IMPACT OF CYBER -SECURITY ON FINANCIAL FRAUD IN COMMERCIAL BANKS IN NIGERIA: A CASE STUDY OF ZENITH BANKS IN ABUJA.

A dissertation presented to the department of Computer Science,
African University of Science and Technology, Abuja-Nigeria
In partial fulfilment of the requirements for a Masters degree in Management of Information Technology

By

Ekong Eyo, Unwana (41028)

Abuja, Nigeria

MAY, 2023

CERTIFICATION

This is to certify that the thesis titled IMPACT OF CYBER -SECURITY ON FINANCIAL FRAUD IN COMMERCIAL BANKS IN NIGERIA: A CASE STUDY OF ZENITH BANKS IN ABUJA submitted to the school of postgraduate studies, African University of Science and Technology (AUST), Abuja, Nigeria for the award of the Master's degree is a record of original research carried out by Ekong Eyo, Unwana in the Department of Computer Science.

07.05.2023

SIGNATURE PAGE

IMPACT OF CYBER -SECURITY ON FINANCIAL FRAUD IN COMMERCIAL BANKS IN NIGERIA: A CASE STUDY OF ZENITH BANKS IN ABUJA

By

Ekong Eyo, Unwana

A THESIS APPROVED BY THE COMPUTER SCIENCE DEPARTMENT

RECOMMENDED:

Supervisor: Dr. Rajesh Prasad

Head of Department: Dr. Rajesh Prasad

APPROVED: _____

Chief Academic Officer

_____

Date

ABSTRACT

The study examined the impact of cyber-security of financial fraud in commercial banks in Nigeria: a case study of Zenith banks in Abuja. The study on the following objectives; the type of electronic frauds perpetrated in the banking sector, causes of cyber fraud in banks, challenges of curbing cyber fraud in the bank, effect of cyber fraud on Nigeria banks, and possible solutions for curbing cyber fraud in banks. The study is hitched on two hypotheses. The study adopted survey research design, and the population of the study consisted of 49 Zenith banks branches in Abuja. Multi-stage sampling techniques was used and 557 bank staff were sampled. Structured questionnaire was used to capture the response of the bank staff and it was analyzed statistical package for social science version 27 (SPSS). The objectives were analyzed using descriptive analysis while the hypotheses were tested using multiple regression and Kendal Tau B. the result of the study showed that major type of cyber fraud in banking system were accounting fraud by bank staff, identity theft, money laundering, hacking/cracking, phishing, pharming, and computer virus. Also, lack of oversight by line managers or senior managers on deviations from existing electronic process/controls, current business pressure to meet set targets, current business pressure to meet set targets, collusion between employees and external parties, insufficient data encryption, the use of services provided by third parties, parodying were the causes of cybercrime in banks. Similarly, findings of the study revealed that lack of standards and national central control, lack of infrastructure, porous nature of the internet, lack of national functional databases, and inadequate awareness by bank customers were the challenges militating the effort towards curbing the cyber fraud in banking system in Nigeria. The findings also revealed that financial loss, reduced productivity, vulnerability of banks Information and Communication Technology (ICT) systems and networks were the effect of cybercrime on banks in Nigeria, and security audit, antivirus and antimalware software, use of multi-factor authentication, use of biometrics, automatic logout were the solutions identified to cybercrime in banks. The study concluded that the place of security in the cyber space of banks in Nigeria cannot be overstretched therefore necessary measures should be put in place towards mitigating cybercrime in Zenith. The study recommended that Zenith bank should employ stringent measure to monitor staff activities especially in the confidentiality of customer information, cyber security audit should be done by Zenith regularly, sensitization of bank customers, and Multi-factor authentication, biometrics and automatic log out, and strong firewall should be adopted by Zenith bank.

ACKNOWLEDGMENTS

I express my deepest sense of gratitude to God for life, good health, finances and strength for seeing me through my MSc. Program.

To my very admirable and distinguished Head of Department Prof. Rajesh Prasad for always going the extra length to ensure all his students are properly carried along during his lectures and ensuring we are never bullied when it comes to academics by any member of the faculty. You sir made the journey a little easier.

Special Thanks to the Acting President of AUST Prof Azikwe Peter Onwalu and the academic Registrar for always ensuring that the quality of education we receive remains Uncompromised.

To my course mates Ayotola Ajosola, Fatima Bala Kawu, and Tamuno Opubo thank you for being my study partners/support systems and to all my lovely lecturers for impacting knowledge without reserve I say a very BIG THANK YOU.

I am also thankful to departments of Cyber security and Science Education of my alma mater, Federal University of Technology Minna Niger state for lending their expertise to this research and zenith bank staff in all the branches in Abuja for their assistance.

DEDICATION

I dedicate this project to My late Mother, Pastor Mrs. Theresa Ekong for even in death, she still remains a guiding light.

LIST OF ABBREVIATIONS AND TERMS

BDC	Bureaux-de-Change
PSB	Payment Service Banks

DEFINITION OF TERMS

Bank customers: any individual who has or had a banking relationship with Bank that was not originated through the Program or acquired under the Purchase Agreement.

Commercial banks: a type of financial institution that accepts deposits, offers checking and savings account services and makes loans.

Cyber security: is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

Financial fraud is defined as a conscious act of deception involving financial transactions with the intent of deceiving others into making financial transactions to gain unauthorized access to their accounts.

Financial institutions are businesses that provide services as intermediaries for different types of financial and monetary transactions.

Impact: a marked effect or influence.

Table of Contents

LIST OF TABLES

CHAPTER ONE
1.0 INTRODUCTION

1.1 Background of the Study

In modern times robbery of banks are beyond physical attack as money is not only kept in bank vaults. In modern computer technologies and data networks a lot of money exists in cyber space. Banks have to adapt to modern trends of doing business electronically and at the same time protect themselves against cyber-crimes due to the increasing number of bank frauds. Authorities must take immediate action to prevent these types of incidents from happening. A report was carried out by the American Customer Satisfaction Index which revealed that it was difficult for bank customers to get adequate compensation after they had experienced various issues related to the misstatements and mistakes made by the Bank's staff.

Cyber security is the protection of digital information and the infrastructure on which it resides. Recently a lot of research has been conducted on cyber security related to banking system as in (Olubisi, 2015). In (Fadare, 2015) believed that cyber technology has bring about a lot of profit to specifically financial institutions and cyber-attack also poses intensive threat to the same institutions the study recommend that there is need for cyber security audit, cyber security training, cyber security assessment and tightening security. In Nigeria (Imran & Sana, 2013) released a risk based cyber security frame work and guidelines for commercial banks in managing cyber security risk. The document comprises six parts: Cyber security Governance and Oversight, Cyber security Risk Management System, Cyber Resilience Assessment, Cyber security Operational Resilience, Cyber-Threat Intelligence and Metrics, Monitoring and Reporting.

Also most banks do not reveal the identities of their employees involved in fraudulent activities. They also do not acknowledge that they were complicit in the actions. Instead, they quietly discipline the employees and absolve themselves of any blame. This is why they often refund the customers who complained about the issue. One of the reasons why banks do not reveal the identities of their employees involved in fraudulent activities is due to the competitive nature of their business. They also do not want to be seen as having bad employees. According to a central bank management staff member, the increasing number of reports about fraudsters in their organization harms their customers. Another issue that banks face when dealing with staff-assisted fraud is the unwillingness of their customers to pursue their complaints even though there are traces of the money being transferred to other banks.

Therefore, it is difficult for bank customers to blame the banks due to the failure of the authorities to monitor and sanction the activities of the company's employees. The Consumer Protection Department of the Central Bank of Nigeria was not able to react to the various issues faced by the Bank's customers. In 2021, the Central Bank revealed that four banks in the country had recorded over 400,000 unresolved complaints. These include Access Bank, United Bank for Africa, and Guaranty Trust Bank. According to the central Bank's data, the country's biggest Bank by customer complaints, which is known as Zenith Bank, had over 167,000 unresolved issues as of December 2021. On the other hand, the country's second-largest Bank, GTB, had recorded over 600,000 complaints.

The number of unresolved consumer complaints has not reached a level expected to be resolved soon. This is due to the endless investigations that have been carried out regarding the activities of the Bank's staff. Reports have shown that some bank employers use kid gloves to avoid creating a negative image for the company. Therefore, Nugraha and Bayunitri (2020), concluded

that fraud is intentional activity by one or more individuals among management, staff, or third parties that might result in a financial statement deceit. Manipulation, fabrication, or alteration of supporting documentation; asset misappropriation; fraudulent practices including the concealment or the absence of transaction consequences from records or documents; transaction documentation that is devoid of substance; and accounting standards that are distorted (Badejo et al., 2018). It is based on the aforementioned background that the study is geared towards to assessing the cyber-security policies and techniques used by Zenith Bank in combating financial fraud in Abuja Municipal Area Council of FCT, Nigeria.

1.1.1 Origin of Modern Bank

The origins of modern banking in Nigeria date back to 1883 when the African Banking Corporation, followed by the British Bank of west Africa in 1884; although the former collapsed after its establishment, it has survived and is still around today as the First Bank of Nigeria. Over the years, more financial institutions such as Bureaux-de-Change (BDCs), Banks, Development, Houses, Finance, Holding, Banks, Micro, Banks, Primary and Payment Service Banks (PSBs) sprung up.

Nigeria has over 24 commercial banks and over 500 micro-financial institutions. These are regulated by different agencies such as the Central Bank of Nigeria and the Federal Ministry of Finance (FMF.) The country's securities and exchange commission are also responsible for overseeing the activities of the banking industry. However, the advent of ICT influenced the banking system towards the use of electronic banking system in the early 2000s. This was supposed to help prevent the use of illicit money. However, it has been reported that the system led to widespread corruption.

1.1.2 Evolution of internet banking

The ability of Nigerian banks to retain and satisfy their customers in the post-consolidation era led to investing in information technology infrastructure adoption of telecommunication and electronic networks, which has led to improved service delivery. The electronic banking system has become widely accepted and adopted by commercial banks in Nigeria. Introducing this electronic banking has improved banking efficiency in rendering services to a customer.

One of the main factors that have contributed to the growth of internet banking is the availability of better flexibility of banking services. Customers can conduct their various banking transactions regardless of their geographical locations with internet banks, mobile banking and automated teller machines. In 2003, Ovia noted that the increasing number of e-commerce, e-banking, and e-everything initiatives launched by financial institutions in the country are expected to help narrow the digital divide.

Despite the various advantages of internet banking, just like everything else, it has its pros and cons**.** Customers' inherent fear about using internet banking in Nigeria is also reinforced by the increasing number of reports about the scamming activities of dubious individuals. These include using fake bank websites to carry out fraudulent transactions.

1.1.3 Evolution Of Cybercrime

The rapid growth of the ICT environment has led to an increase in severe threats and new ways to harm society. Cyber-attacks are now capable of causing immense damage to society in various ways. Some examples of these include online fraud and cyber-attacks. In 2018, the country's commercial banks lost about 15 billion naira to cybercrime and electronic fraud. This is a 537

per cent increase from the previous year's loss of 2.37 billion naira. According to an official report released by the Economic Fraud Forum of Nigeria, the country was ranked 16th globally in cybercrimes.

Cybercrime can be defined as a type of criminal activity that involves the unauthorized access and use of people's personal information. It can be carried out through various (Buchanan, 2016) states that according to a Nigerian bank settlement system report, the country's financial institutions lost over NGN 159 billion to cybercrime from 2000 to 2013. New Horizons Limited, a communications technology company based in Nigeria, stated that the country's financial institutions are losing billions in revenue annually to cybercrime. Despite the cost of cybercrime, it is still costing more than physical crime.

Protecting sensitive and critical information is extremely important for every country. Due to the increasing number of cyber-attacks, the need to improve information security has become more prevalent. Badejo, Okuneye, and Taiwo, (2018) identified various factors that contributed to the rise of cybercrimes in Nigeria. These included the country's high unemployment rate, inadequate law enforcement agencies, porous cyber security measures and the lack of positive role models for the youth. One of the most important factors that people can consider when it comes to tackling issues related to cybercrimes is to increase the number of forensic experts that are being brought in to investigate these types of crimes and thus prevent them from happening in the first place.

1.1.4 OVERVIEW OF ZENITH BANK

In May 1990, Jim Ovia, a CON, founded and incorporated the Bank known as Zenith Bank. Initially, it was a private limited company. In July of that year, operations as a full-service bank.

Company. It started its operations in July of that year as a full-service commercial bank. Since its beginning, the Bank has become one of the country's largest financial institutions. Its total assets are valued at over NGN9.6 trillion. Its shareholders' fund is also over NGN1.28 trillion and has over 10,000 employees globally. The Bank has multiple branches and offices in different parts of the country. It has also subsidiaries in other countries, such as Sierra Leone and the UK.

1.2 Problem Statement

Due to the various financial crises that occurred in the country in the past few years, the regulators and owners of financial institutions have become more concerned about the country's cyber security. One of the main reasons why the country's banks have become more vulnerable to cybercrimes is as a result poor training on how to mitigate risk and lack of insufficient resources (Onodi, Okafor, & Onyali, 2015). Various potential threats can affect the operations of financial institutions in the country as potential threats to the country's financial institutions include:

1. unsolicited /unauthorized cash or debit alerts from various account holders,
2. cases of ATM card cloning,
3. withdrawals under Duress by both armed and unarmed persons,
4. transactions are done with unknown persons (identity theft) dollar inflations, to mention a few.

This research will give more insight into various threats that have been identified with the hope that it brings to light the negative impact of financial crimes, which will assist commercial banks in developing effective cyber security strategies to minimize the loss of funds due to these crimes.

1.3 Research Objective

The aim of the study is to examine the impact of cyber security on financial fraud in commercial banks in Nigeria: a case study of Zenith Bank Abuja.

The specific objectives are to;

1. examine the type of electronic frauds perpetrated in the banking sector
2. Determine the causes of cyber fraud in banks
3. Determine the challenges of curbing cyber fraud in the bank
4. Evaluate the effect of cyber fraud on Nigeria banks
5. Identify possible solutions for curbing cyber fraud in banks

1.4 Research Questions

- What are the type of electronic frauds perpetrated in the banking sector?
- What are the causes of cyber fraud in banks?
- What are the challenges of curbing cyber fraud in the bank?
- What is the effect of cyber fraud on Nigeria banks?
- What are the possible solutions for curbing cyber fraud in banks?

1.5 Hypothesis

The following hypothesis will be tested;

- Ho1: there is no composite impact of the types of electronic frauds and the causes of cyber fraud on the effect of cyber fraud on banks
- Ho2: There is no relationship between the challenges of curbing cyber fraud and the possible solutions of curbing cyber fraud in banks.

1.6 Scope and Limitation of Study

This study aims to find out how prevalent cyber fraud is in Nigerian financial institutions. It also aims to identify ways to minimize this risk.

1.7 Significance of the Study

This research will be of tremendous benefit to the followings:

- **Financial institutions**: this study will clearly show how financial institutions are prone to cyber-attacks and hopefully enable them to adopt appropriate cyber security measures to ensure a safe banking space for their customers.
- **Zenith Bank:** the research will enable them to see the financial issues faced by its customers and help them develop appropriate security measures to combat same.
- **Bank Customers**: to know the appropriate security measures that can be adopted to ensure unauthorized persons do not access their financial information.
- **Nigerian Government:** to see to what extent cyber fraud/threat has affected our economy in the long run
- **Central Bank of Nigeria**: to give an insight into the extent of cyber threats the standard Nigerian faces daily. Hopefully, this research will enable the Central Bank of Nigeria to develop very tight notch and appropriate measures to combat cyber-attacks on our financial institutions.

1.8 Research Outline

The research outline is as follows:

1. **Chapter one** contains an introduction to Nigeria's agricultural sector and weighs in on the factors such as climatic and socioeconomic affecting crop yield. It highlights a problem statement, aims & objectives, the scope of the research, the significance of the research, expected results and deliverables, and then the thesis outline.

2. **Chapter two** contains the related work of research on socioeconomic factors affecting crop yield and machine learning models in evaluation crop yield based on climatic data.
3. **Chapter three** contains a discussion of our proposed model and the method we used to meet the research objectives.
4. **Chapter four** contains the performance evaluation of the models. First, we will compare the three models combining socioeconomic and climatic data and then compare them with results using climatic data only.
5. **Chapter five** contains the summary, conclusion of our research and possible open research directions.

CHAPTER TWO

2. LITERATURE REVIEW

2.1 Introduction

The rapid infrastructural development in Information and communications technologies (ICTs) has dramatically changed how people communicate and execute business transactions across the globe. Today's world has become a global village as geographical barriers rarely impede or obstruct communication. Information and Communication technology offers very effective communication via the World Wide Web.

In a bid to remain relevant with the evolving best global practice, the Nigerian banks invested in using ICT to carry out banking activities. Hanafizadeh, Behboudi, Koshksaray, and Tabar (2014) explained the various factors influencing banks' decision to adopt Internet banking. It also explores the security concerns related to such services. Despite the technological advancements in the banking industry, the security of transactions conducted through the Internet remains a significant concern for users.

2.2 Key Concept of Cyber Security

The International Telecommunication Union (ITU) defines cyber security as a set of tools, policies, procedures, and techniques that help organizations and individuals protect themselves from unauthorized access and use of their computer systems. These unique tools and techniques are used to manage the various risks associated with the cyber environment. Some critical components of a cyber security strategy include the development of policies and procedures, training, and awareness.

Cyber Security is a set of practices and technologies designed to protect computers, programs, and data from unauthorized access and attack. The ITU's main objective is to ensure that network is readily available, data integrity is preserved at all costs, and information remains confidential. To fully understand the concept behind the term cyber security, it is essential to understand the different components of cyber security. And the policies/measures that ensure cyberspace remains confidential.

2.2.1 The Concept of Cyber Crimes

A cyber-attack occurs when a person or group gains illegal access to data stored electronically on a computer network with the intent to inflict malicious or reputational damage to an individual, business, Government or organization. Seissa, Ibrahim, and Yahaya (2017) define a cyber-attack as an attack initiated from any digital device against a network, storage or computer to compromise the integrity, confidentiality, and authenticity of the information stored in the device or network.

Examples of cyber attack:

- Attempting to access confidential information stored on a device or network by unauthorized personnel,
- Disruption of service, which could be causing a network downtime while on a website or service provider, sending or installing a virus, malware or spyware on a system with the intent of disrupting, theft/ monitoring data
- Making unauthorized changes to the characteristics of a computer system's hardware, firmware or software without the owner's knowledge,

2.2.2 Cyber Threats

The term refers to unauthorized persons who attempt to control a system, device or network using a data communications pathway. Most cybercriminals can often access the system network through a trusted or authorized user from within the organization with the aid of the Internet. These threats to a computer network can be caused by various reasons, ranging from disgruntled employees, terrorist groups, and power tussles with hostile Governments, to mention a few. However, cyber threats could be further differentiated by character, impact, origin and actor.

2.2.2.1 Types of Cyber Threats

- Accidental or Intentional Threats can occur without prior intent. For instance, physical failures or malfunctions of a computer system can lead to an unexpected attack. However, intentional threats are those that are carried out through deliberate acts. These include performing a casual network examination, launching sophisticated attacks, and taking advantage of a system's knowledge.
- Active or Passive Threats occur without premeditated, intentional threats are carried out through deliberate actions. These include attacks that are designed to affect an asset's security. Examples of intentional threats include performing routine checks on a computer network or carrying out sophisticated attacks using a system's knowledge.
- Active threats are intentional threats that can cause a change in the state of a system, such as the destruction of equipment or the modification of data. On the other hand, a passive threat is not designed to affect a system's operations or resources. Instead, it aims to collect information from a plan to improve its efficiency. Some techniques that can be used to perform passive threats include monitoring and eavesdropping.
- Threat Source: A threat source is an entity that seeks to gain unauthorized access to a person's or company's security controls. It can also benefit from the breach by making money from the sale of stolen goods.

- A cyber threat actor is a person or group that can perform an attack or take advantage of an accident. For instance, the group is considered the Threat Source if an organization takes advantage of an employee's corruption.
- Vulnerability: The intentions of threat actors and sources are often realized through exploiting weaknesses in security controls. For instance, a vulnerable person could easily access the system if a software patch is unavailable. Even good technical controls can be susceptible to exploitation by social engineering attacks.
- Security Risk: This refers to the possibility that a threat will likely occur if the vulnerabilities in a network system are not fixed. Most network devices operate with some degree of exposure to threats as the complete elimination of risk avenues is too expensive to fix. As such, it is a national cyber security policy strategy to ensure the first approach is that all stakeholders assume responsibility for risk and take necessary steps to mitigate such risk by ensuring government bodies provide reliable services to the public, maintain citizen-to-government communications, protect sensitive information as well as safeguard national security.

2.2.3 Cyber Fraud

Cyber fraud is criminal activity when someone uses a computer to steal another person's financial or personal information. Over the years, this has become a recurring concern to the Government and its citizens, despite various government entities established to address the issue. This may be due to the lack of proper infrastructure and resources to carry out their functions effectively. The immense amount of big data that governments have on their citizens is always a frequent target by hackers as they use very sophisticated techniques to carry out these attacks; they have become more demanding and need more sanctions to protect their businesses and personal information.

2.2.3.1 Types of e-frauds

Electronic fraud could be classified into two categories namely, direct and indirect frauds. Direct fraud would include credit/debit card fraud, employee embezzlement, and money laundering and salami attack. Indirect fraud would include phishing, pharming, hacking, virus, spam, advance fee and malware. Credit card/debit card fraud and identity theft are two forms of e-fraud which are normally used interchangeably. It involves impersonation and theft of identity (name, social insurance number (SIN), credit card number or other identifying information) to carry out fraudulent activities.

It is the unlawful use of a credit/debit card to falsely obtain money or belongings without the awareness of the credit/debit card owner (Dzomira, 2014). Theft of someone's identity can be done through different ways. According to Pal, Herath, and Rao (2019) skimming involves stealing information off a credit card during a legitimate transaction. This type of scheme usually occurs in a business where the patron's credit card is taken out of sight while the transaction is being processed. The fraudster will swipe the card through an electronic device known as a "wedge" or skimming device, which records all information contained on the magnetic strip. To obtain credit card details, offenders may employ sophisticated method such as hacking into merchants' databases or simply engineering the victims into giving their credit card details. However, Dzomira (2014) argued that whilst businesses and banks suffer losses from credit card fraud which continue to increase exponentially, there is not sufficient legislation to enable the eradication of this crime entirely.

In an attempt to maximize the benefits from technology utilization most people end up being victims of technology. Cyber fraudsters design web pages to look like legitimate sites where

victims enter personal information such as usernames, passwords and credit card details. Often emails are sent to recipients asking disclosure and/or verification of sensitive information, and upon disclosure of such information the offenders make online transfers. Smishing and vishing are forms of phishing which are more sophisticated and uses phone text messages and phone calls to bait victims (Dzomira, 2014). This kind of fraud can also be used to target corporates and other merchants. E-commerce merchant sites have been a target as they normally contain valuable loyalty points or stored payment card information that can be used for fraudulent purchases and also a kind of mass-marketing fraud (Tendulkar, 2013). Traditionally, fraud perpetrators targeting bank institutions used "pen and paper" to commit internal fraud. However, upon computerization of the transactions the same perpetrators shifted to computer fraud committing the same type of fraud.

According to Onodi, Okafor, and Onyali (2015), embezzlement, which involves misappropriating money or property for own use that has been entrusted to an employee (for example, an employee uses legitimate access to the company's computerized payroll system to change the data, or moves funds out of the company's bank accounts into a personal account). Moreover, a financial institution may allow trusted employees to access personal customer data that can be used to gain online access to customer accounts. In this way an employee can easily commit fraud.

In some cases fraudsters run a program known as the salami technique as an approach to steal money in small increments. The program makes micro-changes over an extended period, so that the changes are not easily noticeable. An example of this type of fraud is a program that deducts a few dollars per month from the accounts of many clients (Tendelkur, 2013). Fraudsters also run malicious codes and malware programs which take control of individual's computer to spread a

bug. A computer virus is a program that causes an unwanted and often destructive result when it is run. A worm is a virus that replicates itself. A Trojan (or Trojan horse) is an apparently harmless or legitimate program inside which malicious code is hidden; it is a way to get a virus or worm into the network or computer (Efiong, Inyang, & Joshua, 2016).

In the recent global recession period money laundering and/or cyber laundering has been a common unethical practice. It is a form of fraud that involves the electronic transfer of funds to launder illegally obtained money. The competence to transfer limitless amounts of money without having to go through strict checks may makes cyber money laundering an attractive proposition. New technologies and cyberspace offer money launderers new opportunities and present new challenges to law enforcement and difficulties in the investigations of internet-based-money laundering techniques (Okpa, Ajah & Igbe, 2020).

Another type of fraud involves spamming where unsolicited emails or junk newsgroup postings are sent without the consent of the receiver and frequently being malicious and sometimes offenders pretend to be financial institutions or companies (Seissa, Ibrahim & Yahaya, 2017). In light of that, Okpa, Ajah, and Igbe (2020) suggested that the only real solution in the fight against spam is to raise transmission costs for senders. In certain instances victims are redirected from legitimate websites to fraudulent or phony websites which look very identical to real ones; however any personal information entered into the forms (passwords and credit card number) would be sent to the cyber-criminal (Tendelkur, 2013).

More so, hacking/cracking is one of the oldest computer related crimes which refers to unlawful access to a computer system and include breaking the password of password-protected websites and circumventing password protection. These spy hackers are usually sophisticated and use trail

covering techniques like relay computers to make it seem like the attack originates locally and makes it harder to trace them. Hackers gain unauthorized access to large amounts of confidential data with the aim to cause monetary and reputational damages to the targeted entity (Akinbowale, Klingelhöfer & Zerihun, 2020).

In advance fee fraud, offenders send out scam emails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts. The dynamics of advance fee fraud is to trick prospective victims into parting with funds by persuading them that they will receive a substantial benefit, in return for providing some modest payment in advance (Bhasin, 2016). In essence, advance fee fraud encompasses mass marketing frauds and consumer scams, including advance fee scams such as 419 frauds, inheritance frauds, fake charity or disaster relief frauds, fake lotteries and pyramid schemes (Okpa, *et al.*, 2022).

2.2.4 Concept of Internet/Electronic Banking

The Internet is one of the fastest growing areas of technical infrastructure development. In today's business environment, applications such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online. Internet or electronic banking is a unique method of banking that allows bank customers to execute various financial transactions electronically via the Internet. Online banking offers customers almost every service traditionally available through a local branch, including deposits, transfers, and online bill payments, to mention but a few.

Nigeria has 21 Operational banks, namely: Access bank, Citibank Nig Limited, Ecobank, Fidelity Bank, First Bank, Globus Bank, Guaranty Trust Bank, Heritage Bank, keystone Bank, Polaris Bank, Providus, Stanbic ibtc, Standard Chartered, Sterling bank, Sun Trust, Titan Trust bank, Union Bank of Nig, Unity Bank, Wema Bank plc and Zenith Bank. Ebiasuode, Onuoha, and Nwede (2017) opined that the first bank of Nigeria was the first to adopt internet banking in the year 2000 and paved the way for commercial benefits by developing and fostering customers' trust that ensured future innovation success. Today, more than 80% of commercial transactions are done online, which requires a high level of security and confidentiality of personal information and transactions.

The broad scope of Cyber Security extends not only to the safety of Information systems within an organization but also covers cyberspace and critical infrastructures. Cyber security depends on people's care and the decisions they make when they set up, maintain, and use computers and the Internet. Cyber-security covers physical protection (hardware and software) of unauthorized personal information and technology resources. Wapmuk (2017) developed statistical models explaining why some banks adopted Internet banking, and others offered a more comprehensive array of Internet banking products and services.

The results revealed several significant differences between banks that offer Internet banking and those that do not. The covid pandemic experienced in 2020 further drove home the need for Society to fully integrate technology into different aspects of human activities such as commerce, finance, health care, energy, entertainment, communications, and national defense. Research findings also show that public concern for privacy and personal information has increased since 2006, and the investment in Cyber security infrastructure will have a dominant role in securing

and protecting critical information of the Nigerian citizens, businesses, government and economic well-being of the nation.

2.2.5 Overview of Zenith Bank

Jim Ovia founded Zenith Bank in May of 1990, and in June 2004, it was declared a public limited company following its successful Initial Public Offering. Subsequently, On October 21, 2004, its shares were listed on the Nigerian Stock Exchange. The bank's shares are currently listed on the London Stock Exchange. In 2013, the company was valued at $850 million following its listing on the London Stock Exchange. Zenith bank has since grown to become one of the largest commercial banks in Nigeria, with its headquarters in Lagos and over 500 branches nationwide. Besides Nigeria, the bank also has subsidiaries in other countries, such as the United Kingdom, UAE, Ghana, and Sierra Leone. It has offices in China and South Africa, thus employing over 10,000 persons globally. Furthermore, its debit cards provide 24-hour account access from **over 200** countries worldwide.

Some of the banking services offered by zenith include LLC Accounts, Enterprise accounts. NGOs. Embassies and High Commissions, Corporate Card Suite. Multipurpose Cards, Loans, Corporate Internet Banking. Zenith International Money Transfer. Due to the broad coverage of zenith bank globally, this has made the bank an easy target for cyber-attack crimes of recent, there has been a lot of negative media surrounding zenith bank such as poor payment network, fraudulent transactions etc.

2.3 General challenges in combating cyber fraud

The challenges faced by banks mainly include technical disadvantages, lack of knowledge and awareness, and lack of legislation. In emerging and developing economies the issue of fighting electronic fraud is a major problem owing to a number of reasons. Mostly, advances in technology are fast-paced, as are fraudsters, however organisations are often far behind and the easy availability of new technologies with high operational speeds, capacity and connectivity make unlawful activities easier to escape detection. Cyber users in Africa do not have up-to-date technical security measures like anti-virus packages, and many of the operating systems used are not regularly patched (Rajan, Rana, Parameswar, Dhir, & Dwivedi, 2021).

Generally, there is lack of resources to investigate cyber-crime and beef up required instruments to combat electronic fraud. In the wake of ever-increasing ICT advances banking stakeholders need to engage cyber fraud awareness and education. The lack of awareness among the general public of how to maintain a minimum level of security with regard to personal information or electronic property, and it is vital not only to educate the people involved in the fight against cybercrime, but also draft adequate and effective legislation (Ncubukezi, Mwansa, & Rocaries, 2020). This is a very risky situation and means therefore that there is a clear, but certainly not deliberate lack of cyber security awareness and education to make cyber users aware of all possible cyber threats and risks.

Most law enforcement agencies lack the technical expertise as well as sufficient regulatory powers and automated equipment to investigate complicated evidence collection because of intangible nature of cyber space and prosecute fraudulent digital transactions (Ncubukezi, Mwansa, & Rocaries, 2020). Therefore, lack of cyber space legal legislation provides a safe haven for cyber criminals. In light of trying to protect corporate reputation, investor and public confidence most businesses are reluctant to report cyber-criminal activity.

2.4 Effects of Cyber Crime

The effect of cyber-crime cannot be over emphasized on the banking systems as well as on the bank customers. The following are some of the effects of cyber-crime in banking sectors in Nigeria according to Frank, and Odunayo (2013):

- Financial loss: Cybercriminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals.
- Loss of reputation: most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them.
- Reduced productivity: this is due to awareness and more concentration being focused on preventing cybercrime and not productivity.

Vulnerability of their Information and Communication Technology (ICT) systems and networks.

2.5 Causes of Cyber Crime in Banks

Niranjanamurthy, and Chahar (2013) outlined the followings as the causes of cyber-crime in commercial banks:

a. Data That Isn't Encrypted

This is a fundamental but critical aspect of excellent cyber security. All data saved on your banking institution's systems and on the internet should be encrypted. Even if hackers steal your data, if it is encrypted, they will not be able to use it right away, however, if it is not encrypted, hackers will be able to use it right away, causing major difficulties for your financial institution.

b. Viruses

Malware-infected end user devices, such as PCs and mobile phones, represent a threat to your bank's cyber security every time they connect to your network. Sensitive data goes across this

connection, and if the end user device has malware placed on it, that malware might attack your bank's networks if it is not secured properly.

c. Services Provided by Third Parties That Aren't Secure

In order to better serve their clients, many banks and financial institutions use third-party services from other providers. However, if those third-party providers do not have adequate cyber protection in place, your bank might be the one to bear the brunt of the damage. It is critical to consider how you will defend yourself against third-party security dangers before implementing their solutions.

d. Data that has been Tampered with

Hackers do not always go in to take data; they only want to modify it. Unfortunately, this form of assault is difficult to identify immediately away and can cost financial organizations millions, if not billions, of naira in losses. Because altered data doesn't always appear to be different from unmodified data on the surface, it might be difficult to tell what has and hasn't been changed if your bank has been hacked.

Spoofing is a newer sort of cyber security problem, in which hackers imitate a banking website's URL with a website that appears and performs identically. When a user submits his or her login information, hackers steal it and store it for later use. Even more worrying is the fact that modern spoofing techniques do not rely on a slightly different but similar URL to target viewers who have already visited the right URL. It is critical for you, as a bank or financial institution, to identify strategies to limit cyber security dangers while still providing your consumers with easy, technologically sophisticated solutions. SQN has collaborated with Q6Cyber, a pioneer in the cyber security business, to assist provide greater security against potential data breaches.

2.6 Solutions to Cyber Fraud in Bank Settings

Sikdar, and Makkad (2015) suggested the following solutions to cyber-attack in commercial banks:

a. **Security Audit:** Before implementing any new cyber security software, a thorough audit is required. The analysis exposes the current setup's strengths and drawbacks. It also makes recommendations that can help you save money while also allowing you to make the right investments.
b. **Firewalls:** The setting of cyber security banking does not just contain programs. It also necessitates the proper hardware to thwart attacks. Banks can block harmful activity before it reaches other portions of the network with an updated firewall.
c. **Antivirus and Antimalware Software:** While a firewall upgrade improves security, it won't prevent attacks unless anti-virus and anti-malware software is updated as well. Older software may not have the most up-to-date virus signatures and regulations. As a result, it may overlook a potentially catastrophic attack on your system.
d. **Multi-Factor Authentication (MFA):** This security feature, also known as MFA, is crucial for customers who conduct their banking using mobile or web apps. Many users do not change their passwords on a regular basis. Or, if they do, they make minor adjustments. MFA prevents attackers from gaining access to the network by requiring an additional degree of security. A six-digit code, for example, might be transmitted to a customer's cell phone.
e. **Biometrics:** This is a more secure kind of MFA than a texted code. To validate a user's identity, this type of authentication uses retina scans, thumbprints, or facial recognition. Although this form of authentication has been hacked in the past, it is more difficult to do so now.
f. **Automatic Logout:** If a website or app allows it, a user can stay logged in indefinitely. As a result, they can access their data at any moment without having to input their login

credentials. However, attackers will be able to readily get your records as a result of this. Automatic logout reduces this by denying access to a user after a few minutes of inactivity.

g. **Schooling:** All of the aforementioned strategies can help to improve cyber security in the banking industry. They won't be able to help if clients continue to access their data from unsecure areas or save their login credentials incorrectly. This is why it is critical to get a good education. When banks inform their customers about the consequences of these vulnerabilities, they may adjust their behaviour out of fear of losing their money. Much of a bank's or financial institution's business is conducted via technology, especially the Internet. Your bank's sensitive data may be at danger if you don't have strong cyber security procedures in place. The five most serious dangers to a bank's cyber security are listed below.

2.7 Empirical Review

Dzomira (2014) explored the forms of electronic fraud which are being perpetrated in the banking industry and the challenges being faced in an attempt to combat the risk. The study was based on a descriptive study which studied the cyber fraud phenomenon using content analysis. To obtain the data questionnaires and interviews were administered to the selected informants from 22 banks. Convenience and judgemental sampling techniques were used. It was found out that most of the cited types of electronic fraud are perpetrated across the banking industry. Challenges like lack of resources (detection tools and technologies), inadequate cyber-crime laws and lack of knowledge through education and awareness were noted. It is recommended that the issue of cyber security should be addressed involving all the stakeholders so that technological systems are safeguarded from cyber-attacks.

Victory, Promise, and Mike (2022) investigated the impact of cyber-security on fraud prevention in Nigerian commercial banks. The research collected primary data through the interview (WhatsApp video call) conducted with the senior employees of the respective commercial banks who know the subject matter**.** The outcomes of the research demonstrated that cloud security statistically increases fraud prevention in Nigeria**;** also, that application security statistically increases fraud prevention in Nigeria. The study suggested that Nigerian financial industry should be able to effectively detect fraudulent transactions and prevent them from causing financial or reputational damage to the customers or other financial institutions (FI), also, there should be a special awareness program to educate the public on how to always use strong passwords for their devices to prevent hacking, loss of money, or other resources.

More so, Olaniyan, Ekundayo, Oluwadare, and Bamisaye (2021), investigated the use of forensic accounting in Nigeria as a tool for fraud detection and prevention. They used primary sources of information that covered the ten (10) years from 2010 to 2020, findings indicated that while foreign accounts do not completely control fraud detection, forensic accounting has a good and meaningful influence on fraud prevention. It was also discovered that forensic litigation had no appreciable\beneficial effect on the recovery of money stolen through fraud.

In the view of Leukfeldt and Holt (2022), who used a sample of 37 offender networks to study the problem of cybercrime. According to their study's findings, different cybercriminals exhibit different types of criminal activity. In that they sometimes engage in specific types of cybercrime, nearly half of the perpetrator sites in this sample proved to be computer crime specialists, the other half committed a variety of crimes both online and offline. The relative equity between expertise and adaptability, particularly in both online and offline activities, shows that designating fraudsters as a separate offender class may not be of great value. They raise the

subject of what influences an offender's entry into cybercrime, whether they are specialized or general offenders, as a result of their study. Cybercrime actors, whether experts or general practitioners, were a part of larger online criminal networks that may have assisted in identifying and taking advantage of opportunities to commit fraud, ransomware, and other financial crimes.

Alao (2016), the influence of forensic auditing on financial fraud in Nigeria was examined (DMBs). The poll was conducted in a cross-sectional format. The study's participants were bank and audit business employees in Abeokuta, Ogun State. The study's findings demonstrated that forensic audit has a considerable impact on financial fraud control in Nigerian (DMBs), with a P-value of forensic audit reports considerably enhancing court adjudication on financial fraud in Nigeria, with a P value of less than 0.05, and that forensic audit reports greatly improve court adjudication on financial fraud in Nigeria. According to the findings, the use of forensic audits in Nigerians (DMBs) to fight financial fraud is still in its early phases.

In a similar study titled "The influence of forensic investigative processes on corporate fraud deterrence in Nigerian banks," Onodi, Okafor, and Onyali (2015) looked at the function of forensic investigative techniques in discouraging corporate fraud in Nigerian banks. The study employed a survey research approach, relying on data from primary sources such as interviews and questionnaire administration, as well as secondary sources such as financial fraud and forgery complaints. The studies demonstrated a significant connection between forensic investigation approaches and corporate fraud deterrence. The statistics showed that forensic investigators' competence is although this is often necessary in the prosecution of fraud, it is not the case in the overwhelming majority of cases.

Adeniyi (2016), the influence of fraud on the demise of Nigerian banks was investigated. A cross-sectional survey, as well as an ex post facto research approach, were employed in the study. The study's results found that the occurrence of fraud has no significant influence on Nigerian banks' overall anticipated loss, with a P-value of 0.972, which is more than 0.05, and that the occurrence of fraud has no significant impact on Nigerian banks' total expected loss. According to the research, the amount of money involved in bank fraud cases in Nigeria is a reliable predictor of bank failure.

Similarly, Samuel, Pelumi, and Fasilat (2021), investigated the impact of internal control systems on preventing fraud among deposit money institutions. The target audience included all of the financial institutions in the state of Kwara. Purposive random sampling was used to define the sample frame for the study, which focused on all 17 quoted banks in Nigeria that are in the Kwara state. The study found a significant correlation between system of internal control and fraud protection of deposit money institutions in Nigeria.

Badejo et al. (2018), assessed the numerous difficulties in identifying and preventing fraud in Nigeria's banking industry. According to the findings of the descriptive research, the main type of fraud in Nigeria is the looting of funds by bank directors and managers rather than a lack of sufficient motivation. Additionally, it is advised that government bolster already-existing anti-corruption organizations and improve their financial autonomy. To prevent future fraudsters, the managers and directors implicated in the fund plundering should be prosecuted. Before hiring, bank employees, proper screening should be done to assess their moral character and integrity.

Sethi (2021) analysed cyber security in banking sector. Banks are critical to nation-building, particularly in a developing economy like India. Computerization and technology in general have been ingrained in Indian banks from the days of globalization and privatization in the early

1990s. Until this time, the name "bank" conjured up images of a physical institution, a building with a Branch Manager and other officials behind the counters holding massive, voluminous ledgers and people queuing or waiting at cash and other counters. Those were the days. When you say "bank" to a modern-day teen, he doesn't think of a building or a person; instead, he thinks of his computer, an ATM, or his cellphone.

Today's banking is more closely tied with technological delivery channels such as ATMs, mobile phones, point-of-sale terminals, and online banking than with any physical human being. It's no surprise that today's customer is unfamiliar with his banker, and that today's banker is unfamiliar with all of his customers. For hundreds of years, the banking industry has been under threat. The first was the actual theft of funds. Then there was the issue of computer fraud. Hacking into servers to steal a customer's personally identifiable information is now a common occurrence, in addition to cyber fraud (PII). The importance of cyber security in the banking industry is because most people and businesses conduct their business online, the risk of a data breach grows every day. This is why a greater emphasis is being placed on examining the role of cyber security in banking processes.

Oyelakin, Onu, and Akinlabi (2021) studied the effect of security strategies on profitability of selected deposit money banks in Lagos State, Nigeria. The banking industry is considered one of many businesses that have taken advantage of the Internet and IT development by introducing internet banking services to their customers and this bring many benefits to banks and customers. There have been serious threats to the details of customers of banks as there have been an increase in unauthorized access, use, disclosure, disruption, modification or destruction of customer information leading to cases of fraud and poor reputation and performance of several banks across the globe. One of the most challenging issues facing the banking industry currently

is security. Therefore, this study investigated the effect of security strategies on profitability of selected deposit money banks in Lagos State, Nigeria. The population of this study was 433 employees in the IT department of the selected deposit money banks. Total enumeration of the 433 employees of the selected banks was considered. Structured and validated questionnaires were used for data collection. The reliability test yielded Cronbach's alpha for the constructs ranges from 0.947 to 0.990.

Data was analyzed using inferential statistics. The findings of this study revealed that security strategies dimensions had a significant effect on profitability of selected deposit money banks in Lagos State, Nigeria (Adj. $R2 = 0.838$, $F(4, 291) = 383.804$, $p<0.05$). The study concluded that security strategies affect profitability of selected deposit money banks in Lagos State, Nigeria. The study recommended that management of selected deposit money banks in Lagos State should ensure that they implement the right security strategies to avert security threats that could affect their profitability.

Al-alawi, and Al-Bassam (2020) studied the significance of cyber security system in helping managing risk in banking and financial sector. The goal of this study is to show the major impact and benefits of implementing cyber security in an organization's systems, with an emphasis on the banking sector. In addition, the goal of this research is to promote the use of cyber security in order to keep information safe and properly manage risk. Many banking and financial institutions, on the other hand, remain cautious when it comes to the application and usage of cyber security. In fact, many financial organizations may be completely unaware of the advantages of cyber security. Furthermore, its application's higher expenditures could be a factor in its rejection. As a result, numerous questions were posed to measure the level of cyber security awareness and abilities in these banks.

Alghazo, Kazmi, and Latif (2018) studied cyber security analysis of internet banking in emerging countries: user and bank perspectives. Internet banking, also known as Electronic banking (E-banking), Online banking, and Virtual banking, is frequently pushed as a convenient banking alternative, according to the study. In the banking business, internet banking has shown to be an optimal and profitable method of banking. The majority of banks have quickly adopted this technology in order to save money and improve customer service. The adoption of technology is based on the gathering of knowledge and the formulation of a set of beliefs that will assist the user in accepting or rejecting it. The technology acceptance model (TAM) states that user acceptance of technology is influenced by two factors: ease of use and utility.

Ojeka, Ben-caleb, and Ekpe (2017) studied cyber security in the Nigerian banking sector: an appraisal of audit committee effectiveness and noticed that Internet cyber thieves continue to improve their fraud methods, resulting in annual losses of billions of naira. As a result, the audit committee will need to obtain technological skills, as the criminal has more authority and better technical facilities to carry out his or her crime. In the best interests of banks, the audit committee must develop technological knowledge in order to stay up with the worldwide community's developing trend. In terms of financial competence in cyber security, an audit committee needs a high level of financial literacy to successfully manage a company's financial control and reporting.

The responsibility of an audit committee in overseeing managerial accountability is broad, encompassing the entire risk management process. This necessitates accounting skills on the part of the audit committee in order to gain a thorough understanding of the financial repercussions of cybercrime.

Baur-Yazbeck, Frickenstein, and Medine, (2019) studied cyber security. Research discovered that digital financial services (DFS) have a lot of potential for enabling financial inclusion and consequently improving people's lives. Cybercrime, on the other hand, has emerged as a major worry in the financial markets of developing and emerging countries, threatening to stymie global progress toward more equitable financial sectors. FSPs and their clients, as well as financial sector authorities and supervisors, confront difficulties in adapting their behaviors, processes, and regulations to adequately handle the rising risk of cybercrime and technology failure

Rahman, Karim, and Chowdhury (2021) examined the role of boards in cyber security risk profiling: the Case of Bangladeshi commercial banks. Cybercrime becomes costlier than physical crime in developed economies. As a result, it has become the top priority in governance issues in financial institutions. As a developing nation in Bangladesh, the banking sector faces multi-dimensional challenges to adopt IT applications in banking with cybercrime. The paper examines what the banking industry faces cyber security risks and how the board members contribute to identify and mitigate the risk. Through an in-depth interview among the directors of commercial banks in Bangladesh, we identified the possible cyber risk and prepared the risk profile describing the sources, implications, severity of impact, likelihood of occurrence and ranked them. The result shows that the IT governance risk, IT investment risk, and information risk are most critical among the significant cyber security risks. The results of the study have important implications for both corporate boards and policymakers.

Goni, (2019) examined cyber security and computational laws in Nigerian banking system. Banking system is central nervous system of any nation and cyber security and computational law is a major problem of banking system. The main aim of this research work is to examine the

efficiency of cyber security and computational laws in Nigerian banking system, in this survey research method were used both primary and secondary data were used which includes; questionnaire, interview and internet were used in this work the data were analyzed using correlation and regression technique and Chi-square were used to test the hypothesis. From the Chi-square (x2) distribution table, the degree of freedom 3 under the level of significance (0.05) = 7.8 15. Since the x2 calculated is greater than x2 statistical value i.e. 9.389>7.815, the null hypothesis is rejected and the alternative hypothesis is accepted. This means there is an efficiency of cyber security law in the Nigerian banking system.

Aneke, *et al.*, (2020) examined cybercrime technology evolution in Nigeria. With a generation that is highly mobile, there is the desire to quickly access information on the go. These may include logging into the office system to retrieve a file, check bank account status or make one form of payment or the other, or even monitor what the children are doing at home while at work, using IP cameras, etc. Technological advancement in the 21st century while trying to make life easier and better for the global citizens comes accompanied with its associated risks. One of the unknown risks is the situation of not knowing that one is taking a risk by putting one's information on the cyber space through the Internet. It is a known fact that the only assumption that can be made regarding the Internet is that it offers no security whatsoever. With the advent of the mobile phones, accessing the Internet is just a click away.

This accessibility has become a necessary evil, as one is 'compelled' to fill one kind of form or the other with every click of the button, divulging personal information, not knowing who will intercept it for one reason or the other. This research through online survey and analysis tries to find out if cybercrime is a myth or a reality, especially in developing countries. If a reality, how do the cybercriminals extract information that may lead them to stealing vital information or

money from their victims? Results suggest that cybercriminals of recent times seem to target individuals through SMS, E-mails and phone calls.

2.8 Theoretical Framework

2.8.1 Game Theory

Game theory was introduced by Neumann and Morgenstern in 1944. The theory states that in order to achieve fully dependable security system, there is need to permit decision taken by a single component to consider the policies of all the other related mechanism in the network. Game theory helps build models to observe the interactions between attackers and defenders in complex security incidents that plagues commercial bank operations (Amadi, *et al.*, 2017). When introducing strategies such as network security, end-point security, cyber security and physical security, defenders can level up their game. They can play the same “unfair” game that attackers play. Game theory can be adopted in security to observe the nature of a cyber-incident where network defenders, attackers, and users, interact with each other and produce an outcome.

2.8.2 Routine Activity Theory (RAT)

The theory was used in this study since child exploitation is one of the most widespread forms of cyber-crime in the world. This theory was re-appraised by Culatta, Clay-Warner, Boyle, and Oshri (2020). This view focuses on "crime opportunities" in the environment. Where a potential criminal opportunity arises, the action will occur at a time and place when a motivated offender and an acceptable target for victimization collide. This crime will ultimately take place in a location where there is no competent guardian to protect the appropriate target, which is described as a vulnerable person or unprotected property. As a consequence, the absence of any of these three situational elements should potentially prohibit the crime (Valan & Srinivasan, 2021). As a consequence, regular activity theory is seen as a macro-level theory that may be

applied to a broad spectrum of crimes, as it seeks to explain the whole victimization process rather than offenders' particular reasons.

In the absence of a qualified guardian who might perhaps prevent the criminals from committing a crime, the theory predicts that crime will occur when a motivated criminal comes into contact with a suitable victim. The theory suggests that changes in crime rates may be explained by the availability of suitable targets and competent guardians, and from what we can discern, the theory is agnostic about the influence of the supply of motivated criminals (Valan & Srinivasan, 2021).

2.9 Summary of Literature Review

The study has reviewed related information resources using journal articles, conference proceedings, and newspapers. Cybercrime has been seen as a type fraud committed with the aid of ICT infrastructure through the support of either bank customer or staff with little access to information of target. The type of cyber fraud, causes of cybercrime, effect of cybercrime on bank, challenges and solutions of curbing cyber fraud in banks were also reviewed.

The study adopted game theory and routine activity theory. The empirical review of existing studies on the impact of cyber-security of financial fraud in commercial banks in Nigeria was done to identify the gaps in the studies. From the reviewed literature, the following are the identified gaps in knowledge:

1. There is a need to research the types and causes of financial cyber fraud in Zenith bank
2. There is a need to identify the challenges and solutions to financial fraud in Zenith using game theory and routine activity theory.

This research will take into cognizance these gaps and the impact of cyber-security of financial fraud in commercial banks in Nigeria: a case study of Zenith banks in Abuja.

CHAPTER THREE

3. RESEARCH METHODS

3.1 Introduction

This chapter is concerned with the various methods that will adopted for this research. A survey research design will be adopted to guarantee that the researchers reach a larger population. The purpose of this research aimed at establishing a relationship between Cybercrimes and cyber security and the overall impact in the Nigerian banking sector. The primary method of data collection for quantitative analysis will also be adopted to gather information from the 49 branches of zenith bank in the Abuja constitute the population of study. In obtaining the sample technique for this study.

3.2 Research Designs

The concept of research design is a process utilized to create a framework for carrying out a study. The concept involves gathering information and developing a strategy to analyze and discuss the data. The study adopted survey research design, and this was necessitated by the nature of the research. In agreement Adegoke (2012) asserted that survey research design involves the observation and description of the general behaviour of the study population. In other word, this type of research is carried out through a survey, as it involves large group of people. The goal of this type of study is to collect information about the respondents on causes, challenges, effect, and solution to cyber-crime in Zenith bank in Abuja.

3.3 Population of the Study

Table 1.1: Population of the Study

ZENITH		
S/NO	**LOCATION**	**NO OF BRANCHES**
1	WUSE	10
4	CBD	9
3	GARKI	8
2	MAITAMA	4
6	GWAGWALADA	3
5	GWARIMPA	2
7	BWARI	2
8	ASOKORO	1
9	KUCHIGORO	1
10	DUTSE-ALHAJI	1
11	UTAKO	1
12	JABI	1
13	GUDU	1
14	KUBWA	1
15	MPAMPE	1
16	ZUBA	1
17	DEI DEI	1
18	LUGBE	1
	TOTAL	**49**

The information represented in table 1.1 above was sourced from the website of zenith bank and further confirmed from their customer relations department at Gana street Maitama Abuja. The population of the study is the staff in Federal Capital Territory (FCT). However, although, the total number zenith branches in Abuja.

3.4 Sample and Sampling Technique

Multi-stage sampling technique was used. The study selected a branch of Zenith bank to represent a particular area/stratum in FCT Abuja given a total of 18 branches. Thereafter, census sampling was used to capture the staff of Zenith. The sample size of staff is 557.

Table 1.2: Sampling Size

ZENITH			
S/NO	**LOCATION**	**NO OF BRANCHES**	**Size**
1	WUSE	1	43
4	CBD	1	45
3	GARKI	1	39
2	MAITAMA	1	35
6	GWAGWALADA	1	31
5	GWARIMPA	1	36
7	BWARI	1	23
8	ASOKORO	1	21
9	KUCHIGORO	1	19
10	DUTSE-ALHAJI	1	25
11	UTAKO	1	33
12	JABI	1	36
13	GUDU	1	19
14	KUBWA	1	27
15	MPAMPE	1	21
16	ZUBA	1	29
17	DEI DEI	1	34
18	LUGBE	1	41
	TOTAL	**18**	**557**

3.5 Instrument of Data Collection

The study adopted structured questionnaire to capture the responses of the population. The instruments was designed under two headings section A requested for demographic information and section B captured the research questions.

3.6 Validity and Reliability of the Instrument

The research instruments were subjected to face and content validity by an expert in research and evaluation in the department of Science education, Federal University of Technology Minna, Niger State. Similarly, an expert from the department of Cyber Security, Federal University of Technology Minna Niger State was validated. The corrections identified were rectified.

In the same vein, the study conducted a pilot study using Access bank Tunga, Minna branch. A total of 50 questionnaire were distributed and used for the analysis. The Cronbach Alpha values ranges between 0.81- 0.93. The research instrument was found reliable and relevant.

3.7 Method of Data Analysis

Data collected from the administered questionnaires were analyzed using descriptive statistic. Similarly, the hypotheses were analyzed using the Kendal Tau B and multiple regression. The result of findings was presented using table. Statistic Package for Social Science version 27 was used for the analysis.

3.8 Ethical Consideration

An informed consent form was given to respondents to assure them of strict confidentiality of responses and anonymity of respondents in reporting the findings. This is necessary to assure the respondents.

CHAPTER FOUR

4.0 RESULT AND DISCUSSIONS

4.1 Introduction

The chapter presents the result of the findings using tables. The tables are interpreted. The chapter also discussed the findings using relevant research findings. Summary of the findings was also presented.

4.2 Response Rate

Table 4.1: Response Rate table

Total Shared		Total Retrieved	
N	%	N	%
557	100%	497	89.2%

Table 4.1 showed that a total of 557(100%) copies of questionnaire were distributed, while a total of 497(89%) copies of questionnaire were retrieved and found usable.

4.3 Research Questions

Table 4.2: The type of electronic frauds perpetrated in the banking sector

statement	SD	D	A	SA	MEAN	STD
Accounting fraud by bank staff	78	140	116	163	2.7324	1.08082
Money transfer technique	119	174	102	102	2.5763	1.06127
Identity theft	90	149	106	152	2.6439	1.09799
Money laundering	94	79	73	251	2.9678	1.19262

Hacking/cracking	82	119	70	226	2.8853	1.15917
Phishing	43	111	117	226	3.0584	1.01133
Pharming	84	148	118	147	2.6600	1.07532
Spy software	117	148	159	73	2.3783	1.00089
Computer virus (worms, Trojans)	108	133	159	97	2.4930	1.03782
Scams	216	74	134	73	2.6288	1.13037
Wire tapping	216	94	108	79	2.1006	1.13145

Table 4.2 showed the types of cybercrime that existed the Zenith bank Nigeria. The mean score is significant at >=2.5 value. The table showed that some of the fraud that took place in the bank was accounting fraud by bank staff with a mean and standard deviation of 2.73 (1.080). Table 4.2 also showed that money transfer technique is another means whereby Zenith bank customers were been defrauded with a mean and standard deviation of 2.58(1.061). Similarly, table 4.2 showed that identity theft is another fraud technique in Zenith bank with a mean and standard deviation of 2.64(1.098). Also, the table showed that money laundering is another type of fraud used by fraudsters in defrauding Zenith bank customers of their money with a mean and standard deviation of 2.968(1.119).

In the same vein, table 4.2 showed that hacking/cracking is another technique used for cybercrime with a mean and standard deviation of 2.97(1.16). The table also revealed that phishing and pharming are techniques used for cyber fraud in the bank by fraudsters with mean and standard deviation of 2.89(1.16) and 2.67(1.08) respectively. The table however revealed that spy software and wiretapping were not used for cybercrime in Zenith bank with a mean and standard deviation of 2.38(1.00) and 2.10(1.13) respectively. Put differently, table 4.2 showed

that computer virus (worms, Trojans) and Scams were methods used for cyber fraud in banks with the mean and standard deviation of 2.5(1.04) and 2.63(1.13) respectively.

Table 4.3: The causes of cyber fraud in banks

STATEMENT	SD	D	A	SA	MEAN	STD
lack of oversight by line managers or senior managers on deviations from existing electronic process/controls	123	40	141	193	2.8129	1.19441
current business pressure to meet set targets	99	68	99	231	2.9296	1.18163
difficult business scenario	66	111	59	261	3.0362	1.13179
collusion between employees and external parties.	52	118	125	202	2.9598	1.03097
insufficient data encryption	62	170	132	133	2.6761	1.00286
the use of brute force attack with aid of virus by fraudster	160	148	176	13	2.0845	0.88040
the use of Services Provided by Third Parties	92	146	134	125	2.5875	1.05727
Parodying	125	140	107	125	2.4668	1.12137

Table 4.3 showed the causes of cyber fraud in the banks in Nigeria. The mean score is significant at >=2.6 value. The table showed that lack of oversight by line managers or senior managers on deviation from exiting electronic process/controls has strongly influenced the rate of cyber fraud in Zenith banks with a mean and standard deviation of 2.81(1.19). Table 4.3 further showed that current business pressure to meet set targets on bank staff has influenced the rate of cyber fraud in banks with a mean and standard deviation of 2.93(1.18). In the same vein, table 4.3 showed that difficult business scenario has a high cause of cyber fraud in banks with a mean and standard deviation of 3.04(1.13).

The table further showed that collusion between bank employees and external parties also influenced the rate of cyber fraud in banks with a mean and standard deviation of 2.96(1.03). Also, table 4.3 showed that insufficient data encryption protocol has a high risk of system penetration thereby enhancing cyber fraud in banks with a mean and standard deviation of 2.67(1.00). Similarly, the table further showed that the use of services provided by third parties and parodying have a significant influence on the cause of cyber fraud in banks with mean and standard deviation of 2.59(2.06) and 2.5(1.12) respectively. However, the table showed that the use of brute force attack with the aid of virus by fraudster does not influence the cause of cyber fraud in banks with a mean and standard deviation of 2.09(0.88).

Table 4.4: The challenges of curbing cyber fraud in the bank

STATEMENT	SD	D	A	SA	MEAN	STD
Lack of Standards and National Central Control	68	88	79	262	3.0765	1.11722
Lack of Infrastructure	92	125	80	200	2.7807	1.16146
Porous Nature of the Internet	53	121	103	220	2.9859	1.05580
Lack of National Functional Databases:	103	122	118	154	2.6499	1.12440
Domestic and international law enforcement	123	156	140	78	2.3481	1.01876
inadequate awareness by bank customers	113	138	144	102	2.4728	1.05674

Table 4.4 showed the challenges faced in curbing the rate of cyber fraud in Zenith banks. The mean score is significant at >=2.5 value. Table 4.4 showed that lack of standards and national central control have been a major challenge in curbing cyber fraud in banks with a mean and standard deviation of 3.08(1.12). The table further showed that lack of infrastructure also mitigates the curbing of cyber fraud in banks with mean and standard deviation of 2.78(1.16).

Similarly, the table revealed that porous nature of the internet has also contributed to the challenges faced in curbing cyber fraud in banks with mean and standard deviation of 2.99(1.06).

In the same vein, the table revealed that lack of functional databases, and inadequate awareness by bank customers were challenges on the amelioration of cyber fraud in banks with mean and standard deviation of 2.65(1.12), and 2.5(1.06) respectively. However, the table showed that domestic and international law enforcement is not a challenge on curbing cyber fraud in bank with a mean and standard deviation of 2.35(1.02).

Table 4.5: The effect of cyber fraud on Nigeria banks

STATEMENT	SD	D	A	SA	MEAN	STD
Financial loss	228	102	88	79	2.0362	1.12822
Loss of reputation	224	86	105	82	2.5905	1.14734
Reduced productivity	123	40	141	193	2.8129	1.19441
Vulnerability of their Information and Communication Technology (ICT) systems and networks	99	68	99	231	2.9296	1.18163
Lead to creation of more bank account	66	111	59	261	2.0312	1.13179

Table 4.5 showed the effect of cyber fraud on banks. The mean score is significant at >=2.5 value. The table showed that loss of reputation by bank is one of the effect of the occurrence of cybercrime in banks with a mean and standard deviation of 2.59(1.15). Table 4.5 further showed that reduced productivity is another effect that cybercrime has on the banks with a mean and standard deviation of 2.81(1.19). Similarly, the table revealed that the effect of cybercrime on bank is that it leads to high vulnerability of banks information and communication technology,

and networks with a mean and standard deviation of 2.93(1.18). However, the table showed that the effect of cybercrime does to lead financial loss for banks, neither does it lead to creation of more bank account with mean and standard deviation of 2.04(1.12), and 2.03(1.13) respectively.

Table 4.6: Possible solutions for curbing cyber fraud in banks

STATEMENT	SD	D	A	SA	MEAN	STD
Security Audit	62	170	132	133	2.6761	1.00286
Firewalls	160	148	176	13	2.5845	0.88040
Antivirus and Antimalware Software	69	157	102	169	2.7465	1.07206
Multi-Factor Authentication (MFA)	63	118	125	191	2.8934	1.05814
Biometrics:	162	66	152	117	2.4507	1.17178
Automatic Logout	86	202	74	135	2.5191	1.06830
Cyber security education to bank customer on information security	171	110	110	106	2.5038	1.15277

Table 4.6 showed the possible solution to cyber fraud in banks. The mean score is significant at >=2.5 value. The table showed that security audit is necessary in order to be able to mitigate the occurrence of cyber fraud in bank with a mean and standard deviation of 2.68(1.00). In the same vein, the table showed that the use of strong firewall by banks in necessary in order to prevent cyber-attack and fraud in the bank with the mean and standard deviation of 2.58(0.88). Also, table 4.6 revealed that the use of antivirus and antimalware software, multi-factor authentication, biometrics and automatic logout on all the banks platform after a period idle on the platform will help to mitigate the cyber fraud in the bank with mean and standard deviation of 2.75(1.07), 2.89(1.05), 2.50(1.17) and 2.52(1.07) respectively. Finally, table 4.6 showed that there is need to

sensitise the bank customer via cyber security education on information security with a mean and standard deviation of 2.50 (1.15).

4.4 Hypotheses

Table 4.7: There is no composite impact of the types of electronic frauds and the causes of cyber fraud on the effect of cyber fraud on banks

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	13.950	2	6.975	5.281	.005[b]
	Residual	652.513	494	1.321		
	Total	666.463	496			

**Sig<0.05

The result in table 4.7 showed the composite impact of the types of electronic frauds and the causes of cyber fraud on the effect of cyber on banks. From the table the sig. value is 0.005, which implies that there is significance impact of the types of electronic fraud and the causes of cyber fraud on the effect of cyber fraud on banks. Therefore, the null hypothesis is not accepted.

Table 4.8: There is no relationship between the challenges of curbing cyber fraud and the possible solutions of curbing cyber fraud in banks.

challenges of curbing cyber fraud		possible solutions of curbing cyber fraud in banks		
Kendall's tau_b	challenges of curbing cyber fraud	Correlation Coefficient	1.000	-.342**
		Sig. (2-tailed)		0.000
		N	497	497

	possible solutions of curbing cyber fraud in banks	Correlation Coefficient	-.342**	1.000
		Sig. (2-tailed)	0.000	
		N	497	497
**. Correlation is significant at the 0.05 level (2-tailed).				

Table 4.8 showed the relationship between the challenges of curbing cyber fraud and the possible solutions of curbing cyber fraud in banks. The table showed that there is a relationship between the challenges and solution to cyber fraud in banks (r = -0.342), Sig = 0.000, which implies that there is a significance relationship between the challenges of curbing cyber fraud and possible solutions of curbing fraud in banks. Therefore, the null hypothesis is not accepted.

4.5 Discussion of Findings

The findings of the study showed that bank customers experienced different types of electronic fraud such as accounting fraud by bank staff, identity theft, money laundering, hacking/cracking, phishing, pharming, and computer virus. The study is supported by McGuire and Dowling (2013) whose findings showed that hacking/cracking, spamming, running of malicious codes and malware programs, are methods used in defrauding bank customers. In general, cybercriminals execute fraudulent activities with the ultimate goal of accessing a user's bank account to either steal or/and transfer funds to another bank account without rightful authorization. However, in some rare cases in Nigeria, the intention of cyber-criminals is to cause damage to the reputation of the bank by denying service to users (Parthiban, 2014) and sabotaging data in computer networks of organizations.

The findings of the study showed the major causes of cyber fraud in bank. The causes identified are lack of oversight by line managers or senior managers on deviations from existing electronic process/controls, current business pressure to meet set targets, current business pressure to meet set targets, collusion between employees and external parties, insufficient data encryption, the use of services provided by third parties, parodying. The findings were supported by Hassan, (2012), the author asserted that unemployment is one of the major causes of cybercrime in Nigeria. It is a known fact that over 20 million graduates in the country do not have gainful employment.

This has automatically increased the rate at which they take part in criminal activities for their survival. Similarly, Sethi (2021) outlined that electronic process/controls, current business pressure to meet set targets, current business pressure to meet set targets, collusion between employees and external parties, insufficient data encryption, the use of services provided by third parties, parodying are major causes of cyber fraud in banks.

The findings of the study showed that banks are confronted with so many challenges in curbing the rate of cyber fraud. The challenges were lack of standards and national central control, lack of infrastructure, porous nature of the internet, lack of national functional databases, and inadequate awareness by bank customers. The findings was supported by Kritznger and Solms (2012) who asserted that cyber users in Africa do not have up-to-date technical security measures like anti-virus packages, and many of the operating systems used are not regularly patched thereby impinging on the amelioration of cyber fraud.

The findings of the study showed the negative effect of cyber fraud on bank such as financial loss, reduced productivity, vulnerability of banks Information and Communication Technology

(ICT) systems and networks. The findings were supported by Frank and Odunayo (2013) who asserted that the effect of cybercrime on the bank system is alarming. The author further posited that negative effect of cybercrime on bank leads to loss of reputation, reduced productivity, and financial loss.

The findings of the study showed the possible solutions that can be taken in order to curb cybercrime in banking system in Nigeria. The possible identified solutions were security audit, antivirus and antimalware software, use of multi-factor authentication, use of biometrics, automatic logout, and cyber security education to bank customer on information security. The findings were supported by Sethi (2021), the author outlined possible solutions to curbing cyber fraud in banks, and they include the use of firewall on the operating systems of the bank software, frequent security audit by cyber security expert, use of multi-factor authentication and biometrics for security of the information of the customer. The security of bank customer information and fund by bank through efficient cyber protocol, the more the patronage of the bank.

4.6 Summary of Findings

1. The major type of cyber fraud in banking system were accounting fraud by bank staff, identity theft, money laundering, hacking/cracking, phishing, pharming, and computer virus.
2. Lack of oversight by line managers or senior managers on deviations from existing electronic process/controls, current business pressure to meet set targets, current business pressure to meet set targets, collusion between employees and external parties, insufficient data encryption, the use of services provided by third parties, parodying were the causes of cybercrime in banks.

3. Lack of standards and national central control, lack of infrastructure, porous nature of the internet, lack of national functional databases, and inadequate awareness by bank customers were the challenges militating the effort towards curbing the cyber fraud in banking system in Nigeria.
4. Financial loss, reduced productivity, vulnerability of banks Information and Communication Technology (ICT) systems and networks were the effect of cybercrime on banks in Nigeria.
5. The place of security in the cyber space of banks in Nigeria cannot be overstretched. Therefore, security audit, antivirus and antimalware software, use of multi-factor authentication, use of biometrics, automatic logout, and cyber security education to bank customer on information security should be adopted by banks in Nigeria.

CHAPTER FIVE

5.0 Conclusion and Recommendation

5.1 Conclusion

Cybercrime is a menace that should be eradicated or reduced to a very minimal level for our great nation to break even. The research has identified different types of cyber fraud, causes of fraud, effect of cyber fraud, challenges and solutions of curbing cyber fraud in banks in Nigeria. The study was conducted in Zenith bank in Abuja Nigeria. Numerous ways have been proposed to prevent future occurrence of this crime, how-ever much can still be done by commercial banks and bank customers to reduce it. Information technology via cyber security and its likes should be massively use to help in ameliorating the level of fraud and associated crimes which has continued to take different shapes and colours in the Nigerian space. Consequent to these findings, the study concluded that cloud security statistically boosts fraud prevention in Zenith banks.

5.2 Recommendations

The study recommended that:

1. Zenith bank should employ stringent measure to monitor staff activities especially in the confidentiality of customer information. This will help to curtail the collaboration between bank staff and the fraudsters in committing cybercrime.
2. Cyber security audit should be done by Zenith regularly in order to be able mitigate the various techniques used by fraudsters in committing cybercrime. Relevant loop holes identified during security audit should be fixed immediately so as to prevent any attempt of fraud in the bank.
3. Cybercrime does not happen without the customer consent either knowingly or unknowingly. Therefore, the bank should endeavor to sensitize the bank customers on the

various ways in which fraudsters can used in defrauding them. Also, bank customers should be instructed on how to identify the genuine software and to also avoid the use of third party software.

4. Necessary measures should be put in place in order to prevent cybercrime, as it will lead to loss of reputation, productivity and vulnerability of the bank ICT infrastructure, and financial loss for the bank customers.
5. Multi-factor authentication, biometrics and automatic log out, and strong firewall should be adopted by Zenith bank in order to ensure the security of customer information and fund.

5.3 Contribution to Knowledge

1. The study has established the possible solutions to the causes of cyber fraud in banks in which management of banks, policy makers and bank staff can be harnessed in preventing cybercrime in the bank.
2. The study has also contributed to the existing of body of knowledge as no work has been done on the causes of cyber fraud in Zenith bank Abuja Nigeria. Therefore, scholars in academics and researchers can make reference to the work.

5.4 Suggestion for Further Study

1. Lack of knowledge and awareness of bank customer a determinant of prevalent cybercrime in Nigeria banks
2. Bank policies and national policies a solution to cyber fraud in financial institutions in Nigeria
3. ICT infrastructure and cyber security expert recipe to safe cyber system in Nigeria banks.

References

Aaron, M. M., (2012). A Case Study on E-Banking Security–When Security Becomes Too Sophisticated for the User to Access Their Information. *Journal of Internet Banking and Commerce,* 17 (2).

Adeniyi, A. (2016). Analysis of fraud in banks: Evidence from Nigeria. *International Journal of* activity theory explanation. *Journal of interpersonal violence, 35*(15-16), 2800-2824.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime, 27*(3), 945-958.

Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University, 14*(7), 1523-1536.

Alao, A. A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). *European Journal of Accounting, Auditing and Finance Research, 4*(8), 1-19.

Alao, A. A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). *European Journal of Accounting, Auditing and Finance Research, 4*(8), 1-19.

Alghazo, J. M., Kazmi, Z., & Latif, G. (2017, November). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. In *2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS)* (pp. 1-6). IEEE.

Aloraini, B., Nagappan, M., German, D. M., Hayashi, S., & Higo, Y. (2019). An empirical study of security warnings from static application security testing tools. *Journal of Systems and Software, 158*, 110427.

Amadi, E. C., Eze, U., & Ikerionwu, C. (2017). Game theory basics and its application in cyber security. *Advances in Wireless Communications and Networks. 3*(4), 45-49.

Anah, B. B., Funmi, D. D. & Julius, M. (2012). Cybercrime in Nigeria: causes, effects and the way out. *ARPN Journal of Science and Technology*, 2(7).

Andi, K., Kusumanto, R., & Yusi, S. (2022). IoT Monitoring for PV System Optimization in Hospital Environment Application. *Studies in Informatics, Technology and Systems, 1*(1), 1-8.

Aneke, S. O., Nweke, E. O., Udanor, C. N., Ogbodo, I. A., Ezugwu, A. O., Uguwishiwu, C. H., & Ezema, M. E. (2020). Towards determining cybercrime technology evolution in Nigeria. *International Journal of Lates Technology in Engineering, Management and Applied Science,* 9, 37-43.

Babayo, S., Bakri, M., Usman, S., Mohammed, K. T., & Muhammad, A. Y. (2021). Cybersecurity and cybercrime in Nigeria: The implications on national security and digital economy. *Journal of Intelligence and Cyber Security*, *4*(1).

Badejo, B. A., Okuneye, B. A., & Taiwo, M. R. (2018). Fraud detection in the banking system in Nigeria: Challenges and prospects. *Shirkah: Journal of Economics and Business*, *2*(3).

Basil, U. (2015). *Dealing with the Challenge of Cybercrime in Nigeria under the new Cybercrime Act*. The Lagos Chamber of Commerce & Industry 2015 Seminar of the Financial Services Group September 3, 2015.

Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). Cyber Security in Financial Sector Development. *CGAP Background Documents*, 5(2).

Bhasin, M. L. (2016). The role of technology in combatting bank frauds: perspectives and prospects. *Ecoforum Journal*, *5*(2).

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations* UK: Oxford University Press.

Chika, O. V., Promise, E., & Werikum, E. V. (2022). Influence of Liquidity and Profitability on Profits Growth of Nigerian Pharmaceutical Firms. *Goodwood Akuntansi dan Auditing Reviu*, *1*(1), 1-13.

Culatta, E., Clay-Warner, J., Boyle, K. M., & Oshri, A. (2020). Sexual revictimization: A routine activity theory explanation. *Journal of interpersonal violence*, *35*(15-16), 2800-2824.

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*, *4*(2), 16-26.

Ebiasuode, A., Onuoha, B. C., & Nwede, I. G. N. (2017). Human Resource Management Practices and Organisational Innovation in Banks in Bayelsa State. *Human resource management*, *3*(8).

Efiong, E. J., Inyang, I. O., & Joshua, U. (2016). Effectiveness of the mechanisms of fraud prevention and detection in Nigeria. *Advances in Social Sciences Research Journal*, *3*(3).

Fadare, O. A. (2015). Impact of ICT tools for combating cybercrime in Nigeria online banking: A conceptual review. *International Journal of Trade, Economics and Finance*, 6 (5).

Frank, I., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. *International Journal of Cognitive Research in science, engineering and education*, *1*(1), 100-110.

Goni, I. (2019). Cyber Security and Computational Laws in Nigerian Banking System. *Advances in Networks*, *7*(2), 16.

Hanafizadeh, P., Behboudi, M., Koshksaray, A. A., & Tabar, M. J. S. (2014). Mobile-banking adoption by Iranian bank clients. *Telematics and informatics*, 31(1), 62-78.

Heliantono, H., Gunawan, I. D., Khomsiyah, K., & Arsjah, R. J. (2020). Moral development as the influencer of fraud detection. *International journal of Financial, Accounting, and Management, 2*(1), 1-11.

Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F. J., & Urueña, A. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International journal of environmental research and public health,* 18(7), 3763.

Ibrahim, U. (2019). The Impact of Cybercrime on the Nigerian Economy and banking system. *NDIC Quarterly, 34*(12), 1-20.

Imran, S. M. & Sana, R. (2013). Impact of Electronic crime in Indian Banking Sector–An Overview. *International Journal Business Information Technology*, 1 (2).

Leonard, R. J. (1995). From parlor games to social science: von Neumann, Morgenstern, and the creation of game theory 1928-1944. *Journal of economic literature*, *33*(2), 730-761.

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, 126, 106979. doi:10.1016/j.chb.2021.106979

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, *126*, 106979.

Muhattan. (2015). 3 Essential types of cyber security solutions. Retrieved from *Manhattan tech support publishers--www.ilovepdf.com.*

Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020, December). A review of the current cyber hygiene in small and medium-sized businesses. In *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 1-6). IEEE.

Niranjanamurthy, M., & Chahar, D. (2013). The study of e-commerce security issues and solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(7), 2885-2895.

Nugraha, R., & Bayunitri, B. I. (2020). The influence of internal control on fraud prevention (Case study at Bank BRI of Cimahi City). *International journal of Financial, Accounting, and Management, 2*(3), 199-211.

Ojeka, S. A., & Egbide, B. C. (2017). Cyber security in the nigerian banking sector: an appraisal of audit committee effectiveness. *International Review of Management and Marketing*, *7*(2), 340-346.

Okpa, J. T., Ajah, B. O., & Igbe, J. E. (2020). Rising trend of phishing attacks on corporate organisations in Cross River State, Nigeria. *International Journal of Cyber Criminology*, *14*(2), 460-478.

Okpa, J. T., Ugwuoke, C. U., Ajah, B. O., Eshioste, E., Igbe, J. E., Ajor, O. J., ... & Nnamani, R. G. (2022). Cyberspace, Black-Hat Hacking and Economic Sustainability of Corporate Organizations in Cross-River State, Nigeria. *SAGE Open*, *12*(3), 21582440221122739.

Olaniyan, N. O., Ekundayo, A. T., Oluwadare, O. E., & Bamisaye, T. O. (2021). Forensic accounting as an instrument for fraud detection and prevention in the public sector: moderating on ministries, departments and agencies in Nigeria. *Acta Scientiarum Polonorum. Oeconomia,* 20(1), 49-59.

Olaniyan, N. O., Ekundayo, A. T., Oluwadare, O. E., & Bamisaye, T. O. (2021). Forensic accounting as an instrument for fraud detection and prevention in the public sector: moderating on ministries, departments and agencies in Nigeria. *Acta Scientiarum Polonorum. Oeconomia*, *20*(1), 49-59.

Olubisi, F. O. (2015). History and evolution of banking in Nigeria. *Academ arena,* 7 (1), pp. 9-14.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1.

Onodi, B. E., Okafor, T. G., & Onyali, C. I. (2015). The impact of forensic investigative methods on corporate fraud deterrence in banks in Nigeria. *European Journal of Accounting, Auditing and Finance*, *3*(4), 69-85.

Oyelakin, O., G., Onu C, A., & Akinlabi, B, H. (2021). Effect of security strategies on profitability of selected deposit money banks in Lagos state, Nigeria. *Artic Journal*, 74(6).

Pal, A., De', R., Herath, T., & Rao, H. R. (2019). A review of contextual factors affecting mobile payment adoption and use. *Journal of Banking and Financial Technology*, *3*, 43-57.

Pandey, A. K., & Alsolami, F. (2020). Malware Analysis in Web Application Security: An Investigation and Suggestion. *International Journal of Advanced Computer Science and Applications,* 11(7), 191–201. doi:https://doi.org/10.14569/IJACSA.2020.0110725

Rahman, M. B., Karim, T., & Chowdhury, I. U. (2021). Role of Boards in Cybersecurity Risk Profiling: The Case of Bangladeshi Commercial Banks. *Global Journal of Management and Business Research*, *21*(A3), 49-58.

Rahman, R. A., & Anwar, I. S. K. (2014). Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia-Social and Behavioral Sciences,* 145, 97-102.

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change*, *170*, 120872.

Samuel, O., Pelumi, I., & Fasilat, O. (2021). Effect of internal control system on fraud prevention among deposit money banks in Kwara State, Nigeria. *International Journal of Multidisciplinary Research and Growth Evaluation, 2*(1), 264–271.

Seissa, I. G., Ibrahim, J., & Yahaya, N. (2017). Cyber terrorism definition patterns and mitigation strategies: A literature review. *International Journal of Science and Research (IJSR), 6*(1), 180-186.

Sethi, N. (2021). Cyber security analysis in banking sector. *International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)*, 04(03), 59-64

Sikdar, P., & Makkad, M. (2015). Online banking adoption: A factor validation and satisfaction causation study in the context of Indian banking customers. *International Journal of Bank Marketing, 33*(6), 760-785.

Tendulkar, R. (2013). Cyber-crime, securities markets and systemic risk. *CFA Digest, 43*(4), 35-43.

Valan, M. L., & Srinivasan, M. (2021). The application of routine activity theory in explaining victimization of child marriage. *International review of victimology, 27*(2), 211-226.

Victory, C. O., Promise, E., Mike, C, N (2022). Impact of Cyber-Security on Fraud Prevention in Nigerian Commercial Banks. *Jurnal Akuntansi, Keuangan dan Manajemen*, 4(1), 15-27.

Wapmuk, S. E. (2017). *Banking regulation and supervision in Nigeria: an analysis of the effects of banking reforms on bank performance and financial stability*. University of Salford (United Kingdom).

Zheng, Y., Pal, A., Abuadbba, S., Pokhrel, S. R., Nepal, S., & Janicke, H. (2020). *Towards IoT Security Automation and Orchestration.* Paper presented at the 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA).

QUESTIONNAIRE

Impact of cyber security on financial fraud in commercial banks in Nigeria: a case study of Zenith Bank.

Section A:

Gender: Male { } Female { }

Branch:_____

Section B:

1. Examine the type of electronic frauds perpetrated in the banking sector

TYPE OF FRAUD	SA	A	D	SD
Accounting fraud by bank staff				
Money transfer technique				
Identity theft				
Money laundering				
Hacking/cracking				
Phishing				
Pharming				
Spy software				
Computer virus (worms, Trojans)				
Scams				
Wire tapping				

Key: SA: Strongly Agreed; A: Agreed; D: Disagreed; SD: Strongly Disagreed

2. Determine the causes of cyber fraud in banks

causes of fraud	SA	A	D	SD	
lack of oversight by line managers or senior managers on deviations from existing electronic process/controls					
current business pressure to meet set targets					
difficult business scenario					
collusion between employees and external parties.					
insufficient data encryption					
the use of brute force attack with aid of virus by fraudster					
the use of Services Provided by Third Parties					
Parodying					

Key: SA: Strongly Agreed; A: Agreed; D: Disagreed; SD: Strongly Disagreed

3. Determine the challenges of curbing cyber fraud in the bank

challenges of cyber security	SA	A	D	SD
Lack of Standards and National Central Control				
Lack of Infrastructure				
Porous Nature of the Internet				
Lack of National Functional Databases:				
Domestic and international law enforcement				
inadequate awareness by bank customers				

Key: SA: Strongly Agreed; A: Agreed; D: Disagreed; SD: Strongly Disagreed

4. Evaluate the impact of cyber fraud on Nigeria banks

IMPACT OF CYBER FRAUD	SA	A	D	SD
Financial loss				
Loss of reputation				
Reduced productivity				
Vulnerability of their Information and Communication Technology (ICT) systems and networks				
Lead to creation of more bank account				

Key: SA: Strongly Agreed; A: Agreed; D: Disagreed; SD: Strongly Disagreed

5. Identify possible solutions for curbing cyber fraud in banks

Solutions to Cyber Fraud in Bank Settings	SA	A	D	SD
Security Audit				
Firewalls				
Antivirus and Antimalware Software				
Multi-Factor Authentication (MFA)				
Biometrics:				
Automatic Logout				
Cyber security education to bank customer on information security				

Key: SA: Strongly Agreed; A: Agreed; D: Disagreed; SD: Strongly Disagreed