2.40E+08
Skewness	6.498036	2.235706	1.480069
Kurtosis	47.08930	8.600077	4.997521
Jarque-Bera	5193.878	124.1065	31.34992
Probability	0.000000	0.000000	0.000000
Sum	7.88E+11	3.02E+08	1.37E+10
Sum Sq. Dev.	1.01E+23	2.61E+15	3.34E+18
Observations	59	58	59

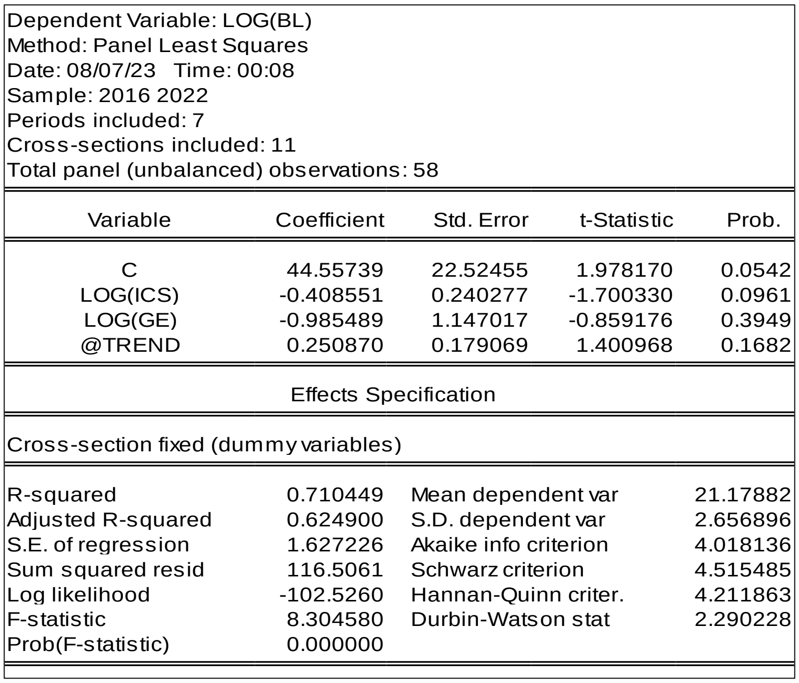
A descriptive analysis of our variables is shown above in Table 4.2. For the 11 sampled banks their average gross earnings for the entire period is N232 billion; the maximum gross earnings attributable to any bank for a particular period is N1.12 trillion (by Access bank in 2022) and a minimum of N2.5 billion (by FCMB in 2017). For the rest of our variables, banks investment in cybersecurity (ICS) for our 11 sampled banks had a mean of N5.2 billion while bank losses (BL) is N1.3 trillion. Access bank having had the highest gross earnings had the highest bank loss of N313 billion in 2022 just as our hypothesis had speculated. However, Jaiz bank in 2017 had the lowest bank loss to cyber theft for the entire review period. Again, Access bank had the highest amount invested in cybersecurity of all the banks N33 billion in 2022.

From Table 4.2 we can also observe the frequency distribution of the individual variables, we find that all our variables are rightward skewed which confirm why their mean is more than the median. Their kurtosis which should be 3 for a normal distribution all have values more than 3 which means our variables are not from a normal distribution. The standard deviation which indicates the degree of variability in our variables are in millions upwards which indicates the presence of outliers in their distribution. Finally, the Jarque-Bera statistic test whether our variables are normally distributed (or follow a normal distribution). Their probability levels are infinitesimally too small and are all less than 1% significant level which sums up the fact that none of our variables are normally distributed. However, this will not be a challenge to our analysis as we are undertaking a panel study and not a timeseries study.

4.3 Panel Data Estimation

The result of our estimation is shown below in Table 4.3. Note that the dependent variable BL and all our independent variables ICS, GE are all in log forms, this means their coefficients will be interpreted in precents. Consequently, the trend variable will be transformed to give the yearly average percent growth in bank losses.

Table 4.3 Panel Data Estimation (Fixed Effects) Result



```
Dependent Variable: LOG(BL)
Method: Panel Least Squares
Date: 08/07/23   Time: 00:08
Sample: 2016 2022
Periods included: 7
Cross-sections included: 11
Total panel (unbalanced) observations: 58

        Variable        Coefficient    Std. Error    t-Statistic    Prob.

           C              44.55739      22.52455      1.978170     0.0542
        LOG(ICS)         -0.408551      0.240277     -1.700330     0.0961
        LOG(GE)          -0.985489      1.147017     -0.859176     0.3949
        @TREND            0.250870      0.179069      1.400968     0.1682

                          Effects Specification

Cross-section fixed (dummy variables)

R-squared                 0.710449    Mean dependent var      21.17882
Adjusted R-squared        0.624900    S.D. dependent var      2.656896
S.E. of regression        1.627226    Akaike info criterion   4.018136
Sum squared resid         116.5061    Schwarz criterion       4.515485
Log likelihood           -102.5260    Hannan-Quinn criter.    4.211863
F-statistic               8.304580    Durbin-Watson stat      2.290228
Prob(F-statistic)         0.000000
```

The result above result show that a 1% increase in investment in cybersecurity expenditure holding all other variables constant leads to 0.41% decrease in bank losses due to cyber theft and it is statistically significant or different from zero at 10% levels. Conversely, the relationship between gross earnings holding all other variables constant leads to 0.99% decrease in bank losses but it is statistically insignificant or not different from zero even at 10% levels. For the result in senior management level, a 1% increase in females in that role leads to a 0.05% increase in profits though it is the only variable that is not statistically significant. Furthermore, the average growth rate of bank losses according to our trend variable is 25% per year. Although not statistically significant, but what this means is that for every year, bank loses increase by 25%.

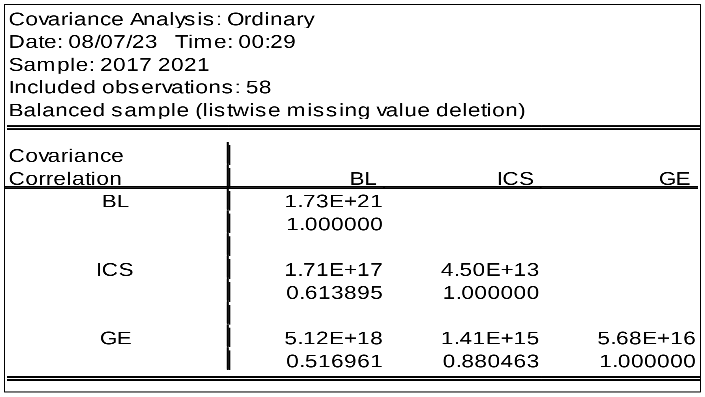
To this end, because our main coefficient of interest being bank investment in cybersecurity is statistically significant, we reject the null hypothesis in favour of the alternative hypothesis that indeed investments in bank cybersecurity systems have a significant relationship on bank losses holding the effect of bank gross earnings (our scale variable) constant.

The other results from our panel estimation shows that the R-square of 71% out of 100% implies that our model is very robust in explaining the variability in our dependent variable (bank losses). The F-statistics which shows the overall impact of all the independent variables in our model was also statistically significant at one percent level. The Durbin-Watson statistic is not far from the optimal point of 2 implying that there is no problem of spatial autocorrelation in our model. So far, the result from our model looks good but we need to perform some further diagnosis to be sure it fulfils relevant regression assumptions.

4.4 Diagnostics

In order to be sure our estimation analysis is without problems, we need to perform a diagnostic to be sure that our independent variables do not correlate with one another, because if they do it means the signs of our coefficients may be misleading.

Table 4.4.1 Covariance Analysis Result



```
Covariance Analysis: Ordinary
Date: 08/07/23   Time: 00:29
Sample: 2017 2021
Included observations: 58
Balanced sample (listwise missing value deletion)

Covariance
Correlation            BL             ICS             GE
        BL          1.73E+21
                    1.000000

        ICS         1.71E+17       4.50E+13
                    0.613895       1.000000

        GE          5.12E+18       1.41E+15       5.68E+16
                    0.516961       0.880463       1.000000
```

The result from Table 4.4.1 shows that the correlation matrix between ICS and GE is 0.88. From 0.95 upwards would have biased our results, therefore we can safely conclude that our result has no multicollinearity problem.

Table 4.4.2 Hausman Test Result

Correlated Random Effects - Hausman Test
Equation: Untitled
Test cross-section random effects

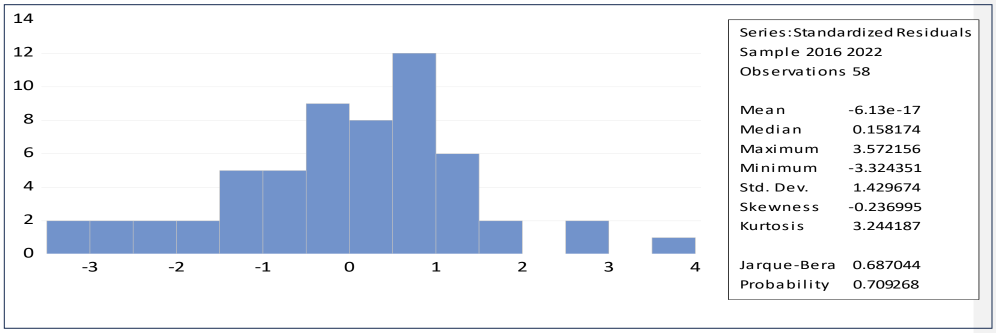
Test Summary	Chi-Sq. Statistic	Chi-Sq. d.f.	Prob.
Cross-section random	6.993774	3	0.0721

Cross-section random effects test comparisons:

Variable	Fixed	Random	Var(Diff.)	Prob.
LOG(ICS)	-0.408551	-0.078953	0.022814	0.0291
LOG(GE)	-0.985489	0.620725	1.132114	0.1311
@TREND	0.250870	0.095474	0.012018	0.1563

The above test was undertaken to choose which is the most robust model between fixed effect and random effects as prescribed by the literature. Indeed, the result show that there is a difference between the two models as it is statistically significant at 10% level. It is interesting to note that even in the random effects model our key variable posted similar negative sign although all the coefficients in the fixed effect model are larger. Furthermore, to avoid omitted variable bias, we were right to have used the fixed effect model over the random effect model as our method of data analysis in section 4.3.

Table 4.4.3 Residual Diagnostic Test Result



Series: Standardized Residuals
Sample 2016 2022
Observations 58

Mean	-6.13e-17
Median	0.158174
Maximum	3.572156
Minimum	-3.324351
Std. Dev.	1.429674
Skewness	-0.236995
Kurtosis	3.244187
Jarque-Bera	0.687044
Probability	0.709268

We move on to perform the last diagnostics being the residual diagnostic to ascertain if indeed the statistical significance in our estimation results are valid. The result from Table 4.4.3 above shows the Jarque-Bera statistic is insignificant which means we cannot reject the null hypothesis that our error term from the estimation is normally distributed. This corroborates the result from Table 4.3.

4.5 Summary of Findings

Based on the results of the analysis from the tables, the researcher found out that;

1. A 1% increase in investments in cybersecurity leads to 0.41% decrease in bank losses due to cyber theft. Therefore, we reject the null hypothesis. Though this impact is very small, but what this means is that the more investments in cybersecurity the more bank losses reduce.

2. A 1% increase in banks gross earnings reduces bank losses due to cyber theft by 0.99% though insignificant. Again, this impact is very minimal, but what this means is that the more bank's gross earnings, the more bank losses will reduce.

3. The average yearly increase in bank losses due to cyber theft is 25%. this value is quite big given that average bank losses per year is N1.3 trillion. Therefore, 25% growth per year will amount to N325 billion yearly growth in bank losses due to cyber theft, this is a huge amount.

Chapter Five

Summary, Conclusions and Recommendations

5.1. Introduction

This chapter deals categorically with the summary of the results of the study, contribution to knowledge and recommendations based on the results of the study conducted. Suggestions for further study and conclusions are also presented.

5.2. Summary of the Study

The research investigated the effectiveness of investment in cybersecurity on bank losses using a sample of 11 Nigerian deposit money banks from the period 2016 to 2022. Bank losses was proxied by resolved claims from customers and bank gross earnings was included as a scale variable. Three research objectives and questions guided the study while one research hypothesis was tested. Relevant theories on technology adoption and motive for theft in the workplace was cited and past research works on effectiveness of cybersecurity in banks were highlighted. The research used secondary data from banks annual financial reports in the form of panel data. A total of 11 banks were sampled and the panel data estimation technique of fixed effect estimation technique was employed for the regression instead of the random effects model as it was found to be more robust. After estimation, diagnostic test was performed to ascertain if the results were found to fulfil all the necessary conditions for unbiased results.

5.3. Conclusions of the Study

From the findings of the study, the major conclusions arrived at are;

1. When banks increase their cybersecurity investments, bank losses due to cyber theft reduces, though the reduction is very minimal.

2. The average yearly investments on cybersecurity by Nigerian banks amount to N5.2 billion.

3. The average yearly growth rate of losses due to cyber fraud in banks is around N325 billion yearly which amount to 0.25% growth per annum.

5.4. Contribution to Knowledge

This study has shown the effectiveness of Nigerian banks investment in cybersecurity and its impact on reducing bank losses. Given that bank transaction channels have increasingly gone electronic in Nigeria due to increasing competition by fintechs on legacy brick and mortar banks forcing this change. Legacy banks have had to adapt quickly and continue to update their technologies. Using a sophisticated technique of panel data estimation, this study has brought to the fore a way to measure the effectiveness of banks investment in cybersecurity systems with the techniques and variables it has used. From the banks sampled, it showed that current investments in cybersecurity indeed reduces bank losses but its impact is paltry and the yearly growth rate in bank losses due to cyber theft is 25%.

5.5 Limitations of the Study

Data on cybersecurity from Nigerian banks are not clearly itemised in their yearly financial reports which is not in line with global practices given the very importance of cyber-attacks in the financial sector and the need for disclosure for stakeholders. The limitations are listed as follows;

1. This study used a composite figure as presented by banks called expenditure on computer software (with slight differences with the way some banks itemise it) under operating expenses of banks. Of course, this line item is bogus (or over stated) as it includes several other software expenditures by banks like desktop and mobile application development and accounting software.

2. Also the data for bank losses is overstated because it is a composite figure involving losses beyond electronic channels. Only very few banks categorise their losses for better understanding which if used do not provide enough sample size for investigation.

3. The study did not take cognisant of the fact that cybersecurity investments by banks also include training their staff on ICT. This was not as a result of oversight; it was just that the data was not available.

5.6 Areas for Further Research

In future, if data reporting standards for Nigerian banks improve, future studies can expand this investigation by disaggregating bank losses according to channels to include mobile, web, ATM and POS. This will enrich the result.

5.7 Recommendations of the Study

The study recommends the following:

1. Banks should massively increase their investments in cybersecurity to have a significant effect in reducing bank losses.

2. The CBN and Nigeria Financial Reporting Council should urgently draw up new financial reporting codes and standards to mandate banks to include their expenditures on cybersecurity as a line item and disaggregate their reporting on losses due to claims from customers so that stakeholders can tell from what channels the losses are from.

3. Some bank customers do not come forward to report cyber breaches on their account because the law puts the burden of proof on them which can be very expensive for some customers to embark on. In some cases, the banks stand ready to appeal the cases up to the supreme court which most customers cannot withstand given the expensive and laborious judicial process in Nigeria. The government can create a special ombudsman that uses state of the art technology to assist customers for a reasonable cost in investigating or building evidence for these cases.

References

Adetiloye, K. A., Olokoyo, F. O. & Taiwo, J. N., 2016. Fraud Prevention and Internal Control in the Nigerian Banking System. *International Journal of Economics and Financial Issues,* 6(3), pp. 1172-1179.

Adeyemo, K. A., 2012. Mediterranean Journal of Social Sciences. May.3(2).

Akintoye, R., Ogunode, O., Ajayi, M. & Abosede, A., 2022. Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria. *Universal Journal of Accounting and Finance,* Volume 10, pp. 643-652.

Aladenusi, T. & Odumuboni, F., 2022. *Nigeria Cybersecurity Outlook,* s.l.: Deloitte.

Baur-Yazbeck, S., Frickenstein, J. & Medine, D., 2019. *CYBER SECURITY IN FINANCIAL SECTOR DEVELOPMENT,* s.l.: CGAP.

Bouveret, A., 2018. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *IMF Working Paper,* June.

Bryman, A. & Bell, E., 2015. *Business Research Methods.* 4th ed. s.l.:s.n.

D'Arcy, J. & Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. EJIS. .. *European Journal of Information Systems,* June, 20(6), pp. 643-658.

Deloitte, 2022. *Nigeria Cybersecurity Outlook 2022,* s.l.: s.n.

Ekran, 2022. *5 Industries Most at Risk of Data Breaches.* [Online]
Available at: https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches
[Accessed 26 December 2022].

Garba, A. & Musa Bade, A., 2021. The Current State of Cybersecurity Readiness in Nigeria Organizations. Volume 3, pp. 154-162.

Ghandi, V. K., 2012. An overview study on cybercrimes in Internet. *Journal of Information Engineering and Applications,* 2(10), pp. 1-5.

Gujarati, D. & Porter, D., 2009. *Basic Econometrics.* s.l.:McGraw Hill.

Guth, K., 2016. Institutional theory of organizations. In: C. E. Carroll, ed. *Encyclopedia of corporate reputation.* s.l.:Sage, pp. 359-361.

Howe, E. & Pelser, A.-M., 2020. Cybercrime in Eswatini: The deterrence theory approach. *Journal for cultural studies.*

Jaiyeola, T., 2023. Nigeria records second highest cyberattacks in Africa, says Kaspersky. *Punch*, 7 June.

Kang, J. & Westskytte, S., 2018. *Diffusion of Cybersecurity Technology,* Sweden: s.n.

Kawugana, A. & Faruna, F. S., 2018. Fraud Prevention in the Nigerian Banking Industry. *IIARD International Journal of Banking and Finance Research,* 4(1).

Khalil, K. et al., 2021. IMPACT OF CYBER SECURITY COST ON THE FINANCIAL PERFORMANCE OF E-BANKING: MEDIATING INFLUENCE OF PRODUCT INNOVATION PERFORMANCE. *Humanities & Social Sciences Reviews,* pp. 691-703.

Kola-Oyeneyin, T., Kuyoro, M. & Olanrewaju, T., 2020. *Harnessing Nigeria's Fintech Potential,* s.l.: s.n.

Makeri Ajiji, Y., 2017. Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 7, pp. 315-321.

Ojeka, S. A., Ben-Caleb, E. & Ekpe, E.-O. I., 2017. Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing,* 7(2), pp. 340-346.

Olowole, V., 2022. 59% of Nigerians have fallen victim to E-Banking fraud, according to a report. *Business Insider*, 5 December.

Orji, U. J., 2019. Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. *Tilburg Law Review,* 24(1), p. 105–124.

Partida, D., 2022. *6 Cybersecurity challenges facing digital banking.* [Online]
Available at: https://cybersecurity.att.com/blogs/security-essentials/6-cybersecurity-challenges-facing-digital-banking
[Accessed 26 December 2022].

Robert J. David, P. T. & Boghossian, J., 2019. *Institutional Theory in Organization Studies.* [Online].

Rogers, E., 1995. *Diffusion of Innovations.* 4th ed. New York: Free Press.

Rufus Akintoye, ,. O. O. & Joshua, A. A., 2022. Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria. *Universal Journal of Accounting and Finance,* 10(3), pp. 643-652.

Saracino, J., 2022. *Banks need best practices to fight rising cyberattacks.* [Online]
Available at: https://fintechmagazine.com/banking/banks-need-best-practices-to-fight-rising-cyberattacks

Saunders, M., Lewis, P. & Thornhill, A., 2016. *Research methods for business students.* 7th ed. s.l.:Pearson.

Scofield, D., 2022. *Cybersecurity trends and best practices for community banks.* [Online]
Available at: https://www.minneapolisfed.org/article/2022/cybersecurity-trends-and-best-practices-for-community-banks

Surry, D. & Farquhar, J., 1997. Diffusion theory and instructional technology. *Journal of Instructional Science and Technology,* 2(1), pp. 24-36.

Uniamikogbo, E., 2019. Forensic audit and fraud detection and prevention in the Nigerian banking sector. *Accounting and Taxation Review,* 3(3), pp. 121-139.

Wang, V., Nnaji, H. & Jung, J., n.d. *Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability,* s.l.: University of Portsmouth.