Scientific Research Publishing

Journal of Information Security, 2024, 15, 494-523
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cybersecurity Challenge in Nigeria Deposit Money Banks

Godwin Agwu Ndukwe Ama, Chibunna Onyebuchi Onwubiko, Henry Arinze Nwankwo

Department of Accounting, Faculty of Economics and Management Sciences, Abia State University, Uturu, Nigeria
Email: gananig77@gmail.com, chibunna_onwubiko@yahoo.com, Henryfayoh@yahoo.com

How to cite this paper: Ama, G.A.N., Onwubiko, C.O. and Nwankwo, H.A. (2024) Cybersecurity Challenge in Nigeria Deposit Money Banks. *Journal of Information Security*, **15**, 494-523.
https://doi.org/10.4236/jis.2024.154028

Received: May 22, 2024
Accepted: October 13, 2024
Published: October 16, 2024

Copyright © 2024 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

The study investigates cybersecurity challenges in Nigerian deposit money banks (DMBs) with a focus on proactive measures taken by banks and customers to overcome these challenges. The research design employs a descriptive approach and census sampling, with data collected from staff of selected DMBs using questionnaires. Data analysis was conducted using SPSS, and findings indicate that the major challenges confronting cybersecurity in banks were pharming, identity theft, SIM Swap fraud, Skimming/Website cloning and Smishing/Vishing. The major factors responsible were found to include loopholes in the banks' internal control system, insider abuse by bank staff, ignorance and lack of security consciousness among the banking customers etc. it was found that banks implement measures such as encryption, password changes, and blocking unsolicited messages to mitigate cybersecurity risks. The study concludes with recommendations for continuous security updates, internal control reviews, and customer education campaigns. While the study addresses an important topic, there are areas where clarity, depth, and methodological rigor could be strengthened for a more robust contribution to the field.

Keywords

e-Fraud, Cyberspace, Cybercrime and Cybersecurity

1. Introduction

1.1. Background to the Study

Cybercrime has taken a back seat in the Nigerian banking sector. Hardly does a day pass without one form of cyber-attack or the other on the bank customers. Cybercrime refers to the series of organized crimes attacking both cyberspace and cybersecurity [1]. Cybersecurity threat especially in the financial service sector is now associated with the use of sophisticated technologies to exploit the vulnerabilities of

computer systems and bypass access or hack into computer servers for the purpose of carrying out cyber-crime or fraud. [2] cited by [3], described cybersecurity threat as any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices such as smart-phones by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. [4] defines Cybersecurity as a body or a combination of technologies, processes, and practices that are designed to protect computer systems, network systems and vital data from outside threats.

The banking industry is one of the most fundamental institutions in any country, and it owes it a duty not only to protect itself but also its customers. Banks have been exposed to various types of cyber risks, which have resulted in the loss of money by banks or their customers through cyber attacks. The emergence of computers reduced many problems associated with banking; however, it came along with different ways people fall prey to different types of cyber-attacks. The astronomic growth in cybercrimes in recent times is a major problem for financial institutions in the 21st century. Nigeria's enactment of the Cybercrimes [5] has not been successful in tackling the vulnerability of bank customers to cybercrimes. Hence, the 2021 Nigerian National Cybersecurity Policy and Strategy (NCPS) was introduced to tackle cybersecurity menace in the banking, finance, and insurance sectors. The Central Bank of Nigeria (CBN) has also developed instruments like the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, the Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions (OFI), the regulatory Framework for Mobile Money Services in Nigeria, and the Nigerian Payment System Risk and Information Security Management Framework [6].

The cyber criminals use various methods to steal money from the unsuspecting public through cyber-attack. An attacker can hack into another computer by copying, or exploiting personal data and information. They can, for instance, copy log-in codes and addresses or retrieve credit card and bank account passwords. The effect is that criminals can either withdraw money from a bank customer's account or make payments online from someone else's account [7]. Cybercrime is one of the world's most prominent and evolving forms of crime. The internet is after all available to everyone and that of course creates serious risks to individuals and institutions.

[8] as cited by [9] reported the increase in cyber bank fraud cases in Nigeria hit 26,182 in 2017 and further increased to 37,817 in 2018, representing an increase of 44.4%. Similarly, the actual amount lost to fraud incidences increased significantly in 2018 to ₦15.15 billion ($39.9 m) as against ₦2.37 billion ($6.2 m) and ₦2.4 billion ($6.3 m) in 2017 and 2016 respectively [8]. Electronic payment channels, which are driven by the internet and advanced technology, are drivers of these e-frauds and forgeries that were perpetrated not only by outsiders but also

by the staff of banks in Nigeria. 899 staff were involved in frauds and forgeries in 2018 compared to 320 Staff in 2017.

Nigerian financial services companies lost ₦2.805 billion to fraud between January and September 2020. This was a 510% increase from the ₦550 million lost to fraudsters in the same period in 2019. For the nine-month period, fraud attempts increased by 186% from 16,128 in 2019 to 46,126 [10].

However, research by [6] revealed that the number of unique phishing sites had increased from 611,877 in 2020 to 637,302 in 2021. The Identity Breach Report shows that identity-based fraud using people's phone numbers has also increased. Therefore, this study sets out to determine critical ways to overcome cybersecurity challenges encountered by bank customers and to recommend appropriate measures to reduce them.

1.2. Statement of the Problem

The advent of the internet and online financial services by the banks in Nigeria came with joy and ease of doing business with banks, most especially for withdrawers and depositors. But, in recent times bank customers' money has been withdrawn from their bank accounts without due authorization through fraudulent ways of sending emails or pop-up web pages purporting to be legitimate financial institutions to stimulate individuals to provide sensitive account information e.g. credit card details and PIN which are used to perpetrate e-fraud. In addition, most fraudulent practices are conducted via a device called a skimmer, which is placed in most ATM and POS terminals to capture customers' card information, thereby aiding electronic fraud. [11] as cited by [12] also affirmed that a Trojan POSRAM malware was used to steal payment card information of about 70 million customers belonging to a retail giant, banking with a commercial bank in Nigeria in 2013. In addition, other cyber fraudsters use unsolicited text messages and calls as means of luring bank customers to provide their bank account details, which they use to commit e-fraud. All these have brought emotional trauma and untold financial problems to customers who have fallen victim to their nefarious acts.

It has also been observed that customers' money is fraudulently withdrawn from their account after using the services of MoMo Agents who are licensed by banks to render financial services on their behalf. These lingering problems have become a nightmarish experience for both customers and the bankers. However, questions are raised as to whether the banks do proper character verification before licensing the MoMo agents that do business on their behalf.

The above problems, including the scantiness of empirical literature on the subject matter, have prompted this research to determine critical ways to overcome the cybersecurity challenges that bank and its customers encounter and recommend appropriate measures to reduce them.

1.3. Objectives of the Study

The general objective of this study is to investigate cybersecurity challenges in

Nigeria deposit money banks. The specific objectives of this study are to:

1) determine the prominent type of cybersecurity challenges deposit money banks are exposed to in Nigeria.

2) ascertain factors responsible for cybersecurity problems in Nigerian deposit money banks.

3) find out measures adopted to reduce/eliminate the various threats of cybersecurity challenges in Nigerian deposit money banks.

1.4. Research Questions

The following questions below are formed to achieve the specific objectives above.

1) What are the prominent types of cybersecurity challenges deposit money banks are exposed to in Nigeria?

2) What are the factors responsible for cyber security problems in Nigerian deposit money banks?

3) What measures were adopted to reduce/eliminate the various threats of cybersecurity challenges in Nigerian deposit money banks?

2. Review of Related Literature

2.1. Conceptual Review

The following concepts that relate to the topic under investigation were reviewed below.

2.1.1. Fraud

Financial fraud globally has been recognized as one of the prime factors undermining the effectiveness and efficiency of financial and non-financial institutions. Financial institutions globally are at the mercy of fraudsters via financial and technological manipulation owing to their tradable commodities of cash and non-cash equivalents. The Federal Bureau of Investigation [13], define fraud as falsified alteration and tracking down of financial transactions end to end under fabricated pretense. However, [14] acknowledged fraud to be a premeditated exploit calculated towards unjustifiable gain to the detriment of naive individuals. Empirical researches identify fraud as a function of theft, asset treachery, and proceedings alternation for direct and indirect gains. Nevertheless, [15] noted that, fraud emanates in the index of three fundamental essentials under the connotation "WOE" (Will, Opportunity, and Exit), with the sum as a product of pressure, opportunity and rationalization of the Donald Cressey's Fraud Triangle Theory of 1950. However, Electronic Fraud (e-fraud) is any act designed to exploit others on the internet through deception, usually with the intent to dispossess others of financial resources.

2.1.2. Cyberspace, Cybercrime and Cybersecurity

As technology has advanced so have also the meaning of cyberspace, cybersecurity and cybercrimes. Cyberspace refers to the interconnected digital environment where computer systems, networks, and information exist [16]. It is a conceptual

space that encompasses the virtual realm created by computer networks, the internet, and digital communication technologies. Cyberspace is not a physical location but rather a collective term for the vast, complex network of computers and data that allows for communication, information exchange, and digital interactions. It is a global domain in the information environment which embraces the interdependence of a network of information systems infrastructures which includes the internet, telecommunication network, computer systems and all other systems that interact in cyberspace. On the other hand, [17] put cybersecurity as the body of rules put in place for the protection of cyberspace. But as we become more dependent on cyberspace, we undoubtedly face a new risk called cybercrime. Cybercrime refers to the series of organized crime attacking both cyberspace and cybersecurity [18]. Sophisticated cyber criminals pose serious risks to our economy and national security. Nigeria's economic vitality and national security depend on a vast array of interdependence and critical networks, systems, services, and resources known as cyberspace. Cyberspace has transformed the ways we communicate, travel, power our homes, run our economy, and obtain government services. [1] offered a comprehensive definition of cybercrime as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

2.1.3. The role of the Central Bank of Nigeria in Shaping Cybersecurity

The Central Bank of Nigeria (CBN) plays a crucial role in shaping cybersecurity compliance in Nigeria's financial sector by:

- Issuing regulations and guidelines: CBN develops and enforces cybersecurity regulations, such as the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers.
- Conducting risk assessments: CBN assesses the cybersecurity risks faced by financial institutions and provides guidance on risk management.
- Implementing cybersecurity levies: CBN mandates a cybersecurity levy on electronic transactions to fund cybersecurity initiatives.
- Overseeing compliance: CBN monitors and ensures compliance with cybersecurity regulations and guidelines by financial institutions.
- Providing guidance and support: CBN offers guidance and support to financial institutions to enhance their cybersecurity posture.
- Collaborating with other agencies: CBN collaborates with other regulatory agencies to ensure a coordinated approach to cybersecurity regulation.
- Promoting cybersecurity awareness: CBN promotes cybersecurity awareness among financial institutions and the general public.

- Developing incident response plans: CBN develops incident response plans to respond to cybersecurity incidents.
- Providing training and capacity building: CBN provides training and capacity-building programs for financial institutions to enhance their cybersecurity capabilities.

2.1.4. Influence of Regulatory Requirement on the Design and Implementation of Cybersecurity Measures in Nigeria

Regulatory requirements significantly influence the design and implementation of cybersecurity measures by:

1) Setting standards: Regulators establish specific requirements for cybersecurity controls, such as encryption, access controls, and incident response plans.

2) Defining risk management frameworks: Regulators require organizations to implement risk management frameworks to identify, assess, and mitigate cybersecurity risks.

3) Mandating compliance reporting: Organizations must report cybersecurity incidents and compliance status to regulators, ensuring transparency and accountability [19].

4) Driving investment in cybersecurity: Regulatory requirements encourage organizations to invest in cybersecurity measures to avoid penalties and reputational damage.

5) Shaping cybersecurity governance: Regulators influence the development of cybersecurity governance policies, procedures, and accountability structures.

6) Influencing cybersecurity talent and training: Regulatory requirements drive the need for specialized cybersecurity talent and training programs.

7) Encouraging cybersecurity awareness: Regulators promote cybersecurity awareness among organizations and the public, fostering a culture of cybersecurity.

8) Fostering collaboration and information sharing: Regulators facilitate collaboration and information sharing among organizations to enhance cybersecurity practices.

9) Driving technology innovation: Regulatory requirements spur the development of new cybersecurity technologies and solutions.

10) Ensuring continuous monitoring and improvement: Regulators require organizations to continuously monitor and improve their cybersecurity posture, ensuring ongoing effectiveness.

By influencing the design and implementation of cybersecurity measures, regulatory requirements play a crucial role in enhancing the overall cybersecurity landscape.

2.1.5. Roles of Artificial Intelligence and Blockchain in Mitigating Cyber Threat

Artificial Intelligence.

Artificial Intelligence consists of a variety of technologies, such as natural language processing, machine learning, and neural Networks, that allow computers

to replicate anthropomorphic intellect and the ability to make decision [20]. According to [21], advanced machine learning algorithms empower AI systems to sift through extensive data volumes, pinpoint patterns, and accurately spot potential threats. The systems maintain continuous vigilance over network traffic, endpoint behaviors, and user activities to detect anomalies and potential security breaches. Importantly, their scope extends beyond structured data to include unstructured information, such as social media posts and content from dark web forums.

They utilize natural language processing to identify emerging threats and malicious activities. AI works in the following ways:

Threat detection: AI-powered systems can analyze network traffic, system logs, and user behaviour to detect advanced threats, such as zero-day attacks and APTs.

Predictive analytics: AI algorithms can analyze historical data and predict the likelihood of a cyber attack, allowing for proactive measures.

Automated incident response: AI can automate the process of responding to cyber attacks, reducing the time and resources required.

Identity and access management: AI-powered systems can analyze user behavior and detect potential identity fraud or unauthorized access.

Malware detection: AI-powered systems can analyze files and detect malware, including zero-day attacks.

Phishing detection: AI-powered systems can analyze emails and detect phishing attempts.

Vulnerability management: AI-powered systems can analyze software vulnerabilities and predict the likelihood of exploitation.

Security information and event management (*SIEM*): AI-powered SIEM systems can analyze security-related data from various sources to detect and prevent cyber threats.

Endpoint protection: AI-powered endpoint protection systems can detect and prevent cyber attacks on endpoints such as laptops and mobile devices [22].

Cybersecurity information sharing: AI-powered systems can analyze and share cybersecurity threat intelligence to help prevent cyber attacks.

Network traffic analysis: AI-powered systems can analyze network traffic to detect and prevent cyber attacks.

User behavior analysis: AI-powered systems can analyze user behavior to detect and prevent insider threats.

AI-powered firewalls: AI-powered firewalls can detect and prevent cyber attacks in real-time.

AI-powered intrusion detection systems: AI-powered IDS can detect and prevent cyber attacks in real-time.

Cybersecurity orchestration: AI-powered cybersecurity orchestration systems can automate the process of responding to cyber attacks.

Blockchain

A blockchain is a distributed database that maintains a continuously growing

list of ordered records, called blocks. The blocks are linked using cryptography and each block contains a cryptographic hash of the previous block, a timestamp and transaction data. Blockchain is one of the current technologies of the Fourth Industrial Revolution which closes the gap between physical and digital spaces. It is capable of creating innovative opportunities and disrupting existing businesses by using decentralized digital information. It is an impenetrable technology that distributes networks that can adjust millions of users across its networks, secured through cryptography and shing. Every user can add information to the blockchain and every other member across the network is responsible for verifying the data being added as authentic, thus, preventing the removal of existing data [23]. Blocchain uses the following procedure to checkmate breaches:

1) It creates a decentralized and immutable ledger that ensures that once data is recorded, it cannot be altered or deleted, making it difficult for hackers to manipulate or destroy data.

2) Transparency is assured using blockchain. Every transaction on the blockchain is time-stamped and publicly visible, allowing for real-time monitoring and detection of suspicious activity.

3) Blockchain uses advanced encryption method making it difficult for hackers to access sensitive information.

4) Identity verification. Blockchain management system ensures secure and decentralized identity verification. This reduces the risk of identity theft and fraud.

5) Blockchain uses a consensus mechanism which requires agreement from multiple parties, before transactions are validated.

The above procedures help to prevent any single entity from manipulating the network. In line with the above methods, blockchain can effectively prevent threats like data breaches, ramsome attacks, phishing attacks, identity theft. DDoS attack and Fraudulent transactions. Blockchain technology offers a robust framework for securing data, transactions and providing strong defence against cyber threats.

2.1.6. Methods of Bank Fraud

[9] explored various means through which e-frauds are perpetrated as follows:

Phishing: The fraudulent practices of sending emails or pop-up web pages purporting to be from legitimate financial institutions to stimulate individuals to provide personal or sensitive business/account information e.g. credit card numbers, PINs or passwords which are subsequently used to perpetuate e-frauds through the Web where physical cards are not required to transact businesses.

Pharming: This technique is used in hijacking the web address of a service provider. This occurs when a user types in a web address and it redirects to a fraudulent website without his knowledge or consent. The website will look like the legitimate site to capture unsuspecting victims' cards confidential information e.g. PIN, Cards numbers and Tokens details.

Skimming: This is a fraudulent collection of payment card details using typically a small electronic device called a skimmer. The device most times is affixed

to an ATM or Point-of-Sale terminals and allows e-fraud perpetrators to capture customer's card information including PIN. The advent of wireless technology has made it easier for criminals to remotely download stolen data without physically visiting the terminals.

SIM Swap fraud: This occurs when the phone number of a customer is hijacked through fraudulent SIM replacement at a Telecom agent outlet. The perpetrator then uses the mobile line to access the account of the victim and conduct all banking services including payments for goods and services and transfer of the funds to another account usually via mobile banking.

Account takeover: This takes place when an e-fraud perpetrator takes over another person's account, first by gathering personal information about the intended victim through Phishing, Pharming, Skimming or any other fraudulent means and then while impersonating the genuine cardholder, the e-fraud perpetrator commits different e-frauds against the victim.

Smishing/Vishing: This takes place when an e-fraud perpetrator sends text messages to defraud victims. Often, the text message will contain a phone number to call and once the victims call the number it would provide a ground for the e-fraud perpetrator to ask for confidential information of the unsuspecting victims. Also, it is vishing when the e-fraudsters use the hidden phone number to call the victims for sensitive information.

Intrusion and system compromise: Without doing anything too suspicious, the perpetrator can use the login credentials or other access tools to enter the flow of network traffic, seeking information to exploit or critical systems to disrupt. As they blend into the typical workings of the network, the attacker can observe activity for months from a remote location without being detected.

Ransomware: This is a type of malware that, when opened, locks the system down and encrypts the device so that no one can use it anymore. Ransomware is one of the most sophisticated and damaging threats out there. The computer or server affected will remain locked until a hefty ransom is paid on its behalf, although some hackers may not unlock the system or decrypt it as promised, even after the ransom has been paid, causing the business to suffer.

Spoofing: In this type of cyber-attack, the cyber thieves impersonate a bank website by creating a website URL that looks and functions exactly like their victims' bank website. Once the customers visit such websites, the cyber thieves steal all their bank login details including other essential data entered on the site.

2.1.7. Methods of Mitigating the Attacks

Cyber security breaches may not have a full proof defense; however, banks should be well informed on how to mitigate breaches. [24] suggested a few ways of mitigating attacks as follows:

Perimeter security: This first line of defense includes firewall and intrusion detection systems, in addition to intrusion prevention systems. These should be configured with appropriate restrictions to block and filter both incoming and outgoing internet traffic.

Endpoint security: Endpoint security requires each computing device on a corporate network to comply with established standards before network access is granted. These measures protect the servers and workstations and include items such as administrative access limitations and anti-virus protection.

Network monitoring: Part of the control environment should include a monitoring program for all IT systems that is frequent and ongoing.

Authentication and administration controls: Authentication controls for the network and all critical systems (especially cloud systems that anyone can access from anywhere) should require complex passwords that expire periodically and restrictions on invalid login attempts, such as three strikes and you are out. Strong controls over user administration are needed as well.

Incident response and business continuity: Organizations should have appropriate business continuity and disaster recovery plans that include specific incident-response procedures for dealing with a cyber event.

Do not underestimate the severity of the threat: Many companies think that their data are not of interest to cybercriminals. But external attackers are moving away from the really big companies that have already implemented robust information security systems and are starting to look at smaller companies instead. Attacks on smaller organizations still have the potential to cause large-scale damage since they often have relationships with, or host systems for, larger companies.

Breaches can often go undetected: It is possible for cyber threats to go undetected. For example, if data are copied, they remain in place, which is not as noticeable as a breach in which something is removed altogether. Many companies do not have advanced monitoring or logging systems, so they often cannot detect attempts by external actors to access or manipulate the data.

Be aware of the emerging threats, *but don't ignore the old ones*. For instance, unsecured web applications still pose a significant risk. A process needs to be established within the company to ensure patches are applied when required.

2.1.8. Automated Teller Machine Fraud

[25] opined that the current upsurge and nefarious activities of automated teller machine (ATM) fraudster is threatening the electronic payment system in the nation's banking sector with users threatening massive dumping of the cards if the unwholesome act is not checked. [17] identified security as well as power outage as major challenges facing the ATM users in Nigeria. A Report on Global ATM Frauds in 2007 identified the following types of ATM Frauds: 1) *Shoulder Surfing:* This is a fraud method in which the ATM fraudster uses a giraffe method to monitor the information the customer keys into the ATM machine unknown to the customers. 2) *Lebanese Loop:* This is a device used to commit identity theft by exploiting an automated teller machine (ATM) user. Its name comes from its regular use among Lebanese financial crime perpetrators, although it has now spread to various other international crime groups. 3) *Card Jamming:* Once the ATM card is jammed, fraudster pretending as a genuine sympathizer will suggest that the victim re-enter his or her security code. When the card holder ultimately

leaves in despair the fraudster retrieves the card with insider assistant and enters the code that he has doctored clandestinely [26].

2.1.9. Point of Sale (POS)

A point of sale (POS) machine accepts the card payment at the point of sale known as POS terminal which can be a shop or the location where a transaction occurs. The point-of-sale machine specifically refers to the hardware and software. POS are used at transaction points such as supermarkets, restaurants, hotels, filling stations, fast-food joints, stadium, and taxi and so on. Secure POS system comprised of a terminal and a PIN Entry Device (PED). The PED accepts smart and other magnetic cards through its slots, and a key pad accepts the imputed PIN. The PED authenticates both the card and cardholder through cryptographic communication with a remote bank via an online method. Two kinds of security information need to be specifically protected; these are the card PIN (Personal Identification Number) and the cryptographic key. For an effective and more protected use of POS, [27] advocated for an end-to-end secure communication solution based on symmetric keys. It is important that banks protect their POS from any kind of intrusion [27].

Security of POS system

Owing to continuous insecurity encountered with POS systems. [28] suggested the following security modalities for any POS intrusion.

Install antivirus software: One of the simplest ways to secure POS system is to ensure you have active antivirus software and always scan your system for viruses and malicious files.

Encrypt your data: Always turn on encryption to avoid cyber thieves from hacking into your POS system via payment stealing malware

Monitor terminals with video surveillance: There have been reports of cybercriminals attaching skimmers to POS systems. These devices capture payment information every time a card is swiped. Consider installing surveillance cameras above all POS terminals to prevent skimmers on your POS terminals.

Secure the network: To prevent POS intrusions, secure all networks with a strong password and ensure a set of a segmented connection for more protection.

Keep all POS software up to date: Like any software, always update programs and devices. With outdated software, hackers are able to identify vulnerabilities and gain access to your system.

Regularly test your system: Always run security tests and checks to assess the strength of your POS system. This will help you identify and fix any weaknesses. It also verifies that all aspects of your system are secure.

Enable two-factor-verification and use complex password: Always add a second layer of security and reconfirm your identity every time you log in. Change passwords every six months and make sure they contain uppercase letters, numbers and symbols.

Physically secure your POS device: POS terminals should be securely fastened and locked down to prevent thieves from breaking in and stealing devices. For

extra security, install monitored alarms to receive an immediate notification in the event of a break-in.

Teach employees how to spot suspicious activity: Your employees can be extremely effective in POS security. Train them to spot unusual activity, check for skimmers and apply best cyber security practices. Additionally, every employee should understand internal cyber security controls and how to report a POS intrusion to help minimize the damage.

2.1.10. Protecting Bank Customers from Identity Theft

Cyber thieves have been pervasive in their approach to extort and trick the unsuspecting public and lure them in for duping. According to [29], scammers have devised means of extorting their victims by contacting them by phone, text or e-mail and claiming to be government agencies or financial institutions. The essence is to convince them to make payments so that they can get details of their account and withdraw money from their account. To avoid this type of scam, banks should follow the following protective measures.

1) Create detailed customer behavior profiles to recognize and distinguish real customer behavior from criminal behavior

2) Educate customers on the best practices for good digital hygiene.

3) Implement two-factor authentication security measures.

4) Monitor inbound and outbound payments, including the movement of payments between accounting rings.

5) Capitalize on existing relationships with e-crime specialists, dark web experts, and internal and external cybersecurity professionals to uncover credential testing and check customer scam reporting.

2.1.11. Cyber Fraud through Phone Number

One of the major ways through which cyber fraudsters get access to customers' bank details is through phone numbers. 60% of world cyber-attacks start with mobile devices. Phone numbers are the easiest access point for cyber thieves. Once they obtain one's phone number, they use it to send phishing text to the victim, which lures the victim to click links which automatically install malware or spyware, or they can use social engineering to get one's personal identification information [30].

2.1.12. Ways Cyber Criminals Get Access to Phone Numbers

Cyber criminals get access to people's phone numbers in the following ways:

1) **Dark-Web**: This is a place where cybercriminals buy and sale the personal information of people stolen during a data breach. This could be phone numbers of sensitive organizations like banks, government and individuals. Phone numbers were the fourth most common piece of personal information leaked via data breaches.

2) **Social Media**: Hackers get access to people's phone numbers through social media. They create websites with enticing phony deals to attract one's attention

and require them to put their numbers while completing online requests, thus they get access to such people numbers and other details which they cunningly require them to disclose.

3) **Phishing scam**: Cyber criminals trick their victims by sending them texts or e-mails that impersonate legitimate organizations. For instance, they use Federal government logo and other symbols to create employment platforms in which victims visit and fill out forms. Once the forms are filled, they get access to personal information of the victim.

4) **Stolen documents**: Cyber thieves dabble through people's garbage to look for old documents that contain their information which includes phone numbers. Ensure documents are properly shredded before they are discarded.

However, [31] revealed the following measures for securing phone numbers from hackers.

a) Use two or multi factor authentication to protect your account.

b) Contact the customer service provider of your phone line and ask them to set a secondary password on your account.

c) Lock SIM card with a PIN.

d) Use password manager to provide strong password.

e) Avoid clicking links from unknown senders.

f) Always research senders.

g) Always ignore one-ring phone scam. Scammers deliberately dial peoples' numbers once and wait for them to dial back to scam them.

h) Do not dial back numbers you do not know that request you for a call back.

i) Ignore all unsolicited text messages that request you to call a number, they are usually from scammers. They are smishing texts to get you to call scammers.

j) Keep your phone safe in public places. Fraudsters would want to get physical access to your SIM card and use it, not only to steal your information but to pose as you as they scam people.

Besides, Stouffer [32] advocated the following ways of stopping unsolicited calls and messages from being received from scammers and spammers.

a) Have knowledge of Spam text. These have the characteristics of being random and confusing, could contain suspicious links and could be immediately accompanied by a phone call.

b) Do not respond directly to a spam text; spammers will easily know that the phone number is genuine. Once they know the number is genuine, they sell the number to other spammers who may send texts or call to offer you free gifts and products.

c) Never click on any suspicious links. This has the danger of installing malware into your phone and can take you to spoof sites that look real but are designed to steal your information. Spammers sell your information to marketers and identity thieves.

d) Block phone numbers. Block phone numbers to stop receiving spam texts and calls from unknown numbers.

e) Report phone numbers that spam you to your network service providers. They will investigate the numbers for appropriate sanctions.

f) Always enable spam filters in your inbox. Your Android phone and iPhones have this special feature to filter unwanted messages to your phone.

g) Exercise caution when you share your phone number on the internet. Fraudsters are interested in getting your phone number and other important personal details for possible hacking. Do not give out your phone number or other personal information to an unknown or untrusted source. This helps to reduce the risk of receiving unwanted texts.

h) Major network service providers offer call blocking services that can help block phone numbers from unknown callers.

2.1.13. Mitigation Controls

In their quest for business growth, mobile money providers and other users of their platforms, including banks, need to implement mitigation controls that strike an appropriate balance between risk management and other business objectives. [30] has suggested such controls to include:

- Customer due diligence measures (KYC) to ensure only subscribers whose identity can be verified (and, in the case of legal entities, who are properly licensed) have access to their networks.
- Agent and consumer fraud awareness programs.
- Agent due diligence and compliance monitoring.
- Ongoing product risk assessment to identify and mitigate risks in new products.
- Transaction monitoring and sanctions screening to detect suspicious transaction patterns.
- System access controls that extend to mobile banking platforms.
- Support for law enforcement efforts.

2.2. Theoretical Review

This research shall be guided by the theory of Fraud Triangle, Fraud Diamond and Deception.

2.2.1. Theory of Fraud Triangle

Three factors that lead to the commitment of any type of fraud by perpetrators. These factors include pressures, opportunities and rationalization. [33] explained that pressures, opportunities and rationalization are assumed but real to e-fraud perpetrators. This theory is relevant to this study because it could be applied to why employees of commercial banks commit e-fraud in their various offices. Pressure can be financial or and non-financial. While financial pressures could be the need to buy a good car, build a house, give good donations to religious organizations to be accorded high status, provide for immediate and extended family needs, and so on, the non-financial pressure could be the need to report better

performance at the branch as the branch is profiled as a profit Centre, frustration with work and fear of job losses because of inability to meet daily or monthly deposit targets and other financial performance indicators set by Management for each of the branch staff. Fear of job losses could also be occasioned by the disruptive technologies that are currently putting pressure on the bottom lines of Nigerian banks which frequently stimulated cost reduction strategies through corporate downsizing and restructuring.

Perceived opportunities must be present before the commitment of successful e-fraud by the employees against the organization [33], maintained that an employee or Executive with firm assurance that an act of fraud could not be hidden without the fraud being detected and the perpetrator caught would refrain from committing fraud. Meanwhile, opportunities exist to commit fraud where the perpetrator believes that he or she would not get caught and if caught, the consequences are not serious. There could be opportunities to commit e-fraud where there is weak internal control, lack of consistent job rotation, the concentration of key roles on temporary or contract employees, knowledge of customers' sensitive financial information and account balances, weak cybersecurity infrastructure from where employees can glean security codes of customers, and bypass cybersecurity infrastructure through expertise knowledge etc.

Finally, perceived rationalization occurs when the perpetrator of fraud rationalizes his fraudulent act as being acceptable. For internal e-fraud in Nigerian banks, perpetrators of fraud may rationalize the act of fraud by the thought of "we are not well-paid compared to the work that we do, the need to meet our branch performance targets for us to retain our jobs, my family members are sick and they need financial help, my immediate family financial needs are more than my salary, we need to be rich through our smartness and so on".

2.2.2. Fraud Diamond Theory

This was postulated by [34] in the December CPA Journal. A fourth dimension named capability was added to the three elements of the Fraud Triangle Theory. This is because without capability it may be seemingly impossible to commit fraud. Therefore, the potential fraud perpetrators must have the skills, be in a position of trust or have the capacity to commit fraud. The theory proposes that an individual's capability, personal trait and abilities could play a major role in determining fraud occurrence [35].

[34] identified the following features that give fraud perpetrators capability to commit fraud as follows: authoritative position or function within an organization; ability to manipulate the weaknesses of the organization's internal control system to perpetrate fraud; boldness to undertake fraudulent actions with the mind that they will not be discovered and ability to cover up fraudulent activities for a long period to protect being caught. The fraud triangle and diamond theories are relevant to the study as they provide the theoretical support that is used to provide explanations on why and how employees of the banks and others commit e-frauds.

2.2.3. Theory of Deception

The Theory of Deception, in the context of philosophy, doesn't have a single well-defined "Propounder" or founder associated with it, as it's a concept that has been discussed and explored by various philosophers and thinkers over time. The theory revolves around the philosophical examination of deception, falsehood, and the nature of truth. Many philosophers, from ancient to modern times, have contributed to the discussions on deception, including figures like Plato, Aristotle, Machiavelli, and contemporary philosophers like Sissela Bok. The purpose is to explore questions and issues related to dishonesty, manipulation, trust, the nature of reality, and the ethical considerations surrounding deception. However, deception is often used by a con artist to dispose of a victim of financial resources and valuables in many business negotiations [36]. The theory of deception specifies seven operational tactics often used by fraud perpetrators to defraud unsuspecting victims [37]. These tactics include Masking (Hiding or destroying critical information), Dazzling (Disguising critical information), Decoying (Distracting the victim's attention away from critical information), Mimicking (Assuming someone's identity, or impersonating someone else), Inventing (Making up information), Relabeling (Misleadingly presenting information), and Double play (Suggesting to the victim that the victim is taking advantage of the deceiver). Since e-frauds are perpetrated through the internet, con artists find it easy to use any of the tactics of deception to fraudulently manipulate a victim. This theory is relevant to the study in the sense that internal e-fraud perpetrators will employ any of the seven tactics to either individually commit e-fraud or in collaboration with other employees most especially those with expert and legitimate power relying on his or her expertise knowledge or position of authority.

2.3. Empirical Review

Few studies have been empirically carried out on the threat of cybersecurity in the Nigerian banking industry, below is the review of some of them.

[38] provided an overview of Cybercrime and Cybersecurity, defined the concept of cybercrime and identified reasons for cyber-crime and its eradication. It also identified those involved and the reasons for their involvement. The paper recommends a combination of technical measures in conjunction with legal deterrents. Government should beef up cybersecurity measures. Cybersecurity awareness should be created in the public as well as government circles. It is also crucial to create an enforcement strategy.

[30] explored the cyber risk in electronic banking and cybersecurity preparedness of women agro-entrepreneurs in the South region of Nigeria. This paper examined cyber risk exposures and cybersecurity preparedness of women agro-entrepreneurs. Women were exposed to risks of unsuccessful transactions through mobile apps and POS in which their accounts were debited; they were also exposed to social engineering threats such as smishing and vishing. With respect to cybersecurity preparedness, the women adopted a few measures such as avoiding lonely

ATM and ignoring text messages and emails that request banking details. Household size, cooperative membership, educational level and internet access were significant factors in accessing digital financial products and services. These findings call for complementary interventions through policies that will enhance customer education to reduce vulnerabilities especially among women.

[14] the researchers focused on cybercrime in online banking and new methods employed by hackers. The paper identified many emerging online banking related cybercrime from various journals and new articles, the information available from the secondary sources of data. The study concludes that there is a need to raise consciousness among consumers about the presence of cybercriminals and to exercise care in the handling of online banking and confidential data and how to defend themselves against these eternal challenges.

[35] investigated e-fraud in Nigerian Banks: Why and How, the study adopted a survey research design. 120 fraud investigation officers completed a structured questionnaire, and the data were analyzed using simple percentages. It was found that e-fraud is committed by staff whose jobs are threatened by not achieving deposit targets. They use experts or legitimate power to connive with other employees to commit e-fraud against the bank. It was further found that disruptive technology and economic challenges led to the disengagement of employees with or without benefits which culminated to e-fraud by the victims. The study recommends that unachievable deposits and sales targets should be discouraged by the bank through labour laws. The human resources department of the bank should create whistle blowing policy that can assist employees get a reprieve from a supervisor who influences workers to commit e-fraud. Bank staff should be trained and educated on the negative effects of e-fraud.

[28] explored the elements needed for cybersecurity implementation and management in organizations. Using qualitative research and semi-structured interviews with some selected cybersecurity professionals, their findings revealed that to manage cybersecurity, a holistic approach to cybersecurity management is needed through a socio-technical system that balances strategic, organizational, risk & technology, and people aspects. According to the research, the main benefit of managing cybersecurity will be compliance with various requirements; however, compliance can be easily imitated by competitors because it is based on operational capabilities. By developing specific dynamic cybersecurity capabilities, companies can achieve strategic value that will be difficult to imitate, thereby achieving a sustainable competitive advantage.

[6] through the Cybersecurity and Capacity Development opined that: cybersecurity consciousness of consumers should always be awakened; financial institutions should invest significantly in and have a robust capacity development plan for their information technology and cybersecurity teams and top executives. Financial institutions, corporations and Cybercrime Advisory Council should collaborate effectively to combat crime; cybersecurity should be made a collective responsibility.

[39] explored cyber threat landscape in Africa of a post Covid-19 experience. The study found that Nigeria has a 73% internet penetration; the study found that within the period of 2020 Nigeria recorded 61.7% cyber-attack which is the highest in Africa. The study recommends total resilience in embedding security into the fabric of business organizations. There should be a high level of protection within processes, people and technology, comprehensive protection gaps between process, people and technology should be closed tightly and finally, an in-depth cybersecurity strategy should be pursued.

[15] analyzed the trend of frauds posing as cybersecurity risk in the Nigerian Deposit Money Banks (DMBs) from 2005 to 2018. Using data collected from the annual reports of the Nigerian Deposit Insurance Corporation (NDIC) and a structured questionnaire, the descriptive statistics method was applied. The analysis revealed that fraud cases and the value of frauds in the Nigerian banking industry have been on the increase particularly at the emergence of e-banking. It also found the effectiveness of the devices and strategies employed to reduce and minimize fraud occurrence. However, the need for more enlightenment of customers on safe handling of security details, timely and effective persecution of fraudsters, compliance with and the enforcement of relevant Fraud Prevention Acts and the strengthening of the internal control units of banks among other things are still desirable.

Gap in Literature

Finally, our research is a groundbreaking one as it combines ATM, POS and phone number cyber fraud which has been ravaging Nigerian banks and their customers.

3. Methodology

This study adopted a descriptive survey design. The study was conducted in the South-Eastern States of Nigeria, comprising of Abia, Anambra, Enugu, Ebonyi and Imo States. The population of the bank is comprised of all the thirty-three (33) deposit money banks in Nigeria. The researcher adopted a purposive sampling technique to select five DMBs prominent in every Southeastern State in Nigeria. These banks include First Bank of Nigeria, Zenith Bank Nig. Plc, Fidelity Bank Nigeria Plc, Access Bank Nig. Plc and Guarantee Trust Bank. The target population of this study is drawn from the bank main staff consisting of Branch Managers, Operational Managers, Fund Transfer Officers, and Cash Officers. 2000 questionnaires were sent out of which 1664 were returned. A total of 336 questionnaire were not returned. Our analysis was done based on the number of returned questionnaires. Appendix shows the distribution of the respondents.

3.1. Instrument for Data Collection and Design

The researchers used a questionnaire to elicit information from the relevant personnel of the banks. The questions were in line with the research specific objectives

of the study. The questionnaire was structured in a five Point-Likert Scale, indicating Agree, Strongly Agree, Disagree, Strongly Disagree and Undecided. The questions were designed to address specifically types of cybersecurity challenges, factors responsible for cybersecurity challenges and measures adopted to eliminate them in deposit money banks in Nigeria.

Reliability of Instrument

Table 1 contains the result of the reliability test conducted.

Table 1. Cronbach Alpha reliability test result.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.712	0.221	22

The table above examines the properties of measurement scales and the items that compose the scales. Ideally, if the alpha value is less than 0.6, it is considered not acceptable, while the alpha value is over 0.6, the result (questionnaire) is acceptable. The Cronbach coefficient for the study performs very well with a value of 0.712 which indicates that the scales and the items of the research instrument show a high measure of internal consistency.

3.2. Method of Data Analysis

Data generated for this study were analyzed using Statistical Package for Social Sciences (SPSS) 20 version. Analyses were carried out using frequency, percentages and mean. The mean decision values for the five rating scales are approximated to scale point as follows:

4.00 − 5.00 = Strongly agree (SA)
3.00 − 3.99 = Agree (A)
2.00 − 2.99 = Undecided (U)
1.00 − 1.99 = Disagree (D)
0 − 0.99 = Strongly Disagree (SD)

4. Presentation and Analysis of Data

Below is the presentation and analysis of questionnaire responses retrieved from the field.

4.1. Research Question One: *What Are the Prominent Types of Cybersecurity Challenges Deposit Money Banks Exposed to in Nigeria*?

Table 2 showed analysis of the responses on major types of cybersecurity challenges deposit money banks are exposed to in Nigeria. A mean score of 5.00 was obtained for SIM swap fraud and pharming, which implies that these are the most prominent types of cybersecurity challenges faced by banks. Firewall bridging,

Hacking of customer account information, Skimming/Website cloning and Smishing/Vishing scored 4.93 respectively which suggests that they are rated by the majority of the respondents equally and are significant levels of cybersecurity challenges faced by most of the banks in Nigeria. It is worth noting that there are high levels of advancement in cyberfraud-related activities and Nigeria has been regarded as one of the safe havens for cyber fraudsters such as constant attempts to the computer or system firewall (which protects intruders from accessing information from the company system), successful bridge of this firewall can result in massive access to unfiltered customer information held by the bank for years as thus exposing customers details and passwords. Account takeover, bypassing banks internal control system and identity Theft scored 4.87 respectively. Unauthorized withdrawal scored 4.73. From the foregoing, it can be deduced that there was a positive response to all the itemized challenges which suggests that deposit money banks are faced with an array of cybersecurity challenges in Nigeria.

Table 2. Major types of cybersecurity challenges deposit money banks are exposed to in Nigeria.

	Strongly Agree		Agree		Undecided		Disagree		Strongly Disagree		Descriptive		
	F	%	F	%	F	%	F	%	F	%	Total	Mean	Std.
Pharming	1662	99.9%	2	0.1%	0	0.0%	0	0.0%	0	0.0%	1664	5.00	0.03
Firewall bridging	1553	93.3%	111	6.7%	0	0.0%	0	0.0%	0	0.0%	1664	4.93	0.25
Hacking of customer account information	1553	93.3%	111	6.7%	0	0.0%	0	0.0%	0	0.0%	1664	4.93	0.25
Account takeover	1442	86.7%	222	13.3%	0	0.0%	0	0.0%	0	0.0%	1664	4.87	0.34
Bypassing banks internal control system	1442	86.7%	222	13.3%	0	0.0%	0	0.0%	0	0.0%	1664	4.87	0.34
Unauthorized withdrawals	1221	73.4%	443	26.6%	0	0.0%	0	0.0%	0	0.0%	1664	4.73	0.44
Identity theft	1442	86.7%	222	13.3%	0	0.0%	0	0.0%	0	0.0%	1664	4.87	0.34
SIM Swap fraud	1662	99.9%	2	0.1%	0	0.0%	0	0.0%	0	0.0%	1664	5.00	0.03
Skimming/Website cloning	1552	93.3%	112	6.7%	0	0.0%	0	0.0%	0	0.0%	1664	4.93	0.25
Smishing/Vishing	1551	93.2%	113	6.8%	0	0.0%	0	0.0%	0	0.0%	1664	4.93	0.25

4.2. Research Question Two: *What Are the Factors Responsible for Cyber Security Problems in Nigerian Deposit Money Banks*?

Table 3 showed analysis of the responses on factors responsible for cyber security problems in Nigerian deposit money banks. The major one is a Loophole in banks internal control system (4.86). The increasing rate of ignorance and lack of security consciousness among banking customers (4.84) especially exposure to internet fraud while using internet banking services, ATM machines, access to their

details by family and friends and lackadaisical attitude towards the safety of their bank account security has been found by the researchers to contribute to this. Fraudulent activities of bank staff with a score of 4.84 definitely stand among the topmost factors responsible for cyber security problems. An increasing number of banks staff are now engaging in frauds especially those perpetuated through the internet due to certain loopholes and lapses they have found within the banking environment and customers' negligence. An increasing rate of sophistication of hackers' activities (4.73) was also indicated which implies that just as the banks and law enforcement agents are finding ways to curb cyberfraud, hackers are developing innovative skills to successfully carry out their crimes. The Public display of passwords/PIN by customers (4.32) especially to family and friends are also factors contributing to cyber security challenges. Nigerians are known to easily trust people around them which exposes them easily to hacking, identity theft and using their password and PIN by third parties to access the money in their bank accounts.

Table 3. Factors responsible for cyber security problems in Nigerian deposit money banks.

	Strongly Agree		Agree		Undecided		Disagree		Strongly Disagree		Descriptive		
	F	%	F	%	F	%	F	%	F	%	Total	Mean	Std.
Ignorance and lack of security consciousness among banking customers	1424	85.6%	225	13.5%	3	0.2%	6	0.4%	6	0.4%	1664	4.84	0.45
Fraudulent activities of bank staff	1421	85.4%	228	13.7%	9	0.5%	5	0.3%	1	0.1%	1664	4.84	0.41
Increasing sophistication of hackers activities	1217	73.1%	445	26.7%	0	0.0%	1	0.1%	1	0.1%	1664	4.73	0.46
Loophole in banks internal control system	1435	86.2%	225	13.5%	4	0.2%	0	0.0%	0	0.0%	1664	4.86	0.35
Public display of passwords/PIN by customers	1086	65.3%	155	9.3%	291	17.5%	132	7.9%	0	0.0%	1664	4.32	1.02

Table 4 showed analysis of the responses on measures adopted to reduce/eliminate the various threats of cybersecurity challenges in Nigerian Deposit Money Banks. Reponses no doubt show that a number of measures have been put in place by the banks. For example, the banks now adopt Full encryption of transaction channels such as POS, Internet Gateway, ATMs (4.91). In addition, they now make use of two-factor-verification and authentication, (4.81), carry out Regular tests and checks of the strength of various systems to identify weaknesses and verify the security of the systems (4.81), carry out constant updating of their Antivirus softwares and frequent scanning for viruses and backdoor bridges (4.81), engage in regular use of social media and SMS to customers on security ad-vice to

issues such as avoiding unsolicited emails, text messages and calls (4.81). Banks are also making use of a second layer of security and reconfirmation of identity each time customers log into ATMs (4.13) and sensitizing customers on the need to change PIN/PASSWORD every six months or at intervals (4.13).

Table 4. Measures adopted to reduce/eliminate the various threats of cybersecurity challenges in Nigerian deposit money banks.

	Strongly Agree		Agree		Undecided		Disagree		Strongly Disagree		Descriptive		
	F	%	F	%	F	%	F	%	F	%	Total	Mean	Std.
Use of two-factor-verification and authentication	1344	80.8%	320	19.2%	0	0.0%	0	0.0%	0	0.0%	1664	4.81	0.39
Use of second layer of security and reconfirmation of identity each time customers log into ATMs	956	57.5%	97	5.8%	480	28.8%	131	7.9%	0	0.0%	1664	4.13	1.08
Regular tests and checks of the strength of various systems to identify weaknesses and verify the security of the systems	1347	80.9%	317	19.1%	0	0.0%	0	0.0%	0	0.0%	1664	4.81	0.39
Full encryption of transaction channels such as POS, Internet Gateway, ATMs	1507	90.6%	157	9.4%	0	0.0%	0	0.0%	0	0.0%	1664	4.91	0.29
Updating of Antivirus softwares and constant scanned for viruses and backdoor bridges	1344	80.8%	320	19.2%	0	0.0%	0	0.0%	0	0.0%	1664	4.81	0.39
Sensitizing customers on the need to change PIN/PASSWORD every six months or at intervals	956	57.5%	97	5.8%	480	28.8%	131	7.9%	0	0.0%	1664	4.13	1.08
Regular use of social media and SMS to customers on security advice to issues such as avoiding unsolicited emails, text messages and calls	1347	80.9%	317	19.1%	0	0.0%	0	0.0%	0	0.0%	1664	4.81	0.39

4.3. Discussion

Findings show that banks in Nigeria are exposed to various types of cyber fraud. The major type of cybersecurity challenge is pharming which is a method for obtaining control of a service provider's website. This happens when a person enters a URL and, without his knowledge or agreement, it is redirected to a fraudulent website. The website will appear authentic in order to obtain sensitive card information from unwary victims, such as PINs, card numbers, and token details. Other cybersecurity challenges include hacking of customer account information, account takeover, bypassing banks internal control system, unauthorized withdrawals, identity theft, sim swap fraud, skimming/website cloning and smishing/

vishing.

Some of the identified factors responsible for the increasing rate of cybersecurity in Nigerian banks were found to include ignorance and lack of security consciousness among banking customers, fraudulent activities of bank staff, increasing sophistication of hacker's activities, loopholes in banks internal control system and public display of passwords/pin by customers. However, it was obvious from the findings that loopholes in the internal control system of the banks posed the most significant challenge to the banks. The problem of fraud in ATM can be attributed to a lack of ignorance of the safe use of ATM machines and cards by customers.

It has been argued that the technology that enables its prevention will probably not change the methods for gathering private data on victims. The weakest security flaws in any socio-technical system are not technical, according to computer security experts, but rather human. Cyber technology, as has previously noted, makes it extremely simple to replicate institutional authority, luring compliant victims into disclosing private information. Through the use of digital technology, fraudsters can readily imitate genuine goods or services that are actually fake or non-existent. This is made possible by a similar application of technology to imitate well-known companies or institutions in order to support claims of legitimacy in a range of fraud types, including financial, counterfeit, and phishing/identity theft crimes. To address these problems, our findings further showed that banks now use enabled two-factor-verification and in some cases one-time passwords (OTP) with complex passwords that are changed every six months for ATMs and POS. The use of POS is increasing and even became the most used e-banking facility during the challenges of CBN cashless policy between February and March 2023. Personal observations show that more and more POS have become popularly used across every region in Nigeria; yet only a few cases of cyber-threat were witnessed in the use of the POS as reported by news emanating from print and online media which goes to show the extent efforts made by the banks are yielding fruits towards reducing or eliminating threats in the use of POS. However, the major problems that arise is the lukewarm attitude of banking customers towards safety of their bank cards especially their PIN disclosure and use by third party which has increased the risk of card cloning, identity theft, and theft of money from their accounts.

The findings support the view of [29] who noted that numerous cyber-attacks on Nigerian commercial banks have caused significant financial and valuable damage. With the help of the internet of things, the introduction of electronic banking has widened the gap for system intruders. Despite the security measures put in place to control and secure customers' cash and information, the rising rates of cybercrime in Nigeria have turned into a serious threat to Nigeria's banking industry. Our findings showed that based on the fact that commercial banks continue to be the financial institutions or corporations that cybercriminals or hackers target the most, the need to secure the ATM and POS terminals has

become necessary to check the trend as no channels of the e-banking are exempted from attack.

The use of SMS as a means of stealing financial details and other information about banks staff and customers is on the rise. To address these problems, commercial banks have been engaging the use of various media channels to educate their customers and staff. Past research [15] and reports emanating from global cybersecurity agencies show that Nigeria has a high rate of cybercrime. It is crucial to note that cybercrime would spread as a result of the general public's involvement in the development of the internet of things and its use to promote the general services of Nigeria's commercial banking system. Therefore, it is proof that the government must strengthen its cyber security plan in order to protect both its domestic and foreign reputations [31]. If properly implemented and overseen, it will significantly reduce and safeguard the rate of cybercrime in Nigeria's commercial banks. Banks would need to be creative to keep up with the expanding trend of technology and security advancement since computer crime cannot be completely tamed and abolished from the financial sector. According to this research, security measures will prevent cybercriminals from gaining access to customers' financial details through spam messages and other fraudulent tactics. This claim is supported by the earlier view of [28] in his study who suggested that a socio-technical system that strikes a balance between strategic, organizational, risk & technology, and people-related components is required to manage cybersecurity while also noting that compliance with various standards will be the key advantage of managing cybersecurity. In other words, one can deduce that being proactive is the way forward in managing cyber security threats.

Some of the specific cybersecurity challenges that the banks faced include phishing, ransomware attacks, insider threats and a lack of cybersecurity professionals. Phishing attacks impacted the deposit money banks to the extent that they incurred financial losses due to unauthorized transactions. There was increased cost to prevent phishing attacks, which led to system downtime and caused incontinence among customers. Ransomware attacks introduced trojan, viruses and worms to the system which encrypted the files, folders and data. A huge fund was paid as ransom to the hackers before the files were decrypted. There was a delay in handling customers transactions which impacted on the reputation the banks. Insider threats come from the bank staff who use the advantage of their knowledge of the bank secret to pull fraud on the bank. Cybersecurity experts were lacking at the bank branches. They only maintained a committed staff for cybersecurity at the head office only. This affected cybersecurity management at the bank branches. These identified threats are not however, peculiar to Nigerian banks, they represent a broader trend in cyber-security risk management.

5. Conclusions and Recommendations

The growing trend of electronic fraud and risks associated with the use of electronic banking gadgets has necessitated the need for more collaborative efforts in

overcoming these menaces. Cyber security has become a tool necessary to overcome cybercrimes. The sophistication of cybercrimes and the way they have been perpetuated have resulted in the loss of millions of naira by banks and customers alike. Sadly, the problem of cybercrime is not peculiar to Nigeria alone; it cuts across the global communities, and no country is exempted from the claws of criminals. Despite the various measures out in place by countries such as USA, England, Canada and Germany which are known for strong financial system securities, they have all fallen victim to cybercrime. This study has shown that Nigerian banks have put in place various security measures aimed at tackling the problem of fraud and cybercrimes and these measures have, to some extent, helped to reduce the amounts lost to fraud by banks in Nigeria.

Based on the findings, it is recommended that bank management should continuously update their security and firewall software based on new trends of cyber risk. Moreover, banks should review their internal control system periodically to check for any form of loophole that can be taken advantage of by both employees and internet fraudsters. Massive campaigns through various media such as social media, broadcasting media, and the company's platform should be carried out to sensitize customers and employees to different types of cybercrimes and how to overcome them. The government must be at the forefront by investing in cybersecurity through training, school curriculums, and the development of cybersecurity centers manned by professional IT with knowledge of tracking hackers and internet fraudsters. Moreover, government should partner with the international community as joint efforts is required since most of the perpetuators work with a ring leader who is most cases reside in a different country coordinating the crime across different countries. Banking customers must also be security conscious with the ATM and online transactions which require the use of their Pins and phone numbers. Customers are advised to raise red flags over messages that require them to provide their BVN, ATM card details and OTP Pins. Employees in the banking industry are enjoined to be careful with email and SMS messages with links and such links have been used to install virus into phones and computer systems which are capable of stealing information such as passwords, employee details and customer details. We recommend the adoption of AI and Blockchain to improve cybersecurity in the Deposit Money banks in Nigeria. These will help to improve detection and enhance incidence responses. They will assist in providing automated scanning for the security of the systems, provide continuous hunting for threats and, streamline analysts' experience in analysing complex data and predicting potential threats very perfectly.

Limitation of the Study

The study was limited by the official privacy of the bank chief executives. Some of them outrightly declined to complete the questionnaire, they complained of its being against the oath of their office and their fiducial responsibility to protect their office. Some of the bank executives do not have deep knowledge of cyber-

security beyond what they know within their working infrastructure. Some of the bank executives were not seen in their seats at the time of the retrieval of the questionnaire, which accounted for the unretrieved questionnaires.

Acknowledgment

The researchers are grateful to TETFUND for their assistance in funding this research.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Ibinkule, F. and Enweniyi, E. (2013) Approaches to Cyber Security Issues in Nigeria. *Journal of Cognitive Research in Science, Engineering and Education*, **1**, 100-110. https://ijcrsee.com/index.php/ijcrsee/article/view/65

[2] Bromwich, J.E. (2016) Protecting Your Digital Life in 7 Easy Steps. New York Times.

[3] Onwubiko, C.O. and Nwankwo, H.A. (2019) Cyber Security Challenge: Roles of Managers and Business Executives. *Journal of Accounting Information and Innovation*, **5**, 1-8.

[4] National Institute of Standard and Technology (2014) A Comprehensive Analysis and Performance Enhancement for IEEE 802 11 AY Group. https://dspace.networks.imdea.org/bitstream/handle/20.500.12761/1585/WoWMoM_2022_camera-ready.pdf?sequence=1

[5] Nigeria Financial Intelligence Unit (2015) Cybercrimes (Prohibition, Prevention, Etc) Act. https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf

[6] Kolade, E. (2022) Cybersecurity in Nigeria's Financial Industry: Enhancing Consumer Trust and Security. https://eucyberdirect.eu/atlas/sources/cybersecurity-in-nigeria-s-financial-industry-enhancing-consumer-trust-and-security

[7] Soni, V.D. (2019) Role of Artificial Intelligence in Combating Cyber Threats in Banking. *International Engineering Journal for Research & Development*, **4**, 1-7. https://ssrn.com/abstract=3654422

[8] Nigeria Deposit Insurance Corporation (2018) Annual Report. https://ndic.gov.ng/wp-content/uploads/2020/08/Year-2018-Annual-Report.pdf

[9] Ololade, B.M., Salawu, M.K. and Adekanmi, A.D. (2020) E-Fraud in Nigerian Banks: Why and How? *Journal of Financial Risk Management*, **9**, 211-228. https://doi.org/10.4236/jfrm.2020.93012

[10] Nigeria Inter-Bank Settlement System (2021) Fraud Report for Quarter 3. Nat ional Cybersecurity Policy and Strategy. Nigerian Government, February 2021. https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf

[11] African Academic Network on Internet Policy (2020) Critical Data Security Issues in the Nigeria Banking Sector. African Academic Network on Internet Policy. https://aanoip.org/critical-data-security-issues-in-the-nigerian-banking-sector/

[12] Ogunwale, H. (2020) The Impact of Cybercrime on Nigeria's Commercial Banking System. https://www.researchgate.net/profile/Hezekiah-Ogunwale/publication/347388290_THE_IMPACT_OF_CYBERCRIME_ON_NIGERIA'S_COMMERCIAL_BANKING_SYSTEM/links/5fda6c7392851c13fe90a613/THE-IMPACT-

[13] Federal Bureau of Investigation (1984) Uniform Crime Reports. U.S. Government Printing Office. https://www.ojp.gov/ncjrs/virtual-library/abstracts/crime-united-states-1984

[14] Eseoghene, J.I. (2010) Bank Frauds in Nigeria: Underlying Causes, Effects, and Possible Remedies. *African Journal of Accounting & Economics*, *Finance & Banking Research*, **6**, 62-80. http://ajaefbr.com/articles/african-vol6-article5.pdf

[15] Israel, A. and Ebenezer, A. (2023) Analysis and Management of Fraud in Nigerian Banking Industry: Stakeholders' Perspectives. *Fountain University Osogbo Journal of Management*, **4**, 47-60.

[16] Amar, J. and Shailendra, K. (2023) Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. *Human Behavior and Emerging Technologies*, **2023**, Article ID: 2103442. https://doi.org/10.1155/2023/2103442

[17] Ibor, B. (2016) An Investigation of Human Resources Nexus to Frauds in the Nigerian Banking Sector. *International Journal of Scientific and Research Publications*, **6**, 231-247. https://www.scirp.org/(S(351jmbntvnsjt1aadkozje))/reference/referencespapers.aspx?referenceid=2819469

[18] Olumide, O.O. and Victor, F.B. (2010) E-Crime in Nigeria: Trends, Tricks, and Treatment. *The Pacific Journal of Science and Technology*, **11**, 343-356. https://www.semanticscholar.org/paper/E-Crime-in-Nigeria%3A-Trends%2C-Tricks%2C-and-Treatment.-Balogun-Obe/f1645526cec00bddc562bcffc4179ad2c9cad919

[19] Central Bank of Nigeria (2021) (Various Issues). Statistical Bulletins. https://www.cbn.gov.ng/documents/statbulletin.asp

[20] Patel, S. (2021) Aspects of Artificial Intelligence. In: Karthikeyan, J., Ting, S.-H. and Ng, Y.-J., Eds., *Learning Outcomes of Classroom Research*, L'Ordine Nuovo Publication, 48-55.

[21] Hitansh, K. (2023) Transformative Impact of AI and ML in Cyber Security. Vulnerability Management. https://www.linkedin.com/pulse/transformative-impact-ai-ml-cybersecurity-hitansh-kataria-e0sdc/

[22] Patel, H. (2023) The Future of Cybersecurity with Artificial Intelligence (AI) and Machine Learning (ML). *Computer Science and Engineering*, **25**, 425-429. https://doi.org/10.20944/preprints202301.0115.v1

[23] Aamir, A.A., Ali, O., Razwan, M. and Ahmed, F. (2020) Using Block to Boost Cybersecurity. *Journal of Natural and Applied Sciences*, **2**, 301-314.

[24] Traina, L. (2018) The Top 5 Cybersecurity Risks for CPAs. AICPA Store. https://us.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/resources/privacy/cybersecurity/downloadabledocuments/top-5-cybercrimes.pdf

[25] Hoffmann, A.O. and Birnbrich, C. (2012) The Impact of Fraud Prevention on Bank-Customer Relationships: An Empirical Investigation in Retail Banking. *International Journal of Bank Marketing*, **30**, 390-407. https://doi.org/10.1108/02652321211247435

[26] Elumaro, A.J. and Obamuyi, T.M. (2018) Cards Frauds and Customers' Confidence in Alternative Banking Channels in Nigeria. *European Scientific Journal*, **14**, 40-60. https://doi.org/10.19044/esj.2018.v14n16p40

[27] Rad, H.A., Tehrani, M.B., Samsidin, K. and Ramli, A.R. (2009) A Simple and Highly Secure Protocol for POS Terminal. 2009 *Second International Conference on Environmental and Computer Science*, Dubai, 28-30 December 2009, 204-207. https://doi.org/10.1109/ICECS.2009.42

[28] Kosutic, D. (2021) The Impact of Cybersecurity on Competitive Advantage. https://www.researchgate.net/publication/357826918_The_Impact_of_Cybersecurity_on_Competitive_Advantage

[29] Enofe, A.O., Abilogun, T.O., Omoolorun, A.J. and Elaiho, E.M. (2017) Bank Fraud and Preventive Measures in Nigeria: An Empirical Review. *International Journal of Academic Research in Business and Social Sciences*, **7**, 40-51.

[30] Akinyomi, O.J. (2012) Examination of Fraud in the Nigerian Banking Sector and Its Prevention. *Asian Journal of Management Research*, **3**, 184-192. https://www.scirp.org/(S(351jmbntvnsjt1aadkozje))/reference/referencespapers.aspx?referenceid=2819460

[31] Geatano, D. (2022) Can Someone Hack Your Phone with Just Your Number? https://www.aura.com/learn/what-can-hackers-do-with-your-phone-number

[32] Norton (2024) How to Stop Spam Texts: An Easy 4-Step Guide. https://www.norton360.org/how-to-stop-spam-texts-An-easy-4-step-guide

[33] Albrecht, C., Albrecht, C.C. and Wareham, J. (2008) The Role of Power and Negotiation in Online Fraud. *Journal of Digital Forensics, Security and Law*, **1**, 29-48. https://www.scirp.org/(S(351jmbntvnsjt1aadkozje))/reference/referencespapers.aspx?referenceid=2819461

[34] Wolfe, D.T. and Hermanson, D.R. (2004) The Fraud Diamond: Considering the Four Elements of Fraud. *The CPA Journal*, **74**, 38-42. https://doi.org/10.1016/S1361-3723(04)00077-6

[35] Babatunde, O., Salawu, M. and Adekanmi, A. (2020) E-Fraud in Nigerian Banks: Why and How? *Journal of Financial Risk Management*, **9**, 211-228. https://doi.org/10.4236/jfrm.2020.93012

[36] Schweitzer, M.E. (1997) Omission, Friendship, and Fraud: Lies about Material Facts in Negotiation. Annual Meeting of Academic Management. https://doi.org/10.1037/e683282011-011

[37] Grazioli, S. and Jarvenpaa, S.L. (2003) Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence. *International Journal of Electronic Commerce*, **7**, 93-118. https://doi.org/10.1080/10864415.2003.11044283

[38] Kaibairu, R.M., Karume, S.M., Kibas, F. and Onga'nyo M.L.B. (2017) Closing the Cybsersecurity Skill in Kenya: Curriculum Intervention in Higher Education. *Journal of Information Security*, **14**, 136-151. https://www.scirp.org/reference/referencespapers?referenceid=3429404

[39] Ikegwu, J., Nnatuanya, B., Okoli, C. and Ndukwe, I. (2022) Africa's Evolving Cyber Threat Landscape. https://phillipsconsulting.net/reports_post/africas-evolving-cyber-threats-landscape/

Appendix: Distribution of Sample Size

Population of Bank Staff.

	State	Branch Managers	Operational Managers	Fund Transfer Managers	Cash Offers	Total
Zenith		18	19	4	19	60
FBN		19	21	6	23	69
Access	Abia	24	24	3	24	75
UBA		19	21	4	19	63
Fidelity		17	18	4	22	61
Total		**97**	**103**	**21**	**107**	**328**
Zenith		23	23	6	24	76
FBN		23	23	9	25	80
Access	Anambra	24	24	8	24	80
UBA		22	22	6	21	71
Fidelity		21	21	8	21	71
Total		**113**	**113**	**37**	**115**	**378**
Zenith		13	13	3	19	48
FBN		13	13	7	14	47
Access	Ebonyi	13	13	4	12	42
UBA		12	12	6	12	42
Fidelity		13	13	4	14	22
Total		**64**	**64**	**24**	**71**	**223**
Zenith		17	17	6	17	57
FBN		19	19	5	19	62
Access	Enugu	21	21	6	22	70
UBA		18	18	9	19	64
Fidelity		17	17	7	18	59
Total		**92**	**92**	**33**	**95**	**312**
Zenith		27	27	5	29	88
FBN		28	28	3	29	88
Access	Imo	27	27	4	28	86
UBA		25	26	3	24	78
Fidelity		27	28	7	21	83
Total		**134**	**136**	**22**	**131**	**423**
Grand Total						**1664**